REPUBLIKA E SHQIPËRISË
UNIVERSITETI "ISMAIL QEMALI" VLORË
FAKULTETI I SHKENCAVE TEKNIKE

DISERTACION

Për marrjen e Gradës Shkencore
"DOKTOR"

KONTRIBUT MATEMATIKO-INFORMATIK NË KRIPTOGRAFINË ME ÇELËS PUBLIK DHE APLIKIMI NË DOKUMENTET BIOMETRIKE TË IDENTITETIT

Doktoranti:
Msc. Gazmend Krasniqi

Udhëheqësit shkencor:
Prof. Dr. Kristaq Filipi
Prof. Dr. Blerim Rexha

Vlorë, 2019

REPUBLIKA E SHQIPËRISË
UNIVERSITETI "ISMAIL QEMALI" VLORË
FAKULTETI I SHKENCAVE TEKNIKE
DEPARTAMENTI I MATEMATIKËS

DISERTACION

i paraqitur nga:

Msc. Gazmend Krasniqi

udhëhequr nga

Prof. Dr. Kristaq Filipi dhe

Prof. Dr. Blerim Rexha

Për marrjen e gradës shkencore

"DOKTOR"

Tema:

KONTRIBUT MATEMATIKO-INFORMATIK NË KRIPTOGRAFINË ME ÇELËS PUBLIK DHE APLIKIMI NË DOKUMENTET BIOMETRIKE TË IDENTITETIT

Mbrohet më datë, .../...../2019 para jurisë:

1. ..... Kryetar
2. ..... Anëtar (Oponent)
3. ..... Anëtar (Oponent)
4. ..... Anëtar
5. ..... Anëtar

Vlorë, 2019

Abstrakt

Zhvillimi i shpejtë i shërbimeve elektronike dhe mobile në internet kërkon mekanizma të fuqishëm të autentikimit të përdoruesve, të vërtetimit se palët komunikuese janë me të vërtetë ato që thonë që janë, duke përdorur autentikim dy faktorësh ose duke përdorur të dhënat biometrike të shfrytëzuesit. Sot jemi dëshmitarë të rritjes së kërkesës për më shumë shpejtësi dhe kapacitet në internet, dhe më shumë fuqi përpunimi dhe ruajtje në çdo pajisje të përdoruesit fundor. Kërkesa për performancë më të madhe është e pranishme në çdo sistem. Pajisjet elektronike dhe aplikacionet e tyre duhet të jenë më të shpejta, por të mos humbasin tiparet kryesore të sigurisë. Zhvillimet e fundit tregojnë një rritje të përdorimit të të dhënave biometrike, të njohjes së fytyrës dhe përdorimit të gjurmëve të gishtrinjëve, për autentikim. Përtej autentikimit të përdoruesit ka shumë raste kur kërkohet edhe firmosja (nënshkrimi) i dokumenteve elektronike. Autentikimi dhe enkriptimi janë proceset kryesore në aspektin e sigurisë, të domosdoshme për një komunikim të sigurt. Këto procese mund të ekzekutohen në pajisje të ndryshme, mes tyre kompjuterët personal (PC), mikroprocesorë, mikrokontrollerë, kartela biometrike ose pajisje të lëvizshme (mobile). Kartelat e identitetit biometrik po bëhen gjithnjë e më popullore, duke sfiduar pajisjet tradicionale të PC.

Në këtë punim dokorature paraqitet një qasje e re duke përdorur identitetin e përdoruesit, që rrjedh nga të dhënat e tij personale dhe biometrike të ruajtura në kartelën nacionale, elektronike të identifikimit (eID), për nënshkrimin kriptografik të dokumenteve elektronike. Këto dokumente elektronike mund të jenë të formatit të ndryshëm, por më i përhapuri është formati PDF (Portable Document Format), i dizajnuar 25 vite më herët. Edhe në këtë disertacion është përdorur formati PDF për të firmosur në mënyrë digjitale dokumente të tilla, pasi është e përshtatshme për të përmbushur kërkesat specifike ligjore për një zgjidhje nënshkrimi në kombinim me një letërnjoftim nacional. Për të mbështetur teknikisht qasjen e paraqitur dhe si pjesë praktike e këtij punimi është dizajnuar dhe zhvilluar aplikacioni që ndërvepron me kartën biometrike (eID) dhe që përmbush kërkesat e mëposhtme: (i) paraqitjen vizuale të nënshkrimit të një dokumenti zyrtar në formatin PDF, (ii) një përfaqësim vizual të vlerës së firmës që garanton origjinalitetin e dokumentit dhe (iii) validimin e nënshkrimit për palët e treta. Kjo metodë është provuar të jetë e besueshme dhe mbështet një nivel të mjaftueshëm sigurie.

Në këtë disertacion do të krahasohen gjithashtu dy sisteme të procesimit, efikasitetin e enkriptimit dhe firmosjes (nënshkrimit) në të dhënat e ekzekutuara në kartelën nacionale biometrike të identitetit (eID) kundrejt PC-së, i njohur edhe si match-on-card kundrejt match-off-card. Ky krahasim konsideron parametra të ndryshëm që ndikojnë në proces dhe rolin që ata luajnë në procesin e përgjithshëm. Rezultatet, të ekzekutuara me një grup të paracaktuar të vektorëve të testimit, përcaktojnë se cili sistem përpunimi duhet të përdoret në një situatë të caktuar. Të gjitha këto arrihen duke përdorur konceptet

kripotografike të cilat janë të nevojshme për krijimin dhe verifikimin e këtyre nënshkrimeve digjitale, e sidomos pjesën e kriptografisë me çelës publik.

Në kriptografinë me çelës publik përdoren dy çelësa, njëri publik për të enkriptuar mesazhet e marrësit dhe tjetri privat, që marrësi e përdor për t'i dekriptuar mesazhet e enkriptuara. Lidhja midis tyre kërkohet e tillë, që të jetë i vështirë gjegjësishtë pa mundur zbulimi i çelësit privat me ndihmën e çelësit publik. Kjo realizohet duke përdorur njohuri nga matematika moderne sidomos nga algjebra modulare dhe nga algjebra e strukturave të grupit, unazës dhe fushës, që janë objekt shpjegimi në këtë punim. Në përbërje të tij do të jenë dhe teknika themelore si algoritmi i Euklidit, funksioni i Ejlerit, teorema kineze e mbetjeve, të cilat të gjitha së bashku janë fundamentale për sistemet kriptografike me çelës publik, të gjitha këto të diskutuara po ashtu në këtë disertacion nga një kënd i aplikimit të tyre me kartelën biometrike të identitetit (eID).

Konkluzionet dhe rekomandimet përfundimtare, të vërtetuara në formë eksperimentale, dhe të nxjerra nga ky disertacion do të shërbejnë si një udhëzues për përdorimin e një sistemi procesimi në mjedis të caktuar, duke pasur parasysh efikasitetin e të dhënave.

Dedikuar:

Prindërve, gruas Edonjetës dhe vajzës Jarës
Nuk do të mund të arrija këtu pa besimin,
Mbështetjen dhe inkurajimin
tuaj të pafund

FALENDERIME

Në këtë pjesë të disertacionit tim shfrytëzoj rastin ti falënderoj udhëheqësit shkencor Prof. Dr. Kristaq Filipi dhe Prof. Dr. Blerim Rexha për ndihmën e dhënë gjatë punës time në këtë disertacion si dhe gjithë miqët dhe kolegët, për bashkëpunimin, të cilët më dhanë mundësinë që unë të kontribuoj dhe të zhvilloj dijen time në fushën e Sigurisë së Teknologjisë së Informacionit, dhe arritjen deri tek ky disertacion doktorature. Një falënderim meritojnë edhe kolegët nga Universiteti i Vlorës për krijimin e atmosferës shumë bashkëpunuese dhe nxitëse gjatë gjithë kësaj kohe.

Në fund, një falënderim i veçantë shkon për prindërit e mi, për gruan time Edonjetën dhe vajzën time Jarën për mbështetjen morale që më kanë ofruar gjatë gjithë kohës deri në arritjen e qëllimit të përfundimit të studimeve të doktoraturës.

Të gjithëve, sinqerisht faleminderit!

Përmbajtja

Lista e Figurave

Lista e Tabelave

Lista e Shkurtesave

ID	Identification Document
ICAO	International Civil Aviation Organization
NFC	Near Field Communication
eID	Electronic Identification Document
eIDAS	Electronic IDentification, Authentication and trust Services
ECC	Elliptic Curve Cryptography
EEPROM	Electrically Erasable Programmable Read-Only Memory
3DES	Triple Data Encryption Standard
CSP	Crypto Service Provider
CPU	Central Processing Unit
RSA CSP	RSA Crypto Service Provider
RAM	Random Access Memory
DES	Data Encryption Standard
AES	Advanced Encryption Algorithm
RSA	Rivest - Shamir - Adleman
PC	Personal Computer
IDEA	International Data Encryption Algorithm
DSA	Digital Signature Algorithm
PGP	Pretty Good Privacy
DSS	Digital Signature Standard
MD2	Message Digest2
MD4	Message Digest4
MD5	Message Digest5
SHA – 1	Secure Hash Algorithm – 1
TLS	Transport Layer Security
PKI	Public Key Infrastructure
CA	Certification Authority
VA	Verification Authority
RA	Registration Authority
PA	Passive Authentication
CSCA	Country Signing Certification Authority
DS	Document Signature
EAC	Extended Access Control
e-MRTD	electronic Machine Readable Travel Documents
HTTPS	Hyper Text Transfer Protocol Secure
PKCS	Public-Key Cryptography Standards
NIST	National Institute of Standards and Technology
HTTP	HyperText Transfer Protocol

IP	Internet Protocol
SSL	Secure Sockets Layer
FTP	File Transfer Protocol
RAM	Random Access Memory
ROM	Read Only Memory
I/O	Input/Output
DoS	Denial of Service
CPU	Central Processing Unit
ICC	Integrated Circuit Chip
RF	Radio Frequencies
ISO/IEC	International Organization for Standardization
GSM	Global System for Mobile
SIM	Subscriber Identity Modules
ICC	Integrated Circuit Chip
ATM	Automated Teller Machine
CMS	Cryptographic Message Syntax
ASN.1	Abstract Syntax Notation One
BER	Basic Encoding Rules
CER	Canonical Encoding Rules
DER	Distinguished Encoding Rules
XER	XML Encoding Rules
CXER	Canonical XML Encoding Rules
E-XER	Extended XML Encoding Rules
PER	Packed Encoding Rules
GSER	Generic String Encoding Rules
CAdES	CMS Advanced Electronic Signature
CAdES – BES	CAdES Basic Electronic Signature
CAdES-EPES	CAdES Explicit Policy-based Elctronic Signature
PDF	Portable Document Format
PAdES	PDF Advanced Electronic Signature
CRL	Certificate Revocation List
OCSP	Online Certificate Status Protocol
VRI	Validation Related Information
DSS	Document Security Store
PIN	Personal Identification Number
RFC	Request for Comments
API	Application Program Interface
CVCA	Country Verifying Certification Authority
DVCA	Document Verifying Certificate Authority
SPOC	Single Point of Contact
PACE	Password Authenticated Connection Establishment

1 HYRJE

1.1 Hyrje

Kohët e fundit, jo vetëm interneti dhe pajisjet mobile po ndryshojnë jetën tonë të përditshme, por edhe përdorimi i shumë kartelave për pagesë dhe autentikim, siç është kartela elektronike e identifikimit (eID) për shërbime elektronike dhe qeveritare. Teknologjitë e reja të dokumenteve të identifikimit bazohen në të dhënat biometrike të poseduesëve të tyre. Të dhënat biometrike janë bërë pjesë të dokumenteve të identifikimit me qëllim të lidhjes së personit fizik (poseduesit) me të dhënat e dokumentit dhe përmbajtjen e tij. Ato i posedon çdo person dhe është e pamundur që dy persona të kenë të njëjta të dhëna biometrike, si dhe janë të pandryshuara përveç në rast të ndonjë aksidenti [24].

Në Republikën Kosovës qytetarët kanë filluar të pajisen me letërnjoftimet biometrike që nga viti 2013 [59]. Letërnjoftimi biometrik përveç funksionit kryesor të tij si dokument identifikimi mund të përdoret edhe për rritjen e sigurisë gjatë procesit të autentikimit nëpërmes internetit, ku letërnjoftimi biometrik mund të shërbejë si një mjet që në mënyrë të sigurt të shpërndahen të dhënat personale në internet. Letërnjoftimi biometrik mund të përdoret si dëshmi e identitetit gjatë blerjeve përmes internetit, gjatë rezervimit të hotelit, hapjes së llogarisë bankare, dërgimit të e-mail-ve në mënyrë të sigurt etj. Letërnjoftimi biometrik i Republikës së Kosovës ka të deponuara të dhëna që mundësojnë autentikimin e shfrytëzuesit, enkriptimin e të dhënave, përdorimin e firmës (nënshkrimit) digjital (kriptografik) në dokumente elektronike dhe dërgimin e sigurt të emailave.

Përveç vërtetimit të qytetarëve këto shërbime elektronike kërkojnë që përdoruesit të enkriptojnë dhe të nënshkruajnë në mënyrë digjitale të dhënat ose dokumentet e tyre. Prandaj, kartelat biometrike përdoren si pajisje përpunimi për aplikacione kriptografike, ku ekzistojnë shumë aspekte të sigurisë të nevojshme për komunikim, autentikim dhe enkriptim të sigurt midis tyre. Këto aspekte të sigurisë janë bosht i këtij disertacioni doktorature, dhe do të testohen në ambiente të ndryshme, platforma, pajisje, PC, pajisje të lëvizshme dhe kartela të mençura. Në këtë disertacion janë krahasuar këto dy sisteme të procesimit, “match-off-card” kundrejtë “match-on-card”, dhe efikasitetin e tyre të enkriptimit dhe nënshkrimet në të dhënat e përdorura. Sa parametra të ndryshëm, koha dhe madhësia e vektorëve të paradefinuar të testimit ndikojnë në procesin dhe rolin që ata luajnë në sistemin e përgjithshëm. Rezultatet e nxjerra do të na shërbejnë si një udhëzues për përdorimin e një sistemi përpunimi në mjedis të caktuar, duke pasur parasysh efikasitetin e të dhënave.

1.2 Motivimi

Shoqëria bashkohore sot ballafaqohet me të arritura dhe zhvillime të mëdha në aspektin tekniko-teknologjik, të cilën e përcjell ekspansioni i shpejtë i teknologjisë së informacionit dhe komunikimit dhe tendenca gjithnjë në rritje e automatizimit të proceseve të punës në të gjitha sferat e jetës shoqërore dhe ekonomike. Ky zhvillim në shoqërinë bashkohore ka sjellur një numër të madh lehtësimesh në njërën anë, ndërsa në anën tjetër keqpërdorimi i paramenduar i këtyre të arriturave teknologjike, ka krijuar edhe një numër problemesh dhe rreziqesh, si për individ dhe grupe, ashtu edhe për shoqërinë në përgjithësi, rreziqe këto që nuk kanë qenë në kohën kur nuk ka ekzistuar ky automatizim i lartë i proceseve të punës.

Zhvillimi i hovshëm i aplikacioneve të cilat kanë për qëllim lehtësimin e punës së shfytëzuesve duke dhënë shërbime në internet, ka bërë që të shtohen gjithashtu edhe sulmet, e qëllimshme, të cilat bëhen në ato aplikacione. Disa nga sulmet nga të cilat kanë qenë të afektuar qytetarët kanë pasur edhe pasoja të mëdha për ta siç është shfrytëzimi i identitetit të qytetarëve për të bërë këto sulme për shkak të pamundësisë së autentikimit të tyre në një mjedis të pasigurt siç është interneti. Gjithashtu shumë shërbime të cilat kanë kërkuar që të autentikojnë me sukses shfrytëzuesit nuk kanë mundur që ta bëjnë këtë për shkak të mos posedimit të një mekanizmi me çelësa publik të lëshuara nga qeveria e atij shteti. Me lëshimin e letërnjoftimeve elektronike nga shumë shtete të botës është hapur mundësia për zhvillimin e shumë aplikacioneve të shërbimeve bankare, administrative, verifikim të dhënave të shfrytëzuesëve duke përdorur letërnjoftimin elektronik (eID). Këto aplikacione kanë për qëllim që të verifikojnë identitetin e shfrytëzuesit në formë të sigurt duke e bërë të pamundur qasjen e informatave të palejuara të shfrytëzuesit nga sulmuesi.

Prandaj përveç sfidave të theksuara më lartë, ndër elementet kryesore motivuese për punën time në këtë studim do të veçoja:

- Trendet aktuale në teknologjinë e informacionit dhe komunikimit po tregojnë që bota virtuale po rritet, shumëfish sesa bota fizike.
- Siguria e aplikacioneve po bëhet kërkesa kryesore e çdo aplikacioni softuerik bashkëkohor.
- Autentikimi (verifikimi i palëve komunikuese para kumunikimit) paraqet hallkën më të rëndësishme në mes botës fizike dhe botës virtuale në një transakcion.
- Kartela e re biometrike e identitetit synon ti plotësoj këto qëllime.
- Kriptografia e bazuar në aparatin matematikor është vegla bazë që siguron kërkesat e lartpërmuendura.

1.3 Përshkrimi i problemit dhe hipotezat

Kriptografia e bazuar në çelësa publik është fushë e re e studimit por që ka evoluar shumë në dhjetë vitet e fundit. Algoritmet kriptografike, të bazuara në aparatin kompleks matematikor, tani i gjejmë në secilën pajisje kompjuterike. Ato janë edhe në pajisjet tona mobile edhe në kartelat e reja elektronike (biometrike) të identitetit.

Dokumentet biometrike me të gjitha të dhënat personale që posedojnë kanë nevojë për siguri maksimale, veçanarisht kur këto të dhëna gjenden në formë elektronike dhe shumë lehtë mund të bëhen pre e keqpërdorimeve.

Me fillimin e lëshimit e letërnjoftimeve elektronike nga shumë shtete të botës qytetarët e atyre shteteve ju është dhënë mundësia e shfrytëzimit të shërbimeve të cilat kanë mundur ti bëjnë vetëm duke qenë prezent dhe duke poseduar një mjet identifikimi. Tani ata do të mund ta identifikojnë veten përmes mekanizmit të çelësave publik në çfarëdo shërbimi administrativ duke mos pasur nevojë që të jenë prezent aty. Mirëpo qasja në të dhënat private të cilat janë të deponuara në një mjedis të pasigurt siç është interneti ka qenë gjithmonë sfidë për zhvilluesit e ueb aplikacioneve që i kanë shfrytëzuar këto shërbime të ofruara nga letërnjoftimi elektronik. Mundësitë që këto të dhëna të cilat shpërndahen nëpër internet të mund të ndryshohen apo në rastin më të keq të mund të qasen nga pala e pa-autorizuar apo sulmuese mund të ketë efekte shumë të mëdha në cenimin e privatësisë së shfrytëzuesit. Prandaj aplikacionet e zhvilluara duhet që të posedojnë masat e nevojshme të sigurisë duke përdorur kriptografinë moderne me çelës publik.

Duke marrë parasysh atë që u theksua më lartë, në vazhdim janë ngritur disa pyetje specifike hulumtuese:

- Pyetja 1: Cila është baza matematikore e kriptografisë?
- Pyetje 2: Cilët janë algoritmet që janë përdorur dhe pse?
- Pyetja 3: Cilat janë kufizimet e këtyre algoritmeve gjatë implementimit praktik?
- Pyetja 4: Cilat janë përparsitë e kartelës biometrike e identitetit?
- Pyetja 5: Si është performanca e kartelës biometrike vs. PC?

2 NJOHURI TË DOMOSDOSHME MATEMATIKORE

Në kriptografinë me çelës publik përdoren dy çelësa, njëri publik për të enkriptuar mesazhet dhe tjetri privat për të dekriptuar mesazhet e pranuara. Lidhja midis tyre kërkohet e tillë që të jetë i pamundur zbulimi i çelësit privat nga ai publik. Kjo realizohet duke përdorur njohuri nga matematika moderne sidomos nga algjebra modulare dhe nga algjebra e strukturave të grupit, unazës dhe fushës, që janë objekt i këtij kapitulli. Në përbërje të tij do të jenë dhe teknika themelore si algoritmi i Euklidit, funksioni i Ejlerit, teorema kineze e mbetjeve, të cilat të gjitha së bashku janë fundamentale për sistemet kriptografike me çelës publik.

2.1 Algjebra Modulare

Përkufizim 1. *Për çdo dy numra të plotë a, b∈**Z** themi se a plotëpjeston b dhe këtë fakt e shënojmë a/b në qoftë se ekziston një numër natyror pozitiv k i tillë që b = ka. Pra,* [2]

$$a \mid b \Leftrightarrow (\exists\, k \in \mathbf{Z}^{+},\ b = k \cdot a). \qquad (1)$$

Le të jenë *X* dhe *Y* dy bashkësi të dhëna dhe *G* një bashkësi çiftesh të radhitura *(x, y).*

Përkufizim 2. *Lidhje dyshe (relacion binar) e bashkësisë X me bashkësinë Y quhet treshja e radhitur (X; Y; G), në të cilën G është nënbashkësi e prodhimit kartezian X×Y.* [1]

Ndërkaq, lidhja (*X; Y; G*) quhet *funksion i X-it drejt Y-ut* në qoftë se çdo elementi $x \in X$ i shoqëron të shumtën një element $y \in Y$; ajo quhet *pasqyrim i X-it në Y* në qoftë se çdo elementi $x \in X$ i shoqëron vetëm një element $y \in Y$.
Le të jetë *B* një bashkësi e çfarëdoshme joboshe.

Përkufizim 3. *Veprim i brendshëm algjebrik në bashkësinë B quhet çdo pasqyrim i B×B në B.* [1]

Për shembull, mbledhja dhe shumëzimi i zakonshëm në ***Z*** janë veprime të brendshme algjebrike në ***Z.***
Në matematikë hasen shpesh lidhjet që fillimin *X* dhe fundin *Y* e kanë të njëjtë, d.m.th., siç thuhet, lidhjet në *X*. Le të jetë *L* një lidhje në *X*.

Përkufizim 4. *Lidhja L në X quhet* [1]

1) *pasqyruese,* në qoftë se $\forall x \in X$, xLx;

2) *simetrike,* në qoftë se $\forall (x;y) \in X^2$, $xLy \Rightarrow yLx$;

3) *antisimetrike,* në qoftë se $\forall (x;y) \in X^2$, $(xLy) \wedge (yLx) \Rightarrow x=y$;

4) *kalimtare,* në qoftë se $\forall (x;y;z) \in X^3$, $(xLy) \wedge (yLz) \Rightarrow xLz$.

Përkufizim 5. *Lidhja L në X quhet lidhje e njëvlerësisë në X, në qoftë se ajo është njëherësh pasqyruese, simetrike dhe kalimtare.* [1]

Le të jetë *L në X* lidhje e njëvlerësisë. Shpesh, në vend të shënimit *xLy*, në këtë rast përdoret shënimi $x \equiv y \ (mod\ L)$, që lexohet "*x* është i njëvlershëm me *y* sipas modulit *L*". Në këto kushte, bashkësia e elementeve $b \in X$ që janë të njëvlershme me elementin e dhënë $a \in X$ sipas modulit *L*, quhet *klasë ekuivalence* e *X sipas L* dhe shënohet $[a]$. Është e qartë që çdo dy elemente të së njëjtës klasë ekuivalence të *X* sipas *L* janë të njëvlershme ndërmjet tyre (sipas vetisë simetrike dhe asaj kalimtare).

Në qoftë se *L* është lidhje ekuivalence në *X*, bashkësia e klasave të ekuivalencës të *X* sipas *L* quhet *bashkësi herës* e *X në lidhje me L* dhe shënohet *X/L*. Ajo gëzon vetitë [1]:

$$a)\ [a_i] \cap [a_j] = \varnothing, \text{ për } i \neq j,$$

$$b)\ \bigcup_i [a_i] = X$$

d.m.th. që çdo element i *X* bën pjesë vetëm në njërën prej klasave $[a_i]$ të ekuivalencës të *X* sipas *L* dhe *X* paraqitet si bashkim i tyre.

Përkufizim 6. *Lidhja L në X quhet lidhje e radhitjes në X në qoftë se ajo është njëherësh pasqyruese, antisimetrike dhe kalimtare.* [1]

Le të jetë *m* një numër i plotë pozitiv i fiksuar në mënyrë të çfarëdoshme dhe *a*, *b* dy numra të plotë të çfarëdoshëm.

Përkufizim 7. *Lidhja* $\{(a, b) \in Z^2 \mid \exists\, k \in Z,\ a - b = k \cdot m\}$ *quhet lidhje e kongruencës sipas modulit m dhe shënohet* $\equiv_m$. [2], [3], [4], [5]

Shënimin $a \equiv_m b$, që shpesh në literaturë e gjejmë $a \equiv b \pmod m$ dhe të tillë do ta përdorim edhe ne, e lexojmë "*a është kongruent me b sipas modulit m*". Pra,

$$a \equiv b \ (mod\ m) \Leftrightarrow (\exists\, k \in Z,\ a - b = k \cdot m). \qquad (2)$$

Për shembull, $10 \equiv 4 \pmod 3$, sepse $10 - 4 = 2 \cdot 3$; $10 \equiv 4 \pmod 2$, sepse $10 - 4 = 3 \cdot 2$; $8 \equiv 5 \pmod 3$, sepse $8 - 5 = 1 \cdot 3$; $117 \equiv 3 \pmod 2$, sepse $117 - 3 = 57 \cdot 2$, $-173 \equiv 5 \pmod 2$, sepse $-173 - 5 = (-89) \cdot 2$.

Ndërkaq, tregohet lehtë që në qoftë se $a \equiv b \pmod m$ dhe $c \equiv d \pmod m$, atëherë, si te barazimet numerike, kemi

$$\begin{aligned} &1.\ a \pm c \equiv b \pm d \pmod{m};\\ &2.\ ac \equiv bd \pmod{m};\\ &3.\ na \equiv nb \pmod{m}, n \in Z^{+};\\ &4.\ a^n \equiv b^n \pmod{m}. \end{aligned} \qquad (2')$$

Me të vërtetë, $a \equiv b \pmod{m}$ dhe $c \equiv d \pmod{m}$, sipas (2) do të thotë që ekzistojnë $k, l \in Z$, që $a=b+km$, $c=d+lm$, prej nga del që

$a+c=b+d+(k+l)m \Rightarrow a+c \equiv b+d \pmod{m}$ dhe $ac=bd+(bl+dk+klm)m \Rightarrow ac \equiv bd \pmod{m}$. Njëlloj dhe për vetitë e tjera.

Teoremë 1. *Lidhja $\equiv_m$ është lidhje e ekuivalencës mbi Z.*

Me të vërtetë, për çdo $a \in Z$ kemi $a \equiv a \pmod{m}$, përderisa $a - a = 0 \cdot m$, që tregon se lidhja $\equiv_m$ është pasqyruese. Për çdo $a, b \in Z$, $a \equiv b \pmod{m}$ sjell $b \equiv a \pmod{m}$, sepse $a - b = km \Rightarrow b - a = (-k)m$, prej nga del se lidhja $\equiv_m$ është dhe simetrike. Së fundi, për çdo $a, b, c \in \boldsymbol{Z}$, në qoftë se $a \equiv b \pmod{m}$ dhe $b \equiv c \pmod{m}$, nga (2) kemi $a - b = k \cdot m$ dhe $b - c = t \cdot m$; duke mbledhur këto të fundit anë me anë, del $a - c = (k+t)m$, d.m.th. $a \equiv c \pmod{m}$, që tregon se lidhja $\equiv_m$ është edhe kalimtare.

Dihet nga Aritmetika që është i vërtetë ky

Pohim 1. *Për çdo dy numra të plotë a, b, ku $b \neq 0$, ekzistojnë dhe janë të vetëm dy numra të plotë q dhe r të tillë që*

$$a=bq+r, \qquad (3)$$

ku $0 \le r < |b|$. Në këtë rast q quhet herës dhe r quhet mbetje e pjesëtimit të a me b.

Mbështetur në këtë pohim, vërtetohet lehtë që bashkësitë

$$[0]=\{0+km\};\ [1]=\{1+km\};\ ...;\ [m\text{-}1]=\{(m\text{-}1)+\text{km}\} \qquad (4)$$

janë klasat e ekujvalencës së lidhjes $\equiv_m$ dhe prandaj

$$Z/\equiv_m = \{[0]; [1]; ...; [\text{m-}1]\}.$$

Klasat (4) janë quajtur *klasat e mbetjeve* (*mod m*). P.sh. për m=4, marrim

$$Z/\equiv_4 = \{[0]; [1]; [2];[3]\},$$

d.m.th. kjo bashkësi herës përbëhet nga katër elemente [0], [1], [2], [3] të cilat janë nënbashkësitë e mëposhtme të Z:

$$[0]=\{0+k\cdot 4\}=\{..., -8, -4, 0, 4, 8, ...\},$$
$$[1]=\{1+k\cdot 4\}=\{..., -7, -3, 1, 5, 9, ...\},$$
$$[2]=\{2+k\cdot 4\}=\{..., -6, -2, 2, 6, 10, ...\},$$
$$[3]=\{3+k\cdot 4\}=\{..., -5, -1, 3, 7, 11, ...\}.$$

Përkufizim 8. Lidhja | në bashkësinë N_0 (e numrave natyrorë pa zeron) e tillë që

$$| = \{(a, b) \in N_0 \times N_0 \mid \exists\, k \in N_0,\ b = k \cdot a\}$$

quhet *lidhja e plotëpjestueshmërisë*.

Teoremë 2. *Lidhja e plotëpjestueshmërisë është lidhje e radhitjes në* N_0.

Me të vërtetë:

1) $\forall a \in N_0$, $a \mid a$, pra është refleksive;

2) $\forall a, b \in N_0$, $a \mid b \wedge b \mid a \Rightarrow a = b$, mbasi $a \mid b$ do të thotë se $\exists k \in N_0$, $b = ka$ dhe $b \mid a$ do të thotë se $\exists m \in N_0$, $a = mb$, prej nga $a = mka$, d. m. th. $m=k=1$ dhe për pasojë $a = b$; në këtë mënyrë rezulton që lidhja $\mid$ është antisimetrike;

3) $\forall a, b, c \in \boldsymbol{N}_0$, $a \mid b$ dhe $b \mid c$, d. m. th. $b = ka$ dhe $c = mb$, implikon c $= mka$, d. m. th. $a \mid c$, që tregon se lidhja $\mid$ është edhe kalimtare.

Le të jetë $Z_n = \{0, 1, 2, \ldots, n-1\}$ bashkësia e numrave të parë natyrorë. Sipas Pohimit 1 mbetja e pjestimit të çdo numri të plotë x me numrin natyror $n \geq 1$, që shënohet $r_n(x)$, është e vetme në Z_n. Kjo lejon që të futet në Z_n veprimi algjebrik $\oplus$ i mbledhjes(mod n) i tillë që

$$\forall (a,b) \in Z_n^2 , a \oplus b = r_n(a+b), \tag{5}$$

dhe veprimi algjebrik $\otimes$ i shumëzimit(mod n) i tillë që

$$\forall (a,b) \in Z_n^2 , a \otimes b = r_n(a \cdot b). \tag{6}$$

Përftohet kështu algjebra me dy veprime (Z_n, $\oplus$, $\otimes$), që njihet me emrin *algjebra modulare*(mod n).

Lidhur me mbetjet $r_n(x)$ ka vend kjo

Teoremë 3. [2] *Në qoftë se* $r_n(x)$ *dhe* $r_n(y)$ *janë përkatësisht mbetjet e pjesëtimit me numrin natyror* $n \geq 1$ *të dy numrave të çfarëdoshëm* $x, y \in Z$, *atëherë*

1) $x \equiv y \pmod{n} \Leftrightarrow r_n(x) = r_n(y)$; (7)

2) $r_n(x + y) = r_n[r_n(x) + r_n(y)]$; (8)

3) $r_n(x \cdot y) = r_n[r_n(x) \cdot r_n(y)]$. (9)

2.2 Grupi. Grupet Ciklike

Struktura algjebrike me një veprim *(B,* □*)* thirret shkurt grupoid. Kur veprimi □ në grupoidin (*B,* □) është shoqërues, d.m.th. *∀a,b,c∈B, (a* □ *b)* □ *c = a* □ *(b* □ *c),* ai quhet *gjysmëgrup* , kurse kur sipas veprimit □ ekziston edhe elementi asnjanës *e në bashkësinë B,* d.m.th**.** i tillë që *∀a∈B, e* □ *a=a* dhe *a* □ *e=a*, atëherë ai quhet *monoid*. Ndërsa kuptimi i grupit jepet sipas këtij

Përkufizim 1. *Grup quhet grupoidi* (*G,* □), *në të cilin*: [1], [2]

- *veprimi* □ *është shoqërues*;
- *ekziston elementi asnjanës sipas* □;
- *çdo element i G ka element simetrik të djathtë sipas* □(d.m.th. $\forall a \in B$, $\exists \bar{a} \in B$, a □ $\bar{a} = e$).

Në qoftë se □ në grup është dhe ndërrues, atëherë (*G*, □) quhet grup *komutativ* (ose *abeljan*).

Pothuajse të gjitha grupet që takohen në kriptografi janë abeliane, pasi vetia komutative është shpesh ajo që i bën ato kriptografikisht interesante.

Teoremë 1. *Grupoidi* $(Z_n, \oplus)$ *është grup abelian.*

Me të vërtetë, le të jenë $r_n(a)$ dhe $r_n(b)$ përkatësisht mbetjet e pjesëtimit me numrin natyror $n \geq 1$ të numrave të plotë të çfarëdoshëm *a, b,* d. m. th. kemi

$$a = qn + r_n(a),\ b = q'n + r_n(b),\ \text{ku } 0 \leq r_n(a), r_n(b) < n.$$

Kështu që $a + b = (q + q')n + r_n(a) + r_n(b)$, prej nga, sipas (5), $a + b \equiv r_n(a) + r_n(b) \pmod{n}$. Prandaj, sipas (8), marrim barazimin

$$r_n(a + b) = r_n(r_n(a) + r_n(b)). \qquad (10)$$

Meqenëse për çdo $x \in Z_n$, kemi $x = r_n(x)$, nga (10) dhe nga vetia shoqëruese e mbledhjes së zakonshme në *Z* marrim

$$\begin{aligned} \forall a, b, c \in Z_n,\ a \oplus (b \oplus c) &= r_n(a + r_n(b + r_n(b + c))) = r_n(r_n(a) + r_n(r_n(b + c))) = \\ &= r_n(a + (b + c)) = r_n((a + b) + c) = \\ &= r_n(r_n(a + b) + r_n(c)) = \\ &= r_n((a \oplus b) + c) = \\ &= (a \oplus b) \oplus c, \end{aligned}$$

që tregon se veprimi $\oplus$ është shoqërues.

Ndërkaq, $\forall a \in Z_n$, duket me një herë që $a \oplus 0 = 0 \oplus a = a$ dhe, në veçanti, $0 \oplus 0 = 0$; po ashtu për çdo *a* jozero nga Z_n, $n\text{-}a \in Z_n$ dhe $a \oplus (n\text{-}a) = 0$. Kështu që 0 është element asnjanës dhe 0, *n-a* janë përkatësisht elementi simetrik i djathtë $\bar{0}$ i 0-ros dhe $\bar{a}$ i *a-së* jo zero. Si përfundim struktura $(Z_n, \oplus)$ rezulton grup, madje sipas (5), ky grup është abelian. Nga kjo del që elementi simetrik i djathtë i elementit *a* është element simetrik i tij lidhur me mbledhjen (mod *n*), të cilin e shënojmë $-a \pmod{n}$ dhe e quajmë *element i kundërt* (mod *n*) i *a*. Pra,

$$\forall a \in Z_n,\quad -a \pmod{n} = \begin{cases} 0, & \text{per } a = 0; \\ n - a, & \text{per } a \neq 0. \end{cases} \qquad (10')$$

Teoremë 2. *Grupoidi* $(Z_n, \otimes)$ *është gjysmëgrup.*

Me qenë se për çdo $x \in Z_n$, kemi $x = r_n(x)$, nga (6), nga (9) dhe nga vetia shoqëruese e shumëzimit të zakonshëm në *Z* marrim

$$\begin{aligned} \forall a, b, c \in Z_n,\ a \otimes (b \otimes c) &= r_n[a \cdot r_n(bc)] = r_n[r_n(a) \cdot r_n(bc)] = \\ &= r_n[a \cdot (bc)] = r_n[(ab)c] \\ &= r_n[r_n(ab) \cdot r_n(c)] = \\ &= r_n[(a \otimes b) \cdot c] = \\ &= (a \otimes b) \otimes c, \end{aligned}$$

që tregon se veprimi $\otimes$ është shoqërues.

Për grupet $(G, \cdot)$ me shënim multiplikativ, ku elementi asnjanës e shënohet 1_G dhe emërtohet *element i njësishëm*, futet kuptimi i fuqisë nga ky

Përkufizim 2. [2] *Le të jetë a një element i grupit* $(G; \cdot)$ *dhe n një numër i plotë. Fuqi e n-të e elementit a quhet elementi* a^n *i grupit i tillë që*

$$a^0=1_G,\ a^n=a^{n-1}\cdot a,\ \text{për } n>0 \text{ dhe } a^n=(a^{-1})^{-n},\ \text{për } n<0. \tag{11}$$

Nga përkufizimi del se $a^1=a$, sepse $a^1= a^{1-1}\cdot a= a^0\cdot a = 1_G \cdot a= a$; pastaj $a^2= a^{2-1}\cdot a=a\cdot a$ dhe, me induksion matematik lidhur me n, për çdo n>0 marrim

$$a^n=\overbrace{a\cdot a\cdots a}^{n \text{ herë}} \tag{12}$$

Fuqitë e elementeve të një grupi multiplikativ kanë veti të ngjashme me fuqitë e numrave, siç del nga këto teorema.

Teoremë 3. [2] *Në një grup* $(G; \cdot)$ *për çdo dy numra të plotë m, n dhe për çdo element* $a\in G$ *janë të vërteta barazimet*

$$a^m\cdot a^n = a^{m+n}, \tag{13}$$

$$(a^m)^n = a^{mn}. \tag{14}$$

Teoremë 4. [2] *Në një grup abelian* $(G, \cdot)$ *për çdo numër të plotë n dhe për çdo dy elemente* $a, b \in G$ *është i vërtetë barazimi*

$$(a\cdot b)^n = a^n\cdot b^n. \tag{15}$$

Shënim.Në rastin e grupit me shënim aditiv $(G, +)$, ku elementi asnjanës ***e*** shënohet θ dhe emërtohet *element zero,* fuqia a^n e një elementi a të tij zëvendësohet me *shumëfishin na* të tij në mënyrë të tillë që barazimet (11) marrin trajtën

$$0a=\theta,\ na=(n\text{-}1)\,a+a,\ \text{për } n>0 \text{ dhe } na=(-n)\,(-a),\ \text{për } n<0 \tag{11'}$$

dhe barazimi (12) për çdo n>0 trajtën

$$na=\overbrace{a+a+\cdots+a}^{n \text{ herë}}. \tag{12'}$$

Prej këndej, barazimet (13), (14) dhe (15) marrin përkatësisht trajtat

$$ma+na=(m+n)a, \tag{13'}$$

$$n(ma) = (n\cdot m)a, \tag{14'}$$

$$n(a+b)=na+nb. \tag{15'}$$

Në rastin e grupit aditiv (Z, +) të numrave të plotë elementi zero θ është numri 0, prandaj nga barazimet (11') marrim $0a=0$ dhe përgjithsisht $na= n\cdot a$, për çdo dy numra të plotë n e a, ku $\cdot$ është shumëzimi i zakonshëm i numrave të plotë.

Le të jenë B një bashkësi joboshe, □ një veprim i brendshëm në të dhe A një nënbashkësi joboshe e B.

Përkufizim 3. [1], [2] *A quhet nënbashkësi e qëndrueshme e B në lidhje me* □ *në qoftë se*

$$\forall\ (a,b)\in A^2,\ a\square b\in A. \tag{16}$$

Në një bashkësi jo boshe B mund të jenë futur disa veprime □; ⊥; .... Në këtë rast sistemi i radhitur (B; □; ⊥; ...) quhet *strukturë algjebrike* (ose *algjebër*). Në qoftë se akoma B' është një nënbashkësi e qëndrueshme e B në lidhje me veprimet □, ⊥, ..., atëherë (B', □, ⊥, ...) quhet *nënstrukturë* e strukturës (B, □, ⊥, ...).

Një nënstrukturë (G', ·) e një grupi (G, ·) mund të jetë vetë grup. Në këtë rast ajo quhet *nëngrup* i grupit (G, ·). Ka vend kjo

Teoremë 5. *Çdo nënstrukturë e fundme (G'; ·) e një grupi (G; ·) është nëngrup i tij.*

Vërtetim. Meqenëse G' është nënbashkësi e qëndrueshme e G lidhur me shumëzimin ·, ajo është jo boshe dhe, sipas (16), $\forall a, b \in G', ab \in G'$. Prandaj ajo përmban sëbashku me një element b të saj edhe fuqitë e b me eksponente të plota pozitive:

$$b, b^2, b^3, \ldots .$$

Për deri sa G' është e fundme, këto fuqi nuk mund të jenë të gjitha të ndryshme. Ka kështu në vargun e mësipërm dy kufiza të barabarta. Le të jenë b^k dhe b^{k+t} , ku t > 0, të tilla që $b^k = b^{k+t}$. Por, në qoftë se 1_G është elementi asnjanës i grupit G, atëherë kemi

$$b^k = b^k \cdot e = b^k \cdot b^t,$$

që, duke thjeshtuar nga e majta sjell,

$$b^t = 1_G.$$

Për rrjedhoj $1_G \in G'$. Më tej, kur $t > 1$ kemi $b^{t-1} \cdot b = b \cdot b^{t-1} = u$ (shih (13)), që tregon se b^{t-1} është i anasjelli i b në G', kurse kur $t = 1$ marrim $b = 1_G$ dhe në këtë rast i anasjelli i b është vetë b. Në këtë mënyrë del që $\forall b \in G', b^{-1} \in G'$, prandaj $\forall a, b \in G', ab^{-1} \in G'$. Sipas një teoreme (A-GJ), përfundojmë që G' është nëngrup i G.

Le të jetë tani a një element i çfarëdoshëm i grupit (G; ·). Shënojmë $\langle a \rangle$ bashkësinë e të gjitha fuqive me eksponent të plotë (pozitiv, zero, negativ) të elementit a, d.m.th. $\langle a \rangle = \{a^n \mid \forall n \in \mathrm{Z}\}$. Nuk është e vështirë të bindemi se *për çdo element a të grupit* (G, ·), ($\langle a \rangle$, ·) *është nëngrup i tij*.

Përkufizim 4. *Nëngrupi* ($\langle a \rangle$, ·) *i grupit* (G, ·) *quhet nëngrup ciklik i tij, kurse elementi a quhet përftues* (*gjenerator*) *i* $\langle a \rangle$.[2]

Në $\langle a \rangle$ nuk përjashtohet mundësia që dy ose më shumë fuqi të elementit a të jenë të barabarta.

Kjo ndodh vetëm atëherë kur ekziston një numër i plotë $t > 0$, që $a^t = 1_G$, që del nga ky

Pohim 1. *Për një element a të grupit (G, ·), ekziston një numër i plotë t > 0 i tillë që* $a^t = 1_G$ *vetëm atëherë, kur në* $\langle a \rangle$ *ka fuqi të barabarta.* [2]

Pohimi i mësipërm na çon në këtë

Përkufizim 5. *Numri më i vogël i plotë pozitiv n i tillë që* $a^n = 1_G$ *quhet rend ose periodë i elementit a të grupit* (G, ·) *Në qoftë se një numër i plotë i tillë nuk ekziston, atëherë thuhet se elementi a i grupit ka rend ose periodë të pafundme.* [2]

Rendi i elementit a të një grupi shënohet o(a). Është e qartë se për elementin e njësishëm 1_G të grupit kemi o(1_G)=1. Ndërkaq, nga Pohimi 1 del që, në qoftë se në $\langle a\rangle$ të gjitha fuqitë e elementit a janë të ndryshme, atëherë elementi a i grupit ka rend të pafundëm. Grupi, elementet e të cilit kanë rend të pafundëm quhet grup *periodik*.

Radhitim më poshtë disa pohime që lidhen me rendin e një elementi të një grupi.

Pohim 2.*Për çdo element a të një grupi (G, ·), $a^k = 1_G$ vetëm atëherë, kur k është shumëfish i o(a).* [2]

Pohim 3. *Në qoftë se n është rendi i elementit a të grupit (G, ·), atëherë*

1) $a^k = a^s \Leftrightarrow k \equiv s(\mathrm{mod}\, n)$;

2) $a^k \cdot a^s = a^{k \oplus s}$, ku $k \oplus s = r_n(k+s)$.

Vërtetim. 1) Vihet re lehtë se, duke shumëzuar me a^{-s} në të dy anët e barazimit nga Pohimi 2 marrim $a^k = a^s \Leftrightarrow a^{k-s} = e \Leftrightarrow k\text{-}s = nq \Leftrightarrow k \equiv s(\mathrm{mod}\, n)$;

2) Duke qenë se $k+s \equiv r_n(k+s)(\mathrm{mod}\, n)$, nga 1) kemi $a^k \cdot a^s = a^{k+s} = a^{k \oplus s}$.

Pohim 4. *Çdo element a i një grupi* (*G*, ·) *dhe i anasjelli i tij a^{-1} kanë të njëjtin rend.* [2]

Përkufizim 6. *Grupit* (*G;* ·) *quhet ciklik në qoftë se përputhet me njërin nga nëngrupet e veta ciklike, ndryshe kur* (*G;* ·) = ($\langle a\rangle$, ·). [2]

Meqenëse në grupin ciklik ($\langle a\rangle$, ·) çdo element i tij është fuqi e a, dhe për çdo dy elemente a^p e a^q kemi

$$a^p \cdot a^q = a^q \cdot a^p = a^{p+q},$$

del se *çdo grup ciklik është grup abeljan*.

Teoremë 6. [2] *Në qoftë se rendi i gjeneratorit a të grupit ciklik* ($\langle a\rangle$, ·) *është numri i fundëm n, d. m. th. $a^n = 1_G$, atëherë*

$$1_G, a, a^2, \ldots, a^{n-1}$$

janë të ndryshëm dhe të vetmit elemente të $\langle a\rangle$,d. m. th.

$$\langle a\rangle = \{1_G, a, a^2, \ldots, a^{n-1}\}.$$

Teorema ndryshe thotë që, në qoftë se rendi i gjeneratorit a të grupit ($\langle a\rangle$,·) është numër i fundëm n, atëherë ai është grup i fundëm me n elemente. Në këtë rast thuhet se ($\langle a\rangle$,·) është grup ciklik i fundëm *i rendit n*.

Në një grup të fundëm ciklik ($\langle a\rangle$,·) të rendit n, për të dalluar ato elemente a^k (1<k<n) të tij, që janë gjeneratorë të tjerë, vlen teorema e mëposhtme.

Teoremë 7. *Në një grup të fundëm ciklik* ($\langle a\rangle$,·) *të rendit n, elementi a^k (1<k<n) i tij është gjenerator vetëm atëherë, kur k dhe n janë të thjeshtë ndërmjet tyre***.** [2], [6]

Prej teoremës del ky përfundim praktik: *në qoftë se rendi i grupit ciklik është i thjeshtë, atëherë çdo element i tij, përveç elementit të njësishëm* 1, *është gjenerator, d.m.th.*

$$\forall x \in \langle a \rangle, x^n = 1_G \tag{17}$$

Në qoftë se rendi n i grupit ciklik $\langle a \rangle$ *është i përbërë, atëherë gjeneratorë janë ato elemente* a^k, *për të cilët Pmp* (k, n) =1. Ndryshe, kur rendi n është i përbërë, numri i gjeneratorëve është i barabartë me numrin e eksponenteve k që janë të thjeshtë lidhur me n dhe nuk e kapërcejnë atë. Numri i numrave të tillë studiohet me anë të *funksionit të Ejlerit* [2], [4]. Kështu quhet funksioni ϕ që çdo numri të plotë pozitiv n i shoqëron numrin e numrave të plotë pozitivë që nuk e kapërcejnë n dhe janë të thjeshtë lidhur me numrin n. Është e qartë se, kur n është i thjeshtë, atëherë $\phi(n) = n - 1$.

2.3 Unazat. Fushat

Përkufizim 1. [1], [2] *Unazë quhet struktura* (B, □, ⊥) *që ka vetitë:*

1) *struktura* (B, □) *është grup abelian*;
2) *veprimi i dytë* ⊥ *është shoqërues*;
3) *veprimi* ⊥ *është shpërndarës në lidhje me veprimin e parë* □.

Në qoftë se veprimi i dytë është edhe ndërrues, atëherë (B, □, ⊥) quhet *unazë komutative* ose *abeliane*.

Veprimi i parë □ në një unazë B zakonisht shënohet me shënjën + të mbledhjes dhe veprimi i dytë shënohet me shenjën · të shumëzimit, duke i dhënë asaj shënimin (B, +, ·). Në qoftë se (B, ·) ka element të njësishëm e, atëherë unaza (B, +, ·) quhet *e njësishme.*

Le të jetë (B, +, ·) një unazë. Meqenëse (B, +) është grup, $\forall a \in B$, $\exists -a \in B$ i tillë që $a+(-a)=\theta$. Prania e $-a$ për çdo $a \in B$ lejon futjen e veprimit *të zbritjes* në unazën B si veprimi që çdo $(a, b) \in B^2$ i shoqëron elementin $a + (-b)$, i cili quhet *ndryshesë e a-së me b-në* dhe shënohet $a - b$.

Pra,

$$a - b = a + (-b). \tag{18}$$

Disa veti elementare të unazave jepen nga ky

Pohim 1. [2] *Në qoftë se a, b, c, janë elemente të çfarëdoshme të një unaze* (B, +, ·) , *atëherë:*

1. $a\,(b-c) = ab - ac$ dhe $(a - b)c = ac - bc$;
2. $a\,\theta = \theta\,a = \theta$;
3. $(-a)\,b = -(ab)$;
4. $b\,(-a) = -(ba)$;
5. $(-a)\,(-b) = ab$.

Teoremë 1. *Algjebra modulare* $(Z_n, \oplus, \otimes)$ *është unazë komutative dhe e njësishme.*

Me të vërtetë, sipas Teoremës 1 dhe Teoremës 2 në pikën 2, grupoidi $(Z_n, \oplus)$ është grup abeljan dhe ai $(Z_n, \otimes)$ është gjysmëgrup, d.m.th. veprimi i dytë $\otimes$ në Z_n është shoqërues. Më tej, sipas (8), (9) dhe vetisë shpërndarëse të shumëzimit $\cdot$ lidhur me mbledhjen + në Z, kemi

$$\forall a, b, c \in Z_n,\ a \otimes (b \oplus c) = a \otimes r_n(b+c) =$$
$$= r_n [a \cdot r_n (b+c)] = r_n [r_n (a) \cdot r_n (b+c)] =$$
$$= r_n[a \cdot (b+c)] = r_n(ab+ac) =$$
$$= r_n[r_n(ab)+r_n(ac)] =$$
$$= r_n (a \otimes b + a \otimes c) =$$
$$= (a \otimes b) \oplus (a \otimes c).$$

Në të njëjtën mënyrë vërtetohet edhe barazimi $(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$. Prej nga del që veprimi i dytë $\otimes$ është shpërndarës në lidhje me veprimin e parë $\oplus$ në Z_n. Si përfundim algjebra modulare $(Z_n, \oplus, \otimes)$ është unazë. Ajo njihet me emrin *unaza e mbetjeve* (mod *n*). Duket menjëherë që ajo është komutative dhe e njësishme, me element të njësishëm numrin 1. Unaza *Zn* e mbetjeve (mod *n*) është me rëndësi qëndrore për kriptografinë moderne me çelësa publik [4], për këtë arsye ajo do të jetë objekt i shtjellimit të mëtejshëm.

Vetia 2 e unazave tek Pohimi 1 shpreh faktin që kur njeri nga dy faktorë është zero, atëherë edhe prodhimi i tyre është zero. Ka unaza që nuk është i vërtetë pohimi i anasjelltë. Në të tilla unaza ka të paktën një element $a \neq \theta$ dhe një element $b \neq \theta$, që $a \cdot b = \theta$. Element të tillë quhen *pjesëtues të zeros.* Një unazë që nuk ka pjesëtues të zeros dhe njëherësh është unazë abeliane dhe e njësishme quhet *unazë e plotë*. Unaza e numrave të plotë Z është shembulli më i thjeshtë dhe më i rëndësishëm i një unaze të plotë.

Kurse unaza $(Z_n, \oplus, \otimes)$ e mbetjeve (mod *n*), nga Teorema 1, është abeliane dhe e njësishme, por nuk është pa pjestues të zeros përgjithsisht. P.sh. për $n = 2m > 2$ kemi $2 \otimes m = r_{2m}(2 \cdot m) = r_n(n) = 0$. Kjo tregon se 2 dhe *m* janë pjesëtues të zeros në Z_{2m}.

Ndër unazat një rëndësi të veçantë kanë *fushat*.

Përkufizim 2. [1], [2] *Fushë quhet unaza F që ka vetitë:*

1) *në F ka të paktën një element të ndryshëm nga zero;*

2) $F^* = F - \{\theta\}$ *është nënbashkësi qëndrueshme e F në lidhje me shumëzimin;*

3) $(F^*, \cdot)$ *është grup abelian.*

Nga përkufizimi duket lehtë se unaza e numrave racional *Q* , ajo e numrave real *R* dhe ajo e numrave kompleks *C* janë shembujt më të familjarizuar të fushave. Ndërkaq, unaza e numrave të plotë *Z* nuk është fushë, sepse $(Z_0, \cdot)$ nuk është grup, mbasi p.sh. numri 4 nuk ka të anasjellë në Z_0.

Duke qenë që një fushë është unazë, atëherë, sipas pikës 2 të Pohimit 1, për çdo element *a* të saj kemi $a\ \theta = \theta\ a$, kurse, nga pika 3 e Përkufizimit 2, për çdo dy element jo zero *a,b* kemi *ab = ba.* Në këtë mënyrë kemi përftuar këtë

Teoremë 2. *Në qoftë se* $(F; +; \cdot)$ *është fushë, atëherë ajo është unazë abeliane.*

Ka vend gjithashtu kjo

Teoremë 3. [2] *Në qoftë se* $(F; +; \cdot)$ *është fushë, atëherë*

1) *ajo është unazë e plotë,*

2) *kanë zgjidhje të vetme në F ekuacionet* $ax=b$ *dhe* $xa=b$, *ku* $a\neq 0$, *b janë dy elemente të çfarëdoshme të F.*

Prej saj del ky

Rrjedhim. [2] *Një unazë me më shumë se një element është një fushë vetëm atëherë kur ajo është abeliane, e njësishme dhe çdo element* $a\neq 0$ *i saj ka element të anasjellë.*

Teoremë 4. *Unaza* $(Z_n, \oplus, \otimes)$ *e mbetjeve (mod n) është fushë, për rrjedhojë unazë e plotë, vetëm atëherë kur n është numër i thjeshtë (d. m. th. pjesëtuesi më i madh natyror i n është 1).*

Me të vërtetë, le të jetë n numër i thjeshtë. Nga Teorema 1, $(Z_n, \oplus, \otimes)$ është unazë komutative dhe e njësishme me element të njësishëm numrin 1. Të tregojmë tani që ajo është fushë. Shqyrtojmë bashkësinë Z_n^* të numrave $a \neq 0$ në Z_n. Meqenëse $a < n$ dhe n është i thjeshtë, pjesëtuesi më i madh i përbashkët i tyre është 1, d. m. th. $Pmp(a, n) = 1$. Nga Aritmetika dihet se për çdo dy numra natyror jozero p, q ekzistojnë dy numra $c, d \in Z$ të tillë që $Pmp(p, q) = cp+dq$. Prandaj edhe për a, n gjenden numrat $s, t \in Z$ të tillë që $1 = sa+tn$. Nga ky barazim, nga (8) dhe kuptimi i shumëzimit $\otimes$ marrim

$$1 = r_n(1) = r_n(sa+tn) = r_n(sa) = r_n(r_n(s)\cdot r_n(a)) =$$
$$= r_n(s) \otimes r_n(a) = r_n(s) \otimes a.$$

Kjo tregon se çdo $a \in Z_n^*$ ka element simetrik lidhur me shumëzimin(mod n) elementin $r_n(s) \in Z_n$. Nga Rrjedhimi i mësipërm del që$(Z_n, \oplus, \otimes)$ është fushë.

Anasjellas, le të jetë unaza $(Z_n, \oplus, \otimes)$ e mbetjeve (mod n) fushë. Të tregojmë se n është numër i thjeshtë. Supozojmë të kundërtën, se n nuk është i thjeshtë. Atëherë ekzistojnë në Z_n^* numrat $p\neq 1$ dhe $q\neq 1$ të tillë që $n = pq$, që sjell nga njëra anë $r_n(n) = 0$ dhe nga ana tjetër $r_n(n) = r_n(pq) = p \otimes q$, d. m. th $p \otimes q = 0$. Kjo tregon se p, q janë pjesëtues të zeros, në kundërshtim me piken 1) të Teoremës 4.

Nga vërtetimi i mësipërm del se në bashkësinë $Z_n^* = \{ a \in Z_n \mid a \neq 0 \} = \{1, 2, ..., n\text{-}1\}$, ku n është i thjeshtë, çdo element a ka element simetrik lidhur me shumëzimin(mod n) elementin $r_n(s) \in Z_n$, të cilin e shënojmë a^{-1}(mod n) dhe e quajmë *element i anasjellë*(mod n) i a. Përftojmë kështu këtë:

Rrjedhim 1. *Për një n të thjeshtë, për çdo* $a \in Z_n^*$, *për të cilin* $sa+tn=1$, *ka vend formula*

$$a^{-1}(mod\ n) = r_n(s). \qquad (19)$$

Veç kësaj, kur n është i thjeshtë, për çdo element $a \in Z_n^*$ kemi $Pmp\ (a, n) = 1$ dhe anasjellas. Në këtë rast, numri n-1 i elementeve të Z_n^* është i barabartë me vlerën $\phi(n)$ të funksionit të Ejlerit. Marrim kështu këtë

Rrjedhim 2. *Në unazën* $(Z_n, \oplus, \otimes)$, *çdo element ka element të anasjellë(mod n) vetëm kur Pmp(a, n) = 1. Në këtë rast grupi* $(Z_n^*, \otimes)$ *ka* $\phi(n)$ *elemente.*

Së fundi, duke patur parasysh Teoremën 3, përftojmë dhe këtë

Rrjedhim 3. *Për një n të thjeshtë, kanë zgjidhje të vetme në fushën Z_n ekuacionet $a \otimes x=b$ dhe $x \otimes a=b$, ku $a \neq \theta$, b janë dy elemente të çfarëdoshme të Z_n.*
Teoremë 5. *Çdo unazë e plotë e fundme është një fushë.* [2]

Në kriptografi kanë interes fushat me numër të fundëm *n* elementesh [4], që quhen *fusha të fundme me karakteristikë n*. Nga Teorema 4 të tilla janë unazat (Z_n, $\oplus$, $\otimes$) të mbetjeve (mod *n*) për të gjithë numrat e thjeshtë *n*. Teorema 5 tregon se fushat e fundme janë unazat e plota të fundme. Çdo fushë e fundme me *p* elemente shënohet *F(p)* ose *GF*(*p*) dhe quhet *fusha e Galluait*. Prej këndej një unazë Z_n e mbetjeve (mod *n*), ku *n* është numër i thjeshtë, është një *GF*(*n*). Shpesh me shënimin *GF*(*n*) nënkuptohet unaza Z_n e mbetjeve (mod *n*), ku *n* është numër i thjeshtë.

Shembull. Në fushën *GF*(5) = {0, 1, 2, 3, 4} të gjenden të kundërtit (mod 5) të elementeve të saj dhe të anasjellët (mod 5) të elementeve jo zero të saj.

Fusha *GF*(5) = {0, 1, 2, 3, 4} është unaza (Z_5, $\oplus$, $\otimes$) e mbetjeve (mod 5). Prandaj, sipas formulës (10), kemi

$$-0(\text{mod } 5) = 0;$$
$$-1(\text{mod } 5) = 5-1=4;$$
$$-2(\text{mod } 5) = 5-2=3;$$
$$-3(\text{mod } 5) = 5-3=2;$$
$$-4(\text{mod } 5) = 5-4=1.$$

Po ashtu, nga kuptimi i shumëzimit $\otimes$, sipas (6), kemi

$$a^{-1}(mod\ 5) \otimes a = 1 \Rightarrow r_5[a^{-1}(mod\ 5) \cdot a]=1 \Rightarrow a^{-1}(mod\ 5) \cdot a = 5q+1.$$

Atëherë

$$1^{-1}(mod\ 5) \cdot 1 = 1 \Rightarrow 1^{-1}(mod\ 5)= 1;$$
$$2^{-1}(mod\ 5) \cdot 2 = 1 \Rightarrow 2^{-1}(mod\ 5)= 3, \text{ sepse } 3 \cdot 2 = 5 \cdot 1+1;$$
$$3^{-1}(mod\ 5) \cdot 3 = 1 \Rightarrow 3^{-1}(mod\ 5)= 2; \text{ sepse } 2 \cdot 3 = 5 \cdot 1 +1;$$
$$4^{-1}(mod\ 5) \cdot 4 = 1 \Rightarrow 4^{-1}(mod\ 5)= 4; \text{ sepse } 4 \cdot 4 = 5 \cdot 3 +1.$$

Rezultatet e mësipërme i marrim më lehtë, duke ndërtuar tabelat e mëposhtëme të veprimeve $\oplus$, $\otimes$, përkatësisht sipas barazimeve (5), (6), që për *n*=5 marrin pamjen $a \oplus b = r_5(a+b)$, $a \otimes b = r_5(a \cdot b)$ për $a,b \in \{0, 1, 2, 3, 4\}$.

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\otimes$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Tabela 1. (a) Tabela e veprimeve $\oplus$ *(b) Tabela e veprimeve $\otimes$*

Një fushë e rëndësishme për AES është fusha *GF*(2), e cila është fusha më e vogël e fundme mbasi elemente të saj janë 0 dhe 1. Tabelat e veprimeve (mod 2) për këtë fushë kanë pamjen

$\otimes$	0	1
0	0	0
1	0	1

Tabela 2. Tabela e veprimeve $\otimes$ për fushën GF(2)

$\oplus$	0	1
0	0	1
1	1	0

Tabela 3. Tabela e veprimeve $\oplus$ për fushën GF(2)

2.4 Njohuri plotësuese mbi numrat e plotë dhe disa algoritme bazike

2.4.1 Pmp dhe algoritmi i Euklidit për gjetjen e tij. Pjesëtuesi më i madh i përbashkët i dy numrave natyror *a, b* është shënuar *Pmp*(*a, b*). Ai mund të përcaktohet nëpërmjet zbërthimit në faktor të thjeshtë të këtyre numrave. Por kjo mënyrë për numra të plotë të mëdhenj është jo eficiente. Në këto raste është i dobishëm algoritmi i Euklidit i pjesëtimeve të njëmbasnjëshme, që paraqitet më poshtë. [2], [4]

Le të jenë *a* dhe *b* dy numra natyror që $a \geq b$. Aplikojmë formulën (3) të pjestimit në fillim të *a* me *b*, mandej të *b* me mbetjen r_1 të pjestimit të parë e kështu në mënyrë të njëmbasnjëshme si më poshtë:

$$\begin{aligned}
a &= bq_1 + r_1 && (0 \leq r_1 < b) \\
b &= r_1 q_2 + r_2 && (0 \leq r_2 < r_1) \\
r_1 &= r_2 q_3 + r_3 && (0 \leq r_3 < r_2) \\
r_2 &= r_3 q_4 + r_4 && (0 \leq r_4 < r_3) \\
&\ldots\ldots\ldots\ldots && \ldots\ldots\ldots\ldots \\
r_{k-2} &= r_{k-1} q_k + r_k && (0 \leq r_k < r_{k-1}) \\
r_{k-1} &= r_k q_{k+1}
\end{aligned} \qquad (20)$$

Mbetjet e këtyre pjestimeve vijnë duke u zvogëluar. Prandaj midis pjestimeve (20) ka një pjestim me mbetje zero. Veç kësaj, nga formula (3) del e qartë, që çdo pjestues i përbashkët i *a* e *b* është edhe pjestues i r_1, dhe çdo pjestues i përbashkët i *b* e r_1 është

edhe pjestues i *a*. Prandaj pjestuesit e përbashkët të *a* e *b* përputhen me pjestuesit e përbashkët të *b* e r_1, që sjell $Pmp(a, b)=Pmp(b, r_1)$. E kështu me rradhë, sipas (20) marrim:

$$Pmp(a,b) = Pmp(b,r_1) = Pmp(r_1,r_2) = ... = Pmp(r_{k-1},r_k) = r_k \neq 0. \qquad (21)$$

Kështu, *Pmp* (*a, b*) është mbetja e fundit e ndryshme nga zero në vargun e pjestimeve të paraqitura tek (20). Rezultatet e pjestimeve të mësipërme përmblidhet në një tabelë, në të cilën vargu i hersave është shkruar mbi atë të pjestuesëve, kurse vargu i mbetjeve poshtë tyre, për të bërë të mundur shkrimin e tyre njëri afër tjetrit. *Pmp* i kërkuar është mbetja e fundit e ndryshme nga zero.

***Shembull* 1.** Të llogarisim *Pmp* (*228, 126*).

Rezultatet e pjestimeve të njëmbasnjëshme i vendosim në tabelën e mëposhtme:

q	1	1	4	4
a=228	b=126	102	24	6
r	102	24	6	0

Tabela 4. Rezultatet e pjestimeve të njëmbasnjëshme

Pmp i kërkuar është mbetja e fundit e ndryshme nga zero, d.m.th. numri 6.

Përdorimi i këtij koncepti në algjebrën modulare ka shtrirje të gjerë. Formulojmë tani një pohim lidhur me të, që në njëfarë kuptimi plotëson tërësinë e formulave ($2'$).

Pohim 1. *Në qoftë se d =Pmp(c, n), atëherë*

$$ac \equiv bc(mod\ n) \Rightarrow a \equiv b(mod\ \frac{n}{d}).$$

Vërtetim. $ac \equiv bc$(mod n) do të thotë se $n|(a-b)c$**.**Ndërkaq, fakti që $d = Pmp(c, n)$ sjell $\frac{n}{d}|(a-b)\ \frac{c}{d}$ dhe $\frac{n}{d}$**,** $\frac{c}{d}$ janë të thjeshtë midis tyre. Për rrjedhojë $\frac{n}{d}|(a-b)$, që tregon se $a \equiv b$(mod $\frac{n}{d}$)**.**

Në rastin e veçantë, kur $Pmp(c, n) = 1$, pra d=1, ajo kongruencë merrë pamjen $a \equiv b$ (mod n). Përftohet kështu ky

Rrjedhim. *Në qoftë se Pmp*(c, n) =1, atëherë

$$ac \equiv bc(\text{mod } n) \Rightarrow a \equiv b(\text{mod } n).$$

Nga ky Rrjedhim dhe nga formulat ($2'$) mbi kongruencat numerike marrim këtë

Pohim 2. *Në qoftë se në një shprehje racionale që përmban vetëm numra të plotë, me koeficenta të plotë, zëvëndësohen numrat e plotë me numra të plotë kongruentë sipas të njëjtit modul n, atëherë fitohet një shprehje kongruente me të parën sipas modulit n.*

2.4.2 Algoritmi i zgjeruar i Euklidit për gjetjen e a^{-1}(*mod n*). Nga Rrjedhimi 1 i mësipërm, për një n të thjeshtë, për çdo $a \in Z_n^*$, ekziston i anasjellti (mod n) i tij, që jepet

nga formula $a^{-1}(\text{mod } n) = r_n(s)$, ku $Pmp\ (a, n)=sa+tn=1$. Për të gjetur numrin e plotë s (*së bashku me t*) shqyrtojmë algoritmin e Euklidit nga një këndvështrim tjetër. Më qenë se $1 \le a < n$ dhe $Pmp\ (a, n) = 1$, në vargun e barazimeve (21) hiqet termi i parë dhe i fundit, mbasi mbetja e fundit është 1. Veç kësaj, në vend të b vendosim n dhe në vend të r_1 vendosim a. Ai merrë pamjen

$$Pmp(n,a) = Pmp(r_1, r_2) = ... = Pmp(r_{k-1}, r_k) = 1. \qquad (22)$$

Në këto kushte proçesi i Euklidit (20) merrë pamjen

$$\begin{aligned}
&n = r_1 q_2 + r_2 && (0 \le r_2 < r_1 = a)\\
&r_1 = r_2 q_3 + r_3 && (0 \le r_3 < r_2)\\
&r_2 = r_3 q_4 + r_4 && (0 \le r_4 < r_3) \qquad 23)\\
&\ldots\ldots\ldots\ldots\ldots\ldots && \ldots\ldots\ldots\ldots\\
&r_{k-3} = r_{k-2} q_{k-1} + r_{k-1} && (0 \le r_{k-1} < r_{k-2})\\
&r_{k-2} = r_{k-1} q_k + r_k && (0 \le r_k < r_{k-1})\\
&r_k = 1
\end{aligned}$$

Nga barazimet, duke filluar nga i pari, gjejmë vargun zbritës të mbetjeve me anë zëvendësimesh të njëmbasnjëshme si më poshtë:

$r_1=a$;

$r_2=n - r_1q_2= -aq_2 + n$;

$r_3= r_1 - r_2q_3 =a -(-aq_2 + n)q_3 =(1+q_2\ q_3)a +(-q_3)n = s_3 \cdot a + t_3 \cdot n$;

$r_4= r_2 - r_3q_4 = (-aq_2 + n) -(s_3\ a + t_3\ n)q_4 = s_4 \cdot a + t_4 \cdot n$; (24)

……

$r_{k-1}= r_{k-3} - r_{k-2}q_{k-1} = s_{k-1} \cdot a + t_{k-1} \cdot n$;

$r_k = r_{k-2} - r_{k-1}\ q_k = s \cdot a + t \cdot n = 1 \quad \Rightarrow a^{-1}(mod\ n) = r_n(s)$.

Vlerat e herësave hap pas hapi gjenden, duke patur parasysh vargun zbritës të mbetjeve

$$0 \le 1 < r_{k-1} < r_{k-2} < r_{k-3} < ... < r_4 < r_3 < r_2 < r_1 = a\,. \qquad (25)$$

Algoritmi (24)-(25) quhet *algoritmi i zgjeruar i Euklidit* [4] për gjetjen e $a^{-1}(mod\ n)$**.** ***Shembull* 2**. Të gjendet $7^{-1}(\text{mod } 23)$ dhe $9^{-1}(\text{mod } 23)$.

Të anasjellët $7^{-1}(\text{mod } 23)$ dhe $9^{-1}(\text{mod } 23)$ ekzistojnë, sepse 23 është numër i thjeshtë. Për gjetjen e secilit përdorim algoritmin e zgjeruar të Euklidit (24)-(25).

Për $7^{-1}(\text{mod } 23)$ kemi n=23, a=7, prandaj:

r_1 =7;

r_2 =23-7 · 3=2;

$r_3 = r_1 - r_2q_3$ =7-2 · 3=1, nga ana tjetër r_3 =7-(23-7 · 3)3=10 · 7- 3 · 23 $\Rightarrow$ 10 · 7- 3 · 23=1 $\Rightarrow$ s=10 $\Rightarrow$

$7^{-1}(\text{mod } 23)=r_{23}(10)=10(\text{mod } 23)$.

Për $9^{-1}(\text{mod } 23)$ kemi n=23, a=9, prandaj

r_1 =9;

r_2 =23-9 · 2=5;

$r_3 = r_1 - r_2q_3$ =9-5 · 1=4, nga ana tjetër r_3 =9 - (23-9 · 2)=3 · 9 - 23 $\Rightarrow$ r_3 =3 · 9 - 23=4;

$r_4 = r_2 - r_3 q_4$ =5 - 4=1, nga ana tjetër r_4 =(23-9·2) - (3·9 - 23)= -5·9 + 2·23 $\Rightarrow$ -5·9 + 2·23=1 $\Rightarrow s$=-5 $\Rightarrow$ 9^{-1}(mod 23) = r_{23}(-5) = 18(mod 23).

2.4.3 Funksioni i Ejlerit. Funksionin e Ejlerit e kemi përmendur edhe në fund të pikës 2. Po japim këtu një trajtim më të hollësishëm të tij, të nevojshëm për shtjellimin e mëtejshëm të materialit.

***Përkufizim* 1**. *Funksion i Ejlerit quhet funksioni* ϕ*, që çdo numri të plotë pozitiv n i shoqëron numrin e numrave të plotë pozitivë që nuk e kapërcejnë n dhe janë të thjeshtë lidhur me numrin n.* [2], [3], [4]

Prej këndej kemi $\phi(1)=1, \phi(2)=1$, $\phi(3)=2$, $\phi(4)=2$, $\phi(5)=4$, …Është e qartë se, kur n është i thjeshtë, atëherë $\phi(n)=n-1$. Ndërkaq, për një numër të thjeshtë n dhe për një numër të plotë pozitiv m, numrat e plotë pozitivë që nuk e kapërcejnë n^m janë 1, 2,…, n^m. Nga këta nuk janë të thjeshtë lidhur me n^m shumëfishat e n: $1\cdot n$, $2\cdot n$,…, $n^{m-1}\cdot n$. Ngelen kështu të thjeshtë lidhur me n^m dhe që nuk e kapërcejnë atë sasia prej $n^m - n^{m-1} = n^{m-1}(n-1)$. Kemi vërtetuar në këtë mënyrë këtë

Pohim 3. *Në qoftë se p është i thjeshtë, për çdo numër të plotë pozitiv m kemi*

$$\phi(p^m) = p^{m-1}(p-1).$$

Provohet gjithashtu se [3], [4] *në qoftë se n është numër i përbërë me zbërthim në faktorë të thjeshtë* $p_1, p_2, \ldots, p_s$ *në trajtën* $n = p_1^{m_1}\cdot p_2^{m_2}\cdots p_s^{m_s}$ *,atëherë*

$$\phi(n) = p_1^{m_1-1}(p_1-1)\; p_2^{m_2-1}(p_2-1)\cdots p_s^{m_s-1}(p_s-1). \qquad (26)$$

Rastet më të rëndësishme për vlerën e $\phi(n)$, sipas (26), në kriptografi janë:

(1) (p i thjeshtë) $\Rightarrow \phi(p)=p-1$;

(2) (p, q janë të thjeshtë dhe $p\neq q$) $\Rightarrow \phi(p\cdot q)=(p-1)(q-1)$.

Me interes janë dhe këto dy teorema.

Teoremë 1. ***(Teorema e Ejlerit).*** [3] *Nqs n është një numër i plotë pozitiv dhe nqs a është një numër i plotë i thjeshtë me n, atëherë*

$$a^{\phi(n)} = 1(\mathrm{mod}\, n) \qquad (27)$$

Rast i veçantë i Teoremës së Ejlerit është teorema e mëposhtme, që njihet si Teorema e Fermait, e cila merret prej saj, duke zëvendësuar n me një numër të thjeshtë p.

Teoremë 2. [3] *Nqs a është një numër i plotë i papjestueshëm nga një numër i thjeshtë p, atëherë kemi*

$$a^{p-1} = 1(\mathrm{mod}\, p). \qquad (28)$$

2.4.4 Ekuacionet *(mod n)* të gradës së parë me një ndryshor. Jepen dy polinome $P(x)$ dhe $Q(x)$ të ndryshorit x me koeficenta numra të plotë. Kërkohet të përcaktohen vlerat e plota të x-it (nëse ekzistojnë), për të cilat vlerat përkatëse të polinomeve rezultojnë kongruente (mod n), d.m.th. të tilla që

$$P(x) \equiv Q(x) (\mathrm{mod}\, n) \tag{29}$$

Një kongruencë të tillë e quajmë *ekuacion modular*, mbasi ka shumë ngjashmëri me atë të një ekuacioni të zakonshëm. Në qoftë se *k* është një zgjidhje e një kongruence me një ndryshor, cilido numër i plotë kongruent me *k* (mod *n*), d.m.th. i formës *k+hn* , ku *h* është një numër i plotë i çfarëdoshëm, në bazë të Pohimit 2, është gjithashtu zgjidhje e kongruencës. Ajo nuk konsiderohet e ndryshme nga *k*, prandaj përcaktimi i zgjidhjeve të një kongruence (mod *n*) kufizohet përgjithësisht tek ato zgjidhje që i përkasin
$Z_n = \{0, 1, 2, \ldots, n\text{-}1\}$. Natyrisht numri i zgjidhjeve të një ekuacioni (mod *n*) nuk mund ta kalojë *n*. Dy ekuacione (mod *n*) që kanë të njëjtat bashkësi zgjidhjesh quhen *të njëvlefshme*. Veç kësaj, si për ekuacionet e zakonshme, tek një kongruencë me një ndryshor mund të zbatojmë vetinë e kalimit të kufizave nga njëra anë tek tjetra, duke përftuar përsëri një kongruencë të njëvlershme. Kështu p.sh. (29) është ekuivalent me ekuacionin modular $P(x) - Q(x) \equiv 0 (\mathrm{mod}\, n)$.

Ekuacionet modulare të gradës së parë me një ndryshor paraqiten në formën

$$ax = b (\mathrm{mod}\, n), \tag{30}$$

ku *a* dhe *b* janë numra të plotë. Për gjetjen e zgjidhjeve të (30) në Z_n ndihmon ky

Pohim 4. *Në qoftë se a është një numër i plotë dhe i thjeshtë me n, atëherë ekuacioni* (30) *është ekuivalent me ekuacionin*

$$x = ba^{\phi(n)-1} (\mathrm{mod}\, n) \tag{31}$$

dhe prandaj ka vetëm një zgjidhje pikërisht mbetjen (mod *n*) *të kufizës në anën e djathtë të* (31).

Vërtetim. Me qenë se *Pmp* (*a, n*) =1, sipas Teoremës së Ejlerit, kemi $a^{\phi(n)} = 1 (\mathrm{mod}\, n)$, që duke shumëzuar të dy anët me *b* sjell $ba^{\phi(n)} = b (\mathrm{mod}\, n)$. Prej saj, duke patur parasysh (30), marrim
$ax = ba^{\phi(n)} (\mathrm{mod}\, n)$. Nga Rrjedhimi i Pohimit 1, kjo sjell (31). Mbetja (mod *n*) e kufizës në anën e djathtë (31) është kështu e vetmja rrënjë e (30).

Pohim 5. [3] *Në qoftë se a është një numër i plotë dhe jo i thjeshtë me n, d. m. th. Pmp* (*a, n*) = *d* ≠ 1, *atëherë ekuacioni* (30) *ka zgjidhje vetëm kur d është një pjestues i b. Në këtë rast ai ka d zgjidhje, që janë*

$$k, k + \frac{n}{d}, k + 2\frac{n}{d}, \cdots, k + (d-1)\frac{n}{d} \tag{32}$$

ku k është zgjidhja e kongruencës

$$\frac{a}{d} x = \frac{b}{d} (\mathrm{mod}\, \frac{n}{d}) \tag{33}$$

Nga dy pohimet e mësipërme, për të zgjidhur ekuacionin modular (30), fillimisht llogarisim *Pmp*(*a, n*), lidhur me të cilin, dallojmë këto raste [4]:

Rasti 1. Në qoftë se *Pmp* (*a, n*) = 1, ekuacioni (mod *n*) (30) ka vetëm një zgjidhje, e cila gjendet si më poshtë: përcaktojmë në fillim një numër natyror *c* të tillë që *a*·*c* = 1 (mod

n). Pastaj, sipas vetisë 3 tek formulat ($2'$), shumëzojmë të dy anët e kësaj kongruence me b, duke përftuar $a\cdot(c\cdot b) = b \pmod n$, që tregon se zgjidhja e kërkuar është $x=cb \pmod n$.

Rasti 2. Në qoftë se *Pmp* (a, n) = $d \neq 1$ dhe d është pjestues i b, ekuacioni (mod n) (30) ka *d zgjidhje*, të cilat gjendet si më poshtë: përcaktojmë në fillim zgjidhjen e vetme $x=k$ të ekuacionit modular (33) si në Rastin 1, e cila është zgjidhje edhe e (30). Pastaj, sipas formulës

$$k+i\frac{n}{d},\ i\in\{1,2,...,(d-1)\},$$

gjejmë edhe d-1 zgjidhjet e tjera të ekuacionit (mod n) (30).

Rasti 3. Në qoftë se *Pmp* (a, n) = $d \neq 1$ dhe d nuk është pjestues i b, ekuacioni (mod n) (30) nuk ka zgjidhje.

2.4.5 Problemi kinez i mbetjeve. Në këtë paragraf shqyrtojmë një sistem ekuacionesh lineare modulare të tipit

$$a_k x = b_k \pmod{n_k} \ \text{ per } k=1,2,\cdots,m\ , \qquad (34)$$

ku a_k dhe b_k janë numra të plotë. *Zgjidhje* të sistemit (34) quhen zgjidhjet e përbashkëta të m ekuacioneve të sistemit. Problemi i gjetjes së zgjidhjeve të mundshme në numra të plotë të një sistemi linear (34) është zgjidhur për herë të parë nga matematicientë kinez rreth shekullit të parë para Krishtit. Për këtë arsye ky problem njihet si *problemi kinez i mbetjes*. Ne do ta hasim këtë problem në disa vende, si në përmirësimin e operacionit të dekriptimit të RSA dhe në një numër protokolesh tjera.

Do të mjaftohemi këtu me zgjidhjen e sistemit të ekuacioneve lineare modulare të tipit të vecantë

$$x = b_k \pmod{n_k} \ \text{ per } k=1,2,\cdots,m \qquad (35)$$

ku modulet n_k janë dy nga dy të thjeshtë. Ka vend kjo

Teoremë 3. (Teorema kineze e mbetjes). *Le të jenë* n_k (k=1, 2,…, m) *numra të plotë pozitiv të thjeshtë dy nga dy, dhe le të jenë gjithashtu* b_k (k=1, 2, …, m) *numra të plotë.* [3] *Le të kemi gjithashtu*

$$N = n_1\cdot n_2\cdots n_m,\ N_k=\frac{N}{n_k}\ \text{ per } k=1,2,\cdots,m.$$

Atëherë sistemi (35) *ka zgjidhje, dhe një zgjidhje është*

$$c=\sum_{k=1}^{m} b_k N_k y_k\ ,\ \textit{ku}\quad y_k\ \textit{është rrënja e kongruencë}\ N_k y = 1 \pmod{n_k}\ \text{ per } k=1,2,\cdots,m.$$

Zgjidhje të tjera të sistemit janë edhe kongruentet me c(*mod N*).

***Shembull* 3.** Të zgjidhet sistemi

$$\begin{cases} x = 4 \pmod 7; \\ x = 3 \pmod 5. \end{cases}$$

Vemë re se n_1 =7, n_2 =5, k=1, 2; *Pmp* (7, 5)=1, N=7 · 5=35, N_1=5, N_2=7. Gjejmë zgjidhjen y_1=3 nga ekuacioni modular 5y = 1(mod 7) dhe zgjidhjen y_2=3 nga ekuacioni modular 7y = 1(mod 5). Atëherë një zgjidhje e sistemit do të jetë

$$c = b_1N_1y_1 + b_2N_2y_2 = 4\cdot 5\cdot 3 + 3\cdot 7\cdot 3 = 60 + 63 = 123 = 18(\mathrm{mod}\,35)\ .$$

Atëherë x=18(mod 35) është zgjidhja e vetme e sistemit në Z_{35}.

***Shembull* 4.** Të zgjidhet sistemi

$$\begin{cases} x = 1(\mathrm{mod}\,2); \\ x = 2(\mathrm{mod}\,3); \\ x = 4(\mathrm{mod}\,5). \end{cases}$$

Këtu, n_1=2, n_2=3, n_3=5, k=1, 2, 3; *Pmp*(2, 3)=1, *Pmp*(2, 5)=1, *Pmp*(3, 5)=1, N=2 · 3 · 5=30, N_1=15, N_2=10, N_3=6. Gjejmë zgjidhjen y_1=1 nga ekuacioni modular 15y = 1(mod 2) dhe zgjidhjen y_2=1 nga ekuacioni modular 10y = 1(mod 3), zgjidhjen y_3=1 nga ekuacioni modular 6y = 1(mod 5). Atëherë një zgjidhje e sistemit do të jetë

$$c = b_1N_1y_1 + b_2N_2y_2 + b_3N_3y_3 = 1\cdot 15\cdot 1 + 2\cdot 10\cdot 1 + 4\cdot 6\cdot 1 = 59 = 29(\mathrm{mod}\,30)\ .$$

Atëherë x=29(mod 30) është zgjidhja e vetme e sistemit në Z_{30}.

3 KRIPTOGRAFIA ME ÇELËS PUBLIK

3.1 Hyrje në Kriptografi

Kriptografia (nga greqishtja kriptos - i fshehtë, dhe grafia - shkrim) është shkenca e kodimit dhe e përçimit të informacioneve dhe të dhënave të fshehta (sekrete). Qëllimi kryesor i kriptografisë është fshehja e kuptimit të mesazheve, por zakonisht jo ekzistencës së tyre. Kriptografia përkufizohet sipas kriptografit të njohur Ron Rivest si "komunikimi në prani të kundërshtarëve". Ajo është pjesë qëndrore e disa fushave: sigurimit të informacioneve dhe çështjeve përkatëse, veçanërisht identifikimit dhe kontrollit hyrës. Kriptografia luan një rol të rëndësishëm edhe në informatikë, veçanërisht në teknikat e përdorura në sigurinë kompjuterike dhe rrjeteve, si p.sh. kontrolli hyrës apo të së drejtës së përdorimit të një aparati kompjuterik dhe besueshmërisë së informacioneve. Kriptografia përdoret gjithashtu në shumë zbatime që ndeshen në jetën e përditshme, si fjalëkalimet kompjuterike, kartelat bankare dhe tregëtinë elektronike.
Kriptografia së bashku me kriptoanalizën formojnë kriptologjinë.

Kriptografia ndryshe është dega që studion mënyrën e fshehjes së mesazheve, domethënë konvertimi i një teksti në një varg simbolesh të pakuptueshme. Një proces kriptografik përdor një cipher, i cili është një çift algoritmesh, të cilat krijojnë enkriptimin dhe të kundërtën: dekriptimin. Gjithashtu, i domosdoshëm është një parametër sekret, i cili quhet çelës dhe zotërohet vetëm nga shkëmbyesit e informacionit. Në ditët e sotme, kriptografia përdoret në shumicën e fushave kompjuterike dhe atyre elektronike, sidomos në aspektet e sigurisë bankare, transmetimit të informacioneve (e-mailet) etj.

Kriptografia moderne bazohet në fuqinë e madhe llogaritëse kompjuterike, në prezantimin binar të informacionit dhe në algoritme shumë të fuqishme që mund të procesohen vetëm nga kompjuterët. Kriptografia, nga ana strukturore mund të ndahet në kriptografi me çelësa simetrike dhe me çelësa asimetrike. Kriptografia simetrike përdor të njëjtin çelës për të enkriptuar dhe dekriptuar mesazhin. Në këtë rast marrësi duhet të zotërojë këtë çelës për të lexuar mesazhin. Kriptografia asimetrike përdor dy çelësa, të cilët lidhen me njëri tjetrin me relacione matematikore. Njëri prej tyre është privat dhe përdoret nga nënshkruesi për të enkriptuar dokumentin, tjetri është publik dhe përdoret vetëm për të lexuar (dekriptuar) dokumentin.

Historia e mesazheve të koduara

"Zgjuarsia njerëzore nuk mund të sajoj asnjë kod që zgjuarësia njerëzore nuk mund ta zgjidh", Edgar Allen Poe**.**

Akti i krijimit të një mesazhi sekret ka ekzistuar ndoshta që prej kohës kur njerëzit filluan të komunikonin. Kodet sekrete janë përdorur gjatë luftërave, në biznes dhe në

marrëdhënie personale për të kamufluar gjithçka, që nga planet e luftës tek komplotet e vrasjeve, që nga marrëveshjet e dyshimta tek dashuritë e ndaluara.

Procesi i thyerjes së këtyre kodeve i ka shkaktuar dhimbje koke zyrtarëve të inteligjencës dhe kriptologjistëve përgjatë gjithë historisë, duke u përpjekur t'i zgjidhin ato. Personi që krijon një kod mund të mendoj se është i pathyeshëm, por faktet kanë treguar që edhe sistemet e kodeve më komplekse kanë arritur në fakt të dekriptohen, duke ndryshuar kursin e historisë së njerëzimit gjatë këtij procesi. Këto janë disa nga kodet më të komplikuara që ka njohur historia.

Kriptografia është shkenca për shkrim sekret me qëllim të fshehjes së kuptimit të mesazhit. Kriptografia është përdorur te:

- Kodi i Cezarit,
- Cilindri i Jeffersonit (shek.XVIII),
- Enigma në Gjermani (gjatë luftës së dytë botërore),
- Kriptimi i Hillit, e kështu me radhë.

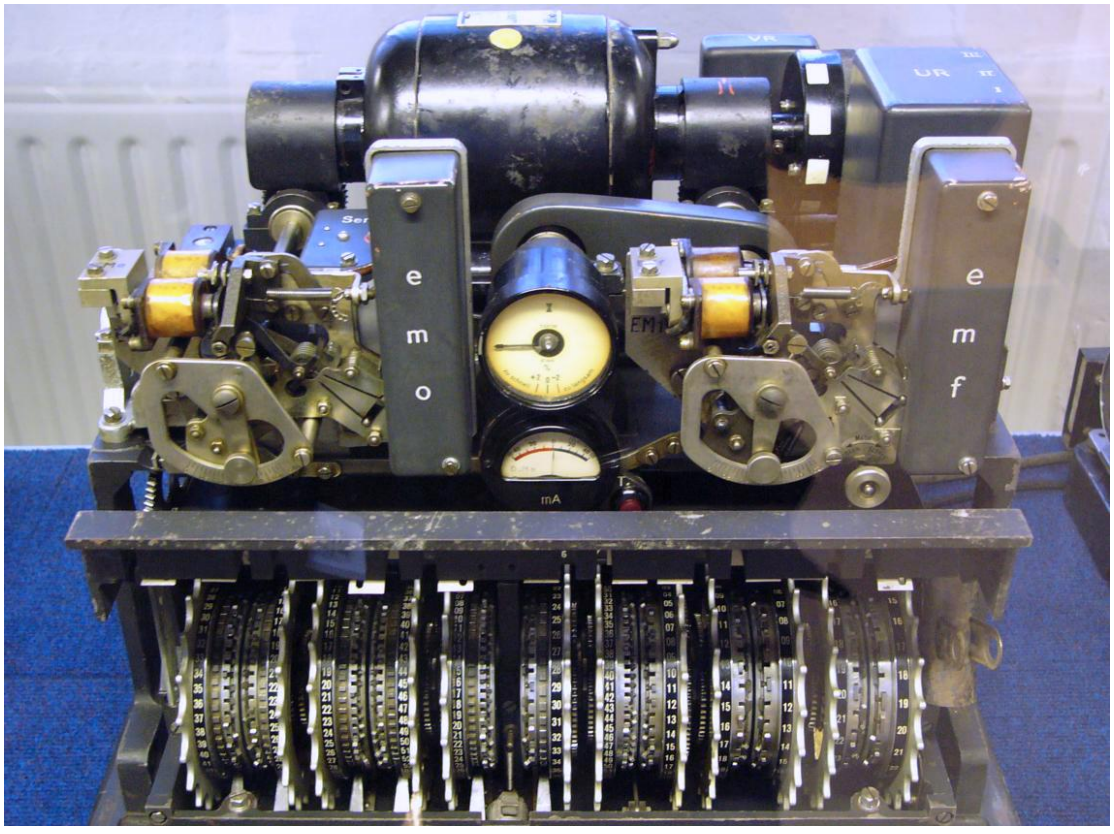


Figura.1: Makina e enkriptimit gjermane "Lorenc" e përdorur në Luftën e Dytë Botërore për dekriptimin e mesazheve tepër sekrete [72]

Pra në përgjithësi kriptografia është përdorur gjatë luftrave për qëllime ushtarake. Megjithatë, shumë shtete kanë kufizime në export/import të teknologjive të bazuara në kriptografi. *Kriptoanaliza* është shkencë dhe ndonjëherë art i thyerjes së sistemit kriptografik. Ndonjëherë mendohet se thyerja e kodit është për të zhvilluar logjikën apo

edhe për krimin e organizuar, dhe që nuk mund të jetë çështje serioze për shkencë disiplinore. Pra, kriptoanaliza është shkencë për analizën e informacionit së enkriptuar pa përdorimin e çelësit përkatës. *Kriptologjia* është shprehje e përbashkët për kriptografinë dhe kriptoanalizën. Kur themi se kemi bërë kodimin e mesazhit atëherë ky proces quhet *enkriptim*, kurse procesi i kundërt quhet *dekriptim*. Teksti apo mesazhi i qartë (para enkriptimit) quhet *plaintext*, kurse ai i enkriptuar quhet *ciphertext*. Në gjuhët programuese përdoren algoritme të ndryshme për fshehje të mesazhit.

Kodi i Cezarit

Kodi i Cezarit në fakt ka qenë një nga kodet më të lehta për t'u thyer. Ai përdorej nga Jul Cezari kurdo që dëshironte të dërgonte një mesazh sekret rreth planeve të tij ushtarake. Në realitet, nuk duhet të ishte një kod shumë kompleks në atë kohë, duke qenë se shumica e njerëzve nuk dinin as të lexonin, por megjithatë ai ndjente se kishte nevojë të tregohej i kujdesshëm.

Kodi i Cezarit është një sistem i thjeshtë, ku çdo shkronjë e alfabetit zhvendoset me tre vende (në vend të B-së përdoret D-ja), në mënyrë që të kamufloheshin fjalët që do të përmbante mesazhi. Marrësi, i cili natyrisht e njihte sistemin e kodimit, duhej vetëm të rizhvendoste çdo shkronjë përsëri tre shkronja para për të lexuar mesazhin. Kodi i Cezarit, ose siç njihet ndryshe Zhvendosja e Cezarit, është përdorur që në atë kohë e deri sot për të përshkruar çdo lloj kodi që ka të bëjë me zhvendosjen e shkronjave të alfabetit.

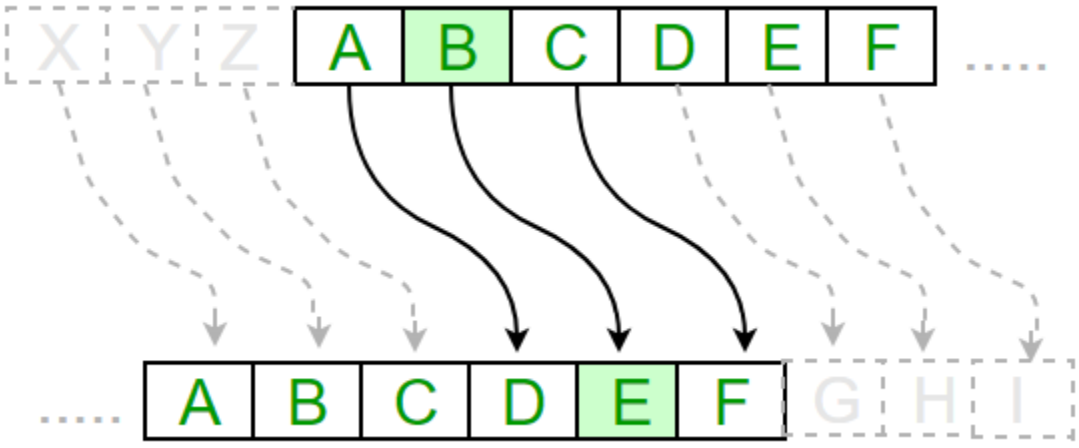


Figura 2. Zhvendosja e Cezarit [73]

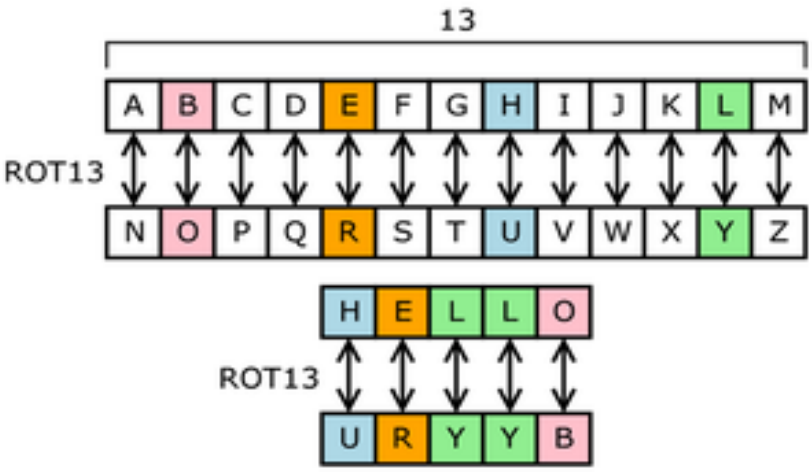


Figura 3. Shembull të përdorimit të mesazhit të enkriptuar [74]

Sistemi Kriptografik

Mënyra më e zakonshme për të përshkruar sistemin kriptografik është që të supozohet se një person (zakonisht i emruar si Alica) dëshiron që t'i dërgoj mesazh një personi tjetër (Bobi). Megjithatë, personi i tretë (Eva) është përcaktuar si përgjues në komunikimin e tyre. Në figurën e mëposhtme është paraqitur relacioni ndërmjet tyre.

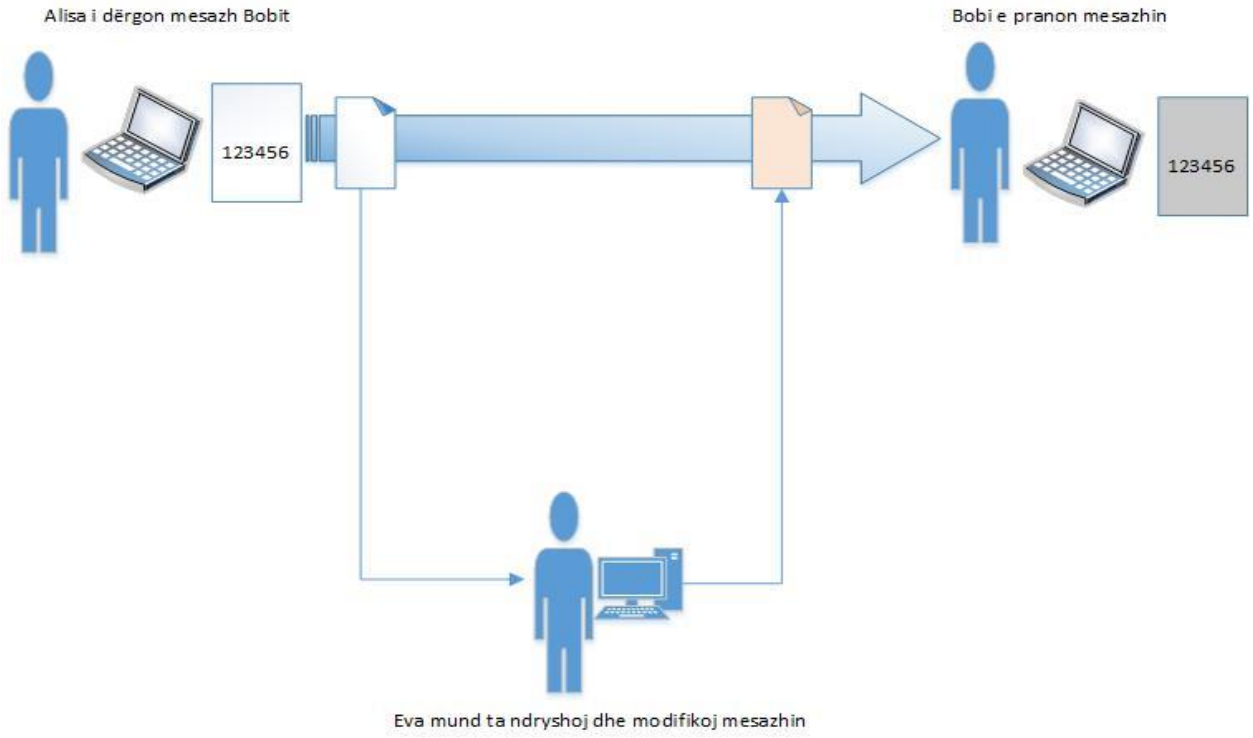


Figura 4: Përshkrimi sistemit të kriptografisë përmes ilustrimit figurativ

Kriptografia ka një histori të gjatë dhe teknika të ndryshme për mbrojtjen e mesazheve të cilat janë përdorur për mijëra vjetë. Gjatë shumicës së kohës emrat Alica (ang.Alice), Bobi (ang.Bob) dhe Eva (ang.Eve) kanë paraqitur njerëzit real apo organizatat. Në shumë raste gjithashtu këta emra janë përdorur edhe si metafora për kompjuterë, andaj edhe gjatë këtij diskutimi do të përdoren të njëjtit. Me gjithë zhvillimin e teknologjisë, kriptografia si proces është bërë i pakthyeshëm në botën e kompjuterëve. Kompjuterët në masë të madhe kanë lehtësuar teknikat e kriptografisë, por në të njëjtën kohë kanë lejuar njerëzit si Eva të rrisin sulmet në kriptografi. Kur thuhet se "Alisa i dërgon mesazh Bobit", nuk konsiderohen detajet se si ajo e bënë këtë.
P.sh. ajo mund ta përdorë emalin që ta kompozoj dhe dërgoj mesazhin, ose ajo mund ta ketë shkruar një aplikacion i cili automatikisht do të komunikoj me bankën e saj për të bërë ndonjë pagesë, apo mënyra tjera të komunikimit.

Llojet e Kriptografisë

Ekzistojnë dy lloje të kriptografisë:

1. Kriptografia me çelës të fshehur, përdor vetëm një çelës. Me anë të këtij çelësi, mesazhi i dhënë në formë të lexueshme do të enkriptohet në mesazh të pakuptueshëm me gjatësi të përafërt sa edhe i lexueshmi. Në rastin e dekriptimit, përdoret i njëjti çelës që është përdorur për enkriptim. Nganjëherë, kriptografia me çelës të fshehur quhet edhe kriptografi tradicionale apo simetrike. Kodi Captain Midnight dhe Monoalphabetic paraqesin dy lloje të algoritmeve të çelësit të fshehur, edhe pse tashmë për të dy ekzistojnë dëshmi se thyhen lehtë. Shembuj të kriptografisë me çelës të fshehur janë: DES, Triple DES apo 3DES, International Data Encryption Algorithm (IDEA) dhe AES.

2. Kriptografia me çelës publik apo kriptografia asimetrike, është një disiplinë e re e shpikur më 1975. Për dallim nga kriptografia me çelës të fshehur, në kriptografinë me çelës publik çelësat nuk ndahen. Këtu, secili individ ka dy çelësa: çelësi privat, që nuk duhet t'i zbulohet askujt dhe çelësi publik, që preferohet të jetë i ditur për secilin. Dallim tjetër i kriptografisë me çelës publik është edhe mundësia e gjenerimit të nënshkrimit digjital në mesazh. Nënshkrimi digjital është një numër i lidhur me mesazhin, që gjenerohet vetëm nga individi që ka çelësin privat. Shembuj të kriptografisë me çelës publik janë: RSA, DSA, ElGamal, Diffie-Hellman, Zero Knowledge Proof Systems, Pretty Good Privacy (PGP) dhe Elliptic Curve Cryptography (ECC).

Gjëja e parë që vërejmë është se termi më i përgjithshëm është kriptologjia dhe jo kriptografia. Kriptologjia ndahet në dy degë kryesore:

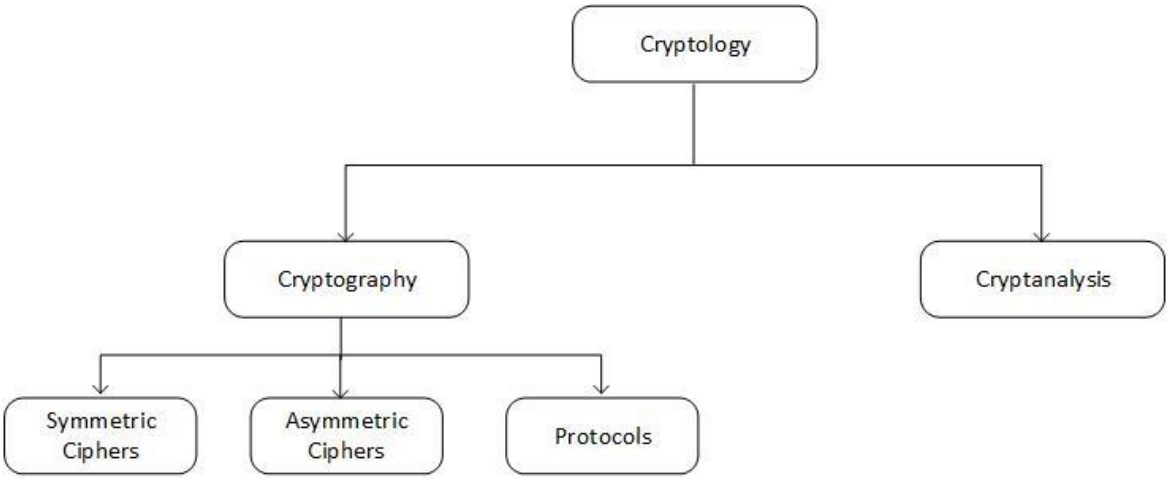


Figura 5: Përshkrimi sistemit të kriptografisë përmes ilustrimit figurativ

Kriptografia është shkenca e shkrimit sekret me qëllim të fshehjes së kuptimit të një mesazhi.

Kriptoanaliza është shkenca dhe ndonjëherë arti i thyerjes së sistemeve kriptografike. Mund të mendoni se thyerja e kodeve është për komunitetin e inteligjencës ose krimin e organizuar dhe nuk duhet të përfshihet në një klasifikim serioz të një disipline shkencore. Megjithatë, shumica e kriptoanalizës bëhet nga studiues të respektuar në akademi në ditët e sotme. Kriptoanaliza është me rëndësi qëndrore për sistemet kriptografike moderne: pa njerëz që përpiqen të thyejnë metodat kriptografike, ne kurrë nuk do të dimë nëse ato janë me të vërtetë të sigurta apo jo. Kriptografia vetë ndahet në tri degë kryesore: Kriptografia me çelës publik, Kriptografia me çelës privat dhe protokolet kriptografike.

Protokolet kriptografike Afërsisht, protokolet kriptografike merren me aplikimin e algoritmeve kriptografike. Algoritmet simetrike dhe asimetrike mund të shihen si blloqe ndërtimi me të cilat mund të realizohen aplikacione të tilla si komunikimi i sigurt në internet. Skema e Sigurisë së Shtresave të Transportit (TLS), e cila përdoret në çdo shfletues web, është një shembull i një protokoli kriptografik.

3.2 Kriptografia me Çelës Publik

Infrastruktura e Çelësit Publik (PKI)

Infrastruktura e Çelësit Publik (PKI) është një grup i përbërë nga hardueri, softueri, njerëzit, politikat dhe procedurat e nevojshme për të krijuar, menaxhuar, shpërndarë, përdorur, ruajtur, dhe për të revokuar certifikatat digjitale.

Në kriptografi, një PKI është një marrëveshje që lidhë çelësat publik me identitetet përkatëse të përdoruesit me anë të autoritetit certifikues (CA). Identiteti i përdoruesit duhet të jetë unik brenda çdo sfere të autoritetit certifikues (CA). Autoriteti i palës së tretë (VA) mund të siguroj këtë informacion në emër të autoritetit certifikues (CA).

Roli i PKI-së është që të siguroj këtë lidhje që njihet si Autoriteti i Regjistrimit (RA), i cili siguron se çelësi publik është i përcaktuar për personin dhe duhet të siguroj pamohueshmërinë.

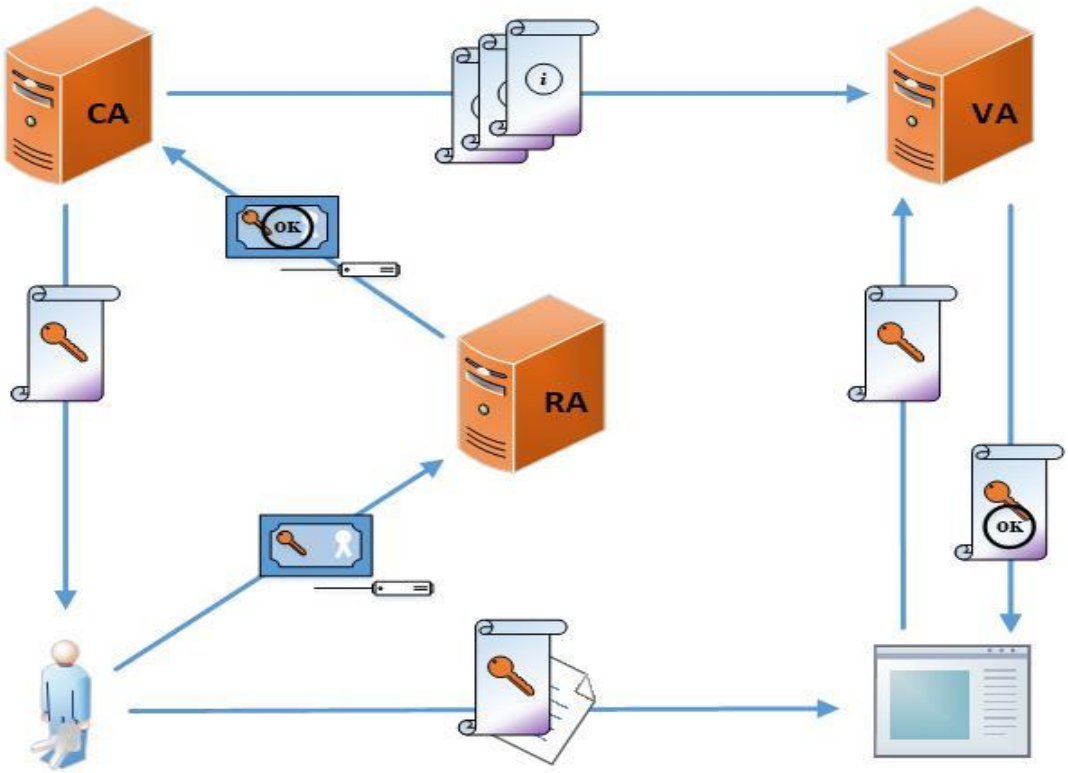


Figura 6: Infrastruktura e Çelësit Publik [7]

Tri PKI të ndryshme janë të nevojshme për inspektim:

- PKI e nënshkruar nga shteti për autentifikim pasiv
- PKI e verfikuar nga shteti për Terminal Authentication
- PKI për sigurinë e komunikimit

PKI e nënshkruar nga shteti për autentikim pasiv

Mekanizmi i autentikimit pasiv (PA) është përdorur në procedurën e inspektimit të një e-MRTD për të verifikuar integritetin dhe vërtetësinë e informacionit në çipin e-MRTD. Për të kryer autentikimin pasiv (PA), një sistem i inspektimit (IS) ka nevojë për certifikatën e shtetit lëshues.

Hierarkia e nënshkrimit nga shteti i PKI përbëhet nga nënshkrimi i certifikatës së autoritetit të shtetit (CSCA) dhe nga një ose më shumë nënshkrime të dokumentit (DS). CSCA dhe DS janë nën përgjegjësinë e autoritetit lëshues. Çelësat e nënshkrimit të dokumentit (DS) përdoren për një kohë të kufizuar dhe ndonjëherë edhe për një numër të

kufizuar të dokumenteve. ICAO rekomandon që koha maksimale e përdorimit të çelësave DS të jetë tre muaj. Disa vende e ndryshojnë çelësin e nënshkrimit pas një numri të caktuar të dokumenteve të lëshuara edhe nëse nuk ka kaluar periudha prej tre muajve. Certifikatat DS janë të vlefshme për kohën që përdoren palët e çelësave që zakonisht janë pesë ose dhjetë vjet plus dhe periudhën për të cilën çelësat DS janë të vlefshëm, pra certifikata DS mund të jetë e vlefshme për një periudhë prej dhjetë vjet e tre muaj.

PKI e verfikuar nga shteti për Terminal Authentication

Mekanizmi i authentifikimit në terminal është përdorur gjatë procedurës së inspektimit, e cila siguron qasjen e sigurt në të dhënat shtesë biometrike të e-MRTD dhe zhvillohet gjatë Extended Access Control (EAC). Për të performuar TA, një IS ka nevojë për një palë të çelësave publik-privat, dhe një zinxhir të certifikatave të çelësave publik që mund të verifikohen nga chipi e-MRTD.

Hierarkia e verifikimit të PKI nga një shtet përbëhet nga procedura e nënshkrimit të certifikatës nga autoritetet e shtetit (CSCA), një ose më shumë autoritete të verifikimit të certifikatave të dokumenteve (DVCA) dhe sistemit të inspektimit (IS). Verifikimi PKI është përgjegjësi e autoriteteteve të verifikimit. Për të marrë qasje në të dhënat shtesë biometrike qofshin eMRTD kombëtare ose të huaja, sistemi i inspektimit (IS) kërkon çelësat dhe kërkon që të kërkohen certifikatat me çelësat me DVCA kombëtare.

Për të siguruar qasjen në të dhënat shtesë biometrike në eMRTD kombëtare, sistemi i inspektimit (IS) duhet të kërkoj një certifikatë nga CVCA kombëtare. Njësoj, nëse sistemi i inspektimit (IS) kërkon qasjen në eMRTD të huaj, ai duhet të kërkoj një certifikatë nga CVCA e shtetit përkatës.

PKI për sigurinë e komunikimit

Për të shkëmbyer certifikatat dhe kërkesat e certifikatave me vendet e tjera është e nevojshme një pikë e vetme kontakti (SPOC). SPOC është krijuar si standard nga Bashkimi Europian me qëllim të leximit dhe këmbimit të certifikatave në mes shteteve për Kontroll të Zgjeruar të Qasjes (EAC).

Për të siguruar komunikimin midis SPOC-ve është përdorur HTTPS (TLS). TLS (Transport Layer Security) është protokol i dizajnuar për të mbrojtur sigurinë e komunikimit në internet.

Një PKI e autoritetit të palës së tretë është e nevojshme për të përdorur mekanizmin HTTPS.

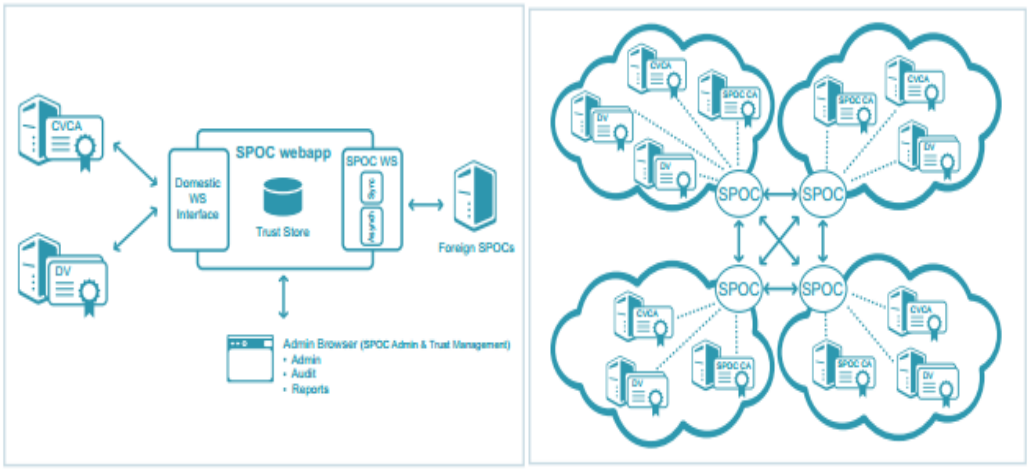


Figura 7: (a) Arkitektura SPOC (b) Arkitektura SPOC në mes shteteve [8]

3.3 RSA

RSA është një algoritëm me çelës publik dhe është i bazuar në vështirësinë e faktorizimit të numrave të thjeshtë [9]. U publikua nga Ron Rivest, Adi Shamir dhe Leonard Adleman në vitin 1977.

RSA përdoret gjerësisht në fushën e sigurisë kibernetike, për enkriptim dhe dekriptim ashtu si dhe për të nënshkruar dhe verifikuar. Përmban një palë të çelësave që njihen si çelësi pubik dhe çelësi privat. Një çelësit privat i përgjigjet vetëm një çelës publik dhe anasjelltas.

Shpërndarja e çelësave publik është njëra ndër shqetësimet kryesore të algoritmeve me çelës publik. Ekzistojnë disa teknika për shpërndarjen e çelësave publik [10], të dhëna si në vijim:

- Shpallja publike
- Direktoriumi publik në dispozicion
- Autoriteti për çelësin publik

Tek algoritmi i enkriptimit RSA, secili pjesëmarrës çelësin publik të tij mund ta shkëmbej me një numër të madh të pjesëmarrësve tjerë. Gjithashtu shumë përdorues të algoritmit të enkriptimit RSA kanë adoptuar praktikën e bashkëngjitjes së çelësit të tyre publik në mesazhet që i dërgojnë ata në formë publike si Usenet [10].

Mirëpo kjo metodë shumë lehtë mund të jetë synim i falsifikimeve ku një person që supozon që është për shembull pala A mundet ta shpërndaj çelësin e vet publik te të gjithë pjesëmarrësit dhe mund ti lexoj të gjitha mesazhet e dërguara për palën A. Kurse metoda përmes direktoriumit të qasshëm publikisht, ofron një siguri më të madhe pasi që secili pjesëmarrës e regjistron çelësin e tij publik në një autoritet të caktuar, i cili e siguron autentikimin e atij personi [10].

Kurse siguria edhe më e lartë nga ana e shpërndarjes së çelësit publik bëhet përmes autoritetit për çelës publik. Tek kjo metodë e shpërndarjes së çelësave, të gjithë çelësat e

pjesëmarrësve vendosen tek një autoritet i cili pranon kërkesa nga pjesëmarrësit e tjerë për çelësat publik të atyre me të cilët dëshirojnë të komunikojnë [10].

Përgjigjja e kërkesës që e bëjnë pjesëmarrësit enkriptohet me çelësin privat të autoritetit dhe kur personi që e bënë kërkesën e dekripton mesazhin ai është si sigurt që mesazhi që ai ka në dispozicion është nga autoriteti i caktuar. Në mesazhin që ai e dekripton ai fiton çelësin publik të personit me të cilin dëshiron të komunikoj në mënyrë të sigurt dhe fillon komunikimin me të [10].

Puna e algoritmit RSA [9]:

1. Zgjedhim dy numrat të thjeshtë *p* dhe *q*, prej tyre krijohet $n=p*q$ *(1)***.**

2. Le te jetë P_i një bllok i tekstit për enkriptim, P_i është numër ekuivalent me mesazhin për sa plotësohet $(p-1)(q-1)=\phi(n)$ (*2*).

3. Zgjedhim numrin rastësishëm *e* (zakonisht me shkronja të vogla) i tillë që *e* të jetë relativisht thjeshtë me $\phi(n)$, pra duhet të vlejë PMVP $(e, \phi(n)) =1$(3). Teksti i enkriptuar llogaritet si më poshtë.

$$C_i = P_i^e \bmod(n) \ (4)$$

Vlerat (*n, e*) përbëjnë çelësin publik [10]. Për të dekriptuar mesazhin ne kemi nevojë për një eksponent *d* i cili është i njohur vetëm nga personi që e deshifron mesazhin. Për ta bërë këtë na nevojitet teorema e Eulerit $e^{(\emptyset(n))} \equiv 1 \bmod(\emptyset(n))$. Përmes algoritmit të Euklidit bëhet e mundur gjetja e çelësit privat *d* e cila do të mundësoj dekriptimin e mesazhit [9]. Pjesa private *d* do të mund të llogaritet vetëm nëse njihen vlerat e numrave të thjeshtë *p* dhe *q*. Sulmuesi për ta bërë këtë duhet që të faktorizoj prodhimin e dy numrave të thjeshtë për ta gjetur eksponentin privat *d*.

$$de \equiv 1 \bmod((p-1)(q-1)) \ (5)$$
$$\emptyset(n) = \emptyset(pq) = (p-1)(q-1) \ (6)$$
$$DE \equiv 1 \bmod(\emptyset(n)) \ (7)$$
$$DE \equiv E^{\emptyset(\emptyset(n))} \bmod(\emptyset(n)) \ (8)$$
$$D \equiv E^{\emptyset(\emptyset(n))-1} \bmod(\emptyset(n)) \ (9)$$

Shprehjet për dekriptimin e mesazhit janë:

$$C_i^d = (P_i^e)^d \equiv P_i^{ed} \bmod(n) \ (10)$$
$$(a^x)^y = a^{xy} \equiv a^z \bmod(n) \ (11)$$
$$P_i = C_i^d = P_i^{ed} \bmod(n) \ (12).$$

Enkriptimi përmes algoritmit RSA krijon ciphertext reprezentativ nga plaintext-i nën kontrollin e çelësit publik, ndërsa dekriptimi fiton përsëri plaintext-in ose mesazhin origjinal nga ciphertext-i nën kontrollin e çelësit korrespodues privat.

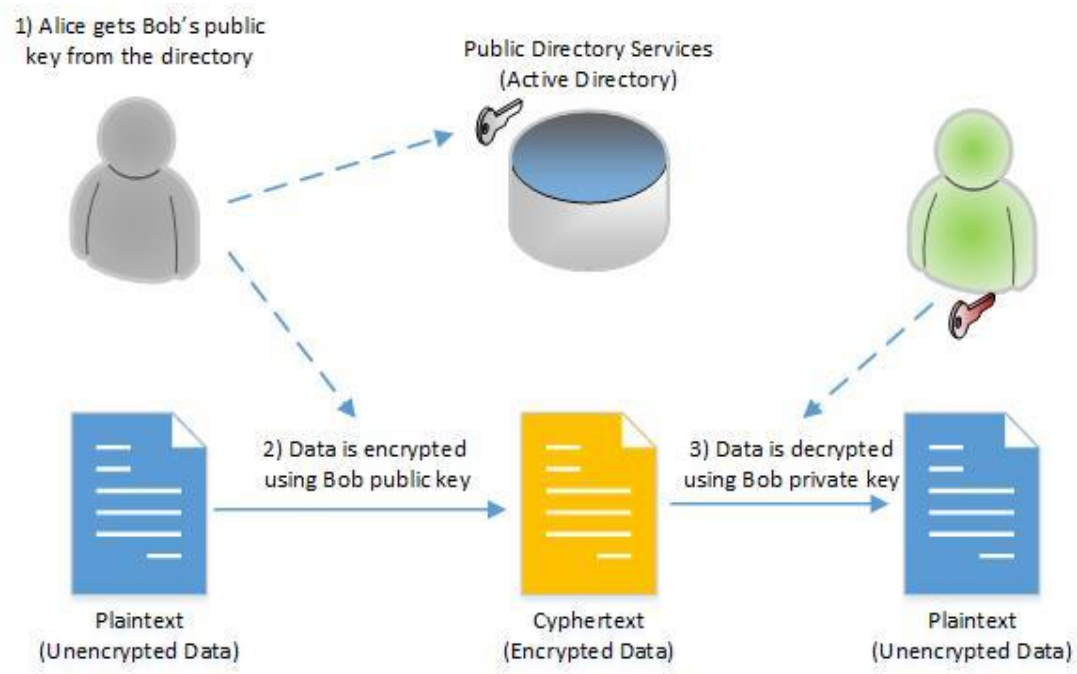


Figura 8: Enkriptimi/Dekriptimi duke përdorur çelësat RSA [11]

Gjersa nënshkrimi vëhet mbi mesazhe nën kontrollin e çelësit publik, verifikimi hap përsëri mesazhin origjinal për lexim përmes çelësit përkatës publik.
Algoritmi RSA implementohet në MRTD nga shtetet për nënshkrimin dhe verifikimin e certifikatave dhe SOd-it. Ky algoritëm duhet të përdoret sipas: "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", February 2003. Specifikuar në dy mekanizma të nënshkrimit: RSASSA-PSS dhe RSASSA-PKCS1_v15. Rekomandohet që nënshkrimet të gjenerohen sipas RSASSA-PSS, por pranimet e shteteve duhet të jenë të përgaditura që verifikimin e nënshkrimeve ta bëjnë sipas RSASSA-PKCS1_v15.

Një shembull i RSA
Tani pasi që kemi shtjelluar të gjitha pjesët e algoritmit RSA dhe i kemi të gjitha formulat që na nevojiten për të enkriptuar dhe dekriptuar mesazhin, le të marrim një shembull për një sistem kriptografik me çelës publik si RSA.
Ne do të fillojmë me numrin e zakonshëm prim 11 dhe 13. Duke i bërë llogaritjet, kemi:

$$p = 11$$
$$q = 13$$
$$n = 11 \times 13 = 143$$
$$\Phi(n) = 10 \times 12 = 120$$

e = 7 (7 është në mes të 1 dhe 120, si dhe emëruesi i përbashket i 7 dhe 120 është 1…kështu që, i plotëson të gjitha kriteret që të jetë vlera e çelësit publik)

$$d = 7^{-1} \pmod{120} = 103$$

çelësi publik është i dhënë me çiftin (7, 143)

çelësi privat është i dhënë me çiftin (103, 143)

Le të fillojmë me një tekst të dukshëm "9" dhe le të enkriptojmë këtë tekst. Duke i shfrytëzuar vlerat më lartë që i kemi përcaktuar, do të gjejmë vlerën e enkriptuar që është:

$$9^7 \bmod 143 = 48$$

Kështu që, vlera e enkriptuar e "9" është "48" duke i shfrytëzuar të gjithë numrat që i kemi zgjedhur më lartë. Normalisht, që vlera e enkriptuar do të ndryshojë nëse marrim vlera tjera për *p, q, n,* etj.

Për të dekriptuar këtë vlerë, ne do të shfrytëzojmë formulën e dekriptimit që e kemi shënuar më lartë që është:

$$48^{103} \bmod 143 = 9$$

Dhe siç mund të vëreni që ne kemi arritur në vlerën e mëparshme.

Duke e shikuar matematikën e përdorur, mund të vëreni se ju mund të tregoni pa ndonjë frikë për vlerën e *"e"* dhe *"n"* që keni dhënë informacion të mjaftueshëm për të llogaritur çelësin privat. Kjo për shkak se *"d"* është llogaritur duke shfrytëzuar *"totient"-in* e *"n"* më mirë se sa me shfrytëzu vetëm vlerën e *"n".*

Është shumë e lehtë të shumëzohen numrat prim së bashku, mirëpo është shumë e vështirë që të gjeni numrat prim të shumëzuar që ka rezultuar në atë numër. Në shembullin tonë, nëse është dhënë numri *143 (vlera e n),* a do të mund t'i kishim llogaritur numrat që janë shfrytëzuar 11 dhe 13? Ndoshta ky është një numër i vogël dhe nuk ka shumë mundësi, mirëpo a do e kishim gjetur për vlerën e *"n"* që ishte 2048 bit e gjatë?

RSA është ende e zbatueshme dhe është një sistem kriptografik me çelës publik shumë i fortë, mirëpo me rritjen e fuqisë së kompjuterëve, është duke u bërë tejet e nevojshme që të rritet madhësia e çelësave në RSA për të arritur një siguri më të lartë. Thënë më thjeshtë, nëse doni siguri më të madhe, madhësia e çelësave duhet rritur, mirëpo kjo ka një kosto më të lartë.

Le të themi që në ditët e sotme kemi shumë shfrytëzues të telefonave mobil, dhe më të vërtetë mendoni që telefonat e mençur të tyre kanë opcione të tilla që të bëjnë të gjitha ato llogaritje që të gjeneroj një çelës me madhësi më të madhe të RSA? Normal që jo. Mirëpo, çka nëse ekziston një mundësi për të shfrytëzuar çelësa me madhësi më të vogël, dhe të mbajmë nivelin e njëjtë të sigurisë [12]?

3.4 Digital Signature Algorithm (DSA)

Algoritmi i Nënshkrimit Digital (DSA) është një Standard i Procesimit të Informacionit Federal (Federal Information Processing Standard) për nënshkrimet digjitale. Ai është propozuar nga Instituti Kombëtar i Standardeve të Teknologjisë (National Institute of

Standards and Technology (NIST)) në Gusht të 1991, për përdorim në Standardin e Nënshkrimi Digital (DSS) të tyre dhe u adaptua si FIPS 186 në vitin 1993.
DSA llogaritet përmes disa formulave matematikore por siguria dhe vërtetësia e tij qëndron se në llogaritjen e nënshkrimit (çelësit) futet dhe vlera hash e dokumentit i cili do të nënshkruhet, dhe gjatë vërtetimit të nënshkrimit llogaritet sërish hash-i dhe një formulë tjetër matematikore, ku nëse nuk është bërë ndonjë ndryshim në dokument të dy vlerat do të përputhen.

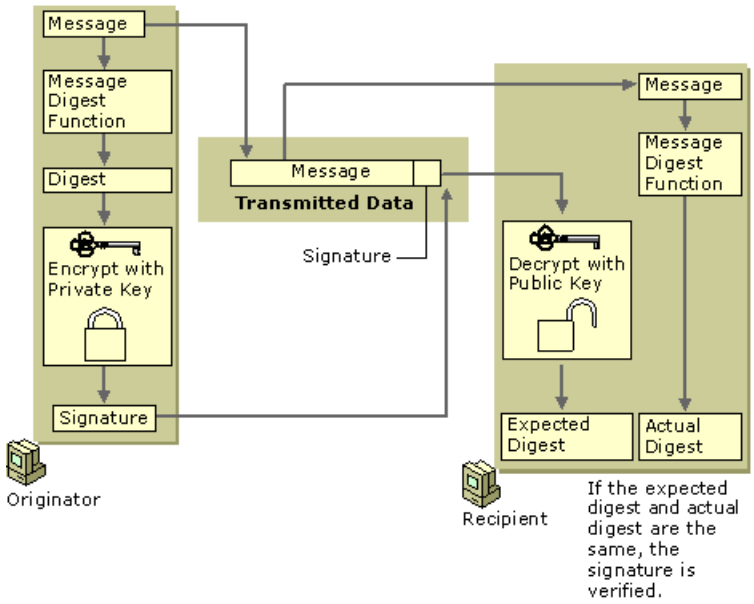


Figura 9: Vendosja dhe verifikimi i nënshkrimit përmes DSA [13]

Në MRTD përdoret sipas specifikimeve të DSA FIPS186-2. Mangësia e këtij versioni është se përkrah vetëm gjatësinë prej 1024 bitësh, gjë që do të përmirësohet në versionin DSA FIPS186-3.

3.5 Elliptic Curve Cryptography (ECC)

Lakorja Eliptike Kriptografike (ECC) është një sistem kriptografik me çelës publik sikurse RSA e cila bazohet në strukturën algjebrike të lakoreve eliptike mbi një fushë të fundme dhe shfrytëzohet si një mekanizëm për krijimin e çelësave publik dhe privat për të enkriptuar dhe dekriptuar të dhëna. Sikurse RSA që është e themeluar në vështirësinë matematikore e faktorizimit të numrave prime, ECC bazohet në vështirësinë matematikore në zgjidhjen e të ashtuquajturës Problemi i Algoritmit Diskret i Lakores Eliptike. Në vijim do të spjegojmë në hollësi për këtë, mirëpo është esenciale të kuptohet se sa hapa janë të nevojshëm që të lëvizim nga një pikë e lakores deri në pikën tjetër të po të njëjtës lakore. Kjo lë të kuptohet, edhe nëse e ke të njohur ekuacionin për atë lakore, mund të prezantohesh me një pikë tjetër në atë lakore dhe prapë të mos keni ide se sa

kërcime janë nevojitur për të arritur prej pikës startuese deri të pika që sapo jeni prezantuar me të. Kjo është vështirësia e Problemit të Algorimit Diskret i Lakores Eliptike, dhe mbi këtë është ndërtuar e gjithë siguria e ECC-së.

Për të kuptuar "Kërcimin nëpër lakore (Hopping around the curve)", le të fillojmë me disa karakterisitka interesante të Lakores Eliptike (Elliptic Curves) si dhe konceptin e njohur "Shtimi i Pikave (Point Addition)". Lakoret Eliptike janë simetrike ndaj boshtit X, dhe çdo drejtëz jo-vertikale do t'a prejë atë lakore në më së shumti 3 pika. Lakoret Eliptike që shfrytëzohen në kriptografi sot janë të definuara nga shprehja si në vijim:

$$y^2 = x^3 + ax + b$$

Variablat *x* dhe *y* janë variablat standarde që shfrytëzohen në funksione algjebrike dhe shfrytëzohen për të përcaktuar pikat *e* në boshtin *X* dhe në atë *Y* në një grafikë standarde. Parametrat e lakores *a* dhe *b* janë vlerat e koeficientave (numra konstant) të cilët përcaktojnë se si do të duket lakorja në një grafikë. Duke u ndryshuar vlerat e *a* dhe *b*, grafika do të merrë një formë tjetër pasi të paraqitet grafikisht.

Më poshtë kemi një shembull për një lakore eliptike të paraqitur grafikisht. Kjo grafikë e caktuar i ka vlerat $a = -6$ dhe $b = 10$

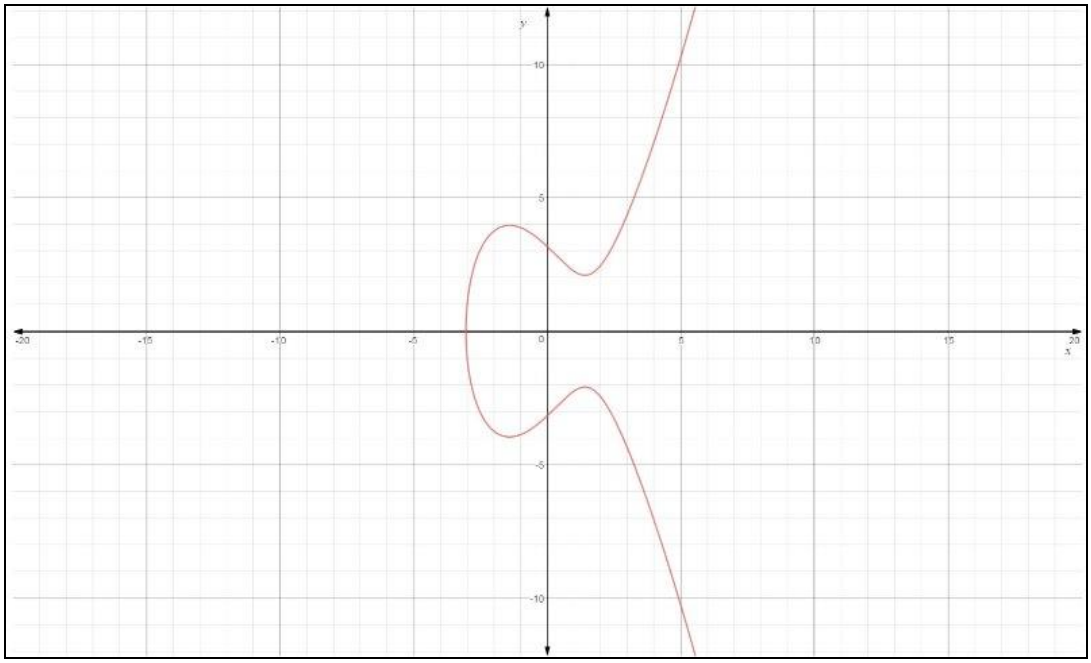


Figura 10: Shembull i Lakorës Eliptike [12]

$$y^2 = x^3 - 6x + 10$$

Shtimi i Pikave (Point Addition)

Është një operacion në Lakoret Eliptike të cilat ju lejojnë të filloni me një pikë dhe në fund të arrini në një pikë tjetër në atë lakore. Kështu funksionon shtimi i pikave: marrim 2 pika në atë lakore (*P* dhe *Q*), më pas i bashkojmë këto dy pika me një drejtëz dhe

vazhdojmë atë drejtëz deri sa ajo të prekë një pikë tjetër në atë lakore (të cilën do të quajmë -*R*). Pastaj, tërheqim një drejtëz vertikale nga pika -*R* deri sa të prekë në ndonjë pikë tjetër lakoren. Kjo pikë pastaj do jetë *R*. Prandaj, $P+Q = R$, ku së pari duhet të gjejmë -*R* në mënyrë që perfundimisht të gjejmë vlerën e *R*. Pasi të kemi gjetur vlerën për *R*, atëherë mund të tërheqim një drejtëz prej *P* në *R* dhe ju do të gjeni se ajo drejtëz do të prejë lakoren në një pikë të tretë. Nga ajo pika e tretë mund ta tërheqim një drejtëz vertikale deri sa t'a prejë lakorën në një pikë tjetër. Kjo pastaj do të ishte shtimi i pikës për pikën *P* dhe *R*. Ne mund të vazhdojmë këtë shtim të pikave sa herë të kemi nevojë. Grafiku më poshtë tregon një shembull për shtimin e pikave:

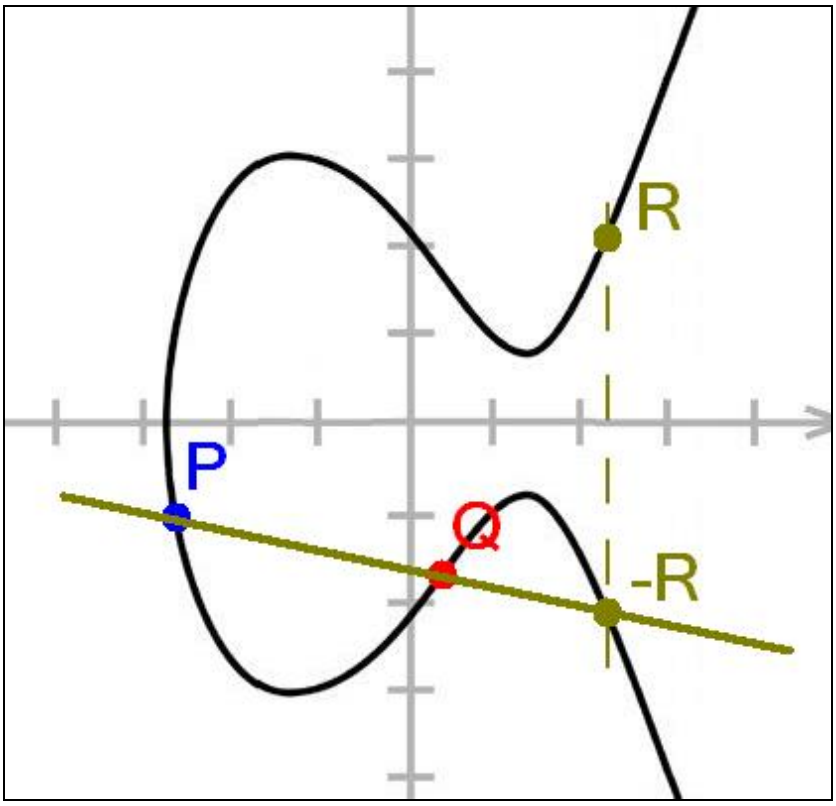


Figura 11: Shtimi i pikave në ECC [12]

Dyfishimi i pikave (Point Doubling)

Një operacion tjetër që shfrytëzohet në ECC quhet Dyfishimi i Pikave (Point Doubling). Dyfishimi i pikave është i ngjashëm me operacionin e shtimit të pikave, përveç që në dyfishimin e pikave, ju e shtoni pikën *P* të vetvetja se sa që e shtoni këtë pikë të një pikë tjetër në lakore. Kur t'i keni dy pika të ndryshme në lakoren eliptike (*P* dhe *Q*), është lehtë të vizatoni një pikë të drejtë ndërmjet tyre, mirëpo kur të keni vetëm një pikë, si do t'a vizatoni një pikë të drejtë ashtu që të pritet me një pikë tjetër në lakore?

Përgjigja është që të vizatoni vijën tangjenciale të pikës *(P)* dhe pastaj leni tangjentën që të prejë një pikë tjetër në lakore. Në pikën prerëse, tërhiqet një pikë vertikale, përderisa drejtëza të prek një pikë tjetër në lakore (koncepti i njëjtë sikurse operacioni *P + Q* më lartë). Në atë pikë prerëse ju e gjeni pikën *P + P*. Operacioni i dyfishimit të pikave është treguar në paraqitje grafike. Mbani mend se vlera e *P + P* është etiketuar si *R*. Kjo pikë shpesh referohet si *2P*.

Në mënyrë që të gjejmë vlerën për *3P*, duhet të kthehemi tek operacioni i Shtimit të pikave dhe të shtohet *P + 2P*. Pastaj, për të gjetur *4P*, duhet të shfrytëzohet prapë Shtimi i Pikave dhe të shtohet *P + 3P* dhe kështu më radhë.

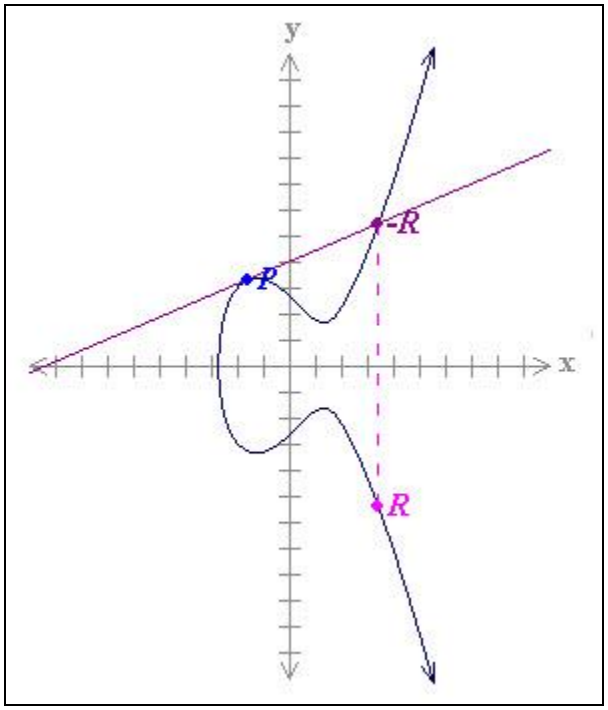


Figura 12: Dyfishimi i pikave në ECC [12]

Shtimi i pikave dhe dyfishimi i pikave janë shumë të rëndësishme për shkak që formojnë bazën e gjetjes së vlerave për enkriptim duke e shfrytëzuar ECC. Ato gjithashtu theksojnë bazën e problemit logaritmik diskret të lakoreve eliptike që është përmendur më lartë. Ky problem tregon që, pikat e dhëna *P* dhe *Q*, ku *Q* është shumëfish i *P*.. gjeje *k* ashtu që *Q = kP*. Pastaj, duke e ditur pikën startuese *P* dhe pikën aktuale në lakore, trego se sa herë ju keni dyfishuar pikën/shtuar pikën në mënyrë që të arrini prej pikës *P* në pikën aktuale. Kjo duket të jetë pakëz e komplikuar, mirëpo është mënyra e duhur për bazën e shfrytëzimit të ECC për enkriptimin e çelësit publik.

Një karakteristikë tjetër e rëndësishme e Lakoreve Eliptike është koncepti i një fushe të fundme. Imagjino, që duke vazhduar të dyfishoni pikën/shtoni pikën në lakoren eliptike, një nga pikat mund të përfundoj në një vlerë shumë të madhe të boshtit X. Në realitet, ju

nuk mund të lejoni që secila vlerë të përfshihet në llogaritjet e juaja (nuk mund të përfundoni në infinit), kështu që një mënyrë që t'i limitoni këto vlera është të përcaktoni një vlerë maksimale në boshtin *X*. Kjo vlerë në sistemin kriptografik të ECC është e njohur si *"p",* si dhe gjithashtu është e quajtur si vlera "modulo" për sistemin. Kjo vlerë gjithashtu është madhësia e çelësit për një system ECC.
Duke e rritur vlerën e *"p"* ju hapni mundësi për më shumë vlera të shfrytëzueshme të lakores, dhe në mënyrë efektive rritet siguria e sistemit duke e shfrytëzuar atë lakore. Prandaj, një rritje e madhësisë së çelësit nënkupton rritjen e sigurisë së lakores.
Tani, pasi i dijmë benefitet e ECC, le të vazhdojmë te vlerat që nevojiten për të përcaktuar sistemin kriptografik të ECC. Ato janë:
Ekuacioni i lakorës: $y^2 = x^3 + ax + b$

- *p:* Specifikon vlerën e fundme në të cilën shtrihet lakorja (vlera modulo)
- *a:* Koeficienti që e definon lakorën
- *b:* Koeficienti që e definon lakorën
- *G:* Pika fillestare në lakore. Kjo është pika kur fillojnë të gjitha operacionet.
- *n:* Rendi i G. Numri i operacioneve të pikës në lakore derisa pika rezultante të jetë vertikale.
- *h:* Bashkë-faktori (co-factor) - numri i pikave në një lakore eliptike i pjestuar nga rendi i G (kjo vlerë është 1 ose shumë afër 1)

Për një lakore eliptike të dhënë që shfrytëzohet në ditët e sotme, ju duhet të zgjedhni një lakore dhe të gjitha vlerat percjellëse duke u bazuar në rekomandimet e matematicientëve dhe shkenctarëve të cilët i kanë gjetë këto vlera dhe i kanë testuar hollësisht për përdorim gjatë enkriptimit. Me fjalë tjera, mos percaktoni lakoren eliptike dhe të prisni që të jetë e sigurt.

Diffie Hellman duke e shfrytëzuar ECC

Tashmë pasi i dijmë të gjitha parametrat e ECC, le të kalojmë në implementimin e ECC duke e shfrytëzuar protokolin Diffie Hellman për shkëmbim të çelësave. Imagjinoni sikur Alice dëshiron të krijojë një lidhje të sigurt me Bob-in dhe ajo vendos të përdor ECC Diffie Hellman si mekanizëm për të shkëmbyer çelësat për enkriptim. Së pari, Alice do të zgjedh një numër të zakonshëm në mes *1* dhe *n – 1*, ne do të quajmë atë α (alpha). Në të njëjtën kohë, Bobi është duke e zgjedhur një numër nga *1* deri në *n – 1,* gjithashtu ne do të quajmë vlerën e Bobit *β (beta).* Tash do të kemi:
α: një numër i rastësishëm i zgjedhur nga *1* deri në *n – 1*. Ky është çelësi privat për Alice
β: një numër i rastësishëm i zgjedhur nga *1* deri në *n – 1*. Ky është çelësi privat për Bobin

Tutje, Bobi llogaritë vlerën $B = \beta (G)$. Bobi mund të llogarisë këtë vlerë pasi i ka të njohura vlerat *β* dhe *G*. Në të njëjtën kohë, Alice llogarit vlerën $A = \alpha (G)$. Alice mund të llogarisë këtë vlerë pasi i ka të njohura vlerat *α* dhe *G*.
Tutje, Bobi i dërgon Alice pikën në lakorën *(x, y),* dhe Alice i dërgon Bobit pikën në lakore *(x, y).* Këto dy pika në lakore janë çelësat publik për Bobin dhe Alice. Ende,

asnjëri nuk e dijnë vlerën e çelësit privat të njëri tjetrit *(α ose β).* Ata i dijnë vetëm vlerat *A* dhe *B* (çelësat publik) sepse i kishin dërguar pikat në lakore të njëri tjetrit. Përderisa, një njeri në mes mund të verifikoj se *A* dhe *B* janë pika në një lakore eliptike të caktuar, ai prapëseprapë nuk do ta dinte se sa kërcime janë pikat nga pika fillestare e gjeneratorit *(G).*

Atij do t'iu nevojiteshin vlerat e α ose β për të ditur numrin e kërcimeve. Tutje, Bob dhe Alice do të llogarisin vlerën *P* duke i shumëzuar vlerat e çelësave përkatës privat me vlerën e pranuar nga personi tjetër. Prandaj,

Bobi llogarit: $P = \beta * A$

Alice llogarit: $P = \alpha * B$

Tash të dy, Bob dhe Alice kanë pikën *P* që mund të shfrytëzojnë si vlerë të çelësave për enkriptim me çelës privat.

Shembull:

Ju lutem të keni parasysh se vlerat për këtë lakore dhe të gjithë parametrat tjerë janë përdorur më parë. Kjo lakore përdor numra shumë të vegjël për *P* dhe *n*, kështu që nuk do të kishit dëshirë të përdorni këtë lakore në jetën e përditshme.

Këto janë vlerat për sistemin kriptografik ECC duke shfrytëzuar protokolin Diffie Hellman për shkëmbim të çelësave:

Lakorja: $y^2 = x^3 + 2x + 2 \ (mod\ 17)$

P: 17 (ky është një numër prime, kështu që kjo konsiderohet të jetë një lakore prime)

a: 2

b: 2

G: (5, 1)

n: 19

Për të gjetur *n*, ju duhet të Dyfishoni Pikën/Shtoni Pikën duke filluar nga *G* derisa të arrini një pikë në infinit. Kështu që, operacionet vazhdojnë derisa vija rezultuese të jetë vertikale. Në këtë rast, *n = 19*. Këtu janë disa prej operatoreve për këtë lakore të caktuar; duke filluar nga pika fillestare *(5, 1):*

2G = G + G = (6, 3) Mbajeni në mend: kjo pikë është gjetur duke Dyfishuar Pikën

3G = 2G + G = (10, 6) Mbajeni në mend: pikët e mbetuara janë gjetur duke shfrytëzuar Shtimin e Pikëve

4G = 3G + G = (3, 1)

…

19G = Pika në infinit

h = 1 (e cila është vlera ideale për *h*)

Tash jemi gati t'i fillojmë llogaritjet për α dhe β.

Alice e zgjedh një vlerë për α. Vlera e α duhet të jetë ndërmjet *1* dhe *n – 1*(18).

$\alpha = 3$

Tutje, Alice e llogarit vlerën e *A:*
*A = α * G = 3G*
A = (10,6) Mbajeni në mend: krahaso këtë pikë *3G* me pikën *3G* të listuar me lartë në llogaritjet për *"n".* Kështu jeni në dijeni se çfarë pike është e treguar përmes *3G.*
Bob e zgjedh një vlerë për *β.* Vlera për *β* duhet të jetë ndërmjet *1* dhe *n – 1 (18).*
B = 9
*B = β * G = 9G*
B = (7,6)
Ata i tregojnë njëri tjetrit vlerat e *A* dhe *B* dhe pastaj të dy i llogarisin vlerat e *P.*
Bobi llogarit *P = β * A = β * 3G = 9 * 3G = 27G.* Për shkak që renditja e lakorës *(n)* është *19, 27G* reduktohet në *8G.* Nëse vlera e *P* rezulton të jetë më e madhe se renditja e lakores, duhet të shfrytëzohet operacioni Modulo për të gjetur vlerën rezultuese. Në këtë shembull, 27 mod 19 = 8. Kështu që, 27G bëhet 8G sepse 27 është më i madh se 19.
Alice llogarit P = α * B = α * 9G = 3 * 9G = 27G. Alice shfrytëzon logjikën e njëjtë sikurse Bob-i në reduktim të 27G në 8G.
Kështu që, P = 8G = (13, 7)
Tash, Bob dhe Alice të dy i kanë pikët (13, 7) si sekreti i tyre i përbashkët, dhe njeriu në mes nuk e ka idenë se çfarë është vlera e P. Ata nuk kanë nevojë të shfrytëzojnë të dyjat boshtin X dhe boshtin Y, kështu që njërën e anulojnë. Tash, ata kanë vlerën 13 si sekret të përbashkët dhe mund t'a shfrytëzojnë këtë për të enkriptuar komunikimin në vazhdim.

Pse është ECC kaq e rëndësishme?

Siç është vërejtur nga pjesa e mëhershme, madhësia e çelësit është një faktor shumë i rëndësishëm për Lakoren Eliptike Kriptografike (ECC). Për çelësa me madhësi të njëjtë, zgjidhja për një algoritëm diskret të ECC është dukshëm më i vështirë se sa faktorizimi, që është si RSA dhe i enkripton çelësat.
Shikuar nga një perspektivë tjetër, bazuar nga një studim i Universal Security, për të thyer një çelës të RSA prej 228 bitëve nevojitet më pak energji se sa energjia e mjaftueshme për të vluar ujin sa një lugë çaji.

Nga ana tjetër, për të thyer një çelës 228 bitësh të ECC do të nevojitet më shumë energji se sa energjia për të vluar të gjithë ujin që gjendet në planetin tokë.
Për këtë arsye, mundësia për të reduktuar madhësinë e çelësave mund të jetë shumë e dobishme për pajisjet të cilat nuk kanë fuçi të mëdha llogaritëse.

3.6 Sulmet Kriptografike

Komunikimi i sigurt është kritik për e-commerce, e-banking, dhe gjithashtu për e-mail. Po ashtu sistemet e informacionit po shpërndahen gjithnjë e më shumë. Në botën e internetit dhe rrjeteve të ndryshme kompjuterike ka shumë individ që përpiqen të përfitojnë nga dobësitë e sistemeve të komunikimit.

Ne dëshirojmë të kemi konfidencialitet dhe privatësi të të dhënave tona, dhe për këtë shkak ekzistojnë dënime për hapjen e pa autorizuar të tyre. Një aspekt tjetër i rëndësishëm i të dhënave është integriteti i tyre, ku persona të pa autorizuar nuk mund të qasen në to.

Një gjë tjetër që ne e kërkojmë është jo mohueshmëria (nuk duhet të mohojmë një veprim tonin nëse e kemi bërë), që shpesh implementohet duke përdorur dokumente zyrtare të nënshkruara dhe dëshmitar. Në mënyrë të ngjashme, edhe filmimet gjatë marrëveshjeve na mbrojnë nga mohueshmëria.

Të gjitha këto veti të një komunikimi të sigurt ekzistojnë, por prapë ka mundësi për manipulime. Nevojiten mjete të ndryshme që garantojnë këto veti të komunikimit të jenë të sigurta në një sistem digjital. Kriptografia na siguron këto mjete dhe na jep siguri në komunikim.

Kriptografia nuk është vetë siguria, por jep një kontribut të jashtëzakonshëm në drejtim të sigurisë së çdo sistemi. Me pak fjalë, ne jemi të interesuar në dy gjëra, informatat e lexueshme dhe të pa kuptushme të bëhen të pa lexueshme dhe e kundërta. Këto dy procese njihen si enkriptimi dhe dekriptimi.

Kriptografët janë ata që na ofrojnë mekanizma për enkriptim dhe dekriptim të të dhënave, dhe janë në luftë të vazhdueshme me kriptoanalistët ose code breakers. Shpesh ndodh që këta dy të punojnë bashkë që të rritet niveli i sigurisë në sisteme të ndryshme [14].

Siç dihet, pjesa kryesore e komunikimit kriptografik në rrjetë është Kriptografia me Çelës Publik (PKI), e cila përdoret për ekriptimin e komunikimit TCP/IP mes dy pikave në rrjetë. PKI përdor algoritma enkriptimi të ndryshëm për sigurinë e të dhënave. E gjithë ideja prapa enkriptimit është që vështirësoj aq shumë saqë procesi i gjetjes së çelësit do të marrë kohë të madhe. Për shembull, nëse një mesazh është enkriptuar me një çelës 8 bitësh, do të thotë që duhet të përdoren 256 kombinime të ndryshme të çelësit, të dekriptohet e dhëna. Këtë detyrë mund ta bëjë çfarëdo kompjuteri. Por nëse përdorim çelës 32 bitësh atëherë kemi 65536 kombinime që duhet ti provojmë. Sa më shumë që e rrisim gjatësinë e çelësit, aq më shumë kohë duhet që të gjendet çelësi. Përdorimi i një çelësi 256 bitësh, do t'i bënte edhe kompjuterët më të fuqishëm në botën të pa përdorshëm. Siç shohim gjatësia e çelësit është një faktor i rëndësishëm. Po aq i rëndësishëm është edhe algoritmi matematik që përdoret për enkriptim dhe dekriptim.

Prej algoritmeve më të njohur janë SHA1, 3DES etj. Ka dy lloje të çelësave, simetrik dhe asimetrik. Në rastin e simetrikut, nevojitet vetëm një çelës për enkriptim dhe dekriptim, ndërsa në rastin e asimetrikut janë dy çelësa të ndryshëm komplementar me njëri-tjetrin.

Sulmet kriptografike kanë për synim gjetjen e çelësit që është përdorur gjatë procesit të enkriptimit. Këto sulme janë të dizajnuara të shkatërrojnë algoritmat kriptografik dhe të provojnë dekriptimin e të dhënave pa e poseduar çelësin. Janë pjesë e kriptoanalizës, artit të deshifrimit të dhënave të enkriptuara.

Ekzistojnë gjashtë metoda sulmi kriptografike, të ndara në dy kategori: Plaintext-based attacks dhe Ciphertext-based attacks.

Plaintext-based attacks

Known plaintext attacks. Janë sulme ku kriptoanalisti ka qasje në *plaintext* dhe në *ciphertext*-in përkatës, dhe përpiqet të zbuloj një lidhje ose korrelacion mes dyjave.

Chosen plaintext attacks. Është sulm ku kriptoanalisti mund të enkriptoj një *plaintext* dhe të analizon *ciphertext*-in që i del. Kjo është e zakonshme kundër kriptografisë me çelës publik, ku kriptoanalisti ka qasje në çelësin publik.

Adaptive chosen plaintext attacks. Një kriptoanalist zgjedh disa *plaintexte* ose *ciphertexte* për sulmin e tij.

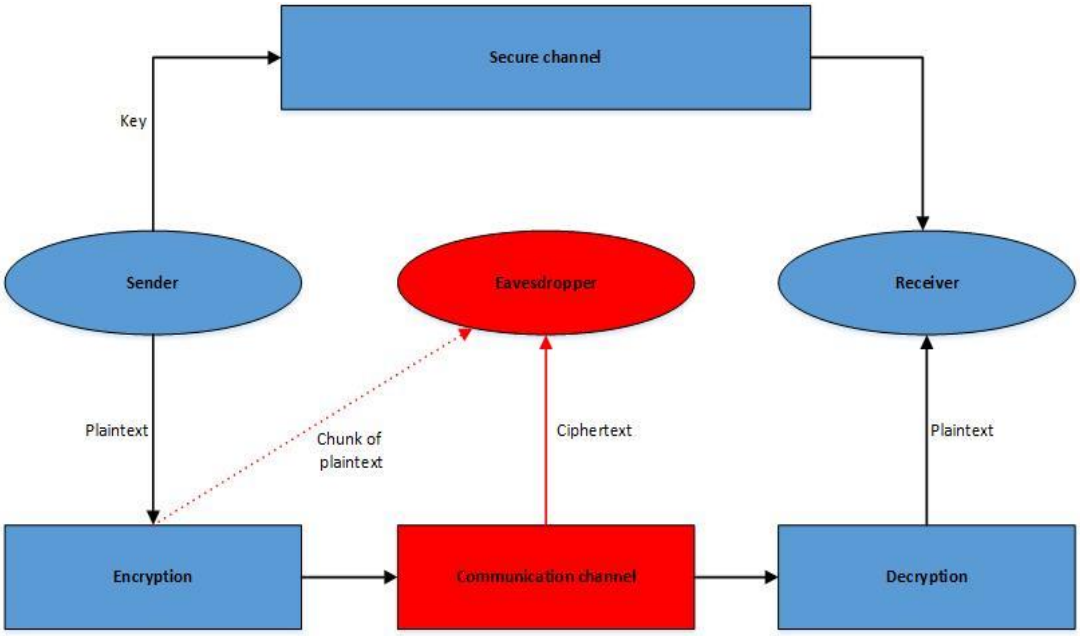


Figura 13: Known Plaintext Attack [75]

Ciphertext-based attacks

Ciphertext-only attacks. Është sulm ku kriptoanalisti ka qasje në *ciphertext*, por nuk e ka *plaintext*-in korrespondues. Me *Caesar Cipher* ai mund të thyej kodin e enkriptimit.

Chosen ciphertext attacks. Në këtë sulm ku kriptoanalisti zgjedh një *ciphertext* dhe provon të gjejë *plaintext*-in përkatës. Kjo arrihet me *decryption oracle* (një makinë që dekripton pa e ekspozuar çelësin). Kjo performohet në sulme ndaj enkriptimit me çelës publik.

Adaptive chosen ciphertext attacks. Një kriptoanalist zgjedh disa *plaintexte* ose *ciphertexte* për sulmin e tij, pastaj provon të gjejë ndonjë lidhje mes tyre derisa e realizon [15].

SSL Main in the middle

Një sulm man-in-the-middle është sulm në të cilin sulmuesi ndërpren dhe transmeton mesazhet mes dy palëve të cilët besojnë se janë duke komunikuar direkt me njëri-tjetrin. Është një formë përgjimi ku e gjithë biseda kontrollohet nga sulmuesi i cili poashtu ka aftësinë të modifikoj përmbajtjen e secilit mesazh. Sulmuesi shikon trafikun HTTPS në qetësi, dhe pret që webfaqja e targetuar të përgjigjet në ndonjë kërkesë HTTPS. Serveri supozohet të dërgojë certifikatën e tij digjitale browserit si pjesë e 'three way handshake' të protokolit SSL. Sulmuesi e merrë këtë çertifikatë, dhe shënon disa detaje kryesore si emrin e domenit, datën e skadimit, fuqinë e algoritmit etj. Pastaj, sulmuesi e krijon certifikatën e tij, e quajtur poashtu certifikatë e vetë-nënshkruar e cila përmban informata të njëjta me certifikatën e rrëmbyer. Prej këtij çasti, sulmuesi me të vërtetë bëhet një man-in-the-middle ku secila kërkesë e browserit ndërprehet dhe përgjigjet me çertifikatën falso. Si një përgjigje normale ndaj një situate të tillë, web browseri i paraqet përdoruesit një lajmërim, i cili në shumicën e rasteve injorohet nga personi i cili po shfleton browserin, dhe kështu sulmuesi përfundon misionin me sukses. Në anën e serverit, sulmuesi vendos një lidhje të ndarë HTTPS për të kompletuar kërkesën dhe rezultati i kërkesës i kthehet browserit në lidhjen e vendosur tashmë. Kjo i jep sulmuesit një kontroll të plotë në trafikun SSL dhe i ndihmon në vjedhjen e informacioneve. Për shkak se ky sulm përfshinë një ndërhyrje në rrjetë, është më pak e mundshme që të ndodh, por mund të rezultoj në humbje serioze të të dhënave. Poashtu, për shkak se sulmuesi nuk është duke ndaluar vargu i kërkesave dhe përgjigjeve, bëhet e vështirë të zbulohet vjedhja e të dhënave.

Ky sulm mund të jetë shumë i suksesshëm nëse sulmuesi mund të shtiret si secila palë për t'iu përshtatur palës tjetër. Sulmet MITM shkaktojnë një kërcnim serioz ndaj sigurisë online për shkak se ato i japin sulmuesit aftësinë për të kapur dhe manipuluar me informata të ndjeshme në kohë reale duke u paraqitur si palë e besueshme gjatë transaksioneve, bisedave dhe transferimit të të dhënave.

Një metodë e zakonshme për ekzektutimin e një sulmi MITM përfshinë shpërndarjen e *"malware"* e cila siguron çasje në web browserin e përdoruesit dhe në të dhënat që ai i merrë dhe i dërgon. Malware poashtu mund të përdoret për të shtuar të dhëna në fajllat e lokal të hostit për të ridrejtuar përdoruesit tek një webfaqe e cila duket njësoj si webfaqja të cilën dëshiron të arrij përdoruesi. Sulmuesi pastaj krijon një lidhje me faqen e vërtetë dhe luan rolin e një *"proxy"*, duke e mundësuar leximin, insertimin dhe modifikimin e trafikut mes përdoruesit dhe faqes legjitime para se ta përcjellë më tutje. Webfaqet e bankave online dhe të e-tregtisë shpeshherë janë cak i sulmeve MITM për shkak se mund

të rrëmbejnë kredencialet gjatë procesit login dhe të dhëna të tjera të rëndësishme edhe nëse faqja enkripton komunikimet duke përdorur SSL/TLS.

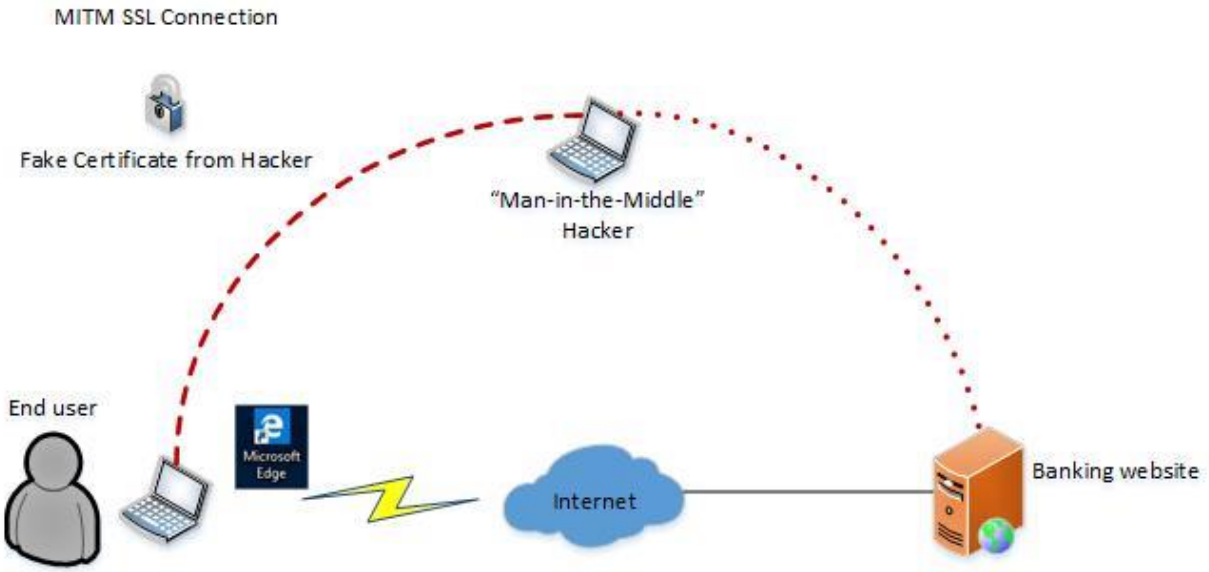


Figura 14: SSL Main in the middle [76]

Një sulmues poashtu mund të shfrytëzoj dobësitë në një konfigurim sigurie të një ruteri pa tela (wireless) siç janë fjalëkalimet e dobëta për të filluar një sulm MITM dhe për të kapur informacione të cilat dërgohen përmes ruterit. Një ruter i sulmuesit mund të vendoset në një vend publik siç është një kafene apo hotel për të njëjtin qëllim.

Shumica e protokoleve kriptografike përfshijnë disa forma të autentikimit veçanërisht për të parandaluar sulmet MITM. Për shembull, TLS mund të autentifikoj një apo të dy palët duke përdorur një autoritet certifikimi që i besojnë të dy palët. Por, nëse përdoruesit nuk kanë kujdes ndaj lajmërimeve kur një certifikatë e dyshimtë paraqitet, sulmet MITM përsëri mund të kenë sukses me certifikata të falsifikuara [16].

SSL Main in the browser

I ngjashëm me sulmin e lartpërmendur, te ky lloj sulmi injektohet një kod JavaScript në browser për të krijuar një situatë man-in-the-browser. Ky kod i monitoron të gjitha aktivitetet SSL dhe dokumenton sesionin. Përderisa ndodh kjo, sulmuesi poashtu dokumenton versionin e enkriptuar të po atij sesioni dhe provon që me anë të programimit të gjejë fuqinë e algoritmit dhe të çelësit, përveç rrëmbimit të të dhënave.

Një sulm man-in-the-browser është i dizajnuar që të ndërprejë të dhënat të cilat lëvizin nëpër një linjë të sigurtë mes përdoruesit dhe aplikacionit online. Një Trojan e bashkangjit veten në browserin e përdoruesit dhe mund të programohet që të aktivizohet kur një përdorues ka qasje në webfaqe specifike, siç janë webfaqet e bankave. Kur aktivizohet, një Trojan man-in-the-browser mund të ndërpresë dhe të manipuloj çfarëdo informacioni që një përdorues i vendos në kohë reale.

Trojan MITB zakonisht performojnë diçka që njihet si *"session hijacking"* - abuzimi i një sesioni të një përdoruesi legjitim në webfaqen në të cilin është i çasur në llogarinë e tij. Duke rrëmbyer sesionin në këtë mënyrë, të gjitha veprimet e performuara nga Trojan bëhen pjesë të sesionit legjitim siç janë aktivitetet keqdashëse (p.sh. transfer parash i jashtëligjshëm, ndërrimi i adresës postale) apo edhe injektimin e kodit JavaScript i cili pastaj performon këtë automatikisht.

Një sulm MITB ndodh në këto hapa:

- Një klient infektohet me një Trojan i cili ka mundësi të krijoj një sulm MITB.
- Gjatë fillimit të një transaksioni legjitim, Trojan hyn në aksion dhe fillon ekzekutimin.
- Përdoruesi kalon të gjitha fazat e autentikimit, përfshirë çfarëdo autentikimi me dy-faktor kur është e nevojshme. Trojan pret në heshtje për login të suksesshëm apo dhe autorizim të transaksionit.
- Trojan manipulon detajet e transaksionit - personit që paguhet, dhe ndonjëherë edhe të shumës. Në shumicën e rasteve, llogaria e personit që paguhet zëvendësohet me një llogari të cilën mund ta përdor mashtruesi.
- Duke përdorur teknika të inxhinierisë sociale, përdoruesi nuk është i vetëdijshëm për faktin që dikush është duke e sulmuar. Trojan i paraqet webfaqe falso përdoruesit, të cilat mund të tregojnë detaje transaksioni të cilat korrespondojnë më ato të përdoruesit. Nëse nevojitet autentikim i mëtutjeshëm për të kompletuar transaksionin, trojan do të ndërveproj me përdoruesin dhe ti kërkoj atij të shkruaj kredencialet e autentikimit të tyre në kohë reale që të aprovohet transaksioni.

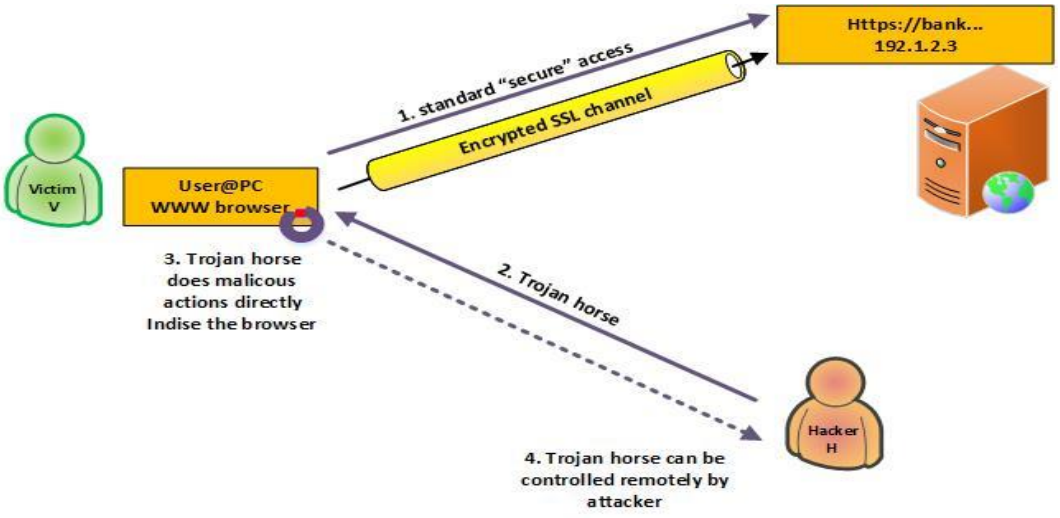


Figura 15: SSL Main in the browser [77]

Ajo që i bënë sulmet MITB të vështira për tu detektuar është fakti që çfarëdo aktiviteti i performuar duket se është me origjinë nga browseri i përdoruesit legjitim. Karakteristika siç janë headerat e HTTP dhe IP adresa do të shfaqen të njëjta me të

dhënat e vërteta të përdoruesit. Kjo krijon një sfidë në ndarjen mes transaksioneve të vërteta dhe atyre keqdashëse [17].

SSL Brute Force Attacks

Përndryshe prej sulmeve që përqendrohen në dobësitë e sistemit, një sulm Brute Force ka për qëllim metodën më të thjeshtë për të pasur çasje në një webfaqe: provon secilin çelës derisa e gjenë atë që funksionon; provon emra dhe fjalëkalime, herë pas here, derisa hyn në sistem. Shumë shpesh të quajtur*"joelegant"*, ata mund të jenë shumë të suksesshëm kur njerëzit përdorin fjalëkalime si *"123456"* dhe emra si *"admin"*.

Këto sulme janë, shkurtimisht, sulm në pikën më të dobët të sigurisë së çfarëdo webfaqeje. Për shkak të natyrës së këtyre sulmeve, ju mund të shihni se memorja e serverit tuaj ngadalësohet shumë, duke shkaktuar probleme në performancë. Kjo është rezultat i numrit të kërkesave HTTP (numri i vizitave në webfaqen tuaj) është aq i madh sa që tejkalon memorien e serverit. Sulmet Brute Force janë të thjeshta për tu kuptuar, por të vështira për tu mbrojtur nga to. Enkriptimi është matematikë, dhe përderisa kompjuterët bëhen më të shpejt në matematikë, ata bëhen më të shpejt në përpjekjen e të gjitha zgjidhjeve dhe të vendosin se cila zgjidhje përshtatet.

Këto sulme mund të përdoren kundër çfarëdo tipi të enkriptimit, me shkallë të ndryshme të suksesit. Sulmet Brute Force bëhen më të shpejta e më efektive ditë pas dite me publikimin e harduerit kompjuterik më të ri dhe më të shpejt.

Algoritmet hash të fuqishme mund të ngadalësojnë sulmet Brute Force. Para së gjithash, algoritmet hash performojnë aktivitete matematikore të mëtutjeshme në një fjalëkalim para se të ruajnë një vlerë të derivuar nga fjalëkalimi në disk. Nëse përdoret një algoritëm hash më i ngadalëshëm, do të kërkoj njëmijë herë më shumë aktivitete matematikore për të provuar çdo fjalëkalim dhe do të ngadalësoj sulmet Brute Force. Por, sa më shumë punë kërkohet, aq më shumë punë do ti duhet të bëjë një serveri apo ndonjë kompjuteri tjetër çdo herë që përdoruesi kyçet me fjalëkalimin e tij. Software duhet të baraspeshoj aftësitë ripërtëritëse kundër sulmeve Brute Force me përdorimin e resurseve.

Nuk ka asnjë mënyrë të mbrohemi plotësisht. Është e pamundur të themi se sa i shpejt do të bëhet hardueri kompjuterik dhe nëse ndonjë nga algoritmet e enkriptimit të cilat i përdorim sot kanë dobësi të cilat do të zbulohen dhe përdoren në të ardhmen. Por, ja ku janë baziket: mbani të dhënat tuaja të enkriptuara në ndonjë vend të sigurt ku sulmuesi nuk do të mund ti gjejë. Kur sulmuesi ka të dhënat e juaja të kopjuara në harduerin e tyre, ata mund të tentojnë ti sulmojnë me Brute Force. Nëse jeni në ndonjë shërbim i cili pranon kyçje (login) në internet, sigurohuni që i limitoni përpjekjet për kyçje dhe bllokoni njerëz që tentojnë të kyçen me shumë fjalkalime të ndryshme në një periudhë të shkurtër kohore [18].

Session Key Hijacking

Në vitet e fundit, sulmi i rrëmbimit të çelësit të sesionit (session key hijacking) është lënë në hije nga spyware, rootkits, botnet, dhe denial of service attacks (DDoS). Megjithëse sulmi i rrëmbimit të sesionit nuk është një sulm me prioritet të lartë në mendjen e të gjithëve, por ajo ende mbetet një sulm i zakonshëm që përdoret. Nëse implementohet me sukses, sulmuesit marrin identitetin e përdoruesit të kompromentuar, duke shijuar të njëjtën qasje në burimet e përdoruesit të kompromentuar.

Sulmet e rrëmbimit të sesionit janë zakonisht kundër përdoruesve që janë anëtar të rrjeteve të mëdha që përmbajnë një numër të konsiderueshëm të seancave të hapura. Protokolet e rrjeteve si FTP, Telnet, dhe rlogin janë veçanërisht tërheqëse për sulmues, për shkak të natyrës së seancës të orientuar nga lidhjet e tyre, dhe gjatësia e sesioneve të tyre të komunikimit. Përveç kësaj, FTP, Telnet, dhe rlogin nuk implementojnë asnjë siguri gjatë kyçjes, autentikimit, apo transmetimit të dhënave. Në fakt, të dhënat që dërgohen duke përdorur këto protokole, dërgohen në tekst të qartë të cilat mund lehtësisht të shihet nga çdokush që merret me monitorimin e rrjetit.

Ekzistojnë tri lloje të ndryshme të sulmeve të sesioneve: aktive, pasive, dhe hibride.

Sulmi aktiv është kur sulmuesi rrëmben një sesion në rrjetë. Sulmuesi do të ndal një nga makinat, zakonisht kompjuterin e klientit, dhe do të marrë përsipër pozicionin e klientëve në shkëmbimin e komunikimit ndërmjet workstation dhe server. Sulmi aktiv gjithashtu lejon sulmuesit të japin komandat në rrjetë duke e bërë të mundur për të krijuar llogari të reja përdorues në rrjet, të cilat më vonë mund të përdoret për të fituar qasje në rrjet, pa pasur nevojë për të kryer sulmin rrëmbej sesionin.

Sulmet pasive të sesioneve janë të ngjashme me sulmet aktive, por në vend që të fshijë përdoruesin nga sesioni i komunikimit, sulmuesi monitoron trafikun në mes workstation dhe serverit. Motivimi kryesor për sulmin pasiv është ajo që i siguron sulmuesit aftësinë për të monitoruar trafikun e rrjetit dhe potencialisht të zbuloj të dhëna të vlefshme ose fjalëkalime.

Lloji i fundit i sulmit të rrëmbimit të sesionit është referuar si sulm hibrid. Ky sulm është një kombinim i sulmeve aktive dhe pasive, të cilat e lejojnë sulmuesit për të monituruar trafikun të rrjetit deri kur diçka me interes është gjetur. Sulmuesi pastaj mund të modifikoj sulmin duke hequr kompjuterin workstation nga sesioni, dhe duke marrë identitetin e tyre.

Pra, çfarë e bënë sulmin e rrëmbimit të sesionit të vlefshëm për sulmuesin? Një nga tiparet më të vlefshme e këtij lloji të sulmit është aftësia për të fituar qasje në një server pa pasur nevojë të vërtetoj autentikimin. Pasi sulmuesi rrëmben një sesion, ata nuk duhet të shqetësohen për të vërtetuar autentikimin me serverin për sa kohë që seanca e komunikimit mbetet aktive. Sulmuesi gjithashtu gëzon të njëjtën qasje në server si përdoruesit e kompromentuar, sepse përdoruesi ka vërtetuar tashmë autentikimin në server para se sulmi të ndodh.

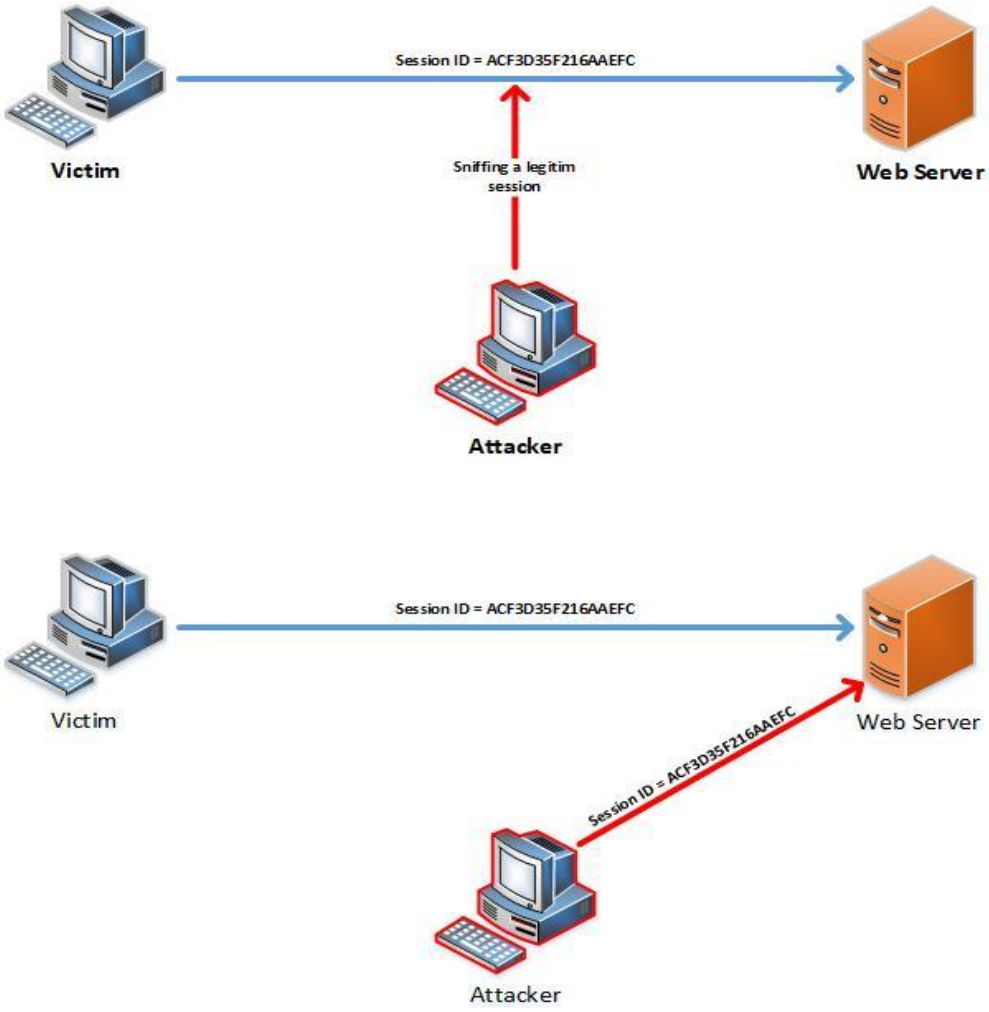


Figura 16: Session Key Hijacking [78]

Një sulm i suksesshëm i rrëmbimit të sesionit gjithashtu i lejon sulmuesit të lëshoj komandat në serverët në rrjet. Kjo është bërë zakonisht për të krijuar llogaritë e përdoruesve që mund të përdoren për të hyrë në burimet në një datë të mëvonshme. Aftësia për të nxjerrë komandat gjithashtu ofron një mënyrë për të maskuar praninë e sulmuesit në rrjet, duke hequr ose ndryshuar mbetjet e sulmit [19].

Compromised Key Attacks

Një sulm i çelesit të kompromentuar (compromised key attacks) ndodh kur sulmuesi përcakton çelësin, i cili është një kod sekret ose numrin e përdorur për të enkriptuar, dekriptuar, ose për të vërtetuar informacionin sekret. Ky çelës korrespondon me certifikatën e lidhur me server. Kur sulmuesi është i suksesshëm në përcaktimin e çelësit, sulmuesi përdor çelësin për dekriptimin e të dhënave të koduara, pa dijeninë e dërguesit të të dhënave. Ka dy çelësa të ndjeshëm në përdorim në infrastrukturën me çelës publik (PKI) që duhet të merren parasysh: çelësi privat që çdo mbajtës certifikate dhe çelësi

session që është përdorur pas një identifikimi të suksesshëm dhe çelësi session pas shkëmbimit të suksesshëm nga ana e partnerëve të komunikimit.

Në mënyrë që të dy palët të komunikojnë në mënyrë të sigurt në një rrjet publik, ata duhet të jenë në gjendje për të vërtetuar njëri-tjetrin dhe të bien dakord mbi një çelës enkriptues sekret. Për të arritur këtë, protokolet kryesore të krijimit janë përdorur në fillim të një sesioni të komunikimit në mënyrë që të verifikoj identitetin e palëve dhe të krijoj një çelës të përbashkët për sesion. Ka dy kategori themelore të protokoleve. E para përfshinë të ashtuquajturat protokole të rëndësishme të transportit, në të cilën çelësi sesion është krijuar nga një entitet dhe është transmetuar sigurt për të tjera. Një kategori e dytë përfshinë protokolet kryesore e marrëveshjeve, ku informatat nga të dy njësitë (entitetet) janë përdorur për të nxjerrë çelësin e përbashkët [20].

Denial of Service (DoS)

Në sulmin *"denial-of-service"* apo DoS, sulmuesi provon t'i ndaloj shfrytëzuesit legjitim t'iu qasen informatave apo shërbimeve. Duke e sulmuar kompjuterin tuaj apo lidhjen e rrjetës, ose kompjuterët dhe rrjetin e webfaqes që ju po provoni ta përdorni, një sulmues mund të jetë në gjendje të ju ndaloj juve qasje në email, webfaqe, llogaritë online (llogari bankare, etj), ose shërbime tjera që mbështeten në kompjuterin e afektuar.

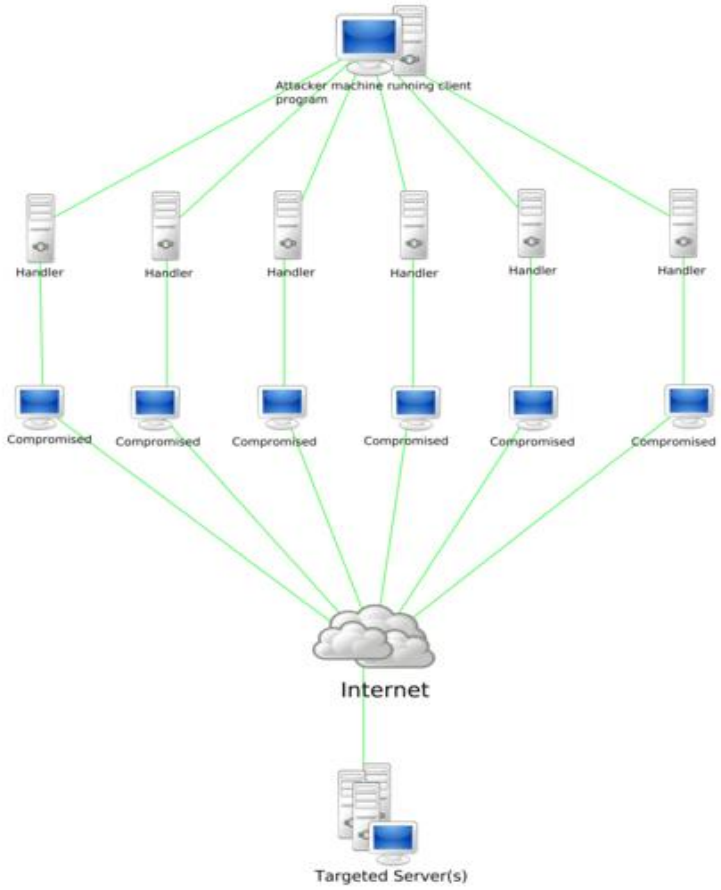


Figura 17: Denial of Service [79]

Tipi më i shpeshtë dhe më evident i një sulmi DoS ndodh kur një sulmues *"përmbyt"* një rrjet me informacione. Kur ju e shkruani një URL për një webfaqe të caktuar në browser, ju po dërgoni një kërkesë tek kompjuter-server i asaj webfaqe për ta shikuar faqen. Serveri mund ti procesoj vetëm një numër të caktuar të kërkesave përnjëherë, kështu që nëse një sulmues e mbingarkon serverin me kërkesa, nuk mund ta procesoj kërkesën tuaj. Kjo njihet si një ndalesë e shërbimit (denial of service) sepse ju nuk mund të keni qasje në atë faqe.

Kemi tipe të ndryshme të sulmuesve të hartuar posaqërishtë për:

- Mbushje të resurseve të rrjetës,
- Shterje të memories së CPU-së,
- Zvogëlim të fuqisë kompjuterike,
- Përdorim të kohëmatësve,
- Helmim të përkthimeve të emrave të domain-ve

Një sulmues mund të përdor spam mesazhe të email-it, për të nisur një sulm të ngjajshëm me llogarinë e e-mail-it tuaj. Edhe nëse jeni duke përdorur llogari të e-mailit e cila është e ofruar nga punëdhënësi juaj ose një llogari e cila përdor shërbimet falas siç është yahoo apo hotmail, juve ju caktohet një kuotë specifike, e cila ju limiton numrin e të dhënave që ju mund të keni në llogari për një periudhë të caktuar kohore. Duke i dërguar shumë e-mail mesazhe apo e-mail mesazhe të mëdha në llogari, sulmuesi mund ta shpenzoj kuotën tuaj duke ju ndaluar juve të merrni mesazhe legjitime. Kur një aplikacion specifik është ndërprerë dhe kur funksionimi normal është i ndaluar, atëherë kjo quhet Ndalesa e Shërbimit në nivel të Aplikacionit (Application level Denial of Service).

Ndalesa e Shërbimit (DDoS) e shpërndarë ka një fuqi të bashkuar të shumë sistemeve të kompromentuara që punojnë për një shkak të caktuar. Faza e parë e këtij sulmi është të ndërtoj një platformë me shumë sisteme mikpritëse që mund të punojnë me komanda të largëta. Grupi i sulmuesve në fillim do ti skanonte rrjetat për të kërkuar sisteme të dobëta që kanë karakteristika të dobëta e sigurisë. Duke u bazuar në hulumtime, ka me miliona makina mikpritëse që janë të dobëta në aspektin e sigurisë dhe përditësimeve të duhura të cilat shpeshherë bien viktimë ndaj këtyre sulmuesve. Në momentin kur procedura skanuese përfundon, sulmuesit do ta merrnin kontrollin e këtyre përdoruesëve duke përdorur shfrytëzime softuerike si Buffer Overflow, dangling pointers, code injection [21].

Birthday SSL Attacks

Sulmi ditëlindje (birthday attacks) përdor probabilitetin se dy mesazhe të cilat përdorin algoritmin e njëjtë hash do të prodhojnë *message digest* të njëjtë. Pra, ky sulm shfrytëzon përplasjet (collisions) në tabelën hash. Ky sulm mbështetet në teorinë matematike të quajtur paradoksi i problemit të ditëlinjdes, i cili tregon se statistikisht, në një set me njerëz të selektuar në mënyrë të çfarëdoshme, një dyshe njerëzish do të kenë

ditëlindjen në datë të njëjtë. Kjo teori do të jetë më e saktë sa më shumë të shtohet numri i njerëzve. Në kriptografi, integriteti i të dhënave sigurohet me algoritme hash dhe checksum, të cilat kalkulohen në dy anët e transmisionit për tu siguruar se të dhënat nuk janë modifikuar. Këto lloje të sulmeve synojnë algoritmet hash, dhe ka nevojë që shumë sulmues të bëhen së bashku të cilët kapin blloqe të të dhënave dhe i ndajnë me njëri tjetrin. Secili bllok pastaj analizohet për të krijuar një set të mëtutjeshëm të të dhënave, në mënyrë që algoritmi hash i saj të jetë i njëjti me atë të bllokut të të dhënave. Me fjalë të tjera, për një bllok të dhënash dhe kombinimi hash, algoritmi matematikor krijon një set të dhënash të njëjtë. Procesi i mëtutjeshëm i bllokut fillestar të të dhënave dhe seti i të dhënave rezultuese, ndihmojnë në gjetjen e çelësit të enkriptimit [22].

4 DOKUMENTET BIOMETRIKE TË IDENTITETIT

Kartelat e mençura janë shumë të përshtatshme për tu përdorur në fushën e identifikimit, të tilla si kartelat e identitetit (ID), dokumentet e identifikimit dhe pasaportat. Ky përdorim është mbështetur nga fakti se mikrokontrollerët e kartelave të mençura kanë siguri të lartë kundër sulmeve [23].

Qytetarët e Republikës së Kosovës pajisen me letërnjoftim biometrik apo kartelë biometrike me të cilën përveç që vërteton identitetin e tij personal si emrin, mbiemrin, shtetësinë, datën e lindjes, vendlindjen, etj. Gjithashtu ajo përmban edhe karakteristika biologjike si shenjat e gishtrinjëve, fytyrën. Në kartelën biometrike të Republikës së Kosovës gjendet edhe certifikata digjitale të cilën qytetarët mund ta shfrytëzojnë për nënshkrime digjitale.

Teknologjitë biometrike janë përcaktuar si metoda të automatizuara për identifikimin dhe verifikimin e identitetit të personave të bazuara në karakteristika biologjike (anatomike dhe fiziologjike) ose të sjelljes. Dokumentet biometrike mund të ofrojnë verifikim shumë të sigurt dhe të përshtatshëm apo identifikim të individit. Këto dokumente janë shumë të vështira për t'u falsifikuar [24].

Karakteristika biologjike është një karakteristikë fizike relativisht e qëndrueshme, të tilla si gjurmë gishtrinjësh, gjeometria e dorës, modeli i irisit, forma e fytyrës dhe struktura e lëkurës, ose modeli i venave të gjakut në dorë. Ky lloj i biometrikut është zakonisht i pandryshueshëm pa ndonjë ndërhyrje.

Karakteristika e sjelljeve është më shumë një reflektim i përbërjes psikologjike të një individi. Modeli i të folurit siguron një metodë për njohjen e folësit dhe është një sjellje biometrike më e zakonshme që përdoret për verifikim. Për shkak se shumë karakteristika të sjelljeve ndryshojnë me kalimin e kohës, një sistem identifikimi ose verifikimi duke përdorur këto duhet të azhurnohet për të regjistruar referenca biometrike të sjelljes.

"Kartela e identifikimit" nënkupton një dokument publik me të cilin shtetasi i Republikës së Kosovës konfirmon identitetin personal, shtetësinë, gjininë, datën e lindjes, vendin e lindjes dhe adresën ku ai/ajo jeton. "Të dhënat biometrike" janë të dhëna unike që paraqesin karakteristikat unike të një personi dhe përdoren për të përcaktuar identitetin përmes pamjes së fytyrës (portreti), gjurmët e gishtërinjëve, ngjyra e syve dhe grupi i gjakut. Të gjitha këto të dhëna janë të ruajtura në mënyrë elektronike në Chip të Integruar të Qarqeve (ICC) në kartelë dhe janë të qasshme nëpërmjet protokolit të komunikimit Near Field Communication (NFC).

4.1 Kartelat e mençura

Kartelat e mençura janë pajisje që përmbajnë çip të integruar, të cilat shërbejnë për transmetim, ruajtje dhe procesim të të dhënave. Të dhënat mund të transmetohen me konektim me kontakt e cila gjendet në sipërfaqe të kartelës ose me fushë elektromagnetike pa përdorim të kontaktit. Kapaciteti i çipit për ruajtje të të dhënave është në rritje e sipër [24].

Megjithatë një nga përparësitë më të rëndësishme të kartelave të mençura është se të dhënat e ruajtura në të mund të mbrohen nga qasja e paautorizuar dhe ndryshimi i tyre. Të dhënat mund të qasen përmes një ndërfaqe seriale që kontrollohet nga sistemi operativ ose logjikës së sigurimit, që nënkupton se të dhënat konfidenciale mund të ruhen në kartelë në një mënyrë që e pengon leximin e kartelës nga jashtë. Këto të dhëna konfidenciale mund të procesohen vetëm nga njësia e procesimit të çipit (chip's processing unit). Në parim mekanizmat softuerik dhe harduerik mund të përdoren për krijimin e kufizimeve në lidhje më përdorimin e funksioneve të memories (leximin, shkrimin dhe fshirjen e të dhënave). Kjo bënë të mundur për të ndërtuar një mori të mekanizmave të sigurisë [24].

Llojet e kartelave të mençura

Smart kartelat mund të ndahen sipas funksionalitetit dhe çmimit në:

- **Memory Cards:** Të dhënat ruhen zakonisht në EEPROM dhe kanë kapacitet të vogël. Këto kartela zakonisht përdoren që vlerën që e posedojnë ta zvogëlojnë pas çdo përdorimi si rasti kur kemi për kartela që i shfrytëzojmë për të telefonuar, të cilat kanë vlerë të caktuar të minutave.
- **Procesor Cards:** Këto kartela kanë kapacitete më të madhe të ruajtjes, siguri të të dhënave konfidenciale dhe aftësinë për të ekzekutuar algoritme kriptografike. Komponenti kryesor i një kartele procesor i njohur zyrtarisht si një mikroprocesor, është procesori, i cili zakonisht është i rrethuar prej katër blloqeve funksionale: ROM (Read Only Memory), EEPROM, RAM (Random Access Memory) dhe I/O (Input/Output).

Kartelat e mençura gjithashtu mund të ndahen sipas transmetimit të të dhënave në [25]:

- **Me kontakt:** e cila gjatë leximit duhet të vendoset brenda lexuesit të kartelës së mençur duke konektuar direkt lexuesin me pjesën kontaktuese (pjesa e artë).
- **Pa kontakt:** kërkohet që kartela vetëm të afrohet pranë lexuesit. Që të dyja edhe kartela edhe lexuesi kanë antena, dhe komunikojnë përmes frekuencave valore (radio frequencies - RF) përgjatë kësaj linje pa-kontakt.

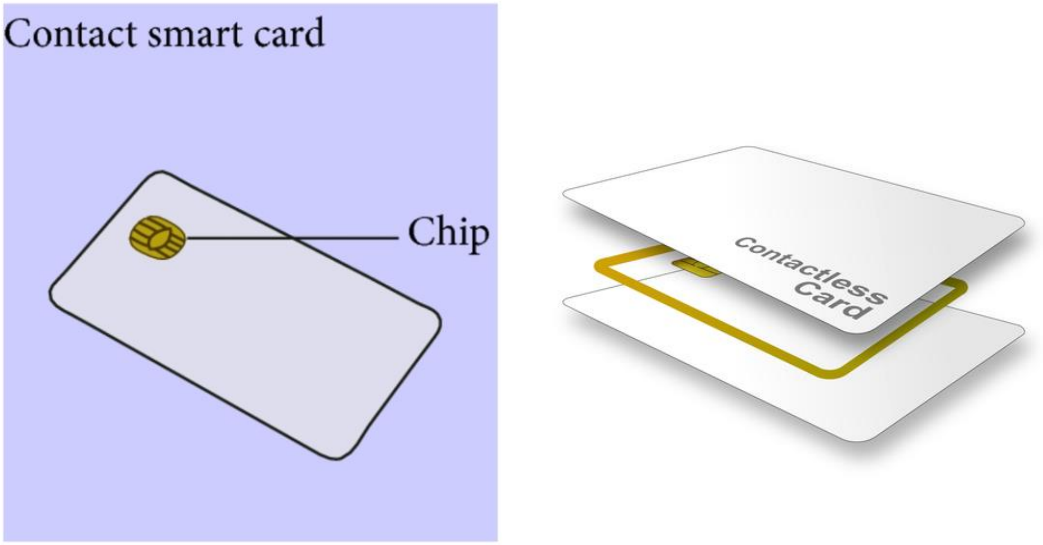


Figura 18: Pamja e karteles së mençur me kontakt dhe pa kontakt [80,81]

Kartelat e mençura në përputhje me standardet ndërkombëtare (ISO/IEC 7816 dhe ISO/IEC 14443) janë në dispozicion në një shumëllojshmëri formash, duke përfshirë kartelat plastike, subscriber identity modules (SIMs) që përdoren për GSM telefonat mobil, USB-based tokens [25].

Kartelat e mençura kanë aplikim të shumtë, duke përfshirë [25]:

- Aplikimi për sigurimin e identitetit - ID për punëtorët, dokumentet identitetit qytetar (ID), pasaporta elektronike, patent shoferi, pajisje për autentikim online.
- Aplikimi në shëndetësi - Karta e identitetit për shëndetësi, kartela e identitetit për mjek, kartela për të dhënat mjekësore.
- Aplikacionet për pagesa - kredit ose debit kartela me kontakt ose pa kontakt, kartela për pagesa transite.
- Aplikimi në telekomunikacion - GSM (Global System for Mobile) SIM (Subscriber Identity Modules), pagesa e shërbimeve të telefonit përmes kartelave.

Kartela e mençur është një pajisje që përmban një çip të integruar të qarqeve (ICC). Kartela është e lidhur me lexuesit me kontakt fizik të drejtpërdrejtë ose ndërhyrje të valëve pa kontakt. Mikrokontrollorët e integruar kanë aftësinë për të mbajtur një numër të madh të të dhënave, për të implementuar funksione të integruara të skedarëve (të tilla si enkriptimi, autentikimi, etj) dhe të ndërveprojnë me lexuesit e kartelave të mençura.

Në kontakt me dokumentet e identifikimit të cilat në shumicën e rasteve përmbajnë të dhëna personale si emri, mbiemri, data e lindjes dhe të dhëna të tjera dhe fotografi, dokumentet elektronike përmbajnë më shumë se të dhënat tjera digjitale, siç janë: certifikatat digjitale, shenjat e gishtrinjëve, ADN-ja, fotografitë digjitale etj. Qasja dhe marrja e të dhënave nga kartela elektronike e identifikimit bëhet përmes protokolit

PACE. Kartelat e mençura mund të vërtetojnë identitetin. Ato shpesh përdorin PKI, ku kartela mban një çertifikatë digjitale të enkriptuar të lëshuar nga PKI së bashku me informacione të tjera relevante.

Sistemet e sigurisë përdorin biometrikët për dy qëllime themelore: Identifikimin dhe Verifikimin.

- Identifikimi - (një-me-shumë ose 1:N)
- Verifikimi - (një-me-një ose 1:1)
- Për më tepër, në kartelën eID janë ruajtur certifikatat e përdoruesit, siç paraqiten në figurën 19, të cilat mund të përdoren për nënshkrim digjital.

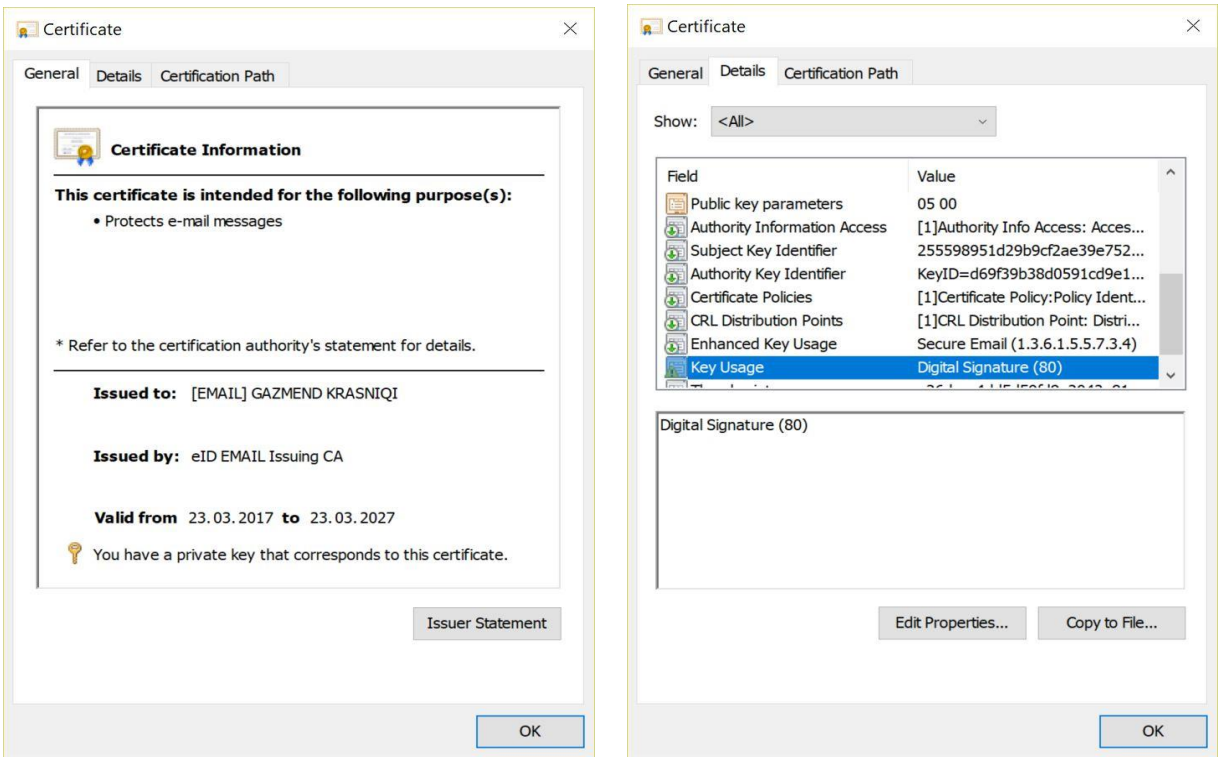


Figura 19: Certifikata X.509 e përdoruesit për nënshkrim digjital

4.2 Sistemi biometrik

Biometrika (ang. Biometrics) është shprehje e përgjithshme, e cila përdoret në mënyrë alternative për të përshkruar karakteristikat ose proceset. Kur përdoret për përshkrim të karakteristikave, shprehja nënkupton karakteristikat biologjike (anatomike dhe fiziologjike) të cilat mund të maten, apo karakteristikat e sjelljes, të cilat mund të shfrytëzohen për njohje.

Në rastin kur shprehja përdoret për përshkrim të procesit, kjo nënkupton metodat e automatizuara për njohjen e personit, bazuar në karakteristikat biologjike (anatomike dhe fiziologjike) ose karakteristikat e sjelljes.

Zbatimi i sistemit biometrik rritet nga dita në ditë, përveç në institucionet shtetërore, dhe në shumë kompani ka filluar përdorimi i sistemeve biometrike për mbrojtje të zonave të ndjeshme etj, p.sh. kompania e Disney World shfrytëzon sistemin biometrik për kartelë sezonale, në mënyrë që të thjeshtësoj hyrjen e klientëve në parqet e tyre, dhe të jenë të sigurt që kartela të përdoret nga personi të i cili është dhënë.

Fushat apo lëmitë në të cilat përdoren sistemet biometrike janë:

a. Shërbimet bankare/financiare/ATM, terminalet për pagesa
b. Sigurinë e teknologjisë së informacionit (paraqitja në sistem, transaksionet përmes internetit)
c. Sigurimet shëndetësore (privatësia e të dhënave)
d. Imigracioni (kontrolli i kufijve)
e. Rendi dhe ligji (ID kartelat, votimet, kontrolli i përdorimit të armëve)
f. Kontrolli i hyrjeve
g. Telekomunikacion
h. Evidenca e kohës së prezencës (kompanitë, shkollat etj).

Sistemi biometrik në thelb është njohja sipas mostrës (*ang. Pattern Recognition System*) i cili njohjen e personit e bënë në mënyrë automatike në bazë të karakteristikave biologjike autentike dhe karakteristikave të sjelljes të cilat i ka personi.

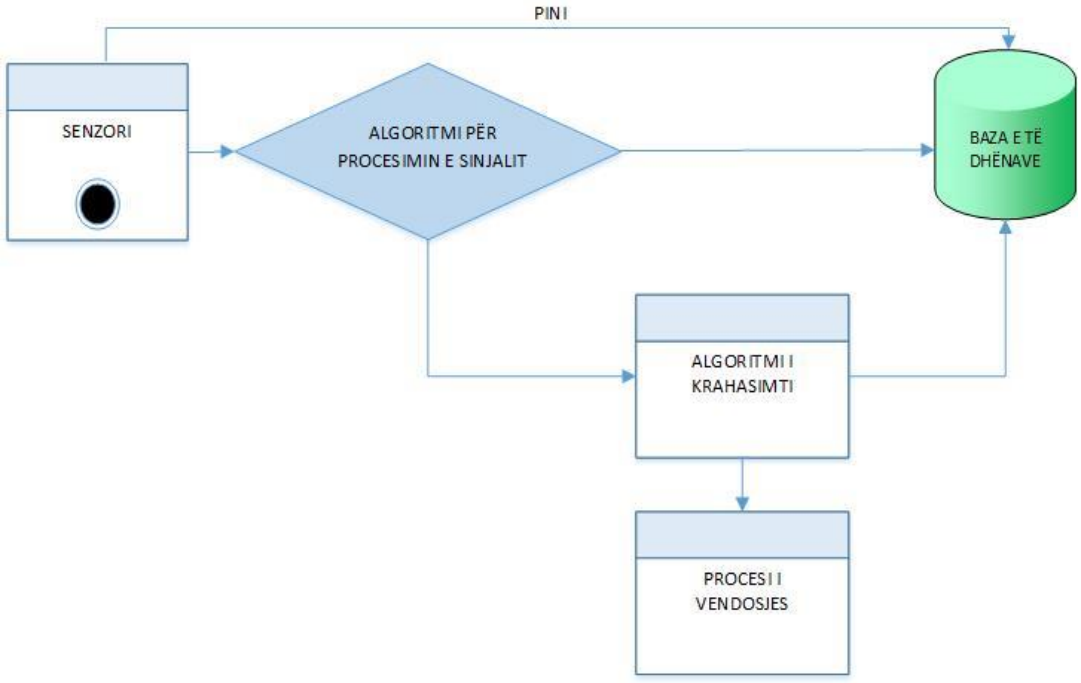


Figura 20. Modeli i përgjithshëm i sistemit biometrik

Komponentët e sistemit biometrik dhe proceset

Katër komponentët kryesore që prezantohen zakonisht në një sistem biometrik janë [24]:

- Mekanizmi për skanim dhe marrjen e një përfaqësimi digjital të karakteristikave biometrike të personit.
- Programi për procesimin e të dhënave të papërpunuara në një format që munden të përdoren për ruajtje dhe krahasim.
- Programi për krahasim që të krahasoj të dhënat e mëhershme biometrike me të dhënat e modelit të tashëm.
- Një ndërfaqe me sistemin e aplikacionit për të treguar rezultatin e krahasimit.

Dy faza të ndryshme përfshihen në procesin e sistemit biometrik - regjistrimi dhe krahasimi [24]:

Regjistrimi - mostra biometrike e individit merret gjatë procesit të regjstrimit (p.sh. duke përdorur senzorët e shenjave të gishtërinjëve, mikrofonin për njohje të zërit, kamerën për njohje të fytyrës, kamerën për njohje të irisit). Karakteristikat unike pastaj ekstraktohen nga mostra biometrike (p.sh. imazhi) për të krijuar shabllonin biometrik të përdoruesit. Ky shabllon biometrik ruhet në bazë të dhënave të sistemit apo kartelë për përdorim të mëvonshëm gjatë procesit të krahasimit e prezentuar si në figurën 21.

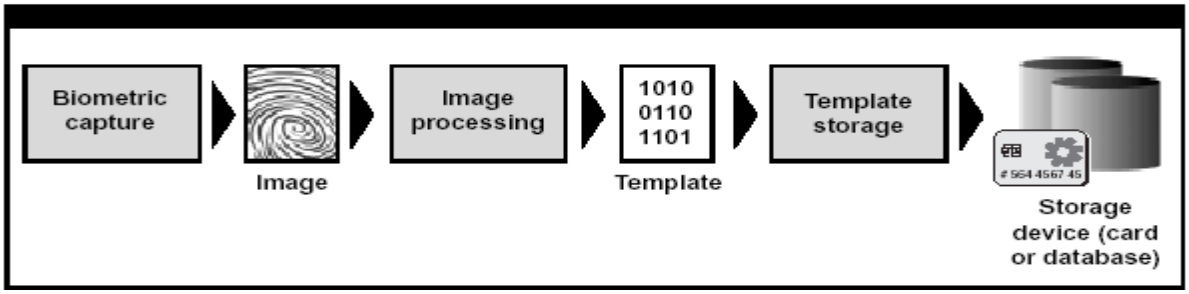


Figura 21. Procesi i regjistrimit të dhënave biometrike [24]

Krahasimi – Mostra biometrike merret përsëri. Karakteristikat unike ekstraktohen nga mostra për të krijuar shabllonin biometrike "direkt" të përdoruesit. Ky shabllon i ri pastaj krahasohet me shabllonet paraprake të ruajtura dhe gjenerohet një rezultat numerik i krahasimeve (i ngjajshmërive) në bazë të elementeve të përbashkëta mes dy shablloneve.

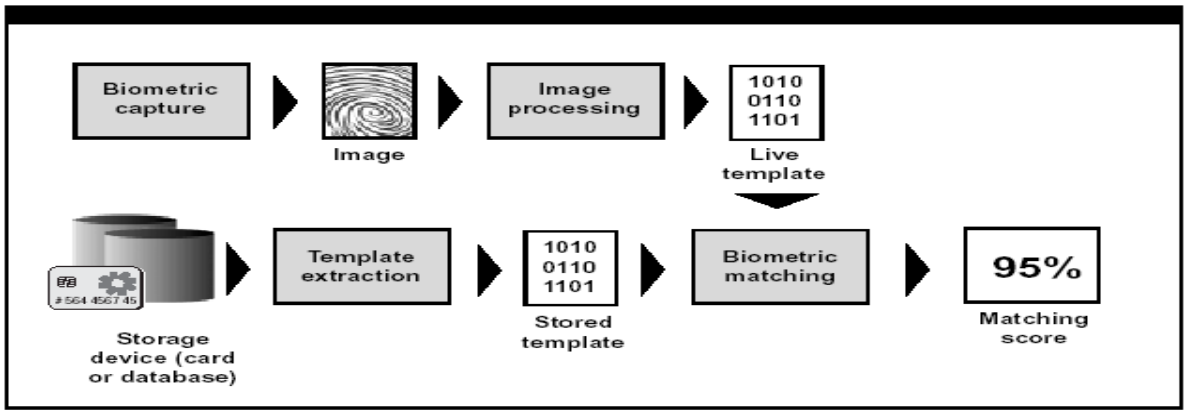


Figura 22: Procesi i verifikimit të dhënave biometrike

Sistemet e sigurisë përdorin biometrikët për dy qëllime bazike: identifikimin dhe verifikimin [24].

Identifikimi – (një-me-disa apo 1:N) përcakton nëse personi ekziston brenda popullatës së regjistruar duke krahasuar shabllonët e ruajtur në sistem.

Verifikimi – (një me një apo 1:1) përcakton nëse shablloni biometrik përshtatet me një shabllon të regjistruar.

Roli i teknologjisë së kartelave të mençura me biometrikët

Kartelat e mençura njihen si formate elektronike të identifikimit më të sigurta dhe të besueshme. Për të ofruar shkallën më të lartë të konfidencialitetit në verifikimin e identitetit, teknologjia biometrike konsiderohet të jetë esenciale në dizajnin e sistemit të identifikimit të sigurt. Kombinimi i teknologjisë së kartelave të mençura me biometrikët ofrojnë mënyrën e krijimit të lidhjes pozitive të kartelës së mençur me mbajtësin e tyre duke mundësuar verifikim dhe autentikim të fortë të identitetit të mbajtësit [24].

Procesimi i biometrikëve

Procesimi i biometrikëve konsiston në dy detyra sekuenciale të ndara. E para, shablloni biometrik "direkt" i përdoruesit duhet të ekstraktohet dhe procesohet. E dyta, shablloni direkt duhet të krahasohet me shabllonin e ruajtur të besueshëm. Ekstraktimi i shabllonit biometrik është detyrë intensive e procesorit. Një ekstraktim i shabllonit të gishtërinjëve, për shembull kërkon rreth dhjetë herë me shumë mund të procesimit se sa një krahasim i shablloneve të gishtërinjëve një me një.

Memoria që përdoret për deponimin e instruksioneve të nevojshme në kartelën e mençur është EEPROM e cila mundëson ruajtjen e të dhënave pa pasur nevojë që të jetë e kyçur në furnizim ku mund të programohet duke ndryshuar kodin që e ekzekuton procesori dhe mund të ndryshohen të dhënat që janë të deponuara në të. Sistemi operativ i depononuar në memorie hynë në funksion në momentin kur kartela biometrike i afrohet

terminalit lexues. Furnizimi me rrymë i kartelës bëhet duke u tranferuar energjia nga fusha magnetike që krijohet kur ajo afrohet në terminalin lexues [26].

Procesorët e kartelave të mençura janë të aftë për performimin e krahasimit biometrik, dhe ekstraktimin e shabllonit direkt në kartelë. Dy çasjet e implementimit kryesor të kartelave të mençura dhe biometrikëve janë "match-off-card" dhe "match-on-card" [24].

Match-off-card - shablloni i regjistruar në fillim ngarkohet në kartelën e mençur dhe pastaj transferohet nga kartela përgjatë ndërfaqës me kontakt apo pa kontakt kur kërkohet nga sistemi i jashtëm biometrik. Pajisja e jashtme pastaj krahason shabllonin biometrik të ri me atë të marrur nga kartela (pajisja e jashtme mund të jetë lexues apo sistem kompjuterik qëndror). Me këtë teknikë, kartela e mençur ruan shabllonët, po nuk është në dijeni për tipin e informatave biometrike, dhe mundësinë e procesimit të tyre. Ky implementim është i përshtatshëm për gjitha tipet e kartelave të mençura, do të funksionoj me memorie, logjikën e telave apo kartela të mençura të bazuara në mikrokontroller.

Match-on-card – Ky implementim së pari ruan shabllonin në memorie të kartelës. Kur kërkohet krahasimi biometrik, pajisja e jashtme dorëzon një shabllon të ri te kartela. Pastaj kartela përformon operacionin e krahasimit në procesorin e tij dhe komunikon rezultatitn te pajisja e jashtme. Me këtë teknikë, kartela e mençur duhet të jetë një pajisje e bazuar në mikrokontroller dhe të jetë e aftë për llogaritjen e krahasimit një me një.

4.3 Të dhënat biometrike

Edhe të dhënat biometrike të papërpunuara (zakonisht një imazh bitmap) apo një shabllon i ekstraktuar mund të ruhet në kartelë. Për qëllimin e krahasimit, përdoret vetëm shablloni. Ruajtja e të dhënave biometrike të papërpunuara kërkon më shumë memorie. P.sh. një imazh komplet i shenjave të gishtërinjëve kërkon 50 deri 100 Kbyte, derisa një shabllon i shenjave të gishtërinjëve kërkon 300 byte deri 2 Kbyte. Kështu që shumica e kartelave bazohen në ruajtjen e shabllonëve e jo të imazheve.

Ruajtja e të dhënave biometrike në kartelë ofron rritje të privatësisë dhe mundësinë për të bartur informatat e tij sigurt me vete mbajtësi i kartelës.

4.4 Teknikat dhe teknologjitë e sistemeve biometrike

Ne kemi deklaruar tashmë se ekzistojnë dy lloje të karakteristikave biometrike. Kështu që, teknikat për autentikim biometrik janë zhvilluar duke u bazuar në këto karakteristika. Detajet e teknikave të ndryshme janë diskutuar më poshtë.

Teknologjia për njohjen e shenjave të gishtërinjëve

Autentikimi me mënyrën e shenjave të gishtrinjëve është shumë i thjeshtë. Së pari shfrytëzuesi lajmërohet në sistem dhe jep mostrën e vetë të shenjës. Senzori e skanon gishtin, fotoja e fituar me algoritme të caktuara përpunohet dhe vendoset në fajll në sistem kompjuterik kryesor apo në procesor lokal tek pajisjet mobile. Shënimi i ruajtur paraqet të ashtuquajturin shabllonin e shenjës së gishtit të personit. Gjatë verifikimit të shenjës shënimet mbi shenjën përmes algoritmit krahasohen me shënimet e ruajtura më parë dhe si përgjigje fitohet përputhja me shenjën apo mospërputhja. E gjithë procedura kryhet me shpejtësi 1-2 sekonda.

Ekzistojnë dy ecuri themelore me rastin e analizës së shenjës së gishtit. E para i analizon kryqëzimet dhe përfundimet e vijave të shenjës, derisa e dyta e përcjell drejtimin e tërësishëm të secilës vijë (linjë).

Shenja e skanuar me metodën e parë kap diku rreth 250KB. Mirëpo ekziston edhe dallimi i shpejtësisë së njohjes së shenjës pasi me metodën e parë krahasohen disa pika karakteristike, derisa me metodën e dytë krahasimi kryhet komplet në bazë të të dhënave e që mund të zgjasë me orë apo ditë.

Janë teknologji të ndryshme me të cilat skanohet shenja e gishtit dhe ajo më së shpeshti bazohet në senzor kapacitiv, optik apo senzor me ultrazë.

Teknologjia e njohjes së fytyrës

Siç është theksuar më parë, çdo fytyrë ka karakteristikat e veta të veçanta të cilat mundësojnë njohjen e saj. Karakteristikat e fytyrës mund të ndahen dhe të shfrytëzohen më vonë për identifikimin e të cilat quhen detaje kyçe.

Ekzistojnë rreth 80 detaje kyçe në fytyrën e njeriut, disa detaje të tilla janë:

- Distanca ndërmjet syve
- Gjerësia e hundës
- Thellësia e gropave të syve
- Mollëza e fytyrës
- Madhësia e fytyrës
- Madhësia e linjave
- Mjekra etj

Detajet kyçe maten dhe formohet kodi numerik gjegjësisht një varg numrash të cilat paraqesin fytyrën në bazën e të dhënave "*faceprint*". Algoritmet për njohjen e fytyrës nuk shfrytëzojnë 80 detaje kyçe. P.sh. softueri Visionics Faceit i shfrytëzon 14 deri 22 detaje kyçe.

Sikurse edhe te sistemet tjera identifikuese biometrike edhe këtu dallohen proceset e regjistrimit, verifikimit dhe identifikimit.

Faza e regjistrimit zgjat zakonisht 20 deri 30 sekonda, gjatë të cilit merren disa foto të fytyrës së njëjtë. Pas marrjes së fotos, ndahen veçoritë karakteristike të fytyrës dhe krijohet *Faceprint*.

Ekzistojnë algoritme të ndryshme për njohje të fytyrës, kryesisht të gjitha përmbajnë këto faza:

- Faza e detektimit
- Faza e akordimit
- Normalizimit
- Faza e kodimit
- Faza e krahasimit

Në fazën e detektimit softueri për njohje të fytyrës e kërkon fytyrën në fushën e dukshme të kamerës. Kur detektohet forma e cila i përngjan formës së kokës së njeriut, softueri vendos kamerën në regjim të punës me rezolucion të lartë. Besueshmëria e identifikimit varet nga kualiteti i fotos.

Pas fazës së detektimit kalohet në fazën e akordimit. Në këtë fazë caktohet pozicioni, madhësia dhe orientimi i kokës, pastaj kalohet në pasqyrim 3D të kokës në foto jofrontale dydimensionale. Në fund fotoja jofrontale dydimenzionale në foto frontale 2D.

Numri më i madh i sistemeve për njohje të fytyrës bëhet me të ashtuquajturin "*foto statike*" ku me foto statike nënkuptohet fotoja frontale, me theks normal të fytyrës së njeriut. Në krahasim te shfrytëzimi i "*fotos së gjallë*" kjo në vend të parë e zvogëlon shumë madhësinë e kodit numerik me të cilin paraqitet fotoja në bazë të dhënave. Që të fitohet fotoja statike pas fazës së akordimit është e nevojshme të normalizohet në foto frontale.

Me normalizim nënkuptojmë teknikën statike me të cilën kryhet korrektimi i dallimeve të fytyrës së të njëjtit person nga foto të ndryshme. Korrektimet normalizuese deri diku i zvogëlojnë dallimet mes fotove të ndryshme. Edhe testimet e deritashme kanë treguar që sistemet për identifikim që e shfrytëzojnë për identifikim ashtuquajturin "*foto e gjallë*" nuk kanë treguar rezultate të dobishme.

Pas fazës së normalizimit qasemi në fazën e kodimit, e cila është kyçe për njohje të personit. Në fazën e kodimit bëhen matje, gjegjësisht i detajeve kyçe me foto të normalizuara frontale 2D të fotos së kokës në kod digjital unik.

Teknologjia IRIS

Sikurse te skanimi i retinës së syrit, skanimi i iridës bazohet në analizë të veçantë të unazës së saj me ngjyrë e cila rrethon irisin. Irida e syrit është muskulaturë e ngjyrosur e cila e rrethon irisin. Irida përmban rreth 200 detaje të cilat mund të përdoren për krahasim dhe identifikim siç janë: unazat, kanalet dhe njollat. Këto larmi janë të veçanta për çdo njeri, si dhe dallojnë nga ana e djathtë me të majtën. Për këtë arsye kjo metodë mund të përdoret me sukses për identifikim e jo vetëm për verifikim. Për incizim të iridës është e

mjaftueshme vetëm kamera e thjeshtë. Algoritmi i Daugmanov-it siguron skanime me 3-4 bita për milimeter katror (rrezja e iridës është rreth 11 milimetra).

Te skanimi i iridës shfrytëzohet individualiteti i enëve të gjakut në sy. Kjo formë e identifikimit është më e përshtatshmja nga të gjitha metodat biometrike, pasi që nuk ka mundësi që irida të falsifikohet, ajo nuk ndryshon gjatë tërë jetës së njeriut, ndërsa irida e të vdekurit shkatërrohet aq shpejt, andaj nuk është e nevojshme vërtetimi a është gjallë personi apo jo.

Teknologjia e njohjes së zërit

Njohja e zërit është teknologji biometrike e cila shpesh përdoret tek sistemet të cilat komandohen pa përdorim të duarëve siç është hand-free tek telefonat mobil. Verifikimi i zërit bazohet në krahasimin e shënimeve akustike me incizimin e mëhershëm dhe ka për qëllim që të caktoj për cilin njeri bëhet fjalë. Te verifikimi i njohjes së zërit shënohet ritmi, frekuenca, lartësia, tonaliteti i zërit etj. Për incizim të zërit mund të shfrytëzohet edhe mikrofoni i thjeshtë i telefonit, edhe pse besueshmëria e skanimit rritet me përdorim kualitativ të mikrofonave. Kjo kryesisht nuk është metodë e besueshme, për këtë shfrytëzohen për qëllime verifikuese ndërsa jo për qëllime identifikuese.

Koha e verifikimit është deri 5s, madhësia e fituar e incizimit të zërit është e rendit 2-10kb. Për të ikur falsifikimit tek shfrytëzimi i incizimit, sistemi kërkon njëkohësisht edhe frekuenca të larta dhe të ulëta të zërit, pasi që te shumica e incizimeve vështirë mund të reprodukohen, saktësisht ato mund të gjenden vetëm në zërin natyral. Te disa sisteme kërkohet nga konsumatori të thuhet një varg numrash.

Përparësia e kësaj metode është përdorimi i pajisjeve të lira dhe kompjuter të përditshëm me një softuer të caktuar mundet të shfrytëzohet si platformë për njohje të zërit. Mirëpo për shkak nivelit të ulët të besueshmërisë të njohjes së zërit, kombinohet me ndonjë metodë biometrike tjetër plotësuese më të besueshme.

Faktorët themelor të cilët mund të ndikojnë në gabime gjatë autentikimit janë:

- Vitet - zëri mund të ndryshoj me kohë.
- Sëmundjet - zëri ndryshon te personat në rast se janë të sëmurë.
- Akustika - varet nga ambienti në të cilin realizohet autentikimi.
- Thënja gabim e fjalëve të përcaktuara, të definuara më herët.
- Emitimi i gjendjes së përkeqësuar të njeriut me të cilin gjendet p.sh. stresi apo brengosja.
- Pozita apo largësia nga mikrofoni si dhe përdorimi i mikrofonit tjetër.

Teknologjia e njohjes së zërit sot më së shpeshti përdoret tek sistemet në të cilat kërkohet identifikimi në largësi. Si shembull mund të merren qendrat automatike të thirrjeve dhe sistemet për përpunimin e transaksioneve përmes telefonit apo sistemit kompjuterik.

Aplikacionet më popullore nga kjo lëmi janë tek transaksionet financiare (qasje tek llogaritësit, transferi i mjeteve, pagesa e çeçeve) dhe mbështetja në sigurinë e biznesit me kartelë kreditore.

4.5 Siguria e sistemeve biometrike

Teknologjia biometrike përdoret me teknologjinë e kartelave të mençura për sistemin e ID-ve, posaqërisht për shkak të aftësisë së tyre për identifikimin e njërëzve. ID-a biometrike lejon verifikimin se "kush ju pretendoni të jeni" (informata të shtypura në kartelën e mbajtësit të saj), bazuar në "kush jeni ju" (informatat biometrike të ruajtura në kartelë), duke shtuar se "çfarë dini ju" (p.sh. PIN-in) [24].

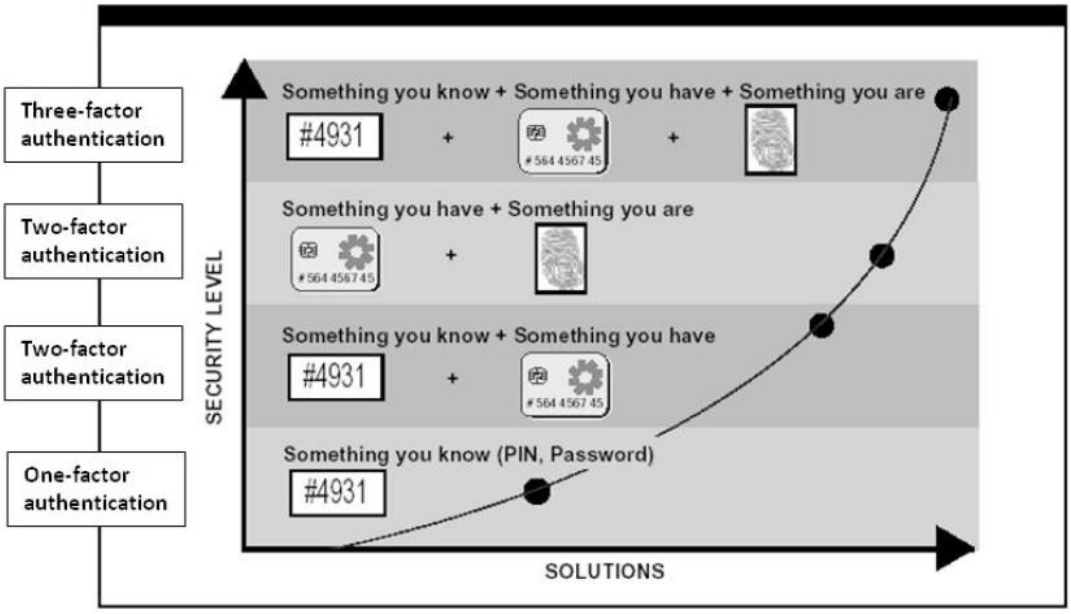


Figura 23: Ndikimi i kartelës së mençur dhe biometrikëve në siguri [24]

Fjalëkalimi CAN përdoret si hyrje në procedurën e shkëmbimit të sigurt të çelësave në protokolin PACE. CAN kërkohet në momentin kur arrihet komunikimi fillestar mes terminalit dhe letërnjoftimit. CAN është fjalëkalim i cili nuk bllokohet pas një numri të caktuar të tentimeve. Ky fjalëkalim është informatë që e posedojnë terminali dhe lexuesi i cili shërben si çelës për enkriptimin e të dhënës që përdoret në fund të protokolit për gjenerimin e çelësave të shkëmbyer të sesionit mes dy palëve.

Biometrika posedon fuqinë për dhënje të sigurisë tek shumica e aplikacioneve. Tani biometrika përdoret për mbrojtje të kompjuterëve, terminaleve ATM, transakcioneve dhe kartelave për pagesë, e-transakcionet e aeroportit, paisjet nukleare dhe kufijve

ndërkombëtar. Por nëse sistemi biometrik ka rolin e rritjes së sigurisë, ai si dhe çdo sistem tjetër i ka edhe të metat e veta.

Ndërhyrjet në nivel të hyrjes

Ka të bëjë me fazën e inçizimeve të mostrave dhe fillimit të përpunimit. Dy forma themelore të ndërhyrjes janë mashtrimi (*ang. spoofing*) dhe tejkalimi (*ang. bypassing*). Te këto dy forma, është rast i shpeshtë i krijimit i tejngarkesës (*ang. overloading*), duke dëmtuar paisjen hyrëse dhe detyrimin që të gjeneroj gabime. Si shembull mund të merret lidhja e shkurtër apo lagështia e senzorit të gjysmëpërçuesve ose vendosja në dritë të fort e senzorit të shenjave apo vizatimit të fytyrës.

Ndërhyrja në nivel të përpunimit dhe transmetimit të të dhënave

Kjo formë e ndërhyrjes gjithashtu e tërhjek vëmendjen. Si shumë sisteme biometrike foton apo shabllonin e shënimeve e dërgon kah sistemi kompjuterik lokal, për përpunim. Është e rëndësisë së madhe që ky transmetim të mos ndërpritet që të mos jetë i lexueshëm dhe të mos ndryshohet.

Autentikimi shumë-faktorësh mund të paraqitet në dy forma, kombinim i shumë metodave në dy forma, si kombinim i shumë metodave biometrike apo kombinim i biometrikës dhe kartelave memorizuese ose PIN-it. Të dyja metodat e zvogëlojnë mundësinë e autentikimit të pa dëshirueshëm. Spoofing-u mbetet me kohë më i kërkuari dhe sfidues nëse është nevoja të kopjohen apo të imitohen shumë karakteristika njerëzore.

Një prej teknikave të reja për dobësim të paisjeve të ndërhyrjes është koncepti i IBM-it i ashtuquajtur fshirjes (anulimit) të sitemit biometrik. Koncepti parasheh përdorimin e algoritmit i cili fut algoritme në shabllonin e ruajtur. Në rastin e shkatërrimit të integritetit të shabllonit, shablloni largohet nga lista e tyre të cilëve u lejohet qasja dhe konsumatori legal mund të lajmërohet përsëri dhe kështu krijohet shablloni i ri me deformime shtesë. Fotoja origjinale nuk ruhet kurrë. Derisa algoritmi i mbrojtur mirë dhe i ndryshëm varësisht prej kompanisë apo edhe vetë sistemit, kjo zgjidhje dërgon kah zvogëlimi i dëmeve eventuale. Zgjidhja kurrë nuk është plotësisht e sigurt. Nëse vie deri te fotoja origjinale, teoritikisht është e mundshme të kryhet lajmërimi i sërishëm me gjenerim të shabllonit të ri të deformuar. Edhe përveç kësaj, kreacioni i fshirjes (anulimit) të sistemit biometrik është hap në rrugë të mbarë.

Pika	Kërcimet	Kundërmasat
1.Grumbullimi i të dhënave	Mashtrimet	Kontrolli gazmor
	Përdorimi i paisjeve jo të besueshme	Autentikimi reciprok i paisjes dhe serverit
	Mbingarkesa	Përdorimi i paisjeve të forta

2. Transmetimi i të dhënave origjinale	Përgjimet	Trasnferimi i të dhënave të koduara autentikimi reciprok, përdorimi i çelësit simetrik
	Sulmi kthyes	Të dhënat e nënshkrimit digjital, përdorimi i etiketës TTL
	Njeriu në mes	Të lidhet biometrika me PKI
	Sulmi me gjitha forcat	Përdorimi i politikës time out/lock out
3.Përpunimi i sinjalit	Futja e të dhënave të rrejshme	Përdorimi i algoritmit të fuqishëm
4.Transmetimi i të dhënave të përpunuara	Përgjimet	Trasnferimi i të dhënave të koduara autentikimi reciprok, përdorimi i çelësit simetrik
	Sulmi kthyes	Të dhënat e nënshkrimit digjital, përdorimi i etiketës TTL
	Njeriu në mes	Të lidhet biometrika me PKI
	Sulmi me gjitha forcat	Përdorimi i politikës time out/lock out
5.Krahasimi	Futja e të dhënave të rrejshme	Përdorimi i algortimit të fuqishëm
6.Marrja mostrës	Përgjimi	Trasnferimi i të dhënave të koduara autentikimi reciprok, përdorimi i çelësit simetrik
	Kundër sulmi	Të dhënat e nënshkrimit digjital, përdorimi i etiketës TTL
	Njeriu në mes	Të lidhet biometrika me PKI
	Sulmi me gjitha forcat	Përdorimi i politikës time out/lock out

7.Ruajtja	Kompromitimi i bazës së të dhënave	Mbrojtja e fuqishme e serverit me anë të shifrimit për vendosjen e shabllonit. Vendosja e shabllonit në kartelat e mençura ose paisje tjera të ngjashme
8.Paraqitja e rezistencës krahasuese	Sulmi "Hill climbing"	Rritja e feedback-ut
9.Vendimi	Sulmi "Hill climbing"	Rritja e feedback-ut
10.Komunikimi me aplikacion	Përgjimi	Trasnferimi i të dhënave të koduara, autentikimi reciprok, përdorimi i çelësit simetrik
11.Aplikacioni	Kodi qëllimkeq (malicious code)	Respektimi i standardeve (BioAPI, CBEFF)

Tabela 5. Pikat e dobëta të sistemit biometrik

4.6 Korniza ligjore (BE dhe Kosovë)

4.6.1 Legjislacioni i BE-së për nënshkrimin elektronik

Historia e kornizës ligjore të BE-së lidhur me nënshkrimin elektronik ka historinë nga viti 1999 kur edhe është aprovuar direktiva e parë lidhur me këtë fushë.

Direktiva e eSignature (1999/93 / KE)

Kjo direktivë është aprovuar në vitin 1999 dhe ka hyrë në fuqi në vitin 2000 duke krijuar bazën ligjore për nënshkrimin elektronik në BE. Deri në vitin 2000, vetëm nënshkrimet e shkruara me dorë ishin ligjërisht të vlefshme.

Direktiva e nënshkruar krijoi kuadrin ligjor në nivel evropian për nënshkrimet elektronike dhe shërbimet e certifikimit. Qëllimi ishte të ofronte sigurinë dhe integritetin ligjor të komunikimit që ndodh në internet duke i bërë nënshkrimet elektronike më të lehta për t'u përdorur dhe të njohura ligjërisht brenda Bashkimit Evropian. Direktiva nuk favorizoi asnjë teknologji specifike.

Direktiva e eSignature u shfuqizua më 1 korrik 2016, kur hynë në fuqi rregullat për shërbimet e besimit sipas rregullorës eIDAS.

Vendimi i Komisionit 2003/511/KE i 14 korrikut 2003 mbi publikimin e numrave referencë të standardeve përgjithësisht të njohura për produktet e nënshkrimit elektronik në përputhje me Direktivën 1999/93/EC të Parlamentit Evropian dhe të Këshillit.

Vendimi i Komisionit 2000/709/KE i 6 nëntorit 2000 mbi kriteret minimale që duhet të merren parasysh nga shtetet anëtare kur përcaktohen organet në përputhje me Nenin 3 (4) të Direktivës 1999/93/KE të Parlamentit Evropian dhe të Këshillit në një kornizë të komunitetit për nënshkrimet elektronike.

Direktiva e Shërbimeve (2006/123/KE) [67]

Direktiva e shërbimeve krijon bazën për përdorimin e nënshkrimin elektronik në tërë shtetet anëtare të Bashkimit Evropian dhe duhet të pranohen të gjitha nënshkrimet elektronike të nënshkruara në shtetet e BE-së.

Kuadri i ri ligjor siguron siguri ligjore për përdorimin ndërkufitar të nënshkrimeve elektronike, e-seal, pullave kohore, shërbimit të dërgimit elektronik dhe certifikatave të vërtetimit të internetit [68].

Të gjitha shtetet anëtare kanë një pikë të kontaktit të vetëm, për të lehtësuar krijimin e lirë të ofruesve të shërbimeve dhe ofrimin e shërbimeve falas në Bashkimin Evropian. Kuadri i ri ligjor në fuqi në Bashkimin Evropian është rregullorja eIDAS.

Rregullorja eIDAS (910/2014 KE) [69]

Kuadri i ri ligjor krijon bazë dhe siguri ligjore për përdorimin ndërkufitar të nënshkrimeve elektronike, e-vula, pullave kohore, shërbimit të eDelivery dhe certifikatave të vërtetimit të internetit. Disa nga ndryshimet kryesore të paraqitura nga rregullorja eIDAS janë:

- Është një rregullore, jo një direktivë, duke e bërë atë direkt të zbatueshme në të gjithë Europën pa nevojën e transpozimit në legjislacionin kombëtar,
- Duke hapur rrugën për zgjidhje të reja të identifikimit të largët të kualifikuar dhe përvoja e përmirësuar e përdoruesit,
- Një harmonizim pan-europian i nënshkrimit elektronik,
- Dokumenteve elektronike nuk mund të mohohet efekti juridik vetëm për shkak se ato janë në formë elektronike etj.

Organet e mëposhtme të BE-së aktualisht menaxhojnë eSignature CEF [70]:

- Drejtoria e Përgjithshme e Komisionit Evropian për Informatikë (DG DIGIT) është përgjegjëse për menaxhimin teknik të CEF eSignature.
- Drejtoria e Përgjithshme e Komisionit Evropian për rrjetet, përmbajtjen dhe teknologjinë e komunikimit (DG CNECT) është përgjegjëse për zbatimin e politikave të BE-së që lidhen drejtpërdrejt me eSignature.

- Agjencia Ekzekutive e Inovacionit dhe Rrjeteve (INEA) është përgjegjëse për zbatimin e granteve të programit CEF Telecom në bashkëpunim me Komisionin Europian.

4.6.2 Legjislacioni i Kosovës për nënshkrimin elektronik

Nënshkrimet elektronike në Republikën e Kosovës rregullohen me Ligjin Nr. 04/L-094 „për shërbimet e shoqërisë informatike“ i miratua në 15 mars 2012 [71].

Neni 1 Pika 1

Ky ligj përcakton se dokumentacioni në formë elektronike është juridikisht i barabartë me dokumentacionin tradicional të paraqitur në format të letrës, për të lehtësuar shërbimet elektronike që përfshijnë, por që nuk kufizohen në shitblerje që bëjnë konsumatorët nëpërmjet internetit (eTregtia), shërbimet elektronike bankare dhe ato financiare (ePagesa), ofrimin e shërbimeve qeveritare (eQeverisja), blerjen në formë elektronike nga ndërmarrjet (eProkurimi) dhe aplikimin e nënshkrimit elektronik.

Me këtë ligj të gjitha format e reja të komunikimit, transmetimit dhe nënshkrimit elektronik do të jenë të barasvlefshme me format e vjetra ose tradicionale të transmetimeve të dhënave, nënshkrimeve klasike ose me dorë.

Ky ligj është në përputhje me kornizën ligjore të Bashkimit Evropian. Fushëveprimi i nënshkrimit elektronik që përfshijnë, por që nuk kufizohen vetëm në administratën publike por edhe në atë private dhe është ligjërisht i pranuar njëjtë si forma e vjetër.

Ky ligj i parasheh:

- Nënshkrimi elektronik Neni 1 pika 1.18 dhe
- Nënshkrimi elektronik i avancuar Neni 1 pika 1.19

Neni 6 pika 1 nënshkrimin elektronik është i barasvlershëm me nënshkrimin me dorë dhe të gjitha organet ose institucionet të cilat kërkojnë nënshkrimin e personit, do ta pranojnë nënshkrimin elektronik dhe si i tillë do të ketë efekt ligjor.

Autoriteti apo organi i pavarur rregullator i themeluar sipas Ligjit të Telekomunikacionit, për të rregulluar dhe për t’u kujdesur për zhvillimin e sektorit të telekomunikacionit në Kosovë është Autoriteti Rregullativ i Telekomunikacionit (ART).

4.7 Nënshkrimi digjital

Lloji i kriptografisë me çelës publik që përdoret për të simuluar vetitë e sigurisë të një nënshkrimi në formë digjitale, më mirë se në formë të shkruar. Skemat e nënshkrimit digjital normalisht japin dy algoritme, një për nënshkrim e cila përfshinë çelësin privat të përdoruesit dhe një për verifikimin e nënshkrimeve që përfshinë çelësin publik të përdoruesit. Rezultati i procesit të nënshkrimit quhet "nënshkrimi digjital".

Është një nënshkrim elektronik që mund të përdoret për të vërtetuar identitetin e dërguesit të një mesazhi ose nënshkruesi të një dokumenti dhe ndoshta për të siguruar që përmbajtja origjinale e mesazhit ose dokumentit që është dërguar është e pandryshuar.

Nënshkrimet digjitale janë lehtësisht të transportueshme, nuk mund të imitohen nga dikush tjetër dhe mund të automatikisht të shtypen me kohë. Aftësia për të siguruar që mesazhi origjinal i nënshkruar arrin do të thotë se dërguesi nuk mund ta refuzoj lehtë atë më vonë.

Nënshkrimi digjital paraqet një analogji të nënshkrimit me dorë, në fakt ofron garanci më të fort të sigurisë. Nënshkrimi digjital shërben si një vegël e fuqishme, e pranuar ligjërisht në shumë shtete. Mund të përdoren për nënshkrimin e kontratave, dokumenteve, autenticitetin e individëve ose kompanive dhe si komponent e shumë protokoleve komplekse. Gjithashtu nënshkrimi digjital përdoret për transmetimin e çelësit publik në mënyrë të sigurt. Pra nënshkrimi digjital përdoret për të ruajtur autenticitetin e mesazhit ose dokumentit të dërguar në mënyrë elektronike. Verifikimi i nënshkrimit bëhet për të vërtetuar autenticitetin e dokumentit [27].

Skema për të krijuar dhe verifikuar një nënshkrim digjital (paraqitur edhe në figurën 24):

- Dërguesi së pari gjeneron çelësin publik dhe privat me ndonjë algoritëm, zakonisht çelësat i krijon autoriteti certifikues përkatës që më pas krijon edhe një certifikatë digjitale.
- Dërguesi nënshkruan dokumentin (mesazhin) me çelësin e tij privat, më detajisht nënshkruesi e enkripton me çelësin e tij privat vlerën e hash-it të krijuar nga dokumenti (mesazhi) dhe kështu krijohet nënshkrimi digjital i tij.
- Dërguesi e dërgon dokumentin (mesazhin) e nënshkruar te pala tjetër, i cili fillimisht bënë verifikimin e nënshkrimit.
- Marrësi bënë verifikimin e nënshkrimit digjital të dokumentit (mesazhit) duke përdorur çelësin publik të nënshkruesit (dërguesit). Në mënyrë më të detajuar, marrësi duke përdorur çelësin publik të dërguesit që e merrë nga certifikata e tij, bënë dekriptimin e vlerës së nënshkrimit, që në fakt është vlera e enkriptuar e hash-it. Pas dekriptimit vlerën e fituar e krahason me vlerën që e fiton nga llogaritja e hash-it të dokumentit të pranuar nëse këto vlera janë të barabarta nënshkrimi rezulton i suksesshëm.

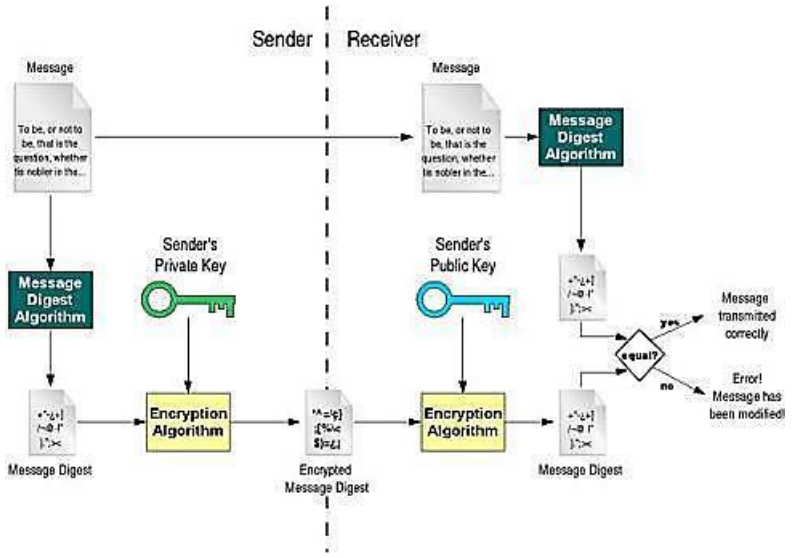


Figura 24: Nënshkrimi digjital dhe verifikimi i tij [28]

Një nënshkrim digjital i vlefshëm i jep arsye marrësit për të besuar se mesazhi i krijuar është nga një dërgues i njohur, dërguesi nuk mund të mohoj dërgimin e mesazhit (autenticiteti dhe jo-mohushmëria) dhe se mesazhi nuk ka ndryshuar gjatë rrugës (integriteti).

Si funksionon nënshkrimi digjital?

Nëse *A* dëshiron të nënshkruaj një dokument, ai duhet të përdor çelësin e tij privat i cili është i njohur vetëm nga ai. Kur *B* merrë mesazhin e nënshkruar nga *A*, ai duhet ta verifikoj nënshkrimin. Për verifikim i nevojitet çelësi publik i *A-së*.

Për nënshkrim digjial të mesazhit, përmbajtja e mesazhit *m*, reduktohet në mesazh digest me një funksion hash. Pastaj ky mesazh digest enkriptohet me çelësin privat të nënshkruesit me algoritëm me çelës publik (p.sh. RSA). Mesazhi dhe digest mesazhi i enkriptuar prezentohen së bashku për të prodhuar nënshkrimin digjital.

Tek rasti i enkriptimit e pamë që të tjerët përdorin çelësin tonë publik për enkriptimin e mesazhit kështu që vetëm personi që posedon çelësin privat mund ta dekriptojë atë.

Por tek rasti i nënshkrimit digjital ndodh e kundërta: ne e enkriptojmë mesazhin duke përdorur çelësin tonë privat, dhe çdokush mund ta dekriptoj atë. Ky nuk është mekanizëm i enkriptimit për tu siguruar që pala e tretë nuk mund ta lexoj mesazhin tonë, por përdoret për ta bërë të qartë që ne jemi autori i mesazhit. Nëse unë mund ta dekriptoj një mesazh duke përdorur çelësin publik të dikujt, jam në dijeni që ai person është autor i atij mesazhi pasiqë vetëm ai ka çasje në çelësin privat të tij.

Kjo është mënyra e zgjidhjes së problemit të integritetit, autenticitetit dhe jo-mohueshmërisë, sepse nëse dikush e ndryshon mesazhin e enkriptuar të dërguar nga unë tek ju, ju nuk do të mund ta dekriptoni atë duke përdorur çelësin publik timin. Në anën

tjetër nëse mesazhi dekriptohet me çelësin publik timin, kjo do të thotë që unë jam autor i atij mesazhi dhe nuk mund ta mohoj atë.

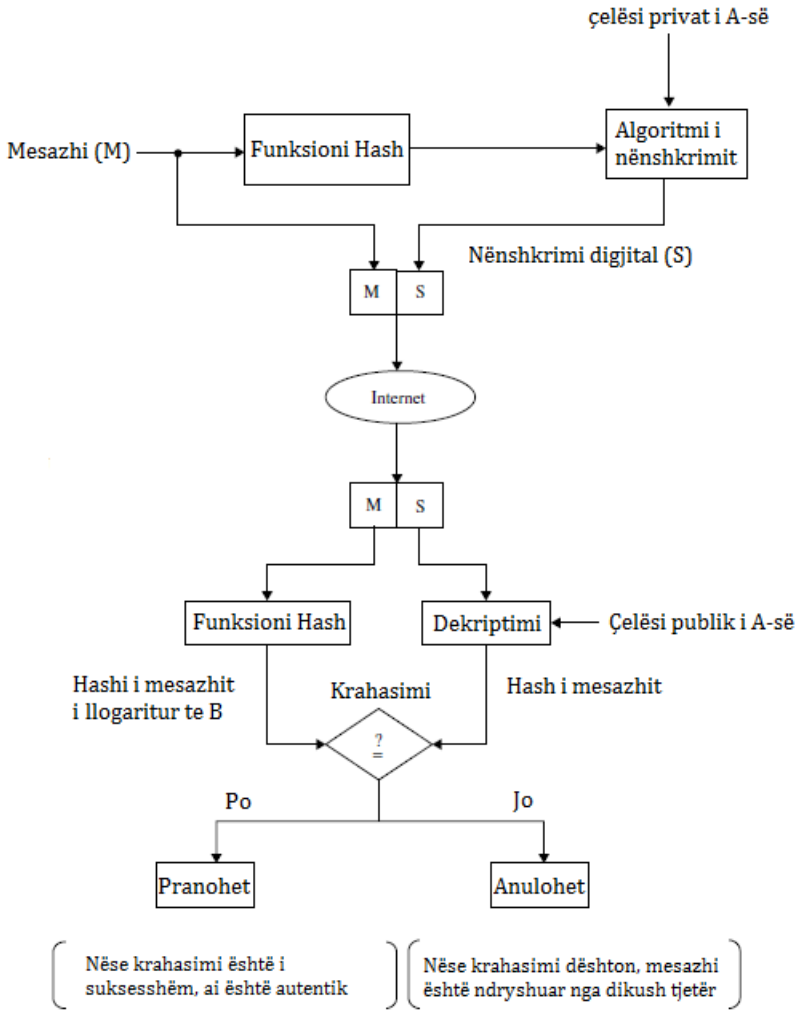


Figura 25: Pamja e përgjithshme e një skeme të nënshkrimit digjital [29]

Në praktikë te përdorimi i nënshkrimit digjital nuk është qëllimi që mesazhi të mos jetë i lexueshëm nga dikush tjetër përveç teje, kështu që pasi enkriptimi dhe dekriptimi i mesazheve të mëdha kërkon resurse të larta, ne mund ta ruajmë kohën dhe CPU në makinën tonë duke enkriptuar hash-in e mesazhit dhe duke ia bashkangjitur atë mesazhit. Kur dikush merrë mesazhin mund ta dekriptoj hash-in dhe të krijoj hash të mesazhit për të krahasuar me hash-in e bashkangjitur [29].

4.7.1 Përfitimet e nënshkrimit digjital

Këto janë arsyet e përbashkëta për aplikimin e një nënshkrimi digjital tek komunikimi:

- Autentikimi - edhe pse mesazhet shpesh mund të përfshijnë informacione rreth subjektit që dërgon një mesazh, ky informacion mund të mos jetë i saktë.

Nënshkrimet digjitale mund të përdoren për të vërtetuar burimin e mesazheve. Kur pronësia e një çelësi sekret të nënshkrimit digjital lidhet me një përdorues të caktuar, një nënshkrim i vlefshëm tregon se mesazhi u dërgua nga ai përdorues. Rëndësia e besimit të lartë në autenticitetin e dërguesit është veçanërisht e dukshme në një kontekst financiar.

- Integriteti - në shumë skenar, dërguesi dhe marrësi i një mesazhi mund të ketë nevojë për konfidencë se mesazhi nuk është ndryshuar gjatë transmetimit. Megjithëse enkriptimi fsheh përmbajtjen e një mesazhi, mund të jetë e mundur të ndryshoj një mesazh të enkriptuar pa e kuptuar atë (disa algoritme të enkriptimit, të njohura si ato jo të lehta, e parandalojnë këtë, por të tjerët nuk e bëjnë). Megjithatë, nëse një mesazh nënshkruhet në mënyrë digjitale, çdo ndryshim në mesazhin do ta zhvlerësoj nënshkrimin.

4.7.2 Standardet për implementimin e nënshkrimit digjital

Ekzistojnë dy standarde për implementimin e nënshkrimit digjital:

CMS (Cryptographic Message Syntax)

CMS është sintaks që përdoret për nënshkrimin digjital, llogaritjen e hash-it, autentikimin apo enkriptimin e përmbajtes së mesazheve. Ky është bazuar në sintaksën PKCS7 (Standard për nënshkrimin dhe enkriprimin e mesazhit nën PKI)

CMS përdor elemente kriptografike për të ofruar enkriptimin dhe nënshkrimi digjital. Ai përdor një format të tipit dhe vlerës si në figurën 26.

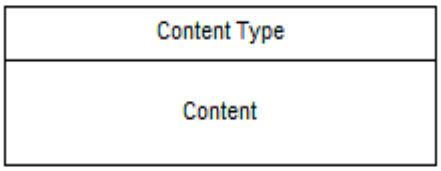


Figura 26: Formati bazik tip-vlerë i CMS [30]

Sintaksa lejon enkapsulime të shumëfishta, ku një enkapsulim mbështjellet në tjetrin. Ngjashëm, një person mund të nënshkruaj disa të dhëna më parë të enkapsuluara. Vlera e CMS gjenerohet duke përdorur ASN.1.

CMS definon gjashtë tipe që e përshkrujnë formën e zgjerimit kriptografik që është aplikuar në të dhëna digjitale [30]. Këto tipe janë:

1. Data - referohet stringjeve octet, dhe është e enkapsuluar në njërën nga tipet tjera.
2. Signed – Data - nënshkruan kriptografikisht përmbjatjen, mund të ketë më shumë se një nënshkrues.
3. Enveloped – Data - përmban përmbajtjen e enkriptuar bashkë me çelësin për dekriptim.
4. Digest – Data - përmban përmbajtjen dhe digest-mesazhin e përmbajtjes për të ofruar integritet të saj.

5. Encrypted – Data - ka vetëm të dhënat e enkriptuara.
6. Authenticated – Data - ky konsiston në përmbajtje, message authentication code (MAC), dhe çelësat autentik të enkriptuar.

Abstract Syntax Notation One – standard dhe shënim i cili përshkruan rregullat dhe strukturën për reprezentimin, enkodimin, transmetimin, dhe dekodimin e të dhënave në telekomunikacion dhe rrjeta kompjuterike [31]. Rregulla të ndryshme të enkodimit ASN.1 ofrojnë sintaksën e transferimit (një reprezentim konkret) të vlerave të të dhënave abstrakti sintaksor i të cilave shpjegohet në ASN.1. Rregullat (formatet) e enkodimit ASN.1 standarde përfshijnë [32]:

- Basic Encoding Rules (BER)
- Canonical Encoding Rules (CER)
- Distinguished Encoding Rules (DER)
- XML Encoding Rules (XER)
- Canonical XML Encoding Rules (CXER)
- Extended XML Encoding Rules (E-XER)
- Packed Encoding Rules (PER, unaligned: UPER, canonical: CPER)
- Generic String Encoding Rules (GSER)

Në praktikë mund të përdoret ASN kompajluesi i cili merrë si input një ASN.1 specifikim dhe e gjeneron kodin kompjuterik (p.sh. në gjuhë programuese C) [32].

CAdES – CMS Advanced Electronic Signature

CAdES (CMS advanced electronic signatures) është standard i ri për nënshkrimin digjital të avancuar. Ky zgjeron standardin e mëparshëm CMS, duke specifikuar profile të ndryshme shtesë. Arsyeja për këtë ishin mungesat e shfaqura në CMS të disa karakteristikave të rëndësishme për të zgjeruar nënshkrimin elektronik, ku më e dukshmja është validimi për një kohë të gjatë (long term validation), ku kjo do të thotë mundësia për të dëshmuar validitetin e nënshkrimit pas një periudhe të gjatë, disa vite apo disa dekada pasi është krijuar.

CAdES specifikon forma shtesë apo profile të cilat përshkruajnë strukturën e nënshkrimit elekronik të avancuar. Këto profile janë CAdES-T, CAdES-C, CAdES-X-L dhe CAdES-A. Secila nga to shtojnë disa veti nga ai paraprak.

Kemi dy forma të nënshkrimeve elektronike të avancuara CMS të specifikuara në standardin CAdES, të quajtura CAdES Basic Electonic Signature (CAdES-BES) dhe CAdES Explicit Policy-based Electonic Signature (CAdES-EPES) [33].

Formatet e Nënshkrimit Elektronik

CAdES Basic Electronic Signature (CAdES – BES)

CAdES-BES përmban [34]:

- Të dhënat e nënshkruara të përdoruesit (p.sh. dokumentin e nënshkruesit) i definuar nga CMS (RFC 3852).
- Një koleksion të atributeve të detyrushme të nënshkruara, të definuara në CMS (RFC 3852) dhe në ESS (RFC 2634).
- Atribute të detyrueshme të nënshkruara shtesë, të definuara më vonë.
- Vlerën e nënshkimit digjital të llogaritur në të dhënat dhe e prezentuar në atributet e detyrueshme siç përcaktohen në CMS (RFC 3852).

CAdES BES, në përputhje me dokumentin e pranishëm mund të përmbaj:

- Një koleksion të atributeve shtesë të nënshkruara dhe
- Një koleksion të atributeve opsionale të pa nënshkruara

Atributet e detyrueshme të nënshkruara janë:

- Content-Type
- Message-digest
- Signing-certificate dhe signing-certificate-v2

Atributet opsionale të nënshkruara janë:

- Signing-time
- Content-hints
- Content-reference
- Content-identifier
- Commitment-type-indication
- Signer-location
- Signer-attributes
- Conent-time-stamp
- Mime-type

Atributet e panënshkruara janë:

- CounterSignature

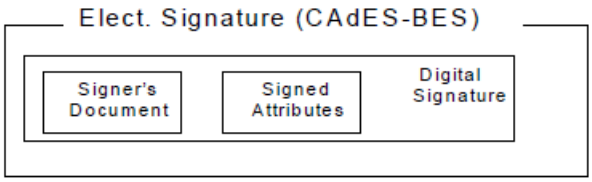


Figura 27: Struktura e CAdES-BES [34]

CAdES Explicit Policy-based Elctronic Signature (CAdES-EPES)

CAdES-EPES zgjeron përkufizimin të nënshkrimit elektronik në përputhje me politikën e identifikimit të nënshkrimit. CAdES-EPES përfshinë një atribut të nënshkruar (sigPolicyID) që tregon politikën e nënshkrimit që do të përdoren për të vërtetuar nënshkrimin elektronik. Ky atribut i nënshkruar është i mbrojtur nga nënshkrimi. Nënshkrimi mund të ketë atribute tjera të nevojshme në përputhje me politikën e mandatuar të nënshkrimit [34].

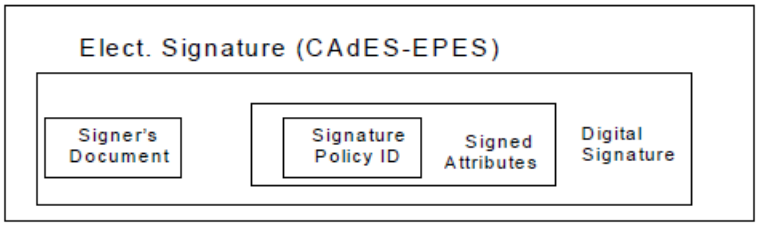


Figura 28: Struktura e CAdES-EPES [34]

Formatet e nënshkrimit elektronik me validimin e të dhënave

Validimi i një nënshkrimi elektronik, në përputhshmëri me dokumentin e tanishëm, kërkon disa të dhëna shtesë për të vërtetuar nënshkrimin elektronik. Këto të dhëna shtesë njihen si të dhëna validuese të cilat përfshijnë:

- Certifikatën e çelësit publik (PKC)
- Informatat e statusit të revokimit për secilën PKC
- Time-stamp i aplikuar në nënshkrimin digjital
- Në raste të nevojshme, detajet e rregullave të nënshkrimit që do të përdoren gjatë verifikimit të nënshkrimit elektronik.

Të dhënat e validimit mund të koleksionohen nga një nënshkrues apo verifikues. Ato përfshijnë CA, statusin e revokimit në formë të Certificate Revocation Lists (CRL) ose certificate status information (OCSP) i ofruar nga një server online, evidencën e nënshkrimit që është krijuar para një kohe të caktuar; kjo mund të jetë një time-stamp apo time-mark [34].

Profilet:

- CAdES-T (Nënshkrimi elektronik me kohë) – shtimi i time-stamp fushës për tu mbrojtur nga mohueshmëria.
- CAdES-C (Nënshkrimi elektronik me komplet referencat e validimit të dhënave) - shton referencat në CAdES-T për certifikata dhe listën revokuese për të verifikuar nënshkrimin, gjithashtu për të verifikuar offline verifikimin e nënshkrimit në të ardhmen.
- CAdES-X (Formati i zgjeruar i nënshkrimit elektronik) - CadES-C mund të zgjerohet duke shtuar atribute të pa nënshkruara në nënshkrimin elektronik, si shtimi i timestamps për tu mbrojtur nga rreziqet e mundshme në të ardhmen.

- CAdES-X Long (Nënshkrimi elektronik extended long) - shton certifikatën dhe listën revokuese në formatin CAdES-C, për të mundur të verifikojmë në të ardhmen edhe nëse nuk është i disponueshëm burimi i tyre origjinal.
- CAdES-A (Nënshkrimi elektronik i arkivuar) - periodikisht shton mundësinë për timestamping (p.sh. çdo vjet) të dokumentit të arkivuar për të parandaluar rrezikun e shkaktuar nga dobësimi gjatë ruajtjes së gjatë.
- CAdES-LT (Nënshkrimi elektronik Long-Term) - shton përdorimin e "tree hashing" algoritmit dhe "evidencën e regjistrave".

PDF (Portable Document Format)

PDF është format i një fajlli që përdoret për të paraqitur dokumente në mënyrë të pavarur prej aplikacioneve softuerike, harduerit dhe sistemit operativ [35]. Secili fajll PDF shfaq një paraqitje të plotë të një dokumenti i cili përmban tekst, fonte, paraqitje grafike si dhe informacione tjera të nevojshme. Në vitin 1991 John Warnock bashkë themeluesi i Adobe System paraqiti një sistem të quajtur "Camelot" që evoluoj në PDF [36]. PDF kontrollohej nga Adobe, derisa u lëshua zyrtarisht si një standard i hapur më 1 korrik 2008 e publikuar nga Organizata Ndërkombëtare për Standardizim si ISO 32000-1:2008. PDF përmban përmbajtje digjitale që mund të ruhen dhe të prezantohen tek përdoruesit.

PDF arriti popullaritetin kur organizatat filluan ti ruajnë dokumentet në formë elektronike për shpërndarje të informacionit ose edhe për tregti. Me shekuj, tregtia ka regjistruar transaksionet e tyre në dokumente në letër. Forma të ndryshme të nënshkrimit janë aplikuar si vula, dyll, etj. në këto dokumente letër si dëshmi e marrëveshjes në mes të personave ose organizatave, ose për të treguar se një dokument i përket një autori të caktuar. Kalimi nga letra në PDF është lehtësuar për shkak të aftësisë së PDF për paraqitje elektronike të çdo forme të dokumenteve në letër dhe mbështetja e saj për nënshkrime digjitale (PAdES) që siguron të njëjtin funksion ose edhe më shumë se nënshkrimet, vulat, dylli.

Me nënshkrimin PDF është i përfshirë direkt brenda dokumentit të nënshkruar, si një nënshkrim i dorës që bëhet në dokumentet letër. Kjo lejon që PDF dokumenti të kopjohet, ruhet dhe shpërndahet si një fajll elektronik [37].

PAdES – PDF Advanced Electronic Signature

PAdES (PDF Advanced Electonic Signatures) është set i kufizimeve dhe zgjerimeve të PDF dhe ISO 32000-1 standardeve që ta bëjnë atë të përshatshëm për nënshkrimin elektronik të avancuar [38].

Përderisa në ditët e sotme formati i dokumentit më të popularizuar i cili ofron mekanizëm të nënshkrimit elektronik është PDF i cili poashtu lejon përdoruesit të shkëmbejnë dokumentet elektronike lehtë dhe besueshëm, pavarësisht nga ambienti në të cilin janë krijuar apo ambientin në të cilin shikohen ose printohen.

Organizata ndërkombëtare për standardizim (ISO) ka publikuar standardin e ri ISO 32000-1 (PDF 1.7) në vitin 2008, ku identifikon mënyrat në të cilat mund të inkorporohet nënshkrimi elektronik në formë të nënshkrimit digjital në dokument PDF për të autentikuar identitetin e autorit dhe për të validuar integritetin e përmbajtjes së dokumentit.

Këto nënshkrime bazohen në teknologjinë CMS dhe teknikën CAdES (CAdES i cili qëndron për CMS Advanced Electronic Signatures, përshkruan përdorimin e nënshkrimit digjital në fajll gjenerik apo e-mail mesazh, përderisa PAdES merret vetëm me PDF dokumente) [39].

Në korrik të 2009, ETSI (European Telecomunication Standards Institute) ka publikuar standardin e ri i cili lehtëson transaksionet e sigurta nëpër Evropë, në përputhje me legjislacionin Europian. Ky standard definon një numër të profileve për PAdES të cilat i plotësojnë kërkesat e Direktivës Evropiane për nënshkrimet elektonike (Directive 1999/93/EC) [40].

PAdES specifikimet konsistojnë në 5 pjesë (profile):

- Pjesa 1: PAdES Overview - framework dokumenti për PAdES.
- Pjesa 2: PAdES Basic - Profilet e bazuar në ISO 32000-1.
- Pjesa 3: PAdES Enhanced - PadES-BES dhe profilet PAdES-EPES.
- Pjesa 4: PAdES Long Term - PadES-LTV profili.
- Pjesa 5: PAdES for XML Content - Profilet për nënshkrimet XAdES.

Pjesa 1 - PAdES Overview

Është pamja e përgjithshme PAdES (overview), që në mënyrë të përgjithësuar shpjegon pjesët tjera të PAdES. Ofron përshkrim të përgjithshëm të mbështetjes për nënshkrime digjitale në dokumente PDF duke përfshirë përdorimin e nënshkrimeve XML për të ruajtur të dhënat XML në dokumente PDF. Këtu listohen karakteristikat e profileve PDF të specifikuara në pjesët tjera të dokumentit.

Nënshkrimi digjital në ISO 32000-1 aktualisht mbështetë tri aktivitete: shtimi i një nënshkrimi digjital menjëherë në dokument, ofrimi i fushës apo hapësirës ku do të shtohet nënshkrimi në të ardhmen, dhe kontrollimi i validitetit të nënshkrimit. Nënshkrimi me disa informata tjera, në strukturën e PDF gjendet në pjesën e quajtur fjalor i nënshkrimit [41].

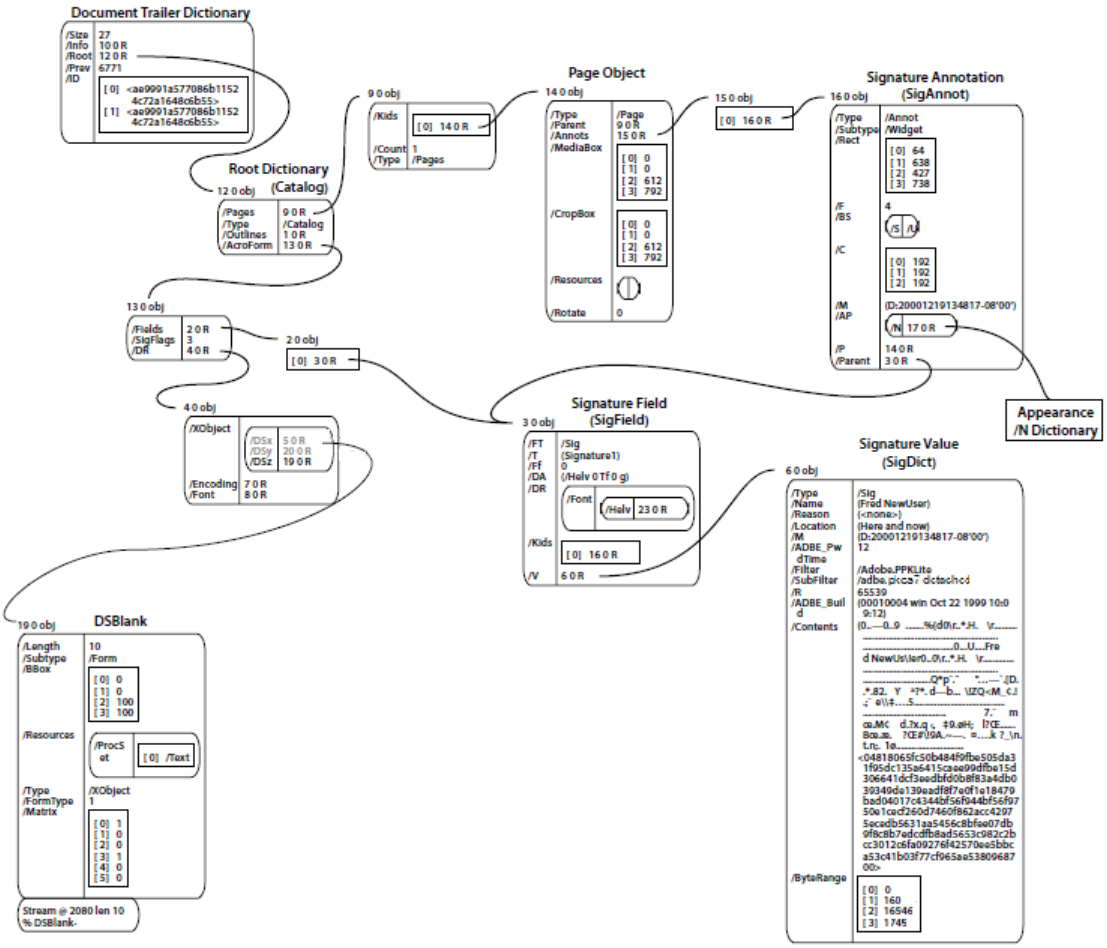


Figura 29: Objektet e nënshkrimit në PDF [40]

Vlera e nënshkrimit është e enkoduar si object binary duke përdorur CMS apo formatet e ngjajshme PKCS#7 dhe CAdES. Formati dhe përmbajtja e vlerës së nënshkrimit varet nga profili.

Ashtu si me implementimin e nënshkrimit të bazuar në CMS, digest llogaritet për një rang të bajtave të skedarit (file). Sidoqoftë me PDF, pasi informata e nënshkrimit do të bashkangjiten në dokument, ky rang është i gjithë skedari, duke përfshirë edhe Signature Dictionary por duke e lënë jashtë vetë nënshkrimin. Ky rang pastaj tregohet nga shënimi ByteRange e signature dictionary [38].

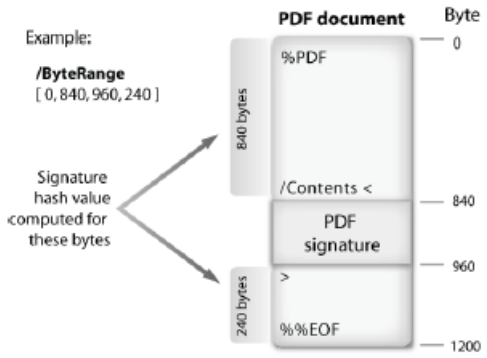


Figura 30: Bajtat e PDF të mbuluar nga nënshkrimi [38]

Vlera binare e nënshkrimit të PDF gjendet në pjesën Content të signature dictionary. Madhësia e pjesës Content llogaritet bazuar në supozimin më të mirë të numrit maksimal që nevojitet për ta mbajtur nënshkrimin e PDF ndonjë informatë tjetër (rreth certifikatës digjitale) dhe informatat rreth time-stamping. Së pari përmbajtja e kësaj fushe është e mbushur me vlerë heksadecimale 0x00 e pastaj kur dokumenti nënshkruhet kjo vlerë zëvendësohet me vlerën aktuale të nënshkrimit.

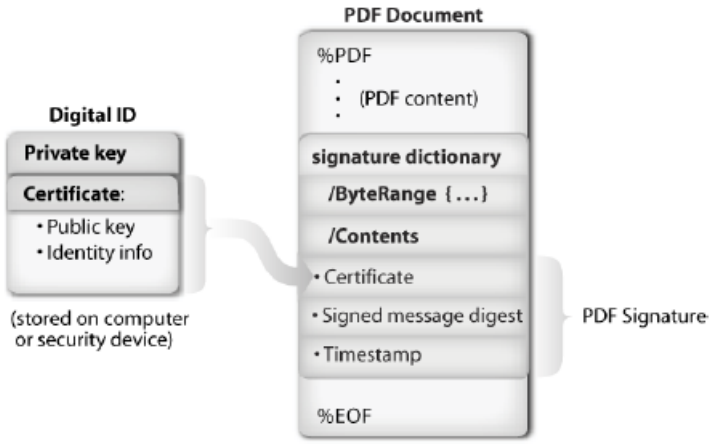


Figura 31: Vendndodhja e vlerës së nënshkrimit digjital në PDF [38]

Tipat e nënshkrimit PDF

Përveç nënshkrimit tradicional të dokumentit, nënshkrimi PDF fut konceptin e certifikatës të cilat punojnë me lejet (MDP, ISO 32000-1). Funksionaliteti i MDP në PDF është përcaktuar prej referencës së nënshkrimit, e lejon modifikimin e dokumenteve në disa mënyra (të tilla si: format mbushëse, pasuese ose komentet) dhe përsëri e ka nënshkrimin origjinal të interpretuar si të vlefshëm [42].

Mbajtësit e nënshkrimit (Signature Handlers)

ISO 32000-1 definon disa implementime për shtimin e nënshkrimit digjital CMS-based në dokument PDF. Secili nga këto implementime definohet nga çifti i vlerave në

nënshkrimin digjital të quajtur Filter dhe SubFilter. Filter definon emrin e mbajtësit të preferuar të nënshkrimit për tu përdorur gjatë validimit të nënshkrimit, ndërsa SubFilter është një emër i cili përshkruan enkodimin e nënshkrimit të PDF dhe informatat e çelësit në signature dictionary [38].

Nënshkrimet serike të PDF

Përderisa format e tjera të bazuar në CMS te nënshkrimet elektronike mbështesin nënshkrimet paralele, ku disa individ nënshkruajnë të njëjtin varg të bajtëve dhe ky koleksion i certifikatave nënshkruese më pas futen në një mbështjellës të vetëm PKCS#7 ndërsa ISO 32000 nuk e përkrah këtë veprim. Si e tillë do të ketë vetëm një nënshkrues në çdo nënshkrim PDF. Në vend të kësaj, ky standard ofron një zgjidhje alternative për nënshkrues të shumëfishtë në figurën 32. Çdo nënshkrim PDF mund të përmbaj vetëm një certifikatë nënshkruese, por mund të ketë disa nënshkrime (signature dictionaries) dhe secili i asociuar me ByteRange e vetë [42].

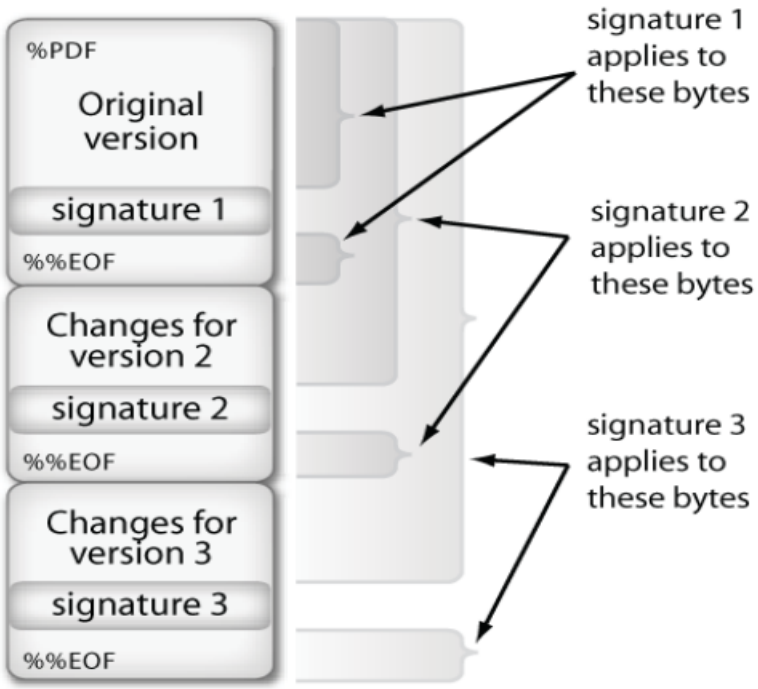


Figura 32: Nënshkrimet serike në PDF [42]

Rrjedha normale për nënshkrimet serike PDF është kur pas nënshkrimit të dokumentit nga personi i parë pasojnë nënshkruesit tjerë e nënshkruan dokumentin por gjithashtu edhe nënshkrimin e mëparshëm PDF.

Vlefshmëria dhe Time-stamping e nënshkrimit PDF

Përdorimi i time-stamping me certifikatën CA dhe statusin e listës së revokimit për validimin e nënshkrimit PDF ndryshon nga profilet që përdoren [42].

Pjesa 2 – PAdES Basic

Specifikon nënshkrimet PDF ashtu siç janë të specifikuara në ISO 32000-1 që lejon ndëroperim më të zgjeruar për nënshkrimet PDF duke ofruar kufizime shtesë përtej atyre të ISO 32000-1. Nënshkrimi bazohet në CMS.

Karakteristikat e nënshkrimit janë [43]:

- Nënshkrimi enkodohet në CMS i definuar sipas PKCS#7.
- Mbështet nënshkrimet serike.
- Opcionalisht përfshinë Time-Stamp të nënshkrimit.
- Opcionalisht përfshinë informata e revokimit.
- Nënshkrimi ruan integritetin e dokumentit dhe autenticitetin e nënshkruesit.
- Nënshkrimi mundet opcionalisht të përfshij "arsyen" e nënshkrimit.
- Nënshkrimi mundet opcionalisht të përfshij "lokacionin" e nënshkrimit.
- Nënshkrimi mundet opcionalisht të përfshij "informatat kontaktuese" të nënshkruesit.

Time Stamping

Kur aplikohet një nënshkrim digjital në dokument, varësisht nga mbajtësi i nënshkimit vulos (stamp) atë me kohën lokale të makinës së nënshkruesit. Pasiqë nënshkruesi mund të ndryshoj kohën në kompjuter ajo kohë zakonisht nuk është e besueshme. Për këtë një timestamp do të aplikohet në dokumentin e nënshkruar nga një server i besuar për timestamp kështu që ky e tregon kohën reale të nënshkrimit të dokumentit. Timestamp përmbushë nevojat kritike në procesin e validimit: nëse një mbajtës i nënshkrimit validon dhe vulos kohën e nënshkrimit duke përdorur një server të besuar të timestamp atëherë nënshkruesi më vonë nuk mund të deklaroj se ai dokument është nënshkruar nga dikush tjetër, është ndryshuar pasi është nënshkruar apo që është nënshkruar në një kohë tjetër [43]. Procesi për timestamp është përshkruar në RFC 3161.

Kontrollimi i revokimit

Mbajtësi i nënshkrimit duhet t'i bashkangjisë informatat e revokimit në nënshkrim për të zvogëluar kohën e verifikimit të nënshkrimit nga marrësi. Pra, përfshirja e informatave të revokimit mbron nga kërcënimet që tentojnë të përdorin certifikata të revokuara të cilat ndikojnë në vetinë e jo-mohueshmërisë së nënshkrimit [43].

Për të kontrolluar statusin e revokimit, një mbajtës i përshtashëm i nënshkrimit mund të përdor njërën nga këto metoda (ose dyjat):

- Listën e certifikatave të revokuara (CRL) – certifikata kontrollohet në listën e certifikatave të revokuara. E cila listë specifikon datën e lëshimit të certifikatës, entitetin që e ka lëshuar si dhe datën e revokimit dhe arsyen.
- Protokoli i statusit të certifikatave online (OCSP) – definon një protokol për të marrur statusin e revokimit të një certifikate nga një server online.

Seed values

Gjatë përgatitjes së nënshkrimit të dokumentit, autori i tij mund të shtoj në fushën e nënshkrimit disa shënime shtesë duke përfshirë një të quajtur seed value dictionary.
Kjo përmban informata të cilat bartin disa rregulla që njoftojnë se autori i dokumentit dëshiron që mbajtësi i nënshkrimit t'iu përmbahet gjatë kohës së nënshkrimit të dokumentit. Këto dëshira mund të specifikohen si rekomandime apo kërkesa. Disa nga to janë specifikimi i metodës hash, informatat e revokimit, autoriteti timestamp dhe atributet e certifikatës [43].

Pjesa 3 – PAdES Enhanced

Profilet PAdES-BES dhe PAdES-EPES përshkruajnë krijimin dhe verifikimin e nënshkrimeve në dokumente PDF që kanë karakteristika të ngjajshme me ato të përshkruara në CAdES nga format e nënshkrimit CAdES-BES, CAdES-EPES dhe CAdES-T. Por këtu në vend të formës së ndarë "-T" si në CAdES, ky set i profileve inkorporon time-stamp të nënshkrimit si opsionale për të dyja PAdES-BES dhe profilet PAdES-EPES duke e bërë nënshkrimin efektivisht një formë CAdES-T [44].

Pjesa 4 – PAdES Long Term

Vlefshmëria i një nënshkrimi elektronik kërkon të dhëna për të verifikuar nënshkrimin në raste të tilla si një certifikatë CA, lista e certifikatave të revokuara (CRL) ose informatat per statusin e certifikatës (OCSP) të ofruara nga një shërbim online. Nëse dokumenti është ruajtur dhe nënshkrimi duhet të verifikohet pas një kohe të gjatë pas krijimit, apo të themi pasi certifikata nënshkruese ka skaduar, të dhënat e validimit origjinal nuk mund të jenë të disponueshme për një kohë të gjatë [45].

Ky profil përdor një zgjerim të ISO 32000-1 të quajtur Document Security Store (DSS) për të bartur këto të dhëna validuese kur nevojitet validimi i nënshkrimit, opsionalisht të lidhur me Validation Related Information (VRI) e cila i lidhë të dhënat validuese me nënshkrimin specifik.

Gjithashtu ky profil përdor edhe një zgjerim tjetër të ISO 32000-1 të quajtur Document Time-Stamp për të zgjeruar jetë-gjatësinë e mbrojtjes së dokumentit. Pasi që DSS të jetë koleksionuar, dhe fusha e nënshkrimit e verifikuar në një kohë para kohës që e tregon Document Time-stamp, kjo kohë e treguar mund të jetë si kohë e supozuar e nënshkrimit në ri-verifikim duke përdorur të dhënat e validimit nga DSS.

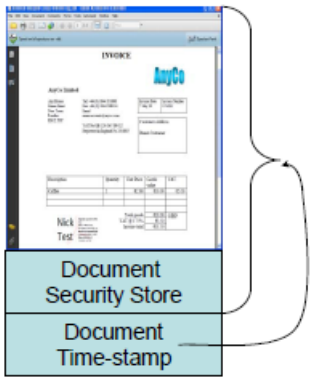


Figura 33: Ilustrimi i PDF dokumentit me LTV [45]

Pjesa 5

Profili për nënshkrimet XAdES (bashkësi e zgjerimeve të nënshkrimit XML duke e bërë atë më të përshtashëm për nënshkrimin elektronik të avancuar) definon përdorimin e një dokumenti XML të nënshkruar i cili është i bashkangjitur brenda një skedari PDF, për të ruajtur integritetin, autenticitetin dhe jo-mohueshmërinë në të dhënat që janë nënshkruar me nënshkrim XAdES [46].

Bouncy Castle

Bouncy Castle është koleksion i API4 të përdorura në kriptografi. Ajo përfshinë API për të dyja gjuhët programuese Java dhe C#. Bouncy Castle ka origjinë nga Australia dhe janë të mbështetura nga një Shoqatë Australiane: Legion of the Bouncy Castle Inc [25].
Disa nga karakteristikat kyçe të Bouncy Castle janë [47]:

- Java API original ka rreth 27000 rreshta kod dhe ofron mbështetje për J2ME, JCE/JCA provider dhe gjeneratën bazike të X.509.
- Lëshimi i fundit Java në Bouncy Castle ka rreth 335713 rreshta kod dhe mbështet funksionalitetin e njëjtë me Java API-në original plus PKCS#10, PKCS#12, CMS, S/MIME, OpenPGP, DTLS, TLS, OCSP, TSP, CMP, CRMF, DVCS, DANE, dhe atribute të certifikatës.
- C# API ka rreth 145.000 rreshta kod dhe mbështet pothuajse të gjitha që i mbështet Java API.

4.8 Aplikacioni - digital pdf signature App

Funksionaliteti i aplikacionit përfshinë nënshkrimin e një dokumenti në formatin PDF me një certifikatë digjitale të ofruar nga kartela biometrike që lexohet përmes lexuesit të kartelave. Leximi i të dhënave të tij bëhet nga programi i zhvilluar tashmë "HIGHSEC eID App", i cili mundëson shikimin e përmbajtjes së kartelës së mençur si dhe lëshimin e certifikatave të ruajtura në kartelën e mençur.
Përveç nënshkrimit digjital të dokumentit, do të përmbajë gjithashtu bllokun me nënshkrime që tregojnë se dokumenti zyrtarisht është nënshkruar nga një autoritet publik.

Me hapjen e aplikacionit shfaqet pamja e tij siç tregohet në figurën 34, ku është e mundur të kërkohet skedari PDF përmes shfletuesit ose ta tërhiqni atë në sipërfaqen e drag and drop. Si rezultat, aplikacioni merrë pamjen ku do të hapet dhe do të jetë e mundur të pozicionohet blloku i nënshkrimit me të dhënat e tij, si dhe të ndryshoj madhësinë e saj sipas nënshkrimit.
Karakteristikat e aplikacionit janë:

- Aplikacion Windows
- Gjuha Programuese C#
- Library iTextSharp

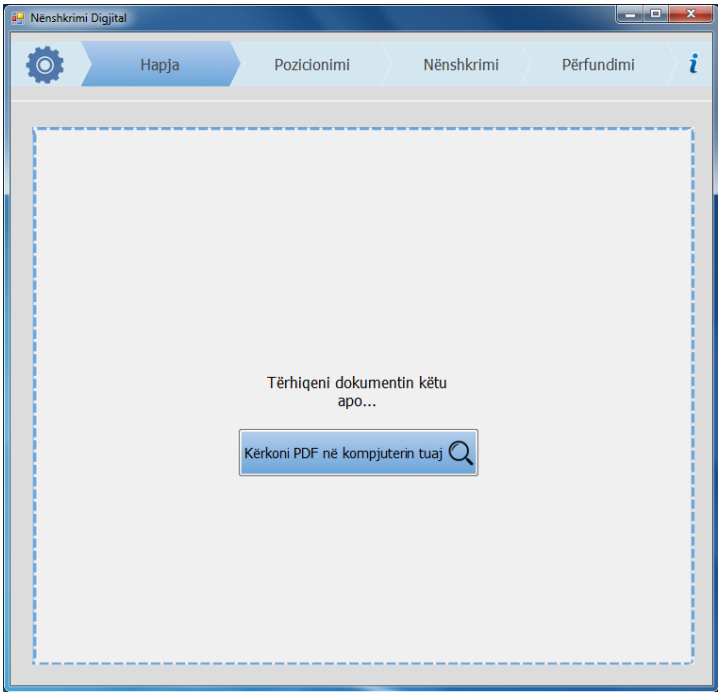


Figura 34: Pamja hyrëse e aplikacionit

Pas klikimit mbi butonin "Sign", aplikacioni merrë imazhin e paraqitur në figurën 35 ku mund të zgjedhim certifikatën me të cilën dëshirojmë të nënshkruajmë dokumentin. Butoni "Sign" e bënë përzgjedhjen e certifikatës nga kompjuteri ashtu siç lexohet nga

lexuesi i kartelave biometrike. Shfaqja e aplikacionit pas nënshkrimit të suksesshëm të dokumentit do të duket si në figurën 36 dhe figurën 37.

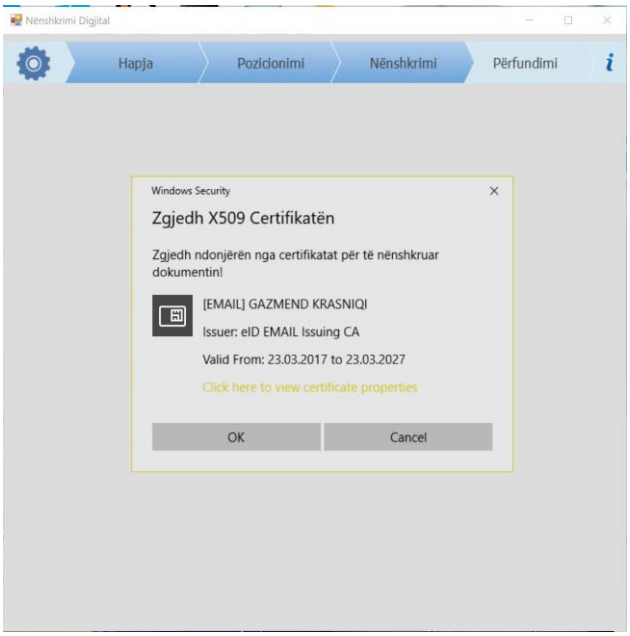


Fig.35: Përzgjedhja e certifikatës për nënshkrim

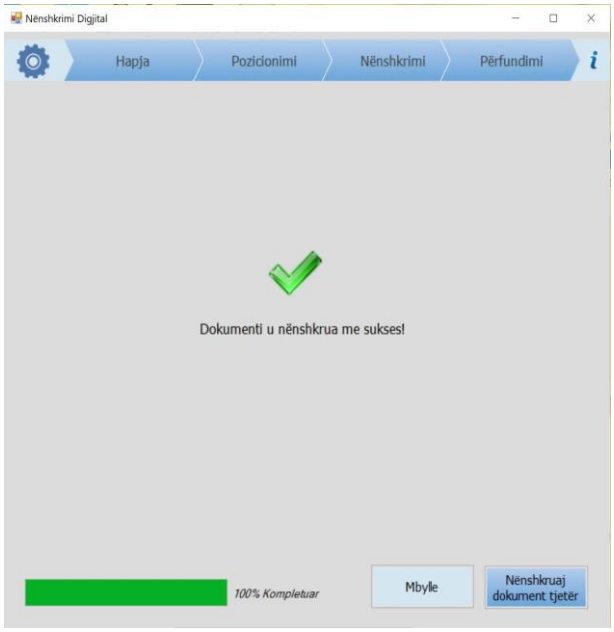


Fig.36:Pamja e App pas nënshkrimit të dokumentit

Në fund, pas nënshkrimit të dokumentit, një skedar i nënshkruar në mënyrë digjitale do të krijohet në të njëjtin vend, i cili do të përmbaj bllokun e nënshkrimit për prezantimin e tij vizual. Gjithashtu, skedari original i panënshkruar dhe i pandryshuar do të gjendet aty.

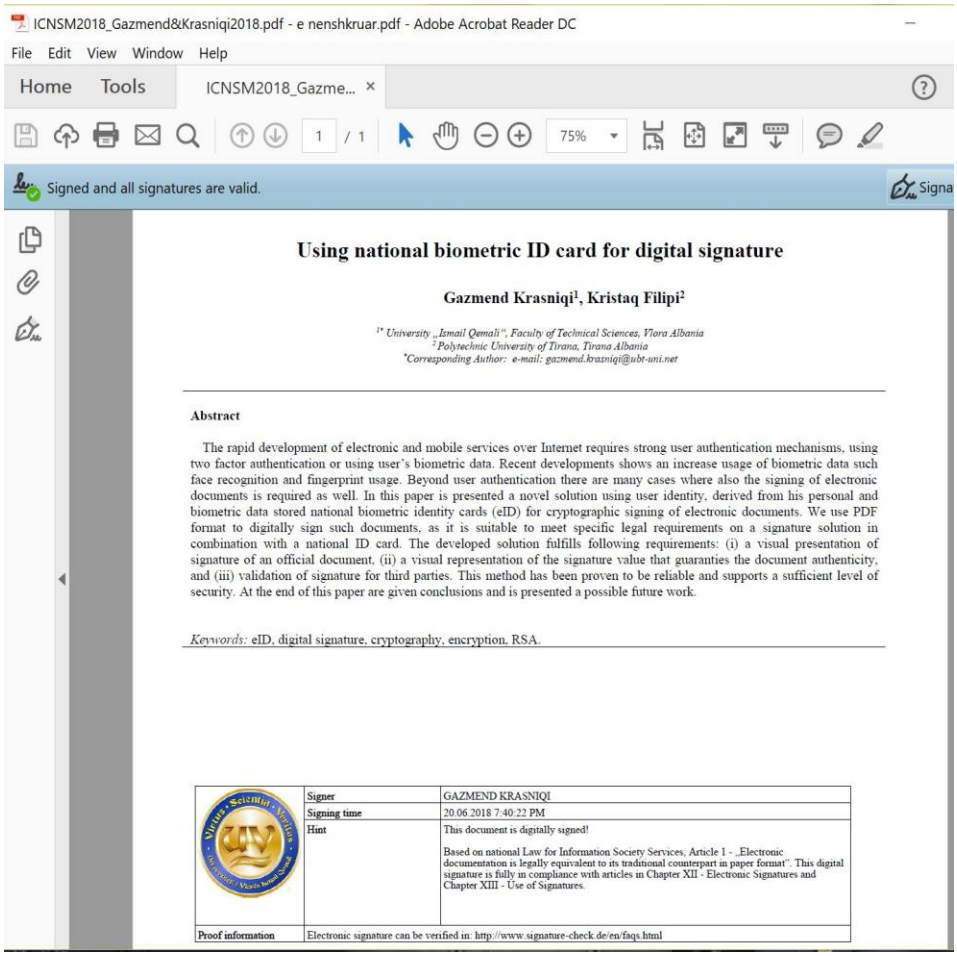


Figura 37: Dokumenti i nënshkruar

5 ANALIZA E PERFORMANCËS eID vs PC

Protokolet biometrike përdoren jo vetëm për të autentikuar një individ në një autoritet zyrtar, por edhe për të enkriptuar ose nënshkruar një mesazh. Këto protokole bazohen në tipare biometrike, të cilat janë universale dhe unike. Ka shumë metoda për të implementuar identifikimin biometrik, dhe një kartelë biometrike, zakonisht e njohur si një kartelë nacionale e identifikimit elektronik (eID), është një prej tyre.

Kartelat biometrike eID mund të kryejnë autentikimin, enkriptimin dhe nënshkrimin e të dhënave, për shkak të parametrave privat (çelësat) të ruajtura në kartelë. Parametrat privat ruhen në një kartelë, si një model biometrik gjatë fazës së regjistrimit. Ky shabllon përdoret për krahasimin midis modelit të ri dhe modelit përkatës në kartelë, duke përdorur dy sisteme procesimi: match-off-card dhe match-on-card. Match-on-card krahason shabllonin e kartelës me modelin e ri, ndërsa procesimi i të dhënave biometrike bëhet në kartelë dhe asnjëherë jashtë kartelës. Nga ana tjetër, procesimi i match-off-card nuk është bërë në kartelë, por brenda dhe jashtë një pajisjeje ose sistemi. Match-off-card dhe match-on-card janë paraqitur në figurat 38 dhe 39.

Çdo sistem procesimi ka përparësitë dhe mangësitë e veta, siç përshkruhet në [48]. Match-off-card është më e shpejt, për shkak të fuqisë procesuese nga sistemi, por për shkak se modeli biometrik e lë kartelën, kjo qasje paraqet një rrezik sigurie për informacionin e ndjeshëm brenda kartelës. Sidoqoftë, match-on-card ka fuqi llogaritëse më të ulët, siguri më të lartë sepse modeli biometrik nuk e lë kartelën dhe mungesa e ndërveprimit është një problem në këtë sistem të procesimit [48]. Një prezantim i përgjithshëm mbi match-on-card mund të gjendet në [49], ku diskutohen përparësitë kryesore të këtij sistemi të procesimit, si një bazë të dhënash biometrike e decentralizuar, mobiliteti i të dhënave, privatësia dhe siguria e rritur [50].

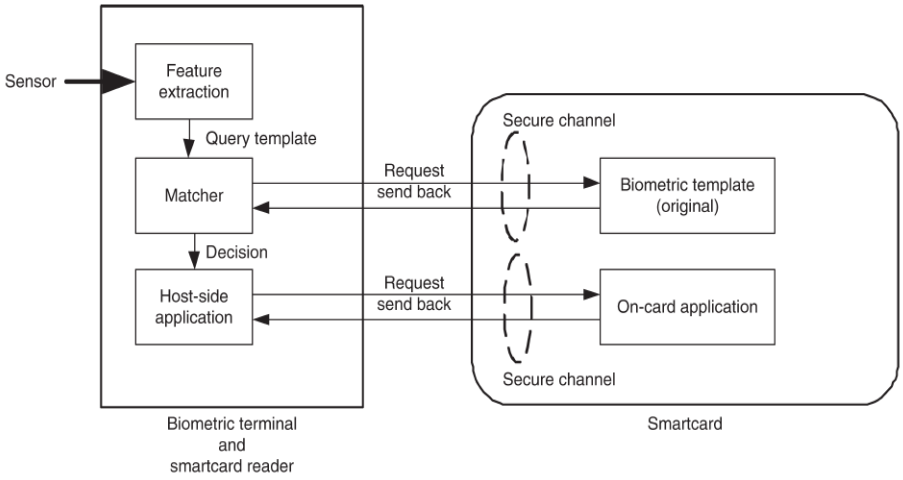


Figura 38. Sistemi Match-Off-Card [49]

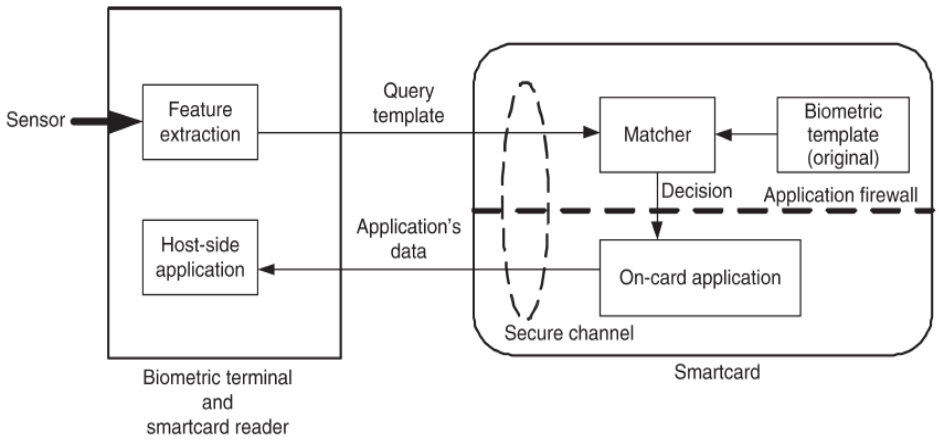


Figura 39. Sistemi Match-On-Card [49]

Enkriptimi i procesuar me një kartelë biometrike u propozua në [51]. Enkriptimi është bërë duke përdorur çelësin biometrik, një çelës unik të gjeneruar nga modeli biometrik brenda kartelës. Përveç procesit të enkriptimit, ky çelës mund të përdoret gjithashtu edhe për procesin e përputhjes dhe të autentikimit [51].

Teksa teknologjia po përparon, nevoja për një sistem të procesimit më të shpejt të të dhënave po rritet gjithashtu, duke e bërë shpejtësinë parametrin kryesor për analizim. Instituti Kombëtar i Standardeve dhe Teknologjisë (NIST) ka bërë një vlerësim të saktësisë dhe shpejtësisë së procesit match-on-card të gishtërinjeve. Shkalla minimale e gabimit, shpejtësia e ekzekutimit dhe saktësia ishin vetëm disa nga parametrat e testuar në këtë eksperiment dhe diskutuar në një raport të zgjeruar [52]. Autentikimi përmes gjurmëve të gishtërinjëve duke përdorur match-on-card është paraqitur gjithashtu në [53], ku kam vëzhguar ecurinë e autentikimit të suksesshëm dhe të pasuksesshëm. Koha e verifikimit pozitiv është më e ngadaltë sesa koha negative e verifikimit, e cila është gjithashtu një çështje sigurie. Në këtë disertacion, janë analizuar gjithashtu edhe performanca e regjistrimit dhe shkalla e pranimit gabim të procesit të verifikimit.

NIST ka bërë një eksperiment tjetër, një studim fizibiliteti, për të përcaktuar nëse autentikimi biometrik match-on-card mund të kryhet në më pak se 2.5 s. Protokoli për këtë operacion përbëhej nga disa hapa, duke paraqitur kartelën tek lexuesi i kontaktit nga mbajtësi i kartelës, duke paraqitur gishtin në skaner, një proces i sigurt i krijimit të sesionit, transmetimin e modelit të enkriptuar të gishtrinjëve në kartelë, dekriptimin e modelit dhe në fund kthimin e rezultatit të testimit që përputhet. Në raport, parametrat kryesor të matur janë koha mesatare për të krijuar një sesion të sigurt, kohën mesatare për transmetimin e të dhënave të enkriptuara biometrike dhe kohëzgjatjen mesatare totale për të kryer këtë proces të plotë [54].

Ky studim propozon një qasje të ndryshme nga punimet e përmendura më lart. Parametri kryesor është efikasiteti i dy sistemeve të procesimit, match-on-card kundrejt match-off-card. Ky studim nuk do të marrë parasysh fazën e regjistrimit ose të verifikimit të kartelës biometrike, por do të përdor vetëm modelin për enkriptim dhe nënshkrimet e

të dhënave, dhe e krahason këtë proces me të njëjtin proces, duke përdorur kompjuterin personal (PC) si pajisje procesimi.

Një kartelë biometrike nacionale eID ruan çelësin privat dhe publik te mbajtësi i saj. Këto çelësa do të përdoren për të enkriptuar dhe nënshkruar të dhënat, të cilat përfaqësojnë sistemin e procesimit match-on-card. Shpejtësia e përpunimit do të krahasohet kundrejt match-off-card.

Për më tepër, ky studim nuk adreson autentikimin e përdoruesit ose shpejtësinë që përdoruesi autentikon veten. Eksperimenti kryesor i këtij studimi krahason efikasitetin e match-on-card dhe match-off-card. Eksperimenti merrë në konsideratë parametra të ndryshëm, në formën e madhësisë së file-ve, algoritmeve të procesimit për enkriptim ose nënshkrim. Secili parametër luan një rol dhe ka një ndikim në të gjithë procesin lidhur me efikasitetin e tij.

Kjo pjesë është e organizuar si më poshtë. Pjesa e parë e këtij kapitulli përshkruan kartelën biometrike nacionale të identitetit dhe karakteristikat e saj të sigurisë. Në pjesën e dytë përshkruajmë arkitekturën e aplikacionit që përdoret për të kryer eksperimentet. Kurse në pjesën e tretë tregojmë rezultatet e eksperimenteve. Dhe në pjesën e fundit do ti përshkruajmë rezultatet kryesore nga ky studim, rekomandimet dhe punën e mundshme në të ardhmen.

Kartelat nacionale biometrike të identitetit

Një kartelë biometrike e identitetit (ID) është një format i madhësisë së kartelës së kreditit dhe përmban informacione personale dhe biometrike në lidhje me mbajtësin e saj në formë të shtypur si dhe në format elektronik dhe përdoret për të vërtetuar bartësin e saj në botën reale dhe në internet. Kartela e tillë elektronike përdor teknologjinë e provuar kartelë e mençur për të komunikuar me botën e jashtme, bazuar në rekomandimet dhe udhëzimet e lëshuara nga Organizata Ndërkombëtare e Aviacionit Civil (ICAO), një organ i drejtuar nga Kombet e Bashkuara me mandat për vendosjen e standardeve ndërkombëtare të dokumenteve të udhëtimit [55]. Një profil përdoruesi i ruajtur në eID biometrike përmban një certifikatë digjitale X.509 dhe çelësin përkatës privat, në përputhje me Infrastrukturën Publike të ICAO (PKI), nënshkruar nga një autoritet certifikimi lëshues i vendit (CA).

Ministria e Punëve të Brendshme e Kosovës lëshoi kartelat biometrike nacionale të identitetit në dhjetor 2013, duke u bërë kështu vendi i parë që mbështeste protokolin e ri të Kontrollit të Qasjes Shtesë (SAC) për autentikimin e ndërsjelltë [56].

Kartela nacionale biometrike ID e Kosovës përmban tri aplikacione, siç është paraqitur në figurën 40, dhe ai përdor një SLE 78CLX1280P 16 bit procesor crypto nga Infineon. Ajo ka 128 kByte memorie të lexueshme vetëm programuese (EEPROM) dhe mbështet Rivist-Shamir-Adleman (RSA) 4096 bit gjatësi çelësi, ECC (Eliptic Curve Cryptography) deri në 521 bit dhe 3DES(triple Data Encryption Standard) dhe

AES(Advanced Encryption Algorithm) deri në 256 bit dhe komunikimi me botën e jashtme bëhet duke përdorur protokolin e NFC(near field communication) [57].

Figura 40. Kartela nacionale biometrike e identitetit (ID) dhe aplikacioni i hostuar

Softueri middleware i kartelave nacionale të identitetit komunikon duke përdorur standardin kriptografik me çelës publik (PKCS) # 11 dhe Crypto Service Provider (CSP) me aplikacione të interesuara kriptografike. Autentikimi në web me kartelë biometrike të identitetit bëhet duke përdorur certifikatat X.509 në dy forma: (i) certifikatën e identitetit ose (ii) certifikatën anonime, ku çelësi përkatës privat 2048 bit asnjëherë nuk e lë kartelën [58]. Qasja në çelësin privat është mbrojtur përmes Numrit të Identifikimit Personal (PIN), i cili i lëshohet qytetarit në formatin e letrës së mbrojtur. Një skenar i autentikimit në internet duke përdorur profilin real dhe anonim të një përdoruesi të ruajtur në kartelën eID është paraqitur në [59].

5.1 Rrethina Testuese

Kjo pjesë ofron një pasqyrë mbi mjedisin e eksperimentit. Nga kjo pjesë, dikush mund ta përsëris eksperimentin dhe të testoj rezultatet, duke përdorur parametra të ndryshëm me vektor testimi të paracaktuar.

Zhvillimi i Aplikacionit

BiometricEfficiency_FIEK është një aplikacion open source për sistemin operativ Windows 10, i zhvilluar në gjuhën programuese C # duke përdorur Microsoft Visual Studio 2015. *BiometricEfficiency_FIEK* nuk instalon libraritë e tjera dhe nuk ka nevojë për parakushte të tjera për tu instaluar. Kodi burimor mund të gjendet në [61].

Softueri Middleware i Kartelës së Mençur

Duke filluar nga Windows 2000, Microsoft ka integruar përdorimin e kartelave të mençura në aplikacionet e Windows, siç paraqitet në figurën 41 [61].

BiometricEfficiency_FIEK përdor funksionalitetin e Crypto Service Provider (CSP) specifike të shitësit, të mbështjellë si softuer middleware, për t'u qasur në funksionalitetin e plotë të funksioneve kriptografike të kartelës biometrike, të tilla si: encrypt, decrypt, nënshkruaj dhe verifiko.

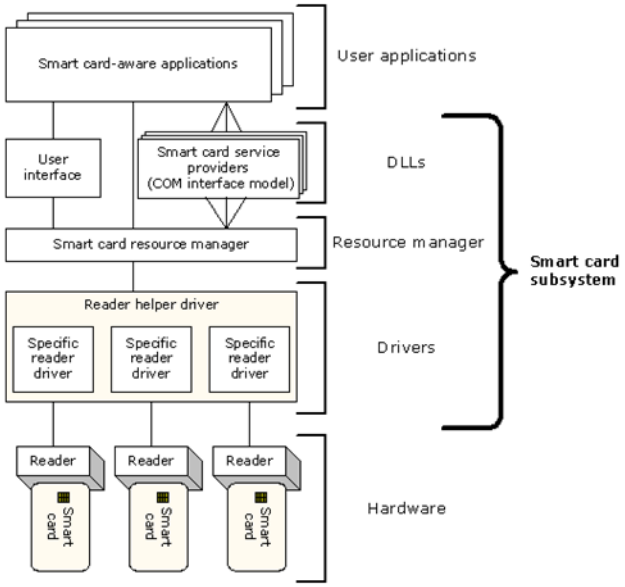


Figure 41. Arkitektura e kartelave të mençura në Windows [61]

Pseudocode

Kodi burimor është i organizuar në klasë ndihmëse, një për enkriptim dhe një klasë ndihmëse për nënshkrim digjital.

Klasa ndihmëse e enkriptimit përmban tre metoda për implementimin e enkriptimit match-on-card dhe match-off-card duke përdorur RSA dhe RSA CSP klasët nga .NET framework. Çdo metodë fillimisht ndan vektorin e testimit në blloqe, për të enkriptuar çdo bllok, pasi ne punojmë me algoritme enkriptimi në bllok. Metodat e mëposhtme janë zhvilluar:

- **`encryptRSACSP_pc(text)`** merrë një tekst argumenti të tipit string, i cili do të enkriptohet duke përdorur PC, duke përdorur çelësin publik të ruajtur lokalisht në PC.

- **`encryptRSACSP_card(text, certificate)`** merrë dy argumente, tekstin e tipit string dhe certifikatën e tipit X509Certificate2. Kjo metodë enkripton duke përdorur klasën RSA CSP, me çelësin publik nga certifikata në kartelën biometrike eID.

- **`encryptRSA_card(text, certificate)`** gjithashtu enkripton duke përdorur kartelën biometrike, por duke përdorur klasën RSA, siç është paraqitur tek Kodi 1.

```
function encryptRSACSP_pc(text)
{
    segmentLength ← 212
    loopLength ← text.Length/segmentLength+1

    RSACryptoServiceProvider rsa
    rsa.setPublicKey ← readPublicKey()

    for i←0 to loopLength do
        if (i=loopLength-1 or text.Length<segmentLength)
            copyLength ← text.Length-(i*segmentLength)
        else
            copyLength ← segmentLength

        segment ← text.Substring(i*segmentLength, copyLength);
        rsa.Encrypt(segment)
}
```

```
function encryptRSACSP_card(text, certificate)
{
    segmentLength ← 212;
    loopLength ← text.Length/segmentLength+1;

    RSACryptoServiceProvider rsa ← certificate.PublicKey.Key;
    for i ← 0 to i < loopLength do
        if (i=loopLength-1 or text.Length<segmentLength)
            copyLength ← text.Length-(i*segmentLength);
        else
            copyLength ← segmentLength;

        segment ← text.Substring(i*segmentLength, copyLength);
        rsa.Encrypt(segment);
}
```

```
function encryptRSA_card(text, certificate)
{
    segmentLength ← 212
    loopLength ← text.Length/segmentLength+1

    RSA rsa ← certificate.GetRSAPublicKey()

    for i←0 to loopLength do
        if (i=loopLength-1 or text.Length<segmentLength)
            copyLength ← text.Length-(i*segmentLength)
        else
            copyLength ← segmentLength

        segment ← text.Substring(i*segmentLength, copyLength);
        rsa.Encrypt(segment)
}
```

Nënshkrimi i klasës ndihmëse përmban tre metoda për implementimin e nënshkrimit digjital në match-on-card dhe match-off-card duke përdorur klasët RSA dhe RSA CSP, si:

- **`signRSACSP_pc(text)`** metoda përdoret për të nënshkruar të dhënat e tekstit, duke përdorur algoritmin me çelës publik RSA CSP, duke përdorur çelësin privat të ruajtur në PC.

- **`signRSACSP_card(text, certificate)`** do të përdoret si një metodë për të nënshkruar të dhënat e tekstit, duke përdorur çelësin privat në certifikatë.

- **`signRSA_card(text, certificate)`** merrë dy argumente, njëri tekstin për të nënshkruar dhe certifikatën, e cila përdor çelësin privat për të nënshkruar në mënyrë digjitale të dhënat, me klasë RSA, siç është paraqitur tek Kodi 2.

```
function signRSACSP_pc(text)
{
    RSACryptoServiceProvider rsa
    rsa.setPublicKey ← readPublicKey()

    rsa.SignData(text);
}
```

```
function signRSACSP_card(text, certificate)
{
    RSACryptoServiceProvider rsacsp ← certificate.PrivateKey
    rsacsp.SignData(text)
}
```

```
function signRSA_card(text, certificate)
{
    RSA rsa ← certificate.PrivateKey
    rsa.SignData(text)
}
```

Kodi 2: Pseudo funksionet kriptografike

5.2Të dhënat testuese

Funksionaliteti i softuerit

BiometricEfficiency_FIEK ka një interface të thjeshtë, siç paraqitet në figurën 42. Aplikacioni përdoret për të enkriptuar ose nënshkruar të dhëna, duke përdorur fuqinë e procesimit të PC-së ose fuqinë procesuese të kartelës biometrike nacionale. Qëllimi kryesor i aplikacionit është të mas efikasitetin, ose kohën e procesimit të të dyja metodave të procesimit: sistemeve match-off-card dhe match-on-card. Ky aplikacion kryesisht përdoret për qëllime eksperimentale, jo për enkriptim ose nënshkrimin e të dhënave.

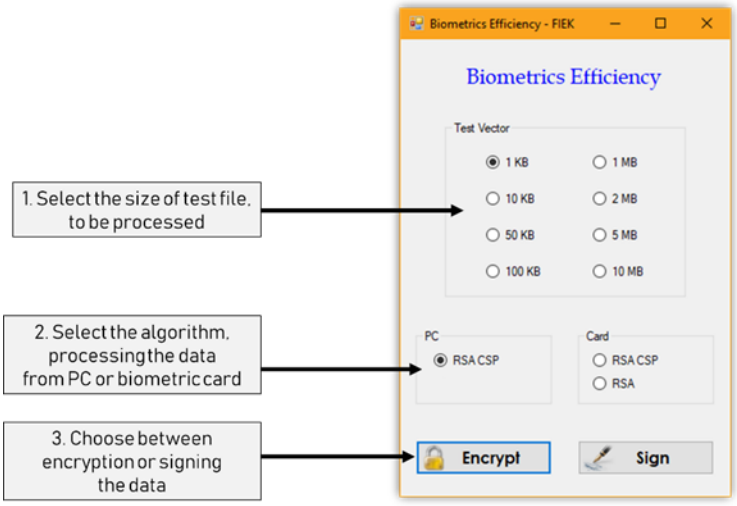


Figura 42. Ndërfaqja e aplikacionit BiometricEfficiency_FIEK

Të dhënat testuese të përdorura këtu janë skedar tekstual të rastësishëm me gjatësi të ndryshme, të cilat ofrojnë mundësinë për të studiuar ndikimin e gjatësisë ose madhësisë së skedarit në kohën e procesimit.

Hapat themelor për enkriptimin ose nënshkrimin e të dhënave, me një nga sistemet e procesimit janë:

1. Hapi i parë është të zgjidhni madhësinë e skedarit tekstual i cili do të enkriptohet ose nënshkruhet. Vektori testues përbëhet nga tetë skedar tekstual me tekst të rastit me madhësi të ndryshme, 1KB, 10KB, 50KB, 100KB, 1MB, 2MB, 5MB, 10MB. Çdo skedar do të ketë ndikim të ndryshëm në kohën e procesimit, i cili do të diskutohet më vonë. Teksti është tekst i rastit, siç paraqitet në figurën 43.

2. Hapi i dytë është zgjedhja e sistemit të procesimit dhe algoritmit për procesimin e të dhënave. Aplikacioni ofron të dyja sistemet e procesimit: match-off-card duke përdor një PC si sistem të jashtëm të procesimit dhe match-on-card duke përdorur kartelën biometrike nacionale eID si sistem procesimi. Ndërfaqja e PC-së implementon vetëm RSA CSP (Crypto Service Provider) [62] nga .NET framework si një algoritëm i vetëm i procesimit. Ndërsa kartela biometrike nacionale eID ofron dy algoritme procesimi: RSA [63] dhe RSA CSP. Ky krahasim është eksperimenti kryesor i kryer në këtë material, ku mat kohën e procesimit të dy sistemeve të procesimit.

3. Dhe hapi i tretë dhe i fundit është të zgjedhësh nëse përdoruesi dëshiron të enkriptoj ose të nënshkruaj të dhënat e zgjedhura, me algoritmin e përzgjedhur dhe sistemin e përzgjedhur të procesimit. Çdo eksperiment është bërë dhjetë herë dhe rezultatet janë shkruar në një skedar tekstual. Ky skedar tekstual tregon kohën e ekzekutimit për secilën prej dhjetë ekzekutimeve dhe kohën më të mirë, kohën më të keqe dhe kohën mesatare nga eksperimenti.

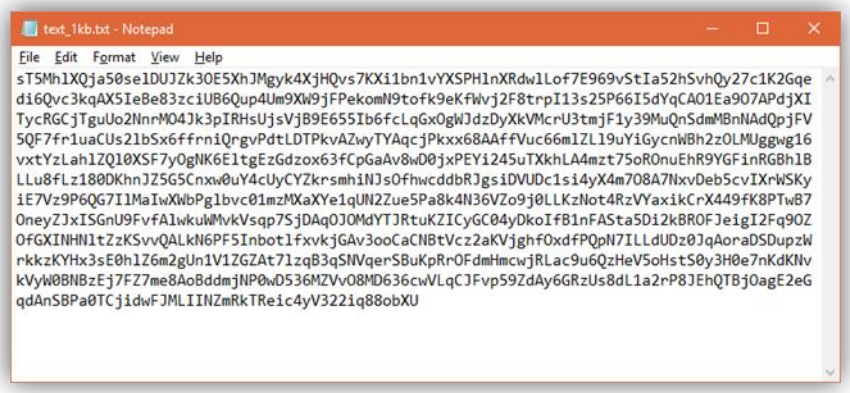


Figura 43. Skedari tekstual 1KB

5.3 Analiza e rezultateve eksperimentale

Të gjitha eksperimentet e kryera në këtë punim janë bërë duke përdorur *biometricefficiency_FIEK*, siç përshkruhet në pjesën e dytë të këtij kapitulli.

Hapi i parë është të zgjidhni madhësinë e skedarit tekstual për eksperiment. Përdoruesi mund të zgjedh midis 1KB, 10KB, 50KB, 100KB, 1MB, 2MB, 5MB dhe 10MB. Këta skedar, secili do të ketë ndikim në të dy proceset në mënyra të ndryshme, të cilat ndikojnë në efikasitetin ose kohën e nevojshme për procesim.

Hapi i dytë, që është hapi kryesor, është zgjedhja e algoritmit. Duke zgjedhur algoritmin, ne gjithashtu zgjedhim sistemin e procesimit. Match-off-card implementon vetëm RSA CryptoServiceProvider, dhe procesimi bëhet në PC. Nga ana tjetër, match-on-card implementon dy algoritme RSA dhe RSA CryptoServiceProvider, dhe kartela nacionale biometrike eID do të përdoret si sistem procesimi. Teksti kryesor i këtij rasti në këtë material do të krahasoj efikasitetin e match-off-card dhe match-on-card, për madhësi të ndryshme, algoritme dhe procese.

Hapi i fundit është të zgjedhësh procesin, enkriptimin ose nënshkrimin. Të dyja mund të përpunohen në PC ose kartelë dhe do të ndikojnë ndryshe në kohën e procesimit.

Siç është shpjeguar më lart, parametra të ndryshëm do të kenë ndikim në efikasitet. Të gjithë këta parametra do të grupohen në tri raste testimi. Rasti i parë i testimit do të krahasoj dy klasat .NET framework RSA dhe RSA CSP, në procesin e enkriptimit duke përdorur teknologjinë match-on-card. Rasti i dytë i testit do të krahasoj efikasitetin e sistemit të procesimit match-off-card and match-on-card tek enkriptimi, duke përdorur klasën RSA CSP. Dhe rasti i tretë i testimit do të krahasoj sërish sistemin e procesimit match-off-card dhe match-on-card, por tani në procesin e nënshkrimit, përsëri duke përdorur klasën e RSA CSP.

Enkriptimi me Kartelë Nacionale Biometrike eID - RSA vs RSA Crypto Service Provider (CSP)

Eksperimenti i parë do të krahasoj klasën RSA dhe klasën RSA CryptoServiceProvider nga .NET framework, në procesin e enkriptimit, duke përdorur sistemin e procesimit match-on-card në kartelë biometrike nacionale eID.

Eksperimenti do të përfshijë të gjithë vektorët e testimit, dhe për çdo skedar tekstual, eksperimenti do të ekzekutohet dhjetë herë. Kjo do të shërbej për saktësinë e eksperimentit dhe do të ndihmoj për të gjeneruar kohën mesatare, kohën më të mirë dhe kohën më të keqe të ekzekutimit.

Rezultatet eksperimentale, për të gjithë vektorët e testimit janë paraqitur në tabelën 6 dhe grafikisht në figurat 44.

	1 KB		**10 KB**		**50 KB**		**100 KB**		**1 MB**		**2 MB**		**5 MB**		**10 MB**	
	RSA	CSP	RSA	CSP	RSA	CSP	RSA	CSP	RSA	CSP	RSA	CSP	RSA	CSP	RSA	CSP
1	3.22	2.53	13.65	18.26	49.58	66.03	90.85	127.79	868.2	1,235.4	1,622.7	2,466.8	4,050.0	6,553.7	8,100.2	12,446.0
2	0.87	1.81	11.41	12.56	41.28	62.38	84.34	123.08	851.6	1,224.2	1,625.2	2,449.4	4,062.8	6,779.2	8,071.2	12,856.5
3	0.87	1.33	7.86	12.91	41.07	60.54	81.37	119.40	812.7	1,295.1	1,626.7	2,467.2	4,056.1	6,801.4	8,304.1	12,174.1
4	0.90	1.33	9.21	12.31	40.49	60.33	78.67	119.22	827.2	1,387.7	1,627.0	2,449.3	4,029.9	6,348.8	8,100.7	12,187.8
5	0.82	2.00	7.86	12.39	42.08	60.52	79.90	118.92	804.6	1,312.5	1,620.0	2,446.6	4,103.8	6,091.3	8,041.1	12,173.6
6	0.81	1.33	8.46	12.22	47.41	59.45	78.41	118.89	804.6	1,603.8	1,608.9	2,445.5	4,214.8	6,096.6	8,617.1	12,258.2
7	1.10	1.30	8.01	12.29	40.30	59.69	78.44	118.77	811.6	1,299.4	1,615.8	2,459.8	4,444.2	6,082.7	8,258.5	13,051.2
8	0.82	1.23	8.44	12.20	39.21	59.52	79.38	118.88	818.6	1,285.9	1,607.6	2,448.7	4,407.9	6,076.6	8,031.8	12,241.2
9	0.83	1.57	7.98	12.33	39.27	59.77	105.83	118.90	804.7	1,254.9	1,631.4	2,448.4	4,048.4	6,131.0	8,126.5	12,189.7
10	0.80	1.23	8.28	12.39	39.36	59.80	105.19	118.83	800.8	1,218.1	1,606.3	2,446.7	4,030.3	6,095.1	8,112.3	12,173.3

Tabela 6. Rezultatet RSA vs. RSA CSP

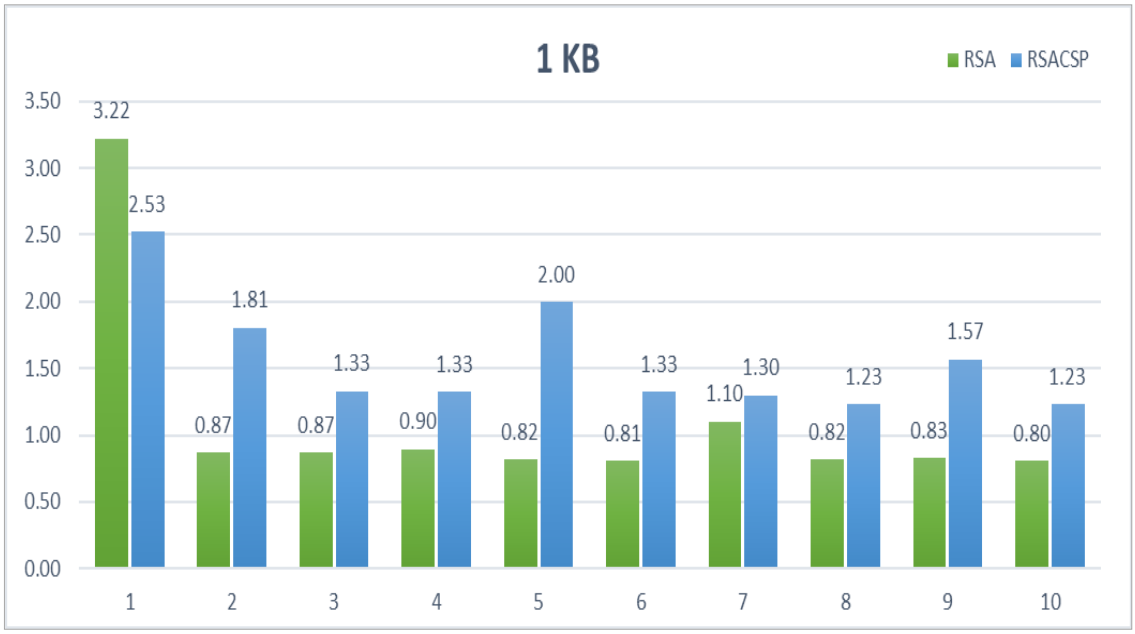


Figura 44(a). Rezultatet grafike të eksperimentit 1KB

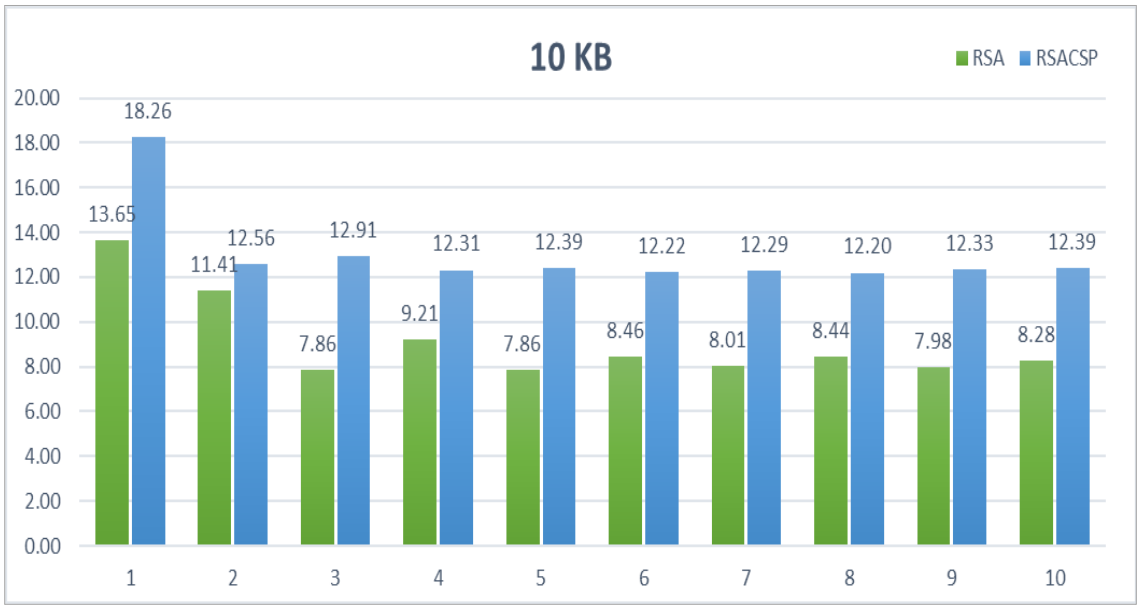


Figura 44(b). Rezultatet grafike të eksperimentit 10KB

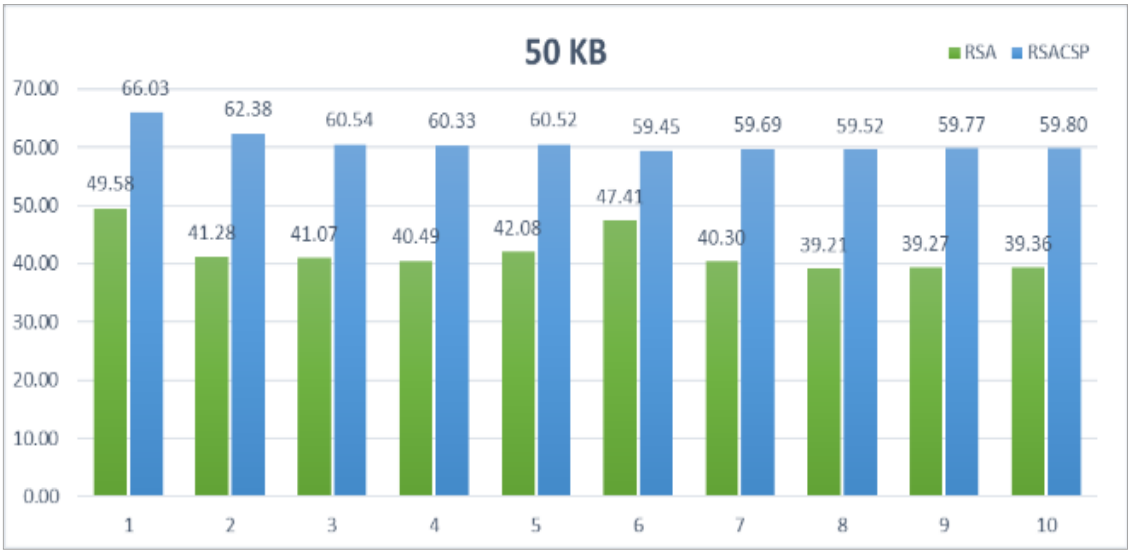
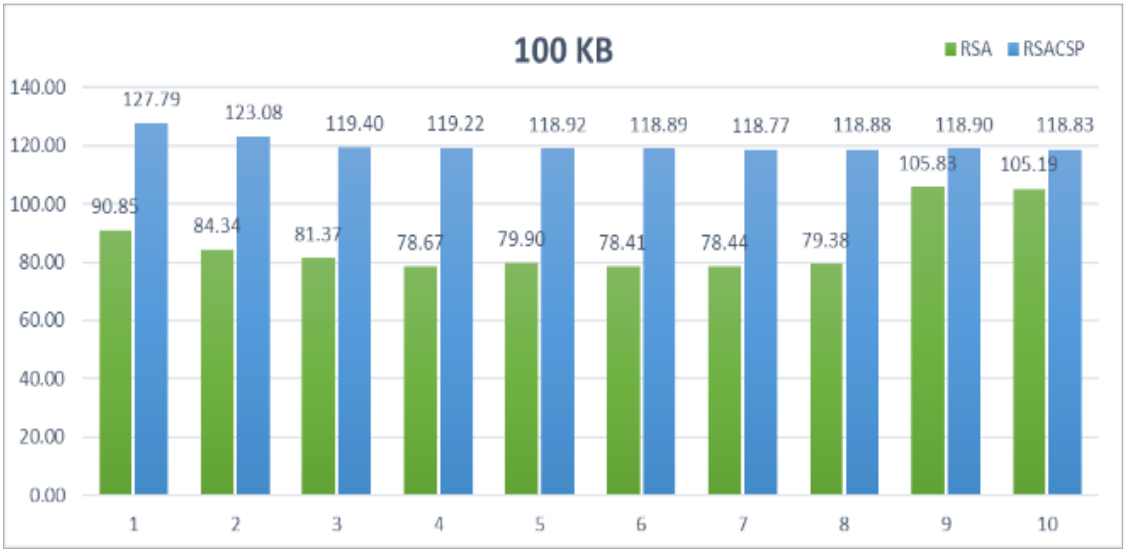


Figura 44(c). Rezultatet grafike të eksperimentit 50KB

Figura 44(d). Rezultatet grafike të eksperimentit 100KB



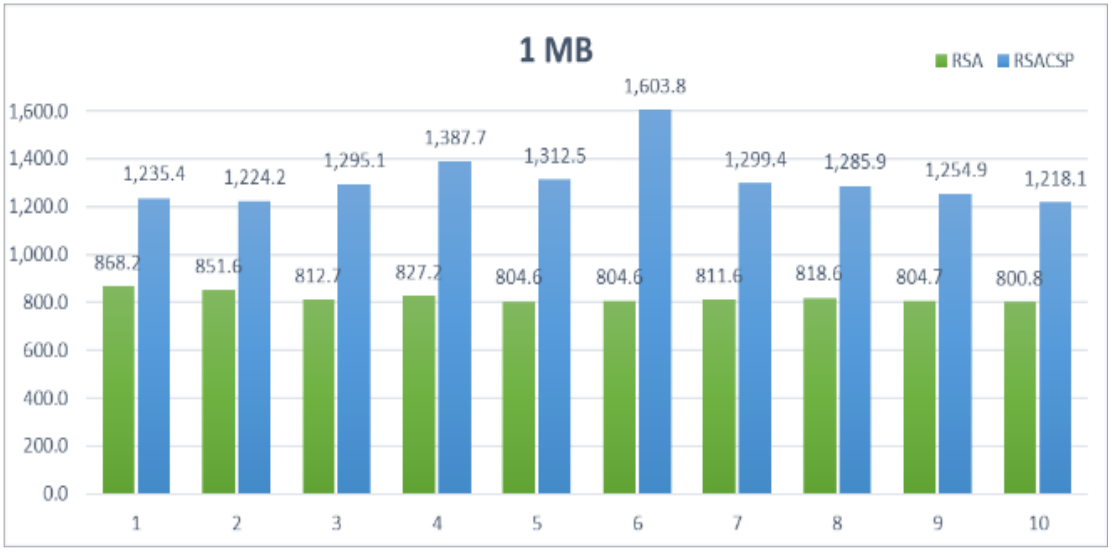


Figura 44(e). Rezultatet grafike të eksperimentit 1MB

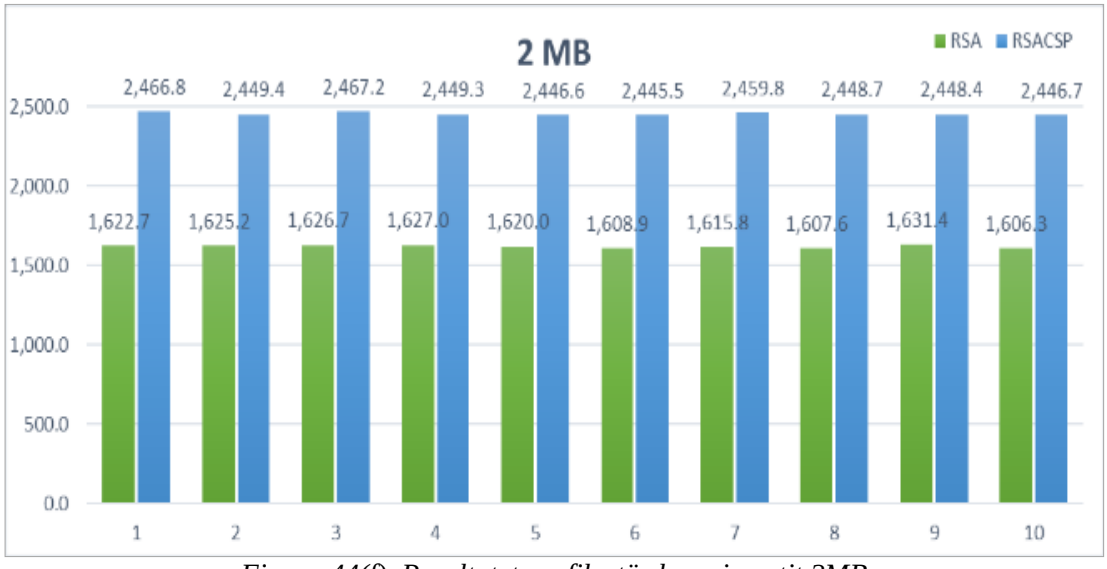


Figura 44(f). Rezultatet grafike të eksperimentit 2MB

Figura 44(g). Rezultatet grafike të eksperimentit 5MB

Figura 44(h). Rezultatet grafike të eksperimentit 10MB

Dy gjëra e karakterizojnë këtë eksperiment. Së pari, siç përshkruhet në figurën 44, mund të shihet nga eksperimenti i parë, që më shumë kohë (e shprehur në milisekonda) do të shpenzohen në fillim të një cikli eksperimentimi. Kjo mund të shihet veçanërisht në eksperiment me 1KB dhe 10KB, ku koha e procesimit është më e madhe në ciklin e parë. Kjo sepse koha e nevojshme për të ngarkuar të dhënat në kujtesë, si koncepte themelore nga organizimi i memories së kartelës së mençur [63]. Pas kësaj, koha e nevojshme për procesim është më e shkurtër.

Gjëja e dytë që duhet vënë re është ndryshimi në kohën e procesimit, kur rrisim madhësinë e të dhënave. Koha e procesimit do të rritet kur përpunojmë një sasi më të madhe të të dhënave, por klasa RSA kryen më mirë sesa klasa RSA CSP. Diferenca në kohën e procesimit rritet me çdo grup të dhënash më të mëdha, siç tregohet në tabelën 7 dhe figurën 45.

Në këtë rast, mund të konkludojmë se klasa RSA është më efikase se RSA CSP, veçanërisht kur kemi një sasi më të madhe të të dhënave.

Average Time [ms]			
	RSA	**RSA CSP**	Diff
1 KB	1.10	1.56	*41.72%*
10 KB	9.12	12.99	*42.45%*
50 KB	42.00	60.80	*44.76%*
100 KB	86.24	120.27	*39.46%*
1 MB	820.46	1,311.71	*59.88%*
2 MB	1,619.16	2,452.83	*51.49%*
5 MB	4,144.82	6,305.64	*52.13%*
10 MB	8,176.34	12,375.17	*51.35%*

Tabela 7. Koha mesatare RSA vs. RSA CSP

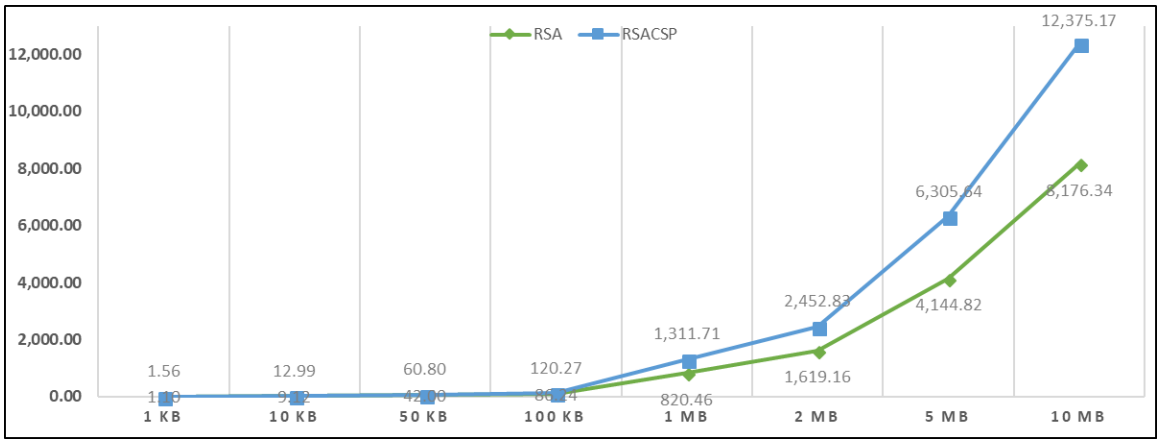


Figura 45. Rezultatet grafike RSA vs. RSA CSP

Enkriptimi duke përdorur klasën RSA CSP - Personal Computer (PC) vs Card

Në eksperimentin e dytë ne do të krahasojmë dy sistemet e procesimit, match-off-card vs match-on-card. Siç u tha më lart, procesimi match-off-card do të bëhet duke përdorur një PC, Intel Core i5 5200U CPU 2.20GHz, 8 GB RAM, sistem operativ Windows 10 64-bitësh dhe duke përdorur klasën RSA CSP nga .NET framework. Ndërsa, match-on-card përdor lexuesin e kartelës së mençur për të transferuar informacionin ndërmjet kartelës së mençur biometrike nacionale dhe PC.

Ashtu si në eksperimentin e parë, ky eksperiment do të përfshij të gjithë tetë skedarët e tekstual dhe eksperimenti do të ekzekutohet dhjetë herë për çdo skedar. Rezultatet eksperimentale, për të gjithë vektorët e testues janë paraqitur në tabelën 8 dhe figurat 46.

	1 KB		**10 KB**		**50 KB**		**100 KB**		**1 MB**		**2 MB**		**5 MB**		**10 MB**	
	RSA	CSP	RSA	CSP	RSA	CSP	RSA	CSP	RSA	CSP	RSA	CSP	RSA	CSP	RSA	CSP
1	3.16	2.53	12.55	18.26	60.67	66.03	120.60	127.79	1,217.8	1,235.4	2,479.8	2,466.8	6,603.3	6,553.7	13,160.6	12,446.0
2	1.48	1.81	20.58	12.56	59.56	62.38	119.04	123.08	1,214.6	1,224.2	2,438.2	2,449.4	6,419.6	6,779.2	12,201.2	12,856.5
3	1.33	1.33	12.12	12.91	59.65	60.54	118.85	119.40	1,216.3	1,295.1	2,434.1	2,467.2	6,257.3	6,801.4	12,180.8	12,174.1
4	1.29	1.33	12.07	12.31	68.15	60.33	119.35	119.22	1,216.6	1,387.7	2,440.3	2,449.3	6,359.9	6,348.8	12,173.6	12,187.8
5	1.28	2.00	12.05	12.39	59.38	60.52	118.84	118.92	1,223.2	1,312.5	2,431.2	2,446.6	6,083.2	6,091.3	12,155.7	12,173.6
6	1.24	1.33	12.54	12.22	59.50	59.45	118.75	118.89	1,219.8	1,603.8	2,434.7	2,445.5	6,084.8	6,096.6	12,931.1	12,258.2
7	1.25	1.30	12.57	12.29	59.45	59.69	118.80	118.77	1,220.2	1,299.4	2,434.5	2,459.8	6,126.9	6,082.7	12,235.5	13,051.2
8	1.24	1.23	12.11	12.20	60.55	59.52	119.10	118.88	1,217.1	1,285.9	2,432.5	2,448.7	6,106.4	6,076.6	12,215.9	12,241.2
9	1.23	1.57	12.06	12.33	60.70	59.77	119.27	118.90	1,217.0	1,254.9	2,429.7	2,448.4	6,079.7	6,131.0	12,179.4	12,189.7
10	1.23	1.23	11.99	12.39	59.44	59.80	118.84	118.83	1,217.6	1,218.1	2,517.4	2,446.7	6,076.0	6,095.1	12,272.7	12,173.3

Tabela 8. Rezultatet PC vs. Card

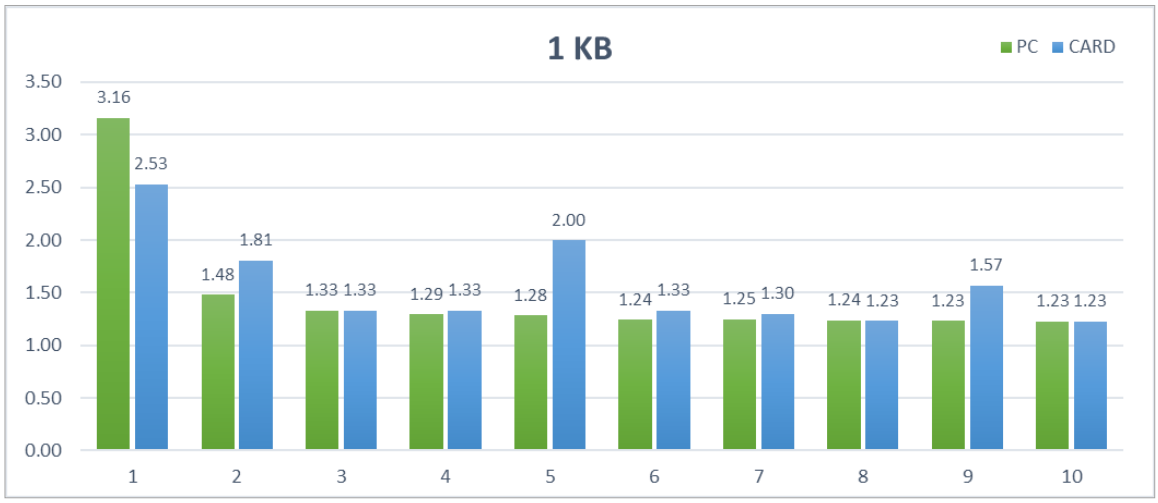


Figura 46(a). Rezultatet grafike të eksperimentit 1KB

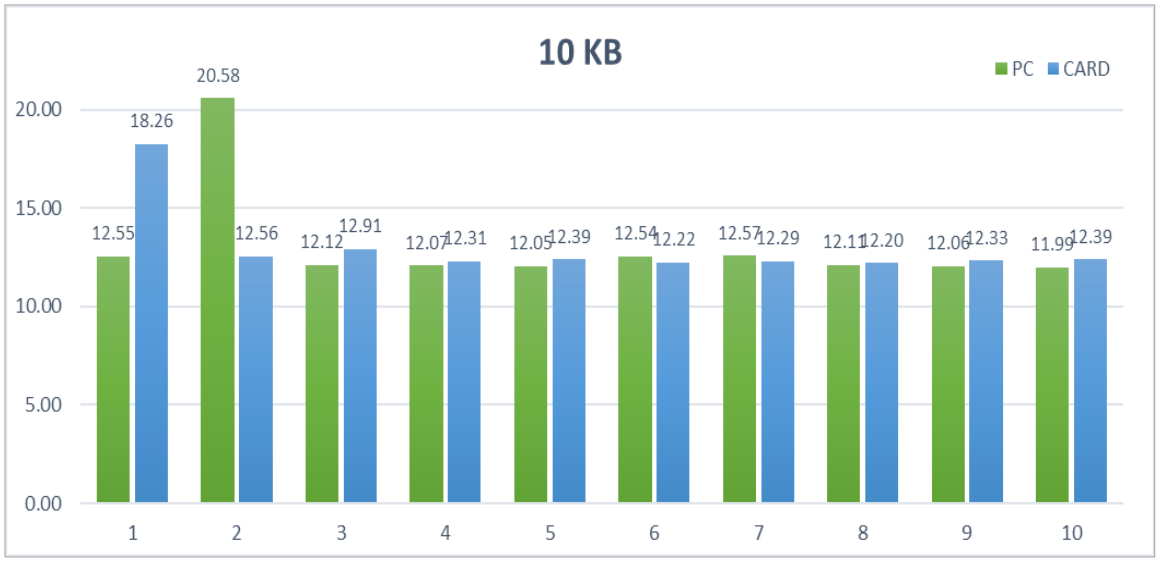


Figura 46(b). Rezultatet grafike të eksperimentit 10KB

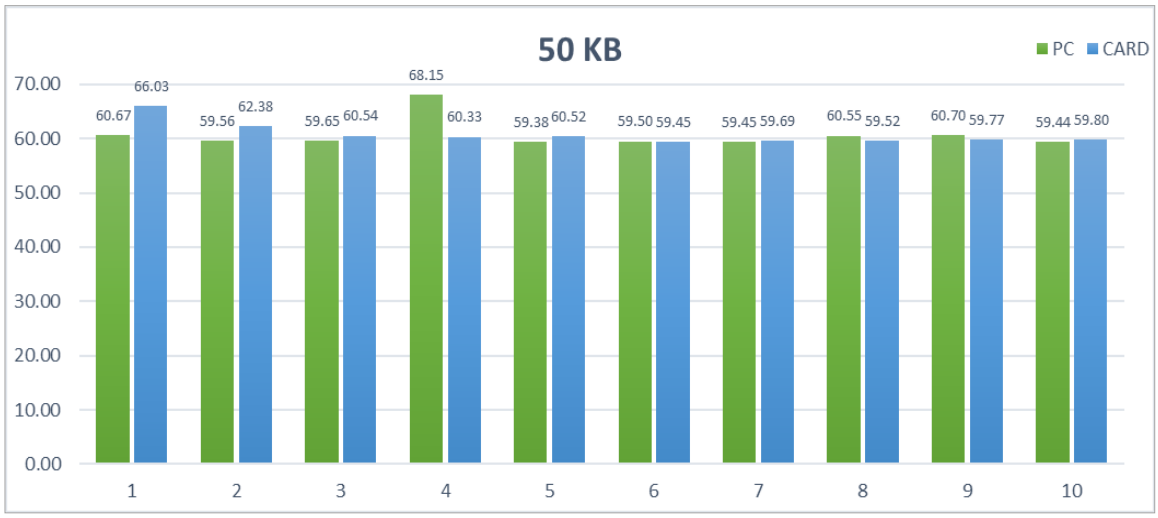


Figura 46(c). Rezultatet grafike të eksperimentit 50KB

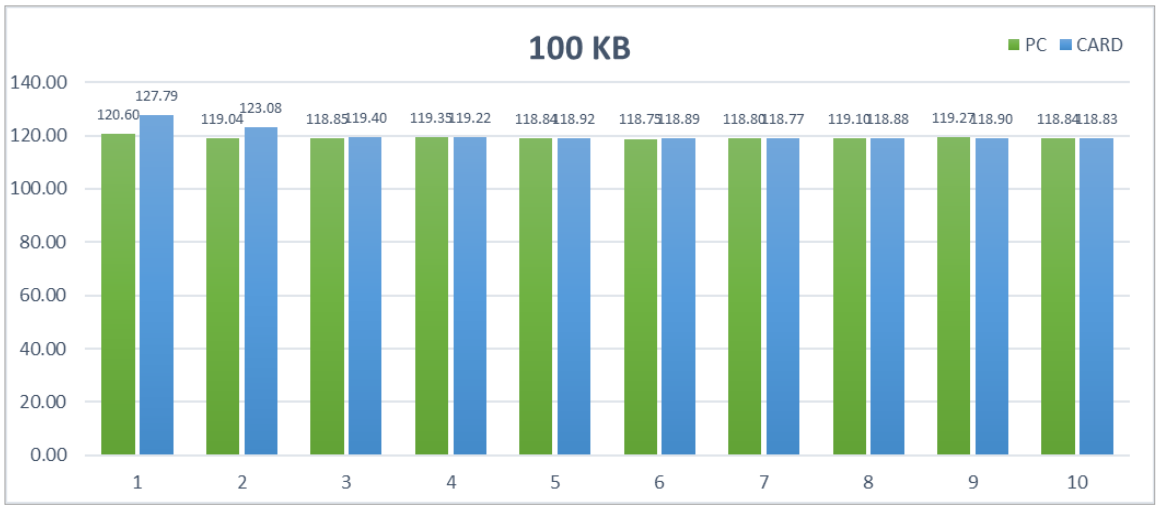


Figura 46(d). Rezultatet grafike të eksperimentit 100KB

Figura 46(e). Rezultatet grafike të eksperimentit 1MB

Figura 46(f). Rezultatet grafike të eksperimentit 2MB

Figura 46(g). Rezultatet grafike të eksperimentit 5MB

Figura 46(h). Rezultatet grafike të eksperimentit 10MB

Ashtu si në eksperimentin e mëparshëm, do të nevojitet më shumë kohë në fillim të çdo eksperimenti, për të njëjtën arsye si më parë. PC-të gjithashtu kanë memorie të brendshme dhe do të nevojitet më shumë kohë për të ngarkuar dhe ruajtur të dhënat [64]. Kokluzioni kryesor që mund të nxjerrim nga ky eksperiment është se koha e përpunimit rritet në mënyrë eksponenciale me madhësinë e një skedari, siç tregohet në tabelën 9 dhe figurën 47. Por, nuk mund të nxjerrim konkluzion se cila kohë e procesimit është më efikase, pasi që të dyja sistemet kryejnë afërsisht të njëjtën gjë. Pra, asnjëra prej sistemeve të procesimit match-on-card ose match-off-card nuk funksionon më mirë dhe të dyja mund të përdoren për enkriptim të informacionit.

Average Time [ms]			
	PC	**Card**	Diff
1 KB	1.47	1.56	6.20%
10 KB	13.06	12.99	-0.59%
50 KB	60.70	60.80	0.16%
100 KB	119.14	120.27	0.95%
1 MB	1,218.03	1,311.71	7.69%
2 MB	2,447.24	2,452.83	0.23%
5 MB	6,219.72	6,305.64	1.38%
10 MB	12,370.65	12,375.17	0.04%

Tabela 9. Koha mesatare PC vs. Card

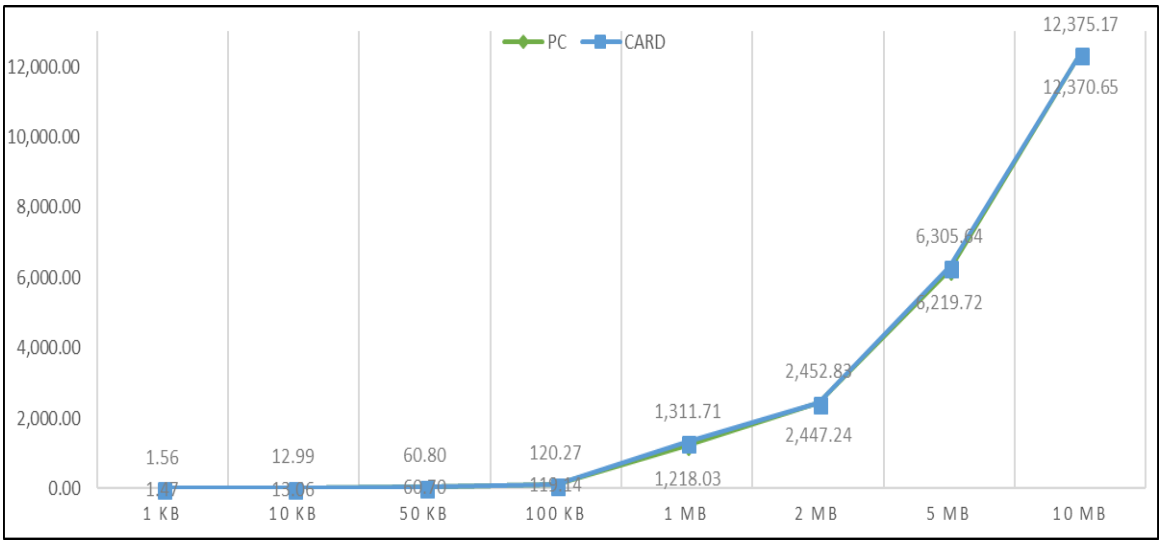


Figura 47. Koha mesatare e PC vs. card

Nënshkrimi duke përdorur klasën RSA CSP - PC vs Card

Eksperimenti i tretë dhe i fundit i krahason përsëri dy sisteme procesimi, match-off-card vs. match-on-card, duke përdorur procesin e nënshkrimit. Ne përdorim të njëjtat pajisje, PC për match-off-card dhe kartën biometrike nacionale eID për match-on-card.

Rezultatet e eksperimentit, për të gjithë tetë skedarët tekstual dhe dhjetë cikleve për çdo skedar, janë paraqitur në tabelën 10 dhe figurën 48.

	1 KB		10 KB		50 KB		100 KB		1 MB		2 MB		5 MB		10 MB	
	RSA	CSP	RSA	CSP	RSA	CSP	RSA	CSP	RSA	CSP	RSA	CSP	RSA	CSP	RSA	CSP
1	10.33	2.38	7.24	17.28	7.41	66.17	7.88	134.81	16.3	1,258.8	21.1	2,448.2	52.5	6,187.9	73.6	12,189.5
2	7.09	2.19	7.29	12.74	7.41	62.28	7.81	123.81	13.8	1,236.4	20.6	2,488.6	48.7	6,125.3	73.1	12,153.6
3	7.10	2.60	7.15	12.37	7.82	62.15	7.81	120.42	13.9	1,249.5	20.3	2,441.4	40.1	6,123.7	73.6	12,157.3
4	7.18	2.67	7.22	11.99	7.41	61.33	7.74	118.84	13.8	1,271.7	20.3	2,429.1	40.3	6,117.0	95.6	12,669.9
5	7.09	2.43	7.23	12.49	7.49	62.36	7.78	118.83	13.8	1,248.7	20.3	2,496.6	40.4	6,119.1	100.9	12,627.0
6	7.12	2.22	7.15	12.66	7.48	59.72	7.81	118.83	13.8	1,231.7	21.2	2,679.9	41.3	6,128.2	74.8	12,154.5
7	7.18	1.96	7.22	13.40	7.40	59.97	7.78	119.57	13.7	1,231.9	20.4	2,608.8	41.0	6,117.7	73.0	12,160.6
8	7.63	1.33	7.23	12.08	7.93	59.54	7.74	118.99	13.7	1,233.5	20.5	2,658.4	40.6	6,303.1	73.0	12,162.9
9	7.16	1.33	7.15	12.30	7.50	59.59	7.86	119.16	13.7	1,236.4	20.5	2,549.1	40.4	6,683.6	73.1	12,300.0
10	7.19	1.33	7.18	12.72	7.46	59.61	7.91	118.72	13.7	1,236.0	20.4	2,428.7	40.4	6,241.6	96.1	13,158.7

Tabela 10. Nënshkrimi RSA vs. card

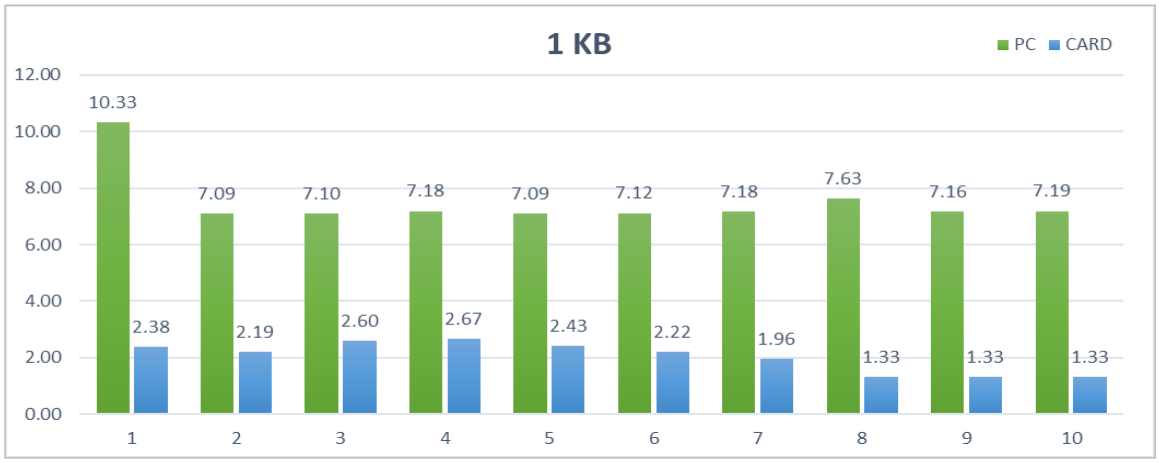


Figura 48(a). Rezultatet grafike të eksperimentit për nënshkrim RSA vs. card 1KB

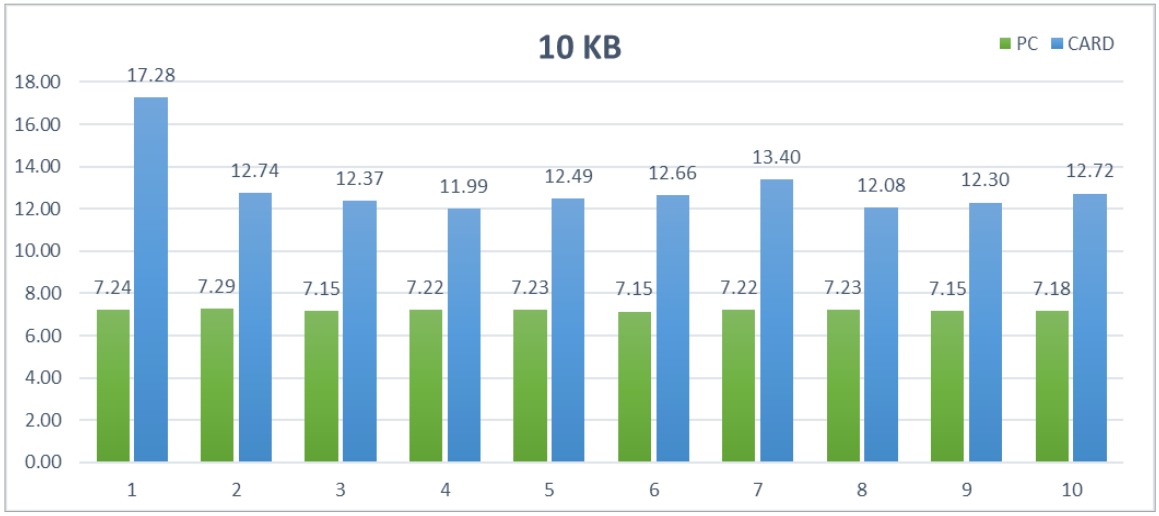


Figura 48(b). Rezultatet grafike të eksperimentit për nënshkrim RSA vs. card 10KB

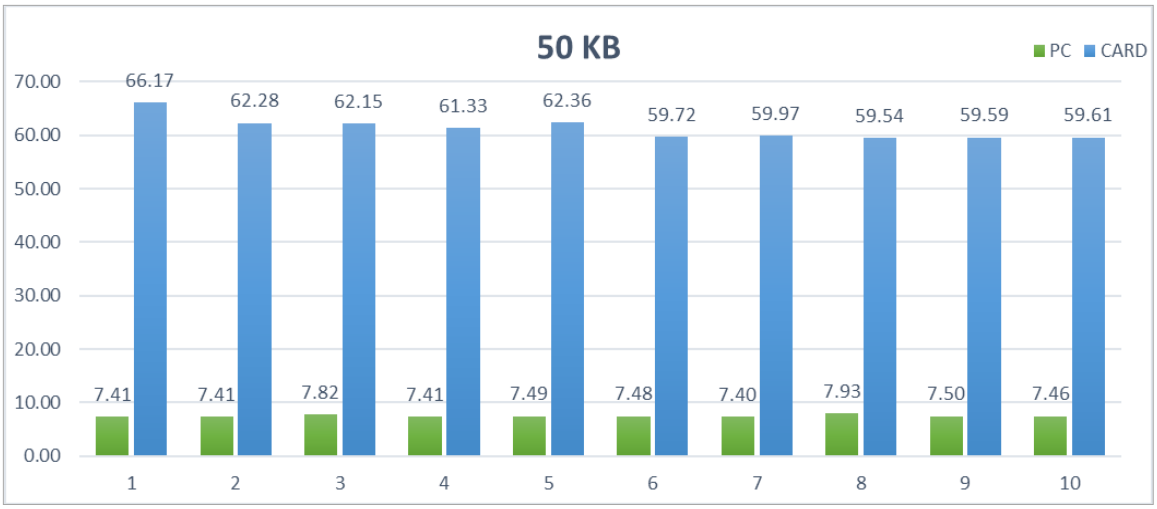


Figura 48(c). Rezultatet grafike të eksperimentit për nënshkrim RSA vs. card 50KB

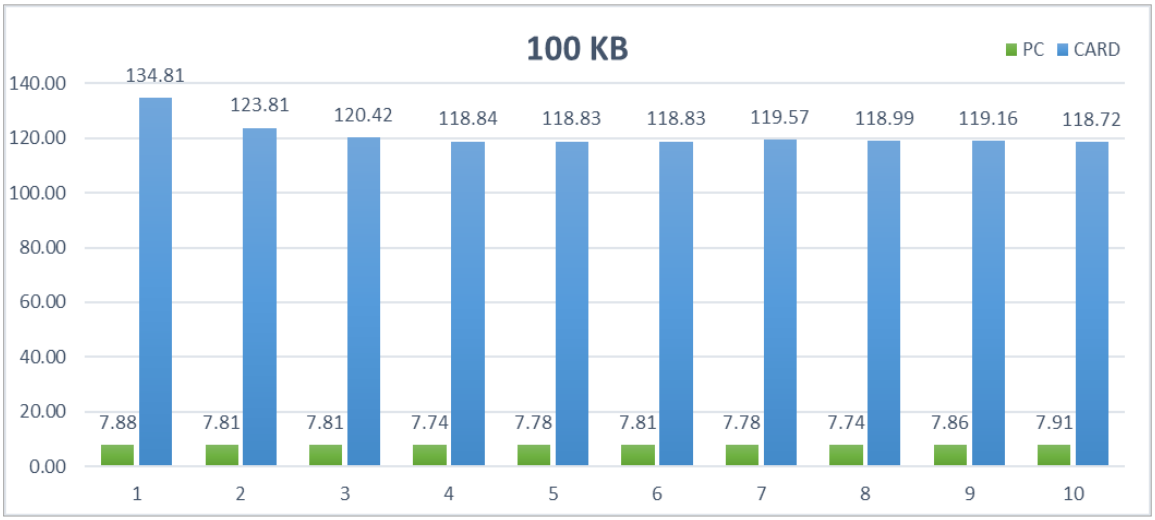


Figura 48(d). Rezultatet grafike të eksperimentit për nënshkrim RSA vs. card 100KB

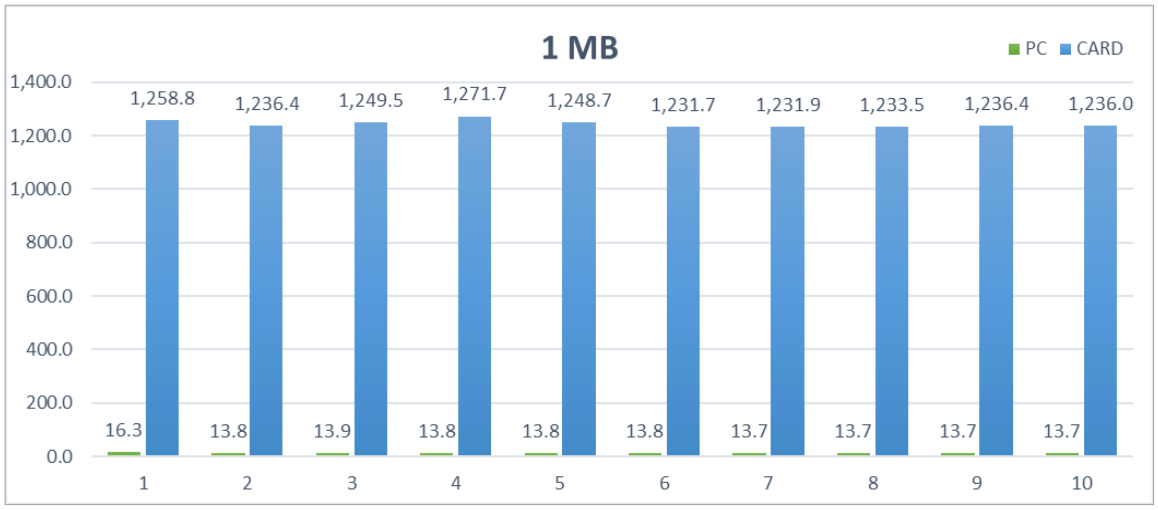


Figura 48(e). Rezultatet grafike të eksperimentit për nënshkrim RSA vs. card 1MB

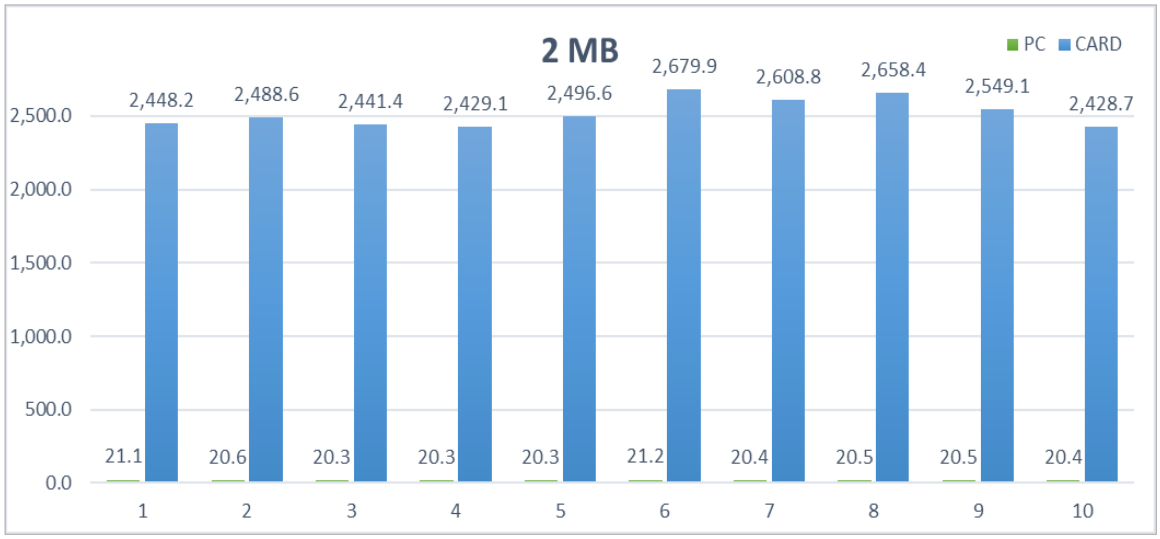


Figura 48(f). Rezultatet grafike të eksperimentit për nënshkrim RSA vs. card 2MB

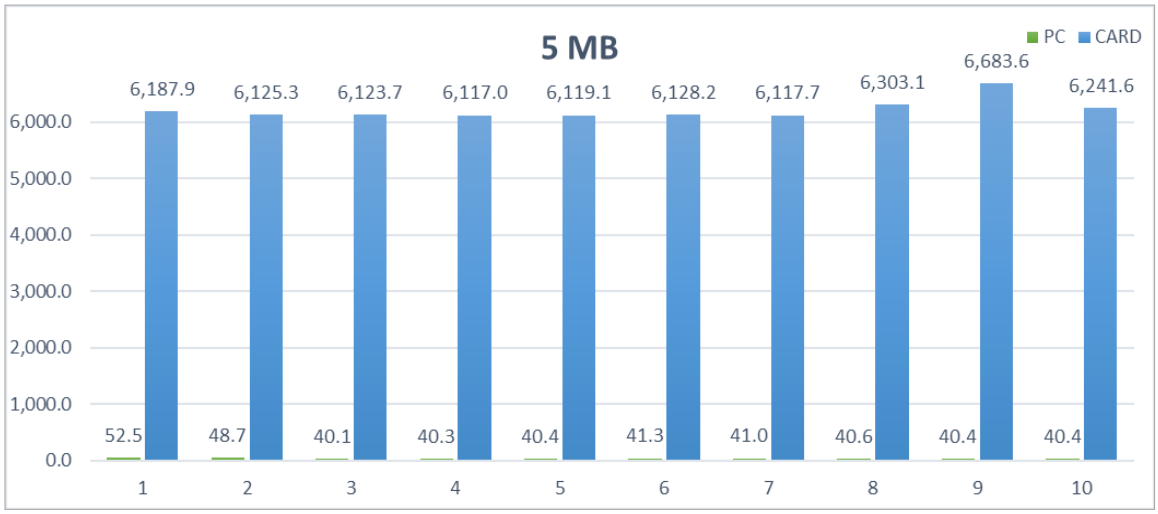


Figura 48(g). Rezultatet grafike të eksperimentit për nënshkrim RSA vs. card 5MB

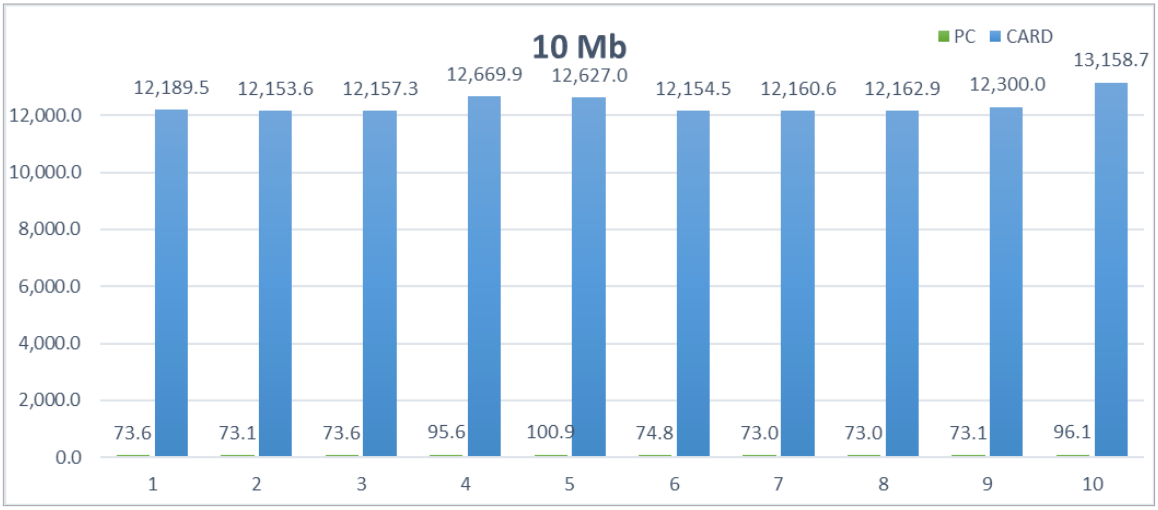


Figura 48(h). Rezultatet grafike të eksperimentit për nënshkrim RSA vs. card 10MB

Ky eksperiment është shumë interesant, nga i cili mund të nxjerrim disa konkluzione. Vetëm në rastin e testit 1KB kartela biometrike nacionale ka performuar më mirë sesa PC-ja. Në shtatë skedarët të tjerë tekstual, kompjuteri personal (PC) ka performuar më mirë sesa kartela biometrike nacionale. Nga tabela 11 dhe figura 49, vëmë re se koha e procesimit të match-off-card rritet shumë pak, kur rrisim madhësinë e skedarëve testues. Ky nuk është rasti me sistemin e procesimit të match-on-card, ku koha e procesimit rritet në mënyrë eksponenciale kur rrisim madhësinë e skedarit.

Pra, nga ky eksperiment ne mund të konkludojmë se, gjatë procesit të nënshkrimit, match-on-card e përgjithshme është më efikase se një match-off-card, veçanërisht për skedarët më të mëdhenj. Match-on-card mund të përdoret ende, në rast se kemi skedar të vegjël për t'u procesuar.

Average Time [ms]			
	PC	**Card**	Diff
1 KB	7.51	2.04	-72.77%
10 KB	7.21	13.00	80.45%
50 KB	7.53	61.27	713.49%
100 KB	7.81	121.20	1451.75%
1 MB	14.01	1,243.48	8772.78%
2 MB	20.57	2,522.90	12165.59%
5 MB	42.56	6,214.72	14500.78%
10 MB	80.68	12,373.40	15237.16%

Tabela 11. Koha mesatare për nënshkrim PC vs. card

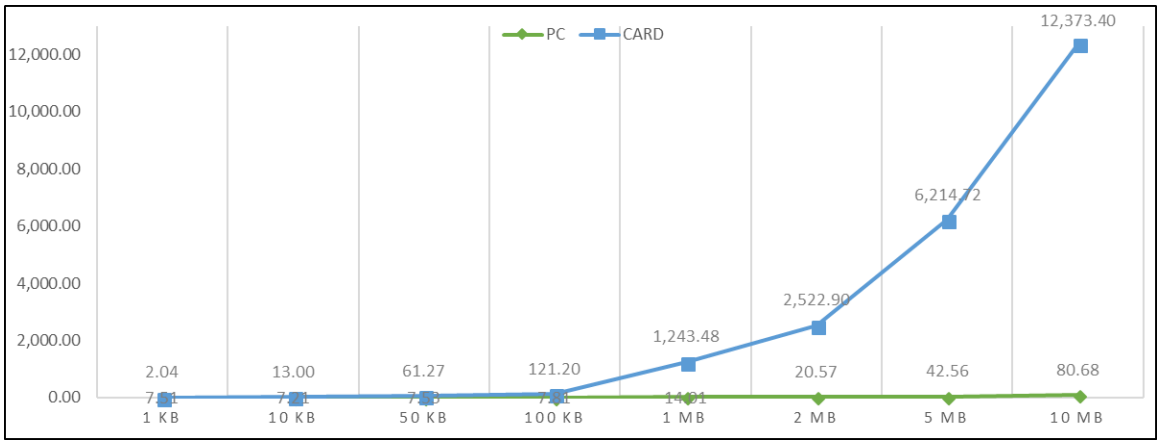


Figura 49. Koha mesatare për nënshkrim RSA vs. card

Një formë tjetër e përfaqësimit të të dhënave mund të përdoret, veçanërisht për përfaqësimin e figurave 45, 46 dhe 49 duke përdorur funksionin Weierstrass-Mandelbrot si në [65] dhe [66], gjë që do të jetë punë për të ardhmen.

6 KONKLUZIONE DHE REKOMANDIME

Rritja e shpejtë e internetit dhe tendenca gjithnjë në rritje për të lidhur të gjitha pajisjet dhe shërbimet ka rritur efikasitetin e shumë shërbimeve qeveritare. Pothuajse shumica e tyre janë konvertuar në shërbime elektronike që qytetari mund ti kryej përmes internetit. I njëjtë ishte rasti gjithashtu edhe me nënshkrimin tradicional, me dorë. Përdorimi i funksioneve kriptografike, në veçanti aplikimi i kryptografisë me çelësa publik, lehtë zëvendëson nënshkrimin me dorë me nënshkrim elektronik (kriptografik). Duke u bazuar në kornizën ligjore të Kosovës por edhe të Bashkimit Evropian (BE), nënshkrimi digjital ka statusin e njëjtë jurdik sikurse nënshkrimi klasik, i shkruar me dorë. Nënshkrimi në formatin PDF është një nga shumë aplikacione që përdorin nënshkrimin digjital. Aplikacioni i zhvilluar në kuadër të këtij punimi përdor standardin PAdES, bazuar në rregulloret eIDAS të BE-së. Në këtë disertacion është përdorur kartela elektronike (eID) e personalizuar edhe me të dhëna biometrike të qytetarit të Kosovës, dhe softueri ndërlidhës (middleware) i saj për të komunikuar me aplikacionin. Duke mundësuar kështu autentikim të sigurt në rend të parë dhe shërbime më efikase nga qeveria tek qytetari, por edhe nga qytetari në qytetar.

Në komunitetin, veçmas akademik, ka pasur debate të vazhdueshme lidhur me përformacën dhe efikasitetin e përdorimit të kartelës elektronike, me të dhëna biometrike, për autentikim në shërbime elektronike qeveritare të ofruara përmes internetit. Për këtë qëllim është zhvilluar aplikacioni *BiometricEfficiency_FIEK*, ku janë krahasuar përformancat e krahasimit të metodave kriptografike "Match-on-Card" kundrejt "Match-off-Card". Match-on-card dhe match-off-card janë dy sisteme procesimi të përdorura sot për procesimin e sigurisë. Në këtë punim, "match-on-card" përdor kartelën biometrike nacionale, me arkitekturë të avancuar harduerike, për të procesuar të dhëna, ndërsa kompjuteri personal (PC) është përdorur si një pajisje në "match-off-card". Midis tyre ka shumë avantazhe dhe disavantazhe, ku secila luan një rol të rëndësishëm kur zgjedh ato si pajisje procesimi.

Siç kanë treguar rezultatet eksperimentale, të paraqitura detajisht në kapitullin paraprak, ka pak raste zakonisht kur merret një sasi e vogël e të dhënave, kartela biometrike ka një performancë më të mirë. Madje edhe për një sasi shumë të vogël të të dhënave, më pak se 1KB, kartela biometrike tejkalon PC, siç paraqitet në figurën 49. Duke rritur sasinë e të dhënave, performanca e kartelës biometrike zvogëlohet, siç pritej, për shkak të kufizimeve të burimeve harduerike të kartelës biometrike, siç përshkruhet në në atë pjesë.

Puna e ardhshme do të shtojë më shumë funksionalitet në aplikacionin biometricefficiency_FIEK, të tilla si përdorimi i algoritmeve të lakorës eliptike, verifikimi i nënshkrimit digjital dhe shtimi i më shumë algoritmeve të enkriptimit si AES, etj.

Referencat

[1] Kristaq Filipi, Algjebra dhe Gjeometria (Ribotim), Tiranë, 2015

[2] Kristaq Filipi, Algjebër Abstrakte, Tiranë, 2013

[3] G.Rodriquez, Algebra per Ingegneria e Informatica, clup 1993, Milano

[4] Nigel Smart, Cryptography: An Introduction (3rd Edition), 2004

[5] Christof Paar and Jan Pelzl, Understanding Cryptography, Springer Heidelberg Dordrecht London New York

[6] Emrush Gashi, Algjebra 1, Universiteti i Prishtinës, Prishtinë 2001

[7] Public Key Infrastructure. *Wikipedia.* Marrur nga: [*http://en.wikipedia.org/wiki/Public_key_infrastructure*] datë: 20.12.2018.

[8] Single Point of Contact. *SecurityON.* Marrur nga: [*https://www.entrust.com/wpcontent/uploads/2013/05/DS_ePassport-SPOC _ web_Aug2012.pdf*], datë: 08.10.2017.

[9] Schneier, Bruce. *Applied Cryptography.* s.l. : John Wiley & Sons,Inc, 1996. ISBN: 0471128457.

[10] Stallings, William. *Cryptography and Network Security.* s.l. : Prentice Hall, 2010. ISBN 0-13-243310-9.

[11] Crypto Basics. *SECURITY, COUNT UPON.* Marrur nga: [*http://countuponsecurity.com/tag/cryptography*], datë: 20.12.2018.

[12] John Wagnon, Senior Solution Developer at F5 Networks. Marrur nga: [*https://www.linkedin.com/pulse/real-cryptography-has-curves-making-case-ecc-john-wagnon*], datë: 12.06.2017.

[13] Digital Signatures. Microsoft. Marrur nga: [*http://technet.microsoft.com/en-us/library/cc962021.aspx*], datë: 18.11.2017.

[14] Attack on Cryptography By Mohd Zaid Waqiyuddin Mohd Zulkifli. Marrur nga: [*https://idazuwaika.files.wordpress.com/2008/06/attack-on-cryptography.pdf*], datë: 25.12.18

[15] Types_of_Cryptographic_Attacks. Marrur nga:[*http://www.academia.edu/4739047/Types_of_Cryptographic_Attacks*]

[16] Man-in-the-Middle-Attack. Marrur nga: [*http://searchsecurity.techtarget.com/definition/man-in-the-middle-attack*]

[17] SANS Institute InfoSec Reading Room, Analyzing Man-in-the-Browser (MITB) Attacks; marrur nga: [*https://www.sans.org/reading-room/whitepapers/forensics/*

analyzing-man-in-the- browser-mitb-attacks-35687], data 25.12.2018

[18] Brute-Force Attacks Explained: How All Encryption is Vulnerable, Chris Hoffman Marrur nga: [*https://www.howtogeek.com/166832/brute-force-attacks-explained-how-all-encryption-is-vulnerable*], datë: 25.12.2018

[19] SANS Institute InfoSec Reading Room, Session Hijacking in Windows Networks; Marrur nga: [*https://www.sans.org/reading-room/whitepapers/windows/session-hijacking-windows-networks-2124*], datë: 25.12.2018

[20] Compromised Key Attacks. Marrur nga: [*https://technet.microsoft.com/en-us/library/dd572304(v=office.13).aspx*], datë: 23.12.2018

[21] Security Tip (ST04-015), Understanding Denial-of-Service Attacks. Marrur nga: [*https://www.us-cert.gov/ncas/tips/ST04-015*], datë: 24.12.2018

[22] Marrur nga: [*http://opensourceforu.efytimes.com/2013/05/cyber-attacks-explained-cryptographic-attacks*], datë: 24.12.2018

[23] Wolfgang Rankl and Wolfgang Effing. Smart Card Handbook. Fourth Edition. 2010. ISBN: 978-0-470-74367-6

[24] Smart Cards and Biometrics, A Smart Card Alliance Physical Access Council White Paper; marrur nga: [*http://www.smartcardalliance.org/resources/pdf/Smart_Cards_and_Biometrics_030111.pdf*], datë: 25.12.2018

[25] Smart Card Technology, Secure Technology Alliance; Marrur nga: [*http://www.smartcardalliance.org/smart-cards-intro-primer*], Datë: 23.12.2018

[26] Wolfgang Rankl & Wolfgang Effing - Smart Card Handbook

[27] Jonathan Katz. Digital Signatures. 2010. ISBN 978-0-387-27711-0

[28] Marrur nga: [*http://www.herongyang.com/PKI/Digital-Signature-Scheme.jpg*]; Datë: 22.12.2018

[29] Man Young Rhee - Internet Security Cryptographic Principles, Algorithms and Protocols

[30] RFC 3852, Cryptographic Message Syntax (CMS); Marrur nga: [*http://tools.ietf.org/pdf/rfc3852.pdf*], datë: 22.12.2018

[31] Introduction to ASN.1; Marrur nga: [*http://www.itu.int/en/ITUT/asn1/Pages/introduction.aspx*], datë: 12.05.2018

[32] Marrur nga: [*http://en.wikipedia.org/wiki/Abstract_Syntax_Notation_One*]

[33] Marrur nga: [*https://www.eldos.com/security/articles/7031.php?page=all*]

[34] ETSI TS 101 733 V2.2.1 - CMS Advanced Electronic Signatures (CAdES)

[35] Adobe System Incorporated. PDF Reference. Six Edition.

[36] John Warnock. The Camelot Project. Marrur nga: [*http://www.planetpdf.com/planetpdf/pdfs/warnock_camelot.pdf*]

Datë: 12.05.2018

[37] The AdES family of standards: CAdES, XAdES, and PAdES. Marrur nga: [*http://blogs.adobe.com/security/91014620_eusig_wp_ue.pdf*] Datë: 24.12.2018.

[38] ETSI TS 102 778-1 V1.1.1 - Part 1: PAdES Overview - a framework document for PAdES

[39] Marrur nga: [*https://www.eldos.com/security/articles/6963.php?page=all#*]

[40] Regulation (EU) No 9010/2014 of the European Parlament and of the Council

[41] Adobe Acrobat 9 Digital Signature Appearance. Marrur nga: [*https://www.adobe.com/content/dam/acom/en/devnet/acrobat/pdfs/acrobat_digital_signature_appearances_v9.pdf*] ; Datë: 12.05.2018

[42] ETSI TS 102 778-1 V1.1.1. Part 1: PAdES Overview - a framework document for PAdES. Marrur nga: [*http://www.etsi.org/deliver/etsi_ts/102700_102799/10277801/01.01.01_60/ts_10277801v010101p.pdf*]; Datë: 12.05.2018

[43] ETSI TS 102 778-2 V1.2.1 - Part 2: PAdES Basic - Profile based on ISO 32000-1

[44] ETSI TS 102 778-3 V1.2.1 - Part 3: PAdES Enhanced – PadES-Bes and PAdES-EPES Profiles

[45] ETSI TS 102 778-4 V1.2.1 - Part 4: PAdES Long Term – PadES-LTV Profile

[46] ETSI TS 102 778-5 V1.1.2 - Part 5: PAdES for XML Content - Profiles for XAdES Signatures. Marrur nga: [*http://www.bouncycastle.org*], Datë: 12.10.2018

[47] Bouncy Castle (cryptography), Wikipedia; Marrur nga: [*http://en.wikipedia.org/wiki/Bouncy_Castle_%28cryptography%29];* Datë: 24.12.2018

[48] Biometrics for Payment Applications the SPA Vision on Financial Match-on-Card; Smart Payment Association (SPA): Munich, Germany November 2013.

[49] Pang, C.T.; Yun, Y.W.; Xudong, J. On-Card Matching. In Encyclopedia of Biometrics; Institute for Infocomm Research: 2009.

[50] Smart Cards and Biometrics. In A Smart Card Alliance Physical Access Council White Paper; Smart Card Alliance: March 2011.

[51] Bringer, J.; Chabanne, H.; Pointcheval, D.; Zimmer, S. An Application of the Boneh and Shacham Group Signature Scheme to Biometric Authentication. In Proceedings of the 3rd International Workshop on Security (IWSEC ‘08), Kagawa, Japan, 25–27 November 2008.

[52] Grother, P.; Salamon, W.; Watson, C.; Indovina, M.; Flanagan, P. MINEX II Performance of Fingerprint Match-on-Card Algorithms Phase II/III Report-NIST Interagency Report 7477; Information Access Division-National Institute of Standards and Technology: 2009.

[53] Security and Performance Evaluation Platform of Biometric Match on Card. In

Proceedings of the International Conference on Mobile Applications and Security Management (ICMASM), Sousse, Tunisia, 22–24 June 2013.

[54] Cooper, D.; Dang, H.; Lee, P.; MacGregor, W.; Mehta, K. Secure Biometric Match-on-Card Feasibility Report; NIST Interagency Report 7452; National Institute of Standards and Technology. Marrur nga: *[https://csrc.nist.gov/publications/detail/nistir/7452/final*]; Datë: 22.08.2018

[55] ICAO Doc9303, Machine Readable Travel Documents, Seventh Edition. Marrur nga:[*https://www.icao.int/publications/Documents/9303_p3_cons_en.pdf*] Datë: 22.08.2018.

[56] Rexha, B.; Imeraj, D.; Shabani, I. Using efficient TRNGs for PSEUDO profile in national eID card. Int. J. Recent Contrib. Eng. Sci. 2018, 6, 57–73.

[57] I. AG, Technical Details for SLE 78CLX1280P. Marrur nga: [*http://www.infineon.com*]; Datë: 22.08.2018.

[58] Giesecke & Devrient GmbH. Help files and technical notes for HIGHSEC eID App. Marrur nga: [*https://mpb.rks-gov.net/eID.html*]; Datë: 22.08.2018.

[59] Rexha, B.; Qerimi, E.; Neziri, V.; Dervishi, R. Using eID pseudonymity and anonymity for strengthing user freedom in Internet.Central and Eastern European e|Dem and e|Gov Days 2015 Independence Day: Time for a European Internet, Budapest, Hungary, 2015.

[60] Krasniqi, G., Rama, P., Rexha, B., Source code of application developed and hosted by GitHub at: [*https://github.com/petritrama-unipr/Biometric Efficiency_FIEK*]; Datë: 20.07.2018.

[61] Microsoft. Smart Card Authentication. Marrur nga:[*https://docs.microsoft.com/ en-us/windows/desktop/secauthn/smart-card-authentication*]; Datë: 22.08.2018

[62] Microsoft. RSACryptoServiceProvider Class. .NET Framework 4.7.2. Marrur nga:[*https://msdn.microsoft.com/enus/library/system.security.cryptography rsacryptoserviceprovider(v=vs.110).aspx*]; Datë: 20.07.2018.

[63] Rankl, W.; Effing, W. Smart Card Handbook; John Wiley & Sons Ltd.: London, UK, 2003.

[64] Stallings, W. Operating Systems: Internals and Design Principles; Prentice Hall, Pearson: New Jersey, NJ, USA, 2012.

[65] Guariglia, E. Entropy and Fractal Antennas. Entropy 2016, 18, 1–17.

[66] Guariglia, E. Spectral Analysis of the Weierstrass-Mandelbrot Function. In Proceedings of the 2nd International Multidisciplinary Conference on Computer and Energy Science, Split, Croatia, 12–14 July 2017.

[67] DIRECTIVE 2006/123/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Marrur nga: [*https://eur-lex.europa.eu/legal-content/EN/TXT/?qid= 1440760565642&uri=CELEX:32006L0123*]; Datë: 29.12.2018.

[68] How does the European Commission support e-signatures in Europe?.Marrur nga: [*https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=46992784*]; Datë: 30.12.2018.

[69] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Marrur nga: [*https://eur-lex.europa.eu/legal-content/EN /TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG*]; Datë: 28.12.2018.

[70] CEF eSignature. Marrur nga: [*https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=46992784*]; Datë: 29.12.2018.

[71] Ligji Nr. 04/L-094 PËR SHËRBIMET E SHOQËRISË INFORMATIKE. Marrur nga: [*https://www.kuvendikosoves.org/common/docs/ligjet/Ligji%20per%20 sherbimet%20e%20shoqerise%20informatike.pdf*]; Datë: 30.12.2018.

[72] Lorenz cipher, Wikipedia; Marrur nga: [*https://en.wikipedia.org/wiki/Lorenz_cipher*]; Datë: 18.11.2018

[73] How to code the Caesar Cipher: an introduction to basic encryption; Marrur nga: [*https://medium.freecodecamp.org/how-to-code-the-caesar-cipher-an-introduction-to-basic-encryption-3bf77b4e19f7*]; Datë: 09.12.2018

[74] Free Code Camp Bonfire Solution: Caesar's Cipher; Marrur nga: [*https://jacklyons.me/bonfire-caesars-cipher/*]; Datë: 12.12.2018

[75] Known Plaintext Attack; Marrur nga: [*https://www.staff.uni-mainz.de/pommeren/Cryptology/ Classic/1_Monoalph/knownplain.html*]; Datë: 15.11.2018

[76] How Hackers hack credit cards or debit cards password Online; Marrur nga: [*https://www.hackingloops.com/how-hackers-hack-credit-or-debit-cards-password-online/comment-page-1/*]; Datë: 19.11.2018

[77] Mobile Banking Adeptness on Man-In-The-Middle and Man-In-The-Browser Attacks; Marrur nga: [*https://pdfs.semanticscholar.org/db48/ 5964513e61ce0d02bfe8054db41fa7eab518.pdf*]; Datë: 20.12.2018

[78] Session hijacking attack; Marrur nga: [*https://www.owasp.org/index.php/Session_hijacking_attack]*; Datë: 20.12.2018

[79] Denial of Service attack; Marrur nga: [*https://en.wikipedia.org/wiki/Denial_of_Service_attack*]*;* Datë: 20.12.2018

[80] Contact Smart Card; Marrur nga: [*https://www.researchgate.net/figure/a-Contact-smart-card-b-contactless-smart-card-and-c-combi-card_fig6_275067120*]; Datë: 24.12.2018

[81] Contactless Smart Card; Marrur nga: [*https://www.indiamart.com/proddetail/contactless-smart-card-19099308612.html*]; Datë: 24.12.2018