Zaštita podataka u kritičnim područjima ljudske djelatnosti -suvremene kripotgrafske metode

Posavec, Emanuel

Veleučilište u Karlovcu

Odjel Sigurnosti i zaštite

Specijalistički diplomski stručni studij sigurnosti i zaštite

Emanuel Posavec

ZAŠTITA PODATAKA U KRITIČNIM PODRUČJIMA LJUDSKE DJELATNOSTI-SUVREMENE KRIPTOGRAFSKE METODE

ZAVRŠNI RAD

Karlovac, 2018

Karlovac University of Applied Sciences

Safety and Protection Department

Professional graduate study of Safety and Protection

Emanuel Posavec

DATAPROTECTION IN THE CRITICAL AREAS OF HUMAN ACTIVITY - MODERN CRYPTOGRAPHYC METHODS

FINAL PAPER

Karlovac, 2018

Veleučilište u Karlovcu

Odjel Sigurnosti i zaštite

Specijalistički diplomski stručni studij sigurnosti i zaštite

Emanuel Posavec

ZAŠTITA PODATAKA U KRITIČNIM PODRUČJIMA LJUDSKE DJELATNOSTI - SUVREMENE KRIPTOGRAFSKE METODE

ZAVRŠNI RAD

Mentor:

dr.sc. Damir Kralj, v.pred

Karlovac, 2018

VELEUČILIŠTE U KARLOVCU
KARLOVAC UNIVERSITY OF APPLIED SCIENCES
Trg J.J.Strossmayera 9
HR-47000, Karlovac, Croatia
Tel. +385 - (0)47 - 843 - 510
Fax. +385 - (0)47 - 843 – 579

HRN EN ISO 9001:2009

VELEUČILIŠTE U KARLOVCU

Stručni / specijalistički studij: Specijalistički diplomski stručni studij sigurnosti I zaštite
(označiti)

Usmjerenje: Zaštita na radu Karlovac 27.08.2018.

ZADATAK ZAVRŠNOG RADA

Student: Emanuel Posavec Matičnibroj:042241602

Naslov: ZAŠTITA PODATAKA U KRITIČNIM PODRUČJIMA LJUDSKE DJELATNOSTI - SUVREMENE KRIPTOGRAFSKE METODE.

Opis zadatka:

- Dati razloge uvođenja i kratki pregled povijesnog razvoja kriptologije i kriptografskih metoda
- Izvršiti analizu primjene suvremenih kriptografskih metoda u okviru kritičnih područja ljudske djelatnosti u cilju zaštite života I zdravlja ljudi te zaštite materijalnih dobara
- S obzirom na izvršenu analizu dati mišljenje o efikasnosti primjenjivanih metoda te pružiti uvid u neke metode u postupku razvoja koje će unaprijediti postojeće stanje

Zadatak zadan:	Rok predaje rada:	Predviđeni datum obrane:
01.09.2018.	03.09.2018.	06.09.2018.

Mentor: Predsjednik Ispitnog povjerenstva:

dr.sc. Damir Kralj, v.pred. mr.sc. Snježana Kirin, v.pred.

PREDGOVOR

Ovom prilikom bih se želio zahvaliti mentoru dr. sc. Damiru Kralju v. pred., koji mi je izašao u susret i pomogao odabrati vrlo zanimljivu i kvalitetnu temu.

Također mu se zahvaljujem na ukazanom povjerenju, pruženoj pomoći, utrošenom vremenu i stručnim savjetima prilikom izrade diplomskog rada.

Zahvaljujem također i drugim profesorima koji su tijekom mojeg dvogodišnjeg studiranja na specijalističkome studiju sigurnost i zaštita doprinijeli kvalitetnom obrazovanju bilo u teoretskom ili praktičnom smislu.

Na kraju, zahvaljujem mojim roditeljima i bratu koji su mi uz moralnu bili i najveća financijska podrška, jer sve što sam postigao s današnjim danom ne bih mogao ostvariti da nije bilo njih. Veliko hvala svima od srca.

SAŽETAK:

Ovaj rad ukazuje na razloge pojave kriptografije te njoj srodnih područja, njenu ulogu kroz povijest te primjenu i važnost kriptografije u cilju zaštite života, zdravlja i okoliša u kritičnim područjima ljudske djelatnosti kao i zaštita samih osoba od curenja osobnih podataka. Dani su osnovni pojmovi kriptografije kao i suvremene kriptološke metode te algoritmi koji se koriste. Navedene su dobrobiti, no, i poneke štetne primjene kriptografije u današnje vrijeme. Kasnije se detaljno opisuje zaštita kritičnih infrastruktura (zdravstvene i vojne ustanove), kao i sustavi kripto zaštite koji se za iste primjenjuju. Analizirana je i kriptološka zaštita podataka građana kao i novi zakon o zaštiti osobnih podataka građana. Na kraju rada prikazane su osnove kvantne kriptografije kao jedne od suvremenih metoda kriptografije u dolasku.

Ključne riječi: kriptografija, povijest kriptografije, kritična područja primjene, suvremene kriptografske metode, kvantna kriptografija.

SUMMARY:

This thesis describes why cryptography and its related areas have appeared, as well as its evolution and part it has had through history, her use and the importance in order to protect life, health and the environment in critical areas of human activity as well as the protection of individuals from the leak of personal data. The basic facts, as well as cryptological procedures and algorithms used in modern times are given. We can see some benefits, but also some harmful uses of cryptography in nowadays. Later in thesis, the protection of critical infrastructures (health and military) as well as the cryptographic methods they use for data protection are described. Cryptological protection of citizen data as well as the new law about protection of citizen personal data are also described. At the end, the basics of quantum cryptography as one of the modern methods of cryptography on arrival is presented.

Keywords: cryptography, history of cryptography, critical areas of application, modern cryprography methods, quantum cryptography.

SADRŽAJ:

1. UVOD

Kraljevi i kraljice te razni vojskovođe, kao i suvremeni državnici i sustavi državne uprave, pri upravljanju svojim zemljama i vođenju svojih vojski već stoljećima ovise o djelotvornoj komunikaciji. No bili su svjesni što bi se dogodilo da te dragocjene informacije dospiju u protivničke ruke. Uvijek aktualna opasnost da bi neprijatelj mogao doći do informacije, potaknula je razvoj šifara, i kodova. Zbog toga su mnoge zemlje počele osnivati odjele i institute za analizu i primjenu šifriranja. Kao rezultat pojave ovih aktivnosti, na neprijateljskim stranama istovremeno su započele mjere i aktivnosti za analizu kriptiranih sadržaja i razbijanje primijenjenih šifarskih sustava kako bi se došlo do tih vrijednih informacija. Svaka je šifra snažna sve dok se ne otkrije njen ključ, te ista postaje beskorisna i mora se napraviti nova te tako sve u krug. Zbog toga dolazi do pojave znanosti koja se zove kriptografija. Kriptografija je znanost koja se bavi logičkom promjenom podataka.

Cilj i zadatak ovog diplomskog rada je opisati kratki povijesni pregled i značaj kriptografije do danas, opisati suvremene kriptološke metode kao i algoritme koji se koriste u moderno doba, obraditi na koje se načine štite osobe u kritičnim područjima ljudske djelatnosti od kriptografskih napada, te nakraju opisati suvremene metode kriptografije koje su u dolasku.

Rad se sastoji od teorijskog dijela istraživanja koji se zasniva na analizi dobivenih podataka iz stručne i znanstvene literature, prikupljanja dostupnih pisanih i internetskih sadržaja, raznih članaka, časopisa te ostalih sekundarnih izvora iz područja kriptografije. U prvom dijelu rada opisana je kriptografija kroz povijest kao i značaj iste u pojedinim slučajevima, dok se kasnije opisuju suvremene metode kojima se štite građani, zdravstvo, MORH od kriptografskih napada. Na samome kraju su opisane kriptografske metode u dolasku koje će obilježiti sljedećih nekoliko desetljeća kriptografije.

2. OSNOVNA NAČELA U KRIPTOGRAFIJI

Kriptografija se stoljećima primjenjuje za osiguravanje tajnosti razgovora između dvije strane, a ponajviše u vođenju vojnih akcija te diplomatskih razgovora. U prošlosti postupci kriptografije svodili su se na različite domišljate kombinacije razmještanja znakova i zamjene slova unutar teksta. Dio kriptografije koji se bavi dešifriranjem poruka bez ključa naziva se kriptoanaliza, a ljudi koji se time bave kriptoanalitičari.

Ponekad nije dovoljno samo zadržati tajnost sadržaja poruke, što čini kriptografija, nego treba sakriti i samo postojanje poruke. Tehnika kojom se skriva poruka zove se steganografija. Moderna steganografija, koja koristi prednosti digitalne tehnologije, najčešće podrazumijeva skrivanje tajne poruke unutar neke multimedijske datoteke, npr. slike, audio ili video datoteke.

Multimedijske datoteke u pravilu sadrže neupotrijebljene ili nevažne podatkovne prostore koje različite steganografske tehnike koriste tako da ih popune s tajnim informacijama. Takve datoteke se potom mogu razmjenjivati bez da itko bude svjestan prave svrhe dotične komunikacije. [1]

2.1. Osnovni pojmovi u kriptografiji

Osnovni pojmovi u kriptografiji su: osnovni algoritam, šifriranje (kodiranje), dešifriranje (dekodiranje), te ključ.

Šifriranje je postupak kojim se podatci pomoću ključa promjene te se više ne mogu čitati (osim ako imate ključ).

Dešifriranje (dekodiranje) je postupak kojim se podatci pomoću ključa promjene u izvorne podatke.

Ključ je način šifriranja i dešifriranja podataka.

Kriptologija je znanost koja obuhvaća kriptografiju i kriptoanalizu. Ona koristi znanja matematike, statistike i lingvistike za kriptiranje i dekriptiranje poruka.

3. POJAVA KRIPTOGRAFIJE KAO DOPUNA STEGANOGRAFIJI

Početkom ratovanja javlja se sve veća potreba za skrivanjem poruka. Najraniji dokumenti i zapisi dosežu iz doba Herodota koji u svojim Historijama daje kroniku sukoba Grčke i Perzije u 5. stoljeću. pr. Kr. Prema Herodotu, Grke je od Kserksovih osvajanja spasilo upravo umijeće tajnog pisanja. Kserkso je krenuo u izgradnju svoje nove prijestolnice, a kako ga Atena i Sparta nisu podržavale on ih je odlučio kazniti. Perzijsko naoružanje je primijetio Demarat, izgnanik iz Grčke, te je odlučio Spartancima poslati poruku i upozoriti ih. U kronici je zabilježena upotreba drvenih pločica na kojima je Demarat napisao poruku. Ogulio je vosak s dviju drvenih pločica, urezao na njih obavijest, a zatim opet prekrio pločice voskom. Tako pločice nisu mogle izazvati sumnju stražara na putu. Poruka je stigla na odredišta te su Grci bili upozoreni i tako porazili perzijske snage. Taj događaj je obilježio početak steganografije odnosno tajnog komuniciranja pri kojem se skriva i samo postojanje poruke.

Steganografija se primjenjivala u mnogo različitih oblika. Vojskovođe su znali obrijati glasniku glavu i na nju napisati poruku, te su pričekali da kosa ponovno naraste, a zatim poslali glasnika na odredište. Kinezi su poruke pisali na tankoj svili, koju bi potom smotali u kuglicu zvanu *„la wan“* i obavili voskom, a zatim bi ju glasnik sakrio u odjeću ili jednostavno progutao. Jedan od načina skrivanja poruke je bila i upotreba nevidljive tinte iz biljaka ili organskih tekućina, koja je nevidljiva kad se osuši, ali pri zagrijavanju postane smeđa. Sve metode tajnog komuniciranja bile su jako opasne jer ih se lako moglo otkriti. Zbog toga se, uz steganografiju, počinje razvijati kriptografija. Prednost kriptografije je što neprijatelj ne može razabrati sadržaj čak ni uhvaćene poruke.

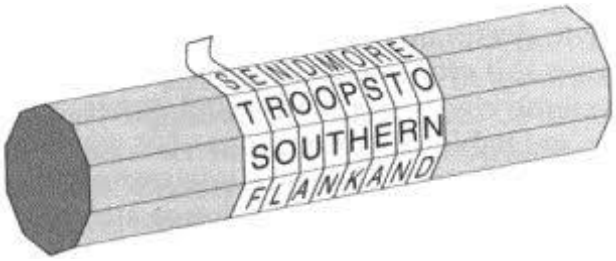
4. POČECI KRIPTOGRAFIJE

Korijeni kriptografije potječu iz rimskih i egipatskih civilizacija. Riječ kriptografija je kombinacija dvije grčke riječi „*krypto*“ što znači skriveni i „*graphene*“ što znači pisati.

Na početku starog vijeka ljudi su kriptografiju smatrali mističnom znanošću te su ju povezivali s crnom magijom. U ono vrijeme većina kriptografa su bili znanstvenici. Neke od najpoznatijih metoda u to vrijeme su bili spartanska skitala, Cezarova šifra. Kasnije u novije doba jedne od istaknutijih šifri su šifra Marije Stuart, Albertovi sustavi, te Vigenereova šifra.

4.1. Spartanska skitala

Prvi sustav vojne kriptografije zabilježen je još u 5. stoljeću pr. Kr. Kod Spartanaca. Oni su upotrebljavali drveni štap imena (*skytale ili skitali)* to je bila prva kriptografska naprava u povijesti kriptografije. Oko skitale bi se omotala vrpca od kože ili pergamente, a onda bi se na njoj napisala poruka. Glasnik bi se opasao vrpcom kao remenom sa slovima s unutrašnje strane i tako sakrio poruku. Poruka se mogla pročitati samo kad bi se vrpca omotala oko štapa potpuno jednake debljine. Skitala je tako postala prva naprava za šifriranje koja koristi transpoziciju jer se nakon odmotavanja na vrpci nalazio anagram otvorene poruke.

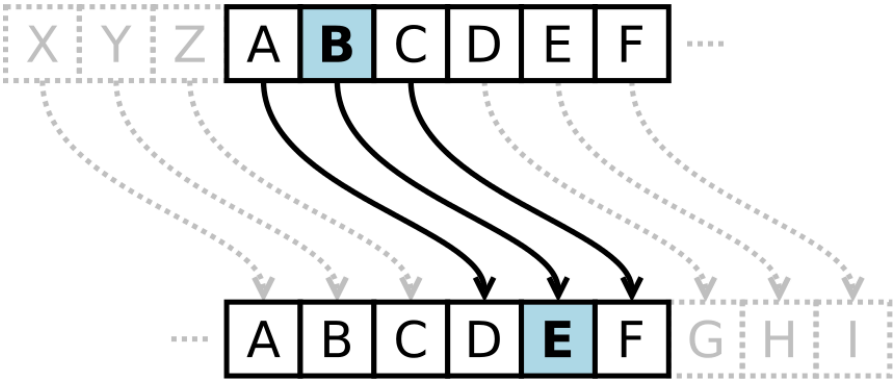


Slika 1. Spartanska Skitala [2]

Kad se poruka čita po redu slova zvuči nerazumljivo „STSFEROLDOTN...“ . No kad se ona stavi na štap prave debljine možemo iščitati poruku „SEND MORE TROOPS TO SOUTHERN FLANK AND...“. [2]

4.2. Cezarova šifra

Supstitucija se u vojne svrhe prvi put pojavljuje u Galskom ratu Julija Cezara. U toj supstituciji rimskih slova su zamijenjena grčkim slovima, te su tako neprijatelji postala nerazumljiva. U Svetoniju „Životu Cezara LVI.“, napisanom u 2. stoljeću detaljno je opisana jedna vrsta supstitucijske šifre kojom se služio Julije Cezar. Ove šifre su monoalfabetske supstitucijske šifre jer se prilikom kriptiranja koristi samo jedna šifrirana abeceda. On bi svako slovo u poruci zamijenio nekim drugim slovom. Šifrirana abeceda nastaje pomakom otvorene abecede za tri mjesta ulijevo, pa se takva supstitucija zove Cezarovom pomičnom šifrom ili samo Cezarovom šifrom. Ključ šifre predstavlja pomak, koji je u ovom slučaju uvijek tri. Kasnije je šifrirao tako što je pojedina slova u tekstu pomaknuo za četiri ili više mjesta u abecedi. Takvu poruku mogli su da dešifriraju samo oni koji su poznavali pravilo pomaknutosti.

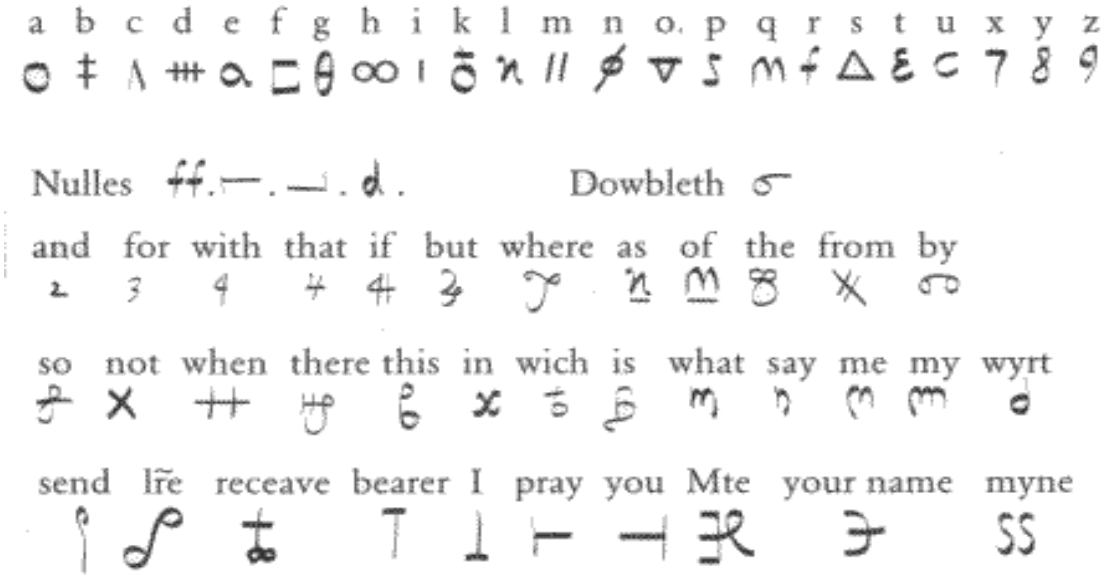


Slika 2. Cezarova šifra [3]

4.3. Šifra Marije Stuart

Svakako jedna od najpoznatijih šifri kroz povijest je upravo šifra Marije Stuart. Nakon što je zatočena u zatvoru zbog mogućnosti preotimanja krune kraljici Elizabeti, Marija i njezini pristaše spremaju urotu. Njezini pristaše u pismima navode kako je papa izopćio Elizabetu iz crkve, što je po njima

dovoljan razlog za početak planiranje Elizabetinog ubojstva. Radi sigurnosti sva pisma šifriraju pomoću nomenklatora kako protivnici ne bi u slučaju pronalaska poruke nešto posumnjali. No, nitko nije znao da je upravo čovjek koji je nosio pisma Mariji dvostruki agent jer je radio i za glavnog tajnika kraljice Elizabete. Svako pismo koje bi preuzeo od ili za Mariju, najprije bi odnio u ured na prepisivanja te tek onda proslijedio pismo. Kako bi se dodatno dokazala urota i ista uništila, šifrolomac kraljice Elizabete je dodao postskriptum u kojem bi se potaknulo na otkrivanja identiteta Marijinih pristaša te ih tako bilo lakše osuditi. Na suđenju je prvi put sudbina čovjeka ovisila o sigurnosti šifre. Šifrolomac je donio sva Marijina prepisana i dekodirana pisma te je ona osuđena na smrt i pogubljena.



Slika 3. Šifra Marije Stuart [4]

4.4. Leon Battist Alberti

I dok je jednostavna monoalfabetska supstitucijska šifra ili šifra jednostavne zamjene stoljećima dostajala za osiguranje tajnosti, pojava frekvencijske analize razotkrila je njezinu sigurnost. Tragično pogubljenje Marije Stuart dramatično oslikava slabost monoalfabetske supstitucije zbog čega je već i tada

postalo jasno da u nadmetanju između kriptografa i kriptoanalitičara ovi posljednji počinju prevladavati. Sad je teret pao na pleća kriptografa, a zadaća je smišljanje nove, jače šifre, nečeg što bi moglo nadmudriti kriptoanalitičare. Iako se ta šifra neće pojaviti sve do kraja 16. stoljeća, njezini korijeni počinju negdje 1460. godine kada je Alberti naletio na prijatelja Leonarda Data, papina tajnika, i ovaj se zapričao o finesama kriptografije. To je čavrljanje Albertija navelo da o toj temi napiše ogled i u njemu doda obrise kako je vjerovao novog načina šifriranja. Do sad su se supstitucijske šifre enkriptirale samo jednom šifriranom abecedom, no Alberti predlaže primjenu dvije ili čak više šifriranih abeceda koje bi se izmjenjivale unutar jedne poruke itekako zbunjivale potencijalne kriptoanalitičare.

Otvorena abeceda: **a b c d e f g h i j k l m n o p r q r s t u v w x y z**

Šifrirana abeceda 1 **F Z B V K I X A Y M E P L S D H J O R G N Q C U T W**

Šifrirana abeceda 2 **G O X B F W T H Q I L A P Z J D E S V Y C R K U H N**

Ovdje vidimo dvije šifrirane abecede, pa poruku možemo enkriptirati naizmjence. Recimo da želimo enkriptirati poruku „**hello**“ tad ćemo prvo slovo enkriptirati prema prvoj šifriranoj abecedi, pa će **h** postati **A**, ali ćemo zato drugo slovo enkriptirati prema drugoj šifriranoj abecedi, pa će **e** postati **F**. Kod enkriptiranja trećeg slova vraćamo se prvoj šifriranoj abecedi, a kod četvrtog ponovno drugoj te peto ponovno po prvoj. Tim redom dolazimo do riječi **AFPAD**. Ključna prednost Albertovih sustava je da se ista slova u otvorenom tekstu ne pojavljuju nužno kao ista slova u šifriranom tekstu.

4.5. Vigenereova šifra

Kasnije je upravo uz pomoć Albertovih spisa francuski diplomat Blaise de Vigenere stvorio novi moćniju šifru poznatu pod njegovim imenom. Snaga iste izvire u činjenici da se ona služi ne jednom ili dvjema šifriranim abecedama, nego poruku enkriptira pomoću 26 abecede, točnije za svako slovo jednom. Vigenereovu šifru su na kraju slomili Babbage I Kasiski. Babbageova kriptoanaliza započinje potragom za sljedovima slova koje se u šifriranom

tekstu pojavljuju više puta čime se određuju duljine ključne riječi. Tada šifrirani tekst podijelimo u toliko dijelova koliko je slova ključne riječi. Taj postupak je isti kao i kod razbijanja Cezarove šifre, jer svako slovo ključa daje po jednu monoalfabetsku šifru. Za svako slovo u ključu ispisuju se sva slova koja se šifriraju tim slovom te se izvodi već poznata frekvencijska analiza.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	D
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	C
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	B
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Slika 4. Vigenereov kvadrat [5]

5. PRIMJENA KRIPTOGRAFIJE U 20. STOLJEĆU I PRVI SVJETSKI RAT

Nakon što je talijanski inženjer i fizičar Guglielmo Marconi izumio novo moćno sredstvo telekomuniciranja, potreba za sigurnim enkriptiranjem postala je još naglašenija. 1914. Godine Britanci pod vodstvom Alfreda otvaraju ured koji se bavio razbijanjem šifri nazvan Soba 40. Ponajviše su se bavili razbijanjem njemačkih šifri zbog strateških i vojnih planova.

Povijesni događaj u kojem je kriptografija učinila veliki korak zbio se 1917. godine kad je ista bila razlog uključenja Amerike u Prvi svjetski rat. Naime Nijemci su se spremali na rat protiv Britanije, ali nisu htjeli uvući Amerikance kao svoje protivnike pošto su oni bili saveznici Britancima. Nijemci su kako bi Amerikance okupirali dok se oni bore s Britancima dogovorili kriptiranim porukama sa Mexicom da će im pripomoći vratiti izgubljeni teritorij od Amerikanaca kako bi Mexico zaratio s Amerikom i time ih potaknuo na vlastiti rat umjesto slanje pomoći Britaniji. Pošto su Britanci dešifrirali tu poruku i poslali je Američkom predsjedniku Woodrow Wilsonu on je na temelju toga objavio rat Nijemcima.

5.1. Razvoj šifrirnih strojeva

U poslijeratnim godinama dolazi do koordiniranog nastojanja da se pronađe nov i siguran sustav enkripcije. A porastom tehnologije u svim područjima bilo je logično da i kriptografi potraže nove načine u istoj. Veliki napredak svakako je bio izum rotora koji se kasnije koristio u mnogim šifriranim strojevima. Svakako najpoznatiji je stroj po imenu Enigma kojeg su 1919. godine konstruirali njemački izumitelj te inženjer elektrotehnike Arthur Scherbius i njegov prijatelj Richard Ritter.

Enigma je elektromehanički uređaj koji se sastoji od tipkovnice s 26 tipki poput pisaćeg stroja, zaslona s 26 žaruljica za prikaz šifriranog izlaza, tri mehanička rotora i električne prespojne ploče, a napaja se putem ugrađene baterije. Pritiskom na tipku kroz mrežu kontakata rotora i prespojne ploče

zatvara se strujni krug i pali se odgovarajuća žaruljica koja označava šifrirano slovo. [6]

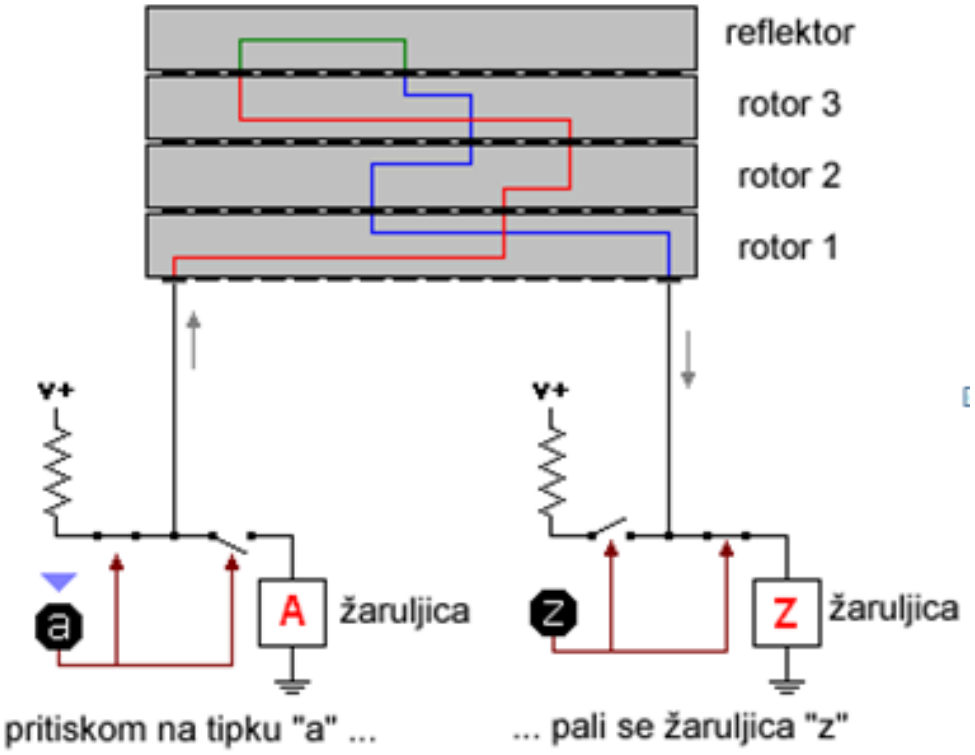
Mehanički rotori sastoje se od diskova s 26 kontakata kružno smještenih na obodu svake stranice. Svaki kontakt na jednoj strani diska povezan je s nekim drugim kontaktom na suprotnoj strani. Većina modela Enigme sastojala se od tri rotora koji su smješteni u ležište tako da se kontakti susjednih stranica međusobno dodiruju, tj „izlaz“ jednog rotora predstavlja „ulaz“ drugom. [6]

Izlaz trećeg rotora povezan je na reflektor- statičan mehanički disk sličan rotoru, s međusobno prespojenim električnim kontaktima samo na jednoj strani. Njegova je zadaća da električni signal šalje natrag kroz rotore, no drugim putem. Kad operater pritisne tipku, električni signal putuje do ulaznog kontakta prvog rotora. [6]

S obzirom na to da interno ožičenje rotora predstavlja transformaciju slova, električni signal na izlazu prvog rotora predstavlja neko drugo slovo, a postupak se nastavlja kroz reflektor te ponovno kroz sva tri motora do odgovarajuće žaruljice za indikaciju. Svakim pritiskom na tipku okreću se mehanički rotori, te se tako dinamički mijenja električni spojni put između tipke i žaruljice, a svako slovo šifrira drugačije. [6]

Prvi rotor svaki se put okrene za jedan kontakt, a kad učini potpun krug, mehanička poluga okrene sljedeći rotor za jedan kontakt. Tako se htjelo izbjeći ponavljanje postavko za šifriranje, čime bi se stvorila jednostavna supstitucijska šifra. [6]

Kako bi se poruka dešifrirala primatelj je morao imati Enigmu kao i primjerak knjige šifara s početnim položajem rotora. Upravo taj početni položaj predstavlja zapravo ključ šifre, kojeg obično diktira knjiga šifara u kojoj su nabrojeni ključevi za svaki dan i dostupna je svima unutar komunikacijske mreže. Na kraju primatelj poruke namješta svoj stroj prema knjizi i utipkava šifrat kako bi dobio otvoreni tekst. Kasnije su se pojavili mnogo modeli stroja enigme s malim preinakama.



Slika 5. Načelo rada enigme [6]

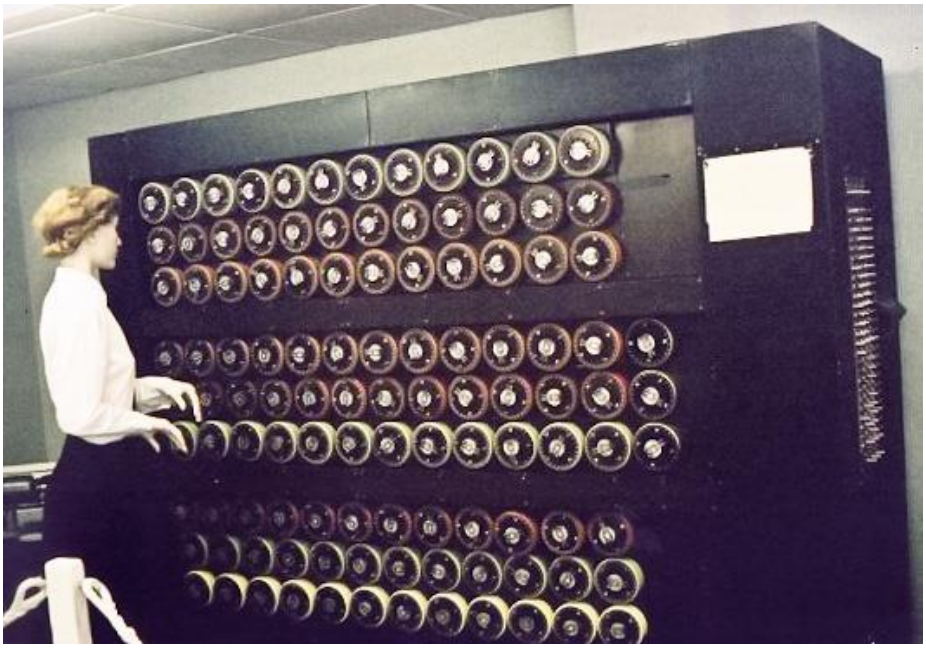
5.2. Razbijanje Enigme

Pojavom Enigme smanjila se učinkovitost kriptografa u prije spomenutoj Britanskoj Sobi 40 što zbog količine podataka, što zbog raznog broja modela Enigme. U koštac razbijanje enigme uključili su se Amerikanci te Francuzi no bez ikakvih konkretnijih rezultata. Sve do 1931. godine kada je Schmidt dopustio da Francuski agent fotografira upute za primjenu Enigme. Upravo zahvaljujući tim uputama sada su Saveznici mogli stvoriti točnu repliku njemačke vojne Enigme. Francuzi nisu ostvarili izvjestan napredak s tom informacijom, no, podijelili su informacije sa svojim saveznicima Poljacima s kojima su prije potpisali sporazum o vojnoj suradnji. Oni su kontradiktorno dosadašnjim uvjerenjima da su najbolji kriptoanalitičari stručnjaci za jezik, krenuli u dešifriranje pomoću matematičara što je upravo bilo i potrebno.

Poljaci su uočili da broj elemenata u ciklusima ovisi isključivo o rotorima, a ne o prespojnoj ploči. Nakon godinu dana istraživanja kakve rastave na produkte ciklusa daje rotor kategorizirali su rezultate. Sada je samo trebalo još odrediti veze na prespojnoj ploči. Tim načinom dešifriranja dobivali su uglavnom nerazumljiv tekst, no dobivali su dijelove tekstova koji su bili u potpunosti čitljivi čime su oni u to vrijeme dešifrirali njemačke poruke. Sve do 1939. godine kada su Nijemci povećali broj ključeva uvođenjem većeg broja rotora. To je bio preveliki zadatak za njih pa su pomoć potražili s engleskim i francuskim saveznicima dijeleći svoje istraživanje.

Britanci formiraju veliku grupu kriptoanalitičara za šifre sa sjedištem u Bletchley Parku. U vrlo kratkom roku ovladavaju tehniku koju su do sad koristili Poljaci te su se zbog znatno većeg proračuna uspijevali nositi sa zadatkom većeg broja kombinacija rotora te ponekad uspjeli pronaći dnevne postavke. Otkrili su par slabosti Enigme kao što su često korištenje susjednih slova na tipkovnici te da se nijedno slovo dešifriranjem ne preslikava u isto slovo. Kasnije jedan od članova grupe kriptoanalitičara Alan Turing usavršava elektromehanički uređaj za razbijanje šifri pod nazivom "Bomba" koja ima za zadaću pretraživanje svih kombinacija postavki rotora u potrazi za ispravnom.

Kasnije Turing odlazi u Sjedinjenje Američke države gdje radi kao savjetnik na konstruiranje „Bombe“ od šest tisuća rotora koja postaje upotrebljiva 1943. godine. Ne samo da te nove „Bombe“ imaju više rotora, nego su i daleko brže i savršenije te će se koristiti sljedećih par godina u svrhu razbijanja šifri.



Slika 6. Turingova Bomba [6]

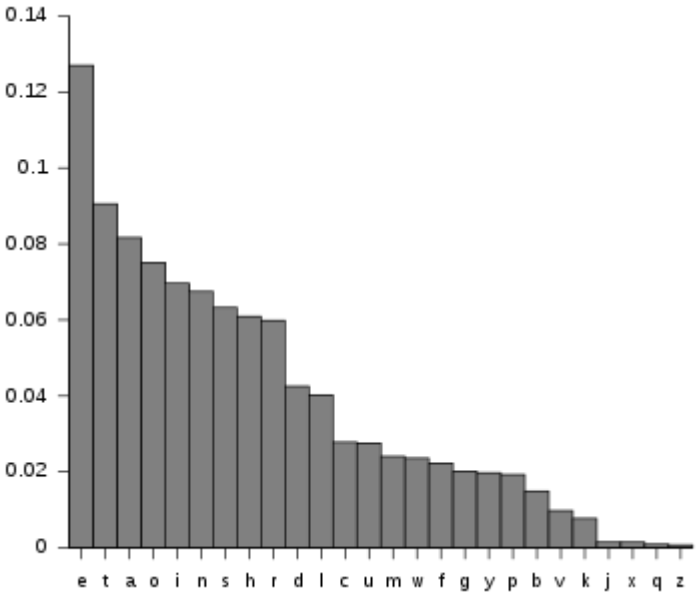
5.2.1. Primjena statistike u kriptografiji

"TGIAB FZU TGPHVGHPB FPB GSB BTTBZVB QR F CQQW; OPBFG KUBFT FPB SQOLFTS."

To je engleska rečenica, ali uz primijenjenu zamjensku šifru. Svako slovo je šifrirano na neko drugo (jedinstveno) slovo. Postavlja se pitanje kako dekriptirati ovu poruku? Jedan od načina je pretražiti sve moguće zamjenske šifre. Relativno je lako izračunati koliko ih ima: A se može šifrirati na 26 slova, B se može šifrirati na preostalih 25, C može biti šifriran na 24, i tako dalje. To znači da postoje $26! = 4 \times 10^{26}$ različite mogućnosti. Dakle, rješavanje ovom metodom može potrajati dosta vremena.

Bolja metoda je korištenje nekih osnovnih statističkih zaključaka. Od presudne je važnosti da izvorna poruka nije slučajna. Ako bi bila slučajna, ne bi sadržavala nikakve informacije i ne bi bila vrijedna šifriranja. Znamo da je izvorna poruka bila engleska rečenica, tako da već znamo određene tonove. Točnije, možemo odrediti približne frekvencije slova u izvornoj poruci gledanjem relativne frekvencije slova u velikom zboru engleskog pisanja. Daleko najčešće

pismo je E. U našem kriptogramu, top 5 frekventnih slova su: B: 10, F: 7, T: 6, P: 5, Q: 5.



Slika 7. Frekvencija korištenja engleskih slova [8]

Dakle, možemo krenuti od pretpostavke da je *E* kriptirano na slovo *B*. Tada, što bi mogla biti riječ *FPB*? Znamo da završava na slovo *E*, a kako se *F* u tekstu pojavljuje kao svojstvena riječ, znamo da je to kriptirano *A* ili *I*. Time dolazimo do najvjerojatnije mogućnosti u kojoj *FPB = ARE*. Koristeći ove supstitucije i statistiku, već smo napravili veliki napredak. Uz pomoć prije dekriptiranih slova slažemo novu rečenicu koja glasi:

"TGIAe aZU TGrHVGHre are GSe eTTeZVe QR a CQQW; OreFG KUeaT are SQOLaTS. (mala slova prikazuju dekriptirana slova, dok velika slova još uvijek nisu dekriptirana)."[cit.8]

Dalje možemo dekriptirati koristeći statistiku slova i riječi, možemo pokušati proučiti statistiku parova riječi. Pogledajmo *"are GSe".* Koja je sljedeća riječ od tri slova po frekvencija na završetak *"e"* koja slijedi iza *"are"*? Vjerojatno *"the"* pa dolazimo do zaključka *G = T* i *S = H*. Primjenom tih novih zaključaka poruka nam glasi:

"TtIAe aZU TtrHVtHre are the eTTeZVe QR a CQQW; Oreat KUeaT are hQOLaTh."

Kratke riječi mogu biti isto od koristi. Odjeljak *"QR a"* vjerojatno je ili *"of a"* ili *"if a",* a *"if a"* ne bi imao gramatički smisao s rečenicom koja slijedi ubrzo nakon toga. Slično tome, "aZU" je vjerojatno *"and".* Zamjenjujući *Q = O, R = F, Z = N i U = D* dolazimo do:

„TtIAe and TtrHVtHre are the eTTenVe of a CooW; Oreat KdeaT are hoOLaTh.“

U ovom trenutku postoji više smjerova kojima možemo dalje dešifrirati. Treba primijetiti da je pojava slova *T* vrlo česta, što znači da može odgovarati jednoj od čestih engleskih slova koja još nisu pronađena (naime, *S, A ili I*). U riječi *"eTTenVe"*, jasno je da T predstavlja suglasnik, pa dolazimo do zaključka T = S. Ta dekripcija nam puno otkriva pa dolazimo do:

„stIAe and strHVtHre are the essenVe of a CooW; Oreat Kdeas are hoOLash.“

Sada bi se moglo donijeti još neke zaključke za pojedine riječi ili slova, ili bi se moglo polako nagađati rješenje. Izvorna rečenica je sporan citat Vladimira Nabokova, a glasi:

"Stlye and structure are the essence of a book; great ideas are hogwash."

(Stil i struktura su bit knjige; odlične ideje su beznačajne.)

Moral ove priče nas dovodi do zaključka kako bi kriptografija bila jednostavna s gledišta šifriranja i nemoguća s gledišta kriptoanalitičara, da nije statističke strukture poruke pomoću enkripcije. Ako je netko htio štititi njihovo "čavrljanje", tako da nitko osim namjeravanog primatelja ne bi mogao pročitati to "čavrljanje", šifra zamjene bi bila dovoljna. Ali ljudi šifriraju važne stvari, a važne stvari imaju strukturu, koja se može iskoristiti pomoću statističkog razmišljanja i to mnogo sofisticiranijeg nego što je bilo potrebno ovdje. [7]

Ovo poglavlje je spomenuto ovdje ponajviše jer je kriptoanalitičar Alan Turing tijekom Drugog svjetskog rata isto koristio sličnu metodu. Pošto je matematički bilo nemoguće pretražiti sve mogućnosti konfiguracije stroja

Enigma, a ako bi to bilo i moguće, Nijemci su svakodnevno mijenjali postavke pa im to ne bi koristilo. [7]

5.3. Počeci primjene računala u kriptografiji

Uz prije spomenutu Enigmu Britanci, konkretnije Tommy Flowers inženjer pri britanskoj pošti je izumio još jednu spravu, ili bolje rečeno – elektroničko računalo za razbijanje šifara i kodova imenom Colossus, koja je predstavljena kao odgovor i sredstvo protiv njemačke šifre Lorenz.

J. Presper Eckert američki inženjer elektrotehnike i John W. Mauchly američki fizičar 1945. godine dovršavaju svoj ENIAC (*Electronic Numerical Integrator and Computer*) koji je korišten za proizvodne testne izračune. ENIAC je kasnije utjecao na usmjerenje razmišljanja prema primjeni računala u kriptografiji.

IBM je 1953. godine na tržište izbacio svoje prvo računalo, a samo četiri godine kasnije Fortran, programski jezik koji je i laicima omogućio pisanje računalnih programa. U šezdesetim su računala postajala sve jača, jeftinija te samim time i pristupačnija. Sukladno ovoj dinamici razvoja sve veći broj tvrtki koristi upravo računala kao sredstvo prijenosa novca ili preko istih obavlja osjetljive trgovačke pregovore. Pojavljuje se potreba za šifrom koja će biti upotrebljiva te povjerljiva svim korisnicima svijeta. Kao rješenje 1976. godine Amerikanci objavljuju algoritam nazvan DES (*Data Encryption Standard*). Algoritam nastaje u prije spomenutom IBM-ovom laboratoriju gdje se primjenom DES šifrira otvoreni tekst duljine od 64 bita.

Godine 1977. dizajniran je RSA algoritam koji primjenjuje metodu šifriranja javnim ključem, te podržava šifriranje poruka i identifikaciju korisnika potrebnu za osiguravanje autentičnosti. Autori su američki kriptograf Ron Rivest, izraelski kriptograf i računalni znanstvenik Adi Shamir, te američki kriptograf i teoretski računalni znanstvenik Leonard Adleman po kojima je algoritam i dobio ime. Ovaj algoritam je svakako najpoznatiji i najviše primjenjivan algoritam javnog

ključa današnjice. Sigurnost mu leži u činjenici da je faktorizacija velikih prirodnih brojeva na produkt sa prostih brojeva izuzetno teška.

Opis odabira parametara RSA kriptosustava:

1. Izabiremo tajno dva velika prosta broja *p* i *q* od preko 150 znamenaka, tako da *q* ima nekoliko znamenaka više od *p*. To radimo tako da pomoću nekog generatora slučajnih brojeva generiramo prirodan broj *m* s traženim brojem znamenaka, a zatim korištenjem nekog testa za testiranje prostosti tražimo prvi prosti broj veći ili jednak *m*;
2. Izračunamo $n = pq$ *i* $\varphi(n) = (p-1)(q-1) = n + 1 - p - q$ (Eulerova funkcija);
3. Izaberemo na slučjno broj *e* takav da je $e < \varphi(n)$ i $nzd(\varphi(n), e) = 1$. To se može napraviti slično kao pod 1. Nakon toga tajno izračunamo *d*, tako da je $de \equiv 1 \pmod{\varphi(n)}$(riješimo linearnu diofantsku jednadžbu $de - t\,\varphi(n) = 1$ pomoću Euklidova algoritma);.
4. Stavimo ključ za šifriranje (*n,e*) u javni direktorij.

Sada je (*n, e*) javni ključ (koji treba znati svatko tko vam šalje poruke), a (*p, q, d*) tajni je (osobni) ključ (koji trebate znati samo vi). Poruka (razbijena na blokove koji odgovaraju brojevima manjim od *n* – tipično *n* ima oko 1024 bita) šifrira se ovako: $e_k(x) = x^e \bmod n$, a dobiveni šifrat dešifrira se ovako: $d_k(y) = y^d \bmod n$. Da su funkcije e_k i $d_k$inverzne, slijedi iz prije navedenog Eulerova teorema. Uočimo da je ovdje e_k „jednosmjerna funkcija“. Naime, iz $e_k(x) = x^e \bmod n$, tj. uz poznavanje samo javnog ključa (*n, e*), ne možemo naći tajni ključ *d*, odnosno inverznu funkciju $d_k(y) = y^d \bmod n$. Za to nam je potreban „dodatni podatak“, a to je u ovom slučaju faktorizacija od *n*.

Zaista, onaj tko zna ili može otkriti faktore *p* i *q* javno poznatog broja n može izračunati $\varphi(n) = (p - 1)(q - 1)$ te saznati tajni eksponent *d* rješavajući linearnu diofantsku jednadžbu $de - t\,\varphi(n) = 1$.[9]

6. SUVREMENE KRIPTOGRAFSKE METODE

Pojavom prvih računala kriptografija se rapidno razvija. Kako je vrijeme prolazilo računala su sve brža i efikasnija, izvršavajući i po nekoliko stotina, a kasnije i milijuna operacija u sekundi. Novom brzinom rada je omogućeno probijanje šifara za sve manje vremena. Usporedno s tim, radilo se i na razvoju novih, sigurnijih i složenijih shema za šifriranje. Pojavom računalnih mreža kriptografija naglo dobiva na značaju. Naročito je bitno osigurati zaštitu važnih podataka koji se prenose mrežom. Naime, podatci se razmjenjuju računalnom mrežom u formi paketa podataka i oni dospijevaju do većeg broja računala na putu od polaznog do određenog računala. Na svakom usputnom računalu moguće je te pakete podataka „uhvatiti“ i pročitati njihov sadržaj, korištenjem analizatora protoka ili nekog programa (*sniffera*). Kriptiranje podataka podrazumijeva korištenje raznih kriptografskih algoritama tj. Skupova pravila po kojima se vrši kriptiranje. Algoritmi za kriptiranje se mogu podijeliti u dvije grupe:

- Tajni algoritmi kod kojih se sigurnost zasniva na tajnosti algoritma,
- Algoritmi zasnovani na ključu: sigurnost se zasniva na ključevima, a ne na detaljima algoritma koji se može iznijeti na javnost i analizirati. Ovdje je algoritam javno poznat, a ključ se čuva u tajnosti, da nije tako korisnici bi morali da razumiju i ključ i algoritam. Ključ je niz podataka koji se koristi za kriptiranje drugih podataka koji se prema tome mora koristiti i za dekriptiranje podataka.

U današnje vrijeme se najčešće koriste algoritmi za kriptiranje zasnovani na ključu, a mogu se klasificirati u tri grupe:

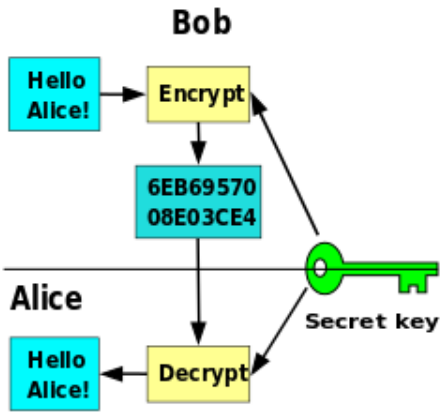
- Simetrične kriptosustave,
- Asimetrične kriptosustave,
- Hibridne kriptosustav.

U cilju postizanja što bolje zaštite podataka algoritam za kriptiranje mora zadovoljiti sljedeće zahtjeve. Cijena „probijanja“ algoritma mora biti veća od

cijene šifriranog podataka. Vrijeme potrebno za „probijanje“ algoritma mora biti duže od vremena u kojem podatci moraju ostati tajni. Broj podataka kriptiranih pomoću jednog ključa treba biti manji od broja potrebnih podataka da se dati algoritam „probije“. Isto tako, prilikom formiranja algoritama za kriptiranje/dekriptiranje, teži se da postupci kriptiranja odnosno dekriptiranja budu identični tj. inverzni. Tako se postiže neophodna kompatibilnost između postupaka kriptiranja i dekriptiranja u smislu korištenja istih operacija ali obrnutim redoslijedom i korištenje istog ključa u oba postupka. Veoma je važno i da proces kriptiranja/dekriptiranja ima što je moguće kraće vrijeme izvršavanja. Postizanje što boljih performansi se ostvaruje ako se ovi procesi realiziraju hardverski. Kako bi algoritmi za kriptiranje bili što je jednostavniji za hardversku realizaciju potrebno je da se izračunavanja u okviru njih baziraju na skupu jednostavnih operacija, kao što su aritmetičko sabiranje, XOR, operacije rotiranja i druge.

6.1. Simetrična kriptografija

Osnovna osobina simetričnih kriptosustava s tajnim ključem je da za kriptiranje/dekriptiranje poruka koriste isti ključ.



Slika 8. Simetrična kriptografija [10]

Na prethodnoj slici vidimo prikaz principa rada simetričnog kriptosustava. Bob želi poslati poruku Alice. Bob prvotnu poruku enkriptira uz pomoć tajnog ključa pa takvu šalje preko nezaštićenog komunikacijskog kanala. Alice prima

kriptiranu poruku i vrši dekripciju uz korištenje tajnog ključa kojeg je i Bob koristio za kriptiranje. Nakon dekriptiranja Alice dobiva prvotnu originalnu poruku koju joj je Bob htio poslati. Pošto je taj kanal nezaštićen tu poruku može presresti neželjeni gost, no on može tu poruku odgonetnuti samo ako dođe u posjed ključa kojeg je Bob prvotno koristio. Zato se ključ drži u tajnosti i nikad se ne smije prenositi nezaštićenim komunikacijskim kanalom.

Najčešći primjer u praksi slanja ključa različitim komunikacijskim kanalom je primanje PIN-a (Personal Identification Number) od strane banke za korištenje raznih kreditnih i debitnih kartica putem pošte umjesto slanje preko internet stranica. Također kod potražnje usluge kao što su mobilno internet bankarstvo jedan dio koda se dobije u banci, a drugi porukom na broj.

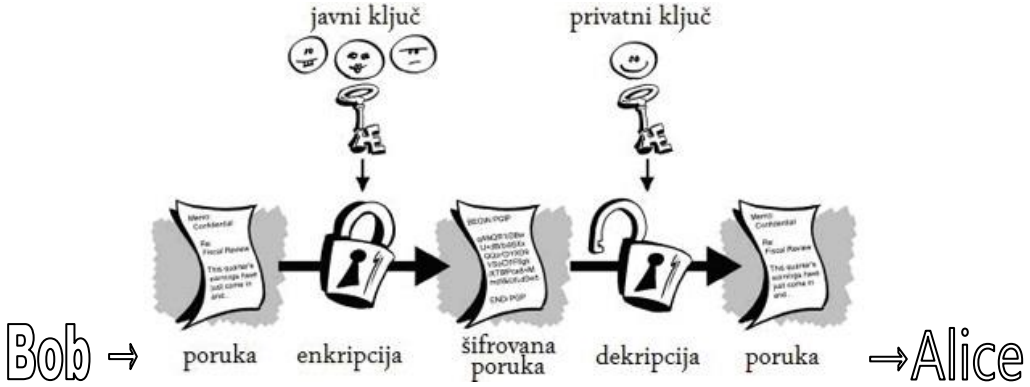
Najpoznatiji algoritmi simetričnih kriptosustava koji se danas koriste su: DES, 3DES, DES-CBC, IDEA, RC5, RC6, AES i drugi.

Prednosti su relativno kratko vrijeme kriptiranja zbog upotrebe kratkih ključeva. No uz to tu postoje i dva velika nedostatka jer za svaku poruku mora postojati jedinstveni ključ, time se javlja potreba za velikim brojem potrebnih ključeva. Uz to problem je i razmjena ključa koja je najpouzdanija ako se korisnici fizički sretnu, ali u velikoj većini su korisnici razdvojeni pa im ta opcija nije zgodna. I tu se javlja potreba za slanjem ključa nekim drugim zaštićenim kanalom.

6.2. Asimetrična kriptografija

Asimetrična kriptografija koja se temelji na dva ključa, privatnom (tajnom) i javnom potječe iz 1976. godine od dvojca američkih kriptografa Whitefield Diffiea i Martina Hellmana.

Glavna razlika između simetričnih i asimetričnih je u tome što kod simetričnih koristimo isti ključ i za kriptiranje i dekriptiranje dok se kod asimetričnog algoritma koriste različiti ključevi za kriptiranje i dekriptiranje. Dakle, informacije koje su kriptiranje javnim ključem mogu dekriptirati samo tajnim ključem, od strane osobe koja posjeduje isti.



Slika 9. Asimetrična kriptografija [11]

Na prethodnoj slici vidimo klasičan primjer jedne asimetrične poruke. Ako Bob želi poslati poruku Alice uz asimetričnu kriptografiju to bi izgledalo ovako. Bob će kodirati poruku uz pomoć javnog (*public*) ključa koji je javno dostupan putem maila ili web stranice. Ako neovlaštena osoba presretne poruku ona ne može uz poznavanje javnog ključa pristupiti toj poruci. Poruku može dešifrirati samo Alice koja ima tajni (privatni) ključ.

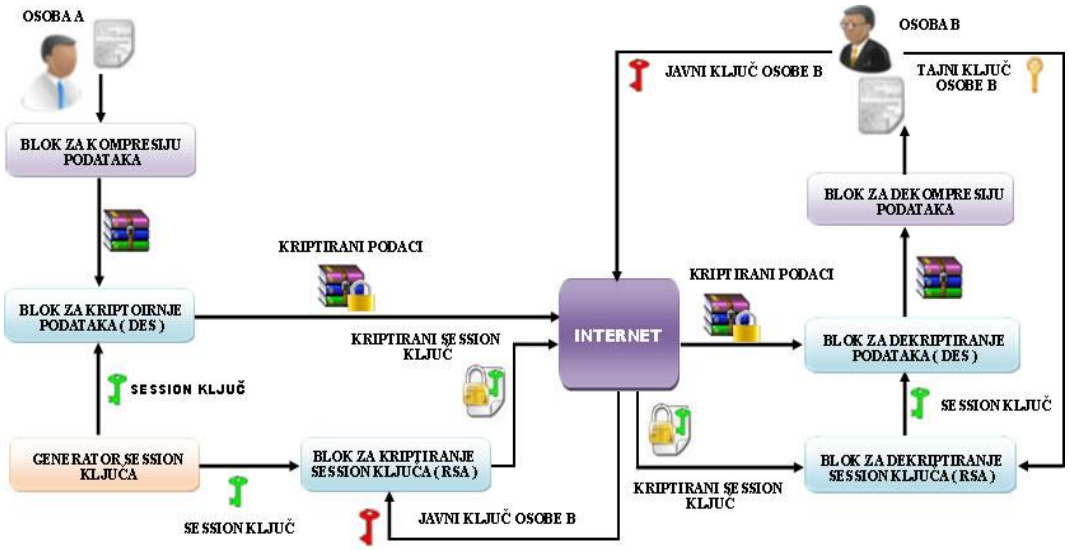
Nedostatak ovog načina kriptiranje je sporost i neprimjerenost za kriptiranje velikih količina podataka, te nesigurnost u ovome slučaju Alice da li je uistinu Bob taj koji je poslao poruku.

Najpoznatiji asimetrični algoritmi su RSA, Diffie-Hellman, ElGamal, Eliptične krivulje, Rabin i drugi.

Velika prednost u odnosu asimetrične kriptografije na simetričnu se javlja u broju ključeva koji su potrebni, dok je nedostatak ogromna veličina ključeva koji time zahtijevaju mnogo vremena da se obrade. Zaključujemo da je za duže poruke bolja simetrična kriptografija, dok za kraće se puno češće koristi asimetrična kriptografija.

6.3. Hibridna kriptografija

Simetrični sustavi imaju već spomenutu manu u svojem dizajnu te ju je nemoguće zaobići, a to je sigurna izmjena ključa između pošiljatelja i primatelja, dok asimetrični kriptosustavi imaju manu drukčijeg karaktera. Asimetrični kriptosustavi su računski vrlo zahtjevni, te nisu najpogodniji za izmjenu velikih podatkovnih datoteka, tj. dugačke poruke. Iz tih razloga proizašla je ideja kombiniranja oba sustava te stvaranje novog koji bi imao prednosti oba sustava, a koji bi zaobišao njihove mane.



Slika 10. Hibridna kriptografija[12]

Na prethodnoj slici prikazan je hibridni kriptografski algoritam popularno nazvan PGP (*Pretty Good Privacy)* najčešće korišten softver email enkripcije koji je kreirao Phill Zimmerman su-osnivač i glavni znanstvenik u tvrtki "*Silent Circle*" 1991. godine.

Osoba A izvornu poruku komprimira, radi lakšeg i bržeg slanja te dodatne zaštite. Tako kompresirana poruka se kriptira nekom od metoda simetičnog kriptiranja pomoću simetričnog ključa. Generiranje simetričnog ključa vrši generator pseudo-slučajnog broja u kombinaciji sa raznim korisnikovim

podacima unesenim tokom procesa generiranja. Tako dobiveni simetrični ključ se kriptira nekom od metoda asimetričnih algoritama pomoću javnog ključa osobe kojoj se poruka šalje te zajedno sa kriptiranom porukom šalje primaocu poruke. Dekriptiranje se vrši obrnutim postupkom. Osoba koja je primila poruku prvo dekriptira primljenu poruku koja sadrži simetrični ključ svojim tajnim ključem. Na taj način dolazi do simetričnog ključa kojim je kriptiran izvorni tekst. Dakle kod hibridnih sustava koristi se duplo kriptiranje i tri ključa: javni i tajni ključ osobe kojoj se šalje poruka i simetrični ključ osobe koja šalje poruku. [12]

Zbog svojih svojstva, tj. prednosti, hibridni sustavi postali su najrašireniji kriptosustavi te se koriste kao sigurnosni mehanizam komunikacije za gotovo sve usluge dostupne putem interneta i šire.

7. VAŽNOST ZAŠTITE PODATAKA U SMISLU ZAŠTITE ŽIVOTA I ZDRAVLJA POPULACIJE

U današnje vrijeme mete terorističkih napada su razni objekti, javna događanja, skupovi, a ponajviše kritične nacionalne infrastrukture: vojska, policija, financijske te zdravstvene institucije. Najčešći razlog napada je ostvarenje različitih političkih prednosti ili ciljeva. Iako je većina oružanih te eksplozivnih napada, sve češći su napadi i preko informatičke infrastrukture na spomenute institucije. No, osim institucija, cilj napada mogu biti i sami građani zbog dobivanja korisnih informacija za napadača.

U većini slučajeva, kod spomenutih institucija, lokalnim se mrežama vrši najveći dio prijenosa osjetljivih podataka te je njima potrebno pružiti i najveću pozornost u kontekstu zaštite i sigurnosti. Neprimjereno zaštićene računalne mreže izložene su rizicima neovlaštenog pristupa i zlouporabe što može posredno dovesti do narušavanja zdravlja, osjećaja sigurnosti, povjerljivosti građana, cjelovitosti i dostupnosti važnih privatnih informacija te velikih financijskih gubitaka, koji su u krajnjem slučaju na teret građana i države.

Stoga u suvremeno doba državna tijela, jedinice lokalne i područne (regionalne) samouprave te pravne osobe s javnim ovlastima koje svoje informacijske sustave javnim i nezaštićenim komunikacijskim kanalima povezuju s drugim informacijskim sustavima u svrhu međusobne razmjene klasificiranih podataka moraju, pored ostalih mjera informacijske sigurnosti, primijeniti mjere kriptografske zaštite. Osim tajnosti, kriptografske metode osiguravaju i cjelovitost, izvornost i neporecivost pojedinog klasificiranog podatka.

Zavod za sigurnost informacijskih sustava propisuje standarde kriptografske zaštite klasificiranih podataka koje tijela i pravne osobe, kao vlasnici informacijskoga sustava, primjenjuju u uspostavi sustava kriptografske zaštite. U Republici Hrvatskoj za kriptografsku zaštitu klasificiranih podataka stupnja tajnosti „Ograničeno“, „Povjerljivo“, „Tajno“ i „Vrlo tajno“ dopušteno je koristiti isključivo kriptografska rješenja ili proizvode koje je odobrio Zavod za sigurnost informacijskih sustava i koji su upisani u Registar proizvoda odobrenih za

zaštitu klasificiranih podataka. Zavod za sigurnost informacijskih sustava pojedini proizvod upisuje u Registar nakon provedenog postupka certificiranja i prihvaćanjem postojećeg certifikata za proizvod koji je već upisan u odgovarajući registar međunarodne organizacije. [13]

7.1. Certifikacija kriptografskih rješenja

Postupkom certificiranja Zavod za sigurnost informacijskih sustava provjerava usklađenost kriptografskog rješenja s međunarodnim normama kako bi utvrdio ima li odabrani proizvod sposobnost osigurati razinu zaštite na očekivani način, a primjereno stupnju tajnosti podataka koji se njime štiti. Certificiranje se provodi na zahtjev državnog tijela koji pojedino kriptografsko rješenje planira koristiti u vlastitom informacijskom sustavu.

Zavod za sigurnost informacijskih sustava provodi i poslove istraživanja, razvoja i ispitivanja tehnologija namijenjenih kriptografskoj zaštiti klasificiranih podataka te upravljanja kriptografskim materijalom stranih zemalja i organizacija koji se u informacijskim sustavima državnih tijela u Republici Hrvatskoj koriste za zaštitu međunarodnih klasificiranih podataka.

Kriptografski certifikati, omogućuju sigurnu autentikaciju, a time i komunikaciju između dvije točke na Internetu, ali i sigurnu identifikaciju suprotne strane. Iako na internetu postoje tvrtke koje prodaju certifikate, kod nas certifikate većinom izdaje FINA (više o tome nešto kasnije u poglavlju 9.2.2.).

7.2. Vrste podataka

Pošto računalne mreže predstavljaju dio informacijskog sustava pomoću kojeg se prenosi najveći broj podatak, velika pažnja treba biti usmjerena upravo njihovoj zaštiti. Podatci u informacijskim sustavima javljaju se u sljedećim oblicima:

- Javni podatci - podatci koji nisu povjerljivi i čiji integritet nije važan, može ih koristiti bilo tko bez ikakvih posljedica. Primjer ovakvih podataka su javni servisi za pružanje informacija.

- Interni podatci - pristup ovim podatcima dozvoljen je samo određenoj grupi korisnika. Javno objavljivanje internih podataka nije dozvoljeno, ali objavljivanje ove vrste podataka nije od kritične važnosti. Primjer ovakvih vrsta podataka su podatci u razvojnim grupama, firmama, radni dokumenti i projekti, interni telefonski imenici.
- Povjerljivi podatci - povjerljivi podatci unutar određene grupe (kompanije) koji su zaštićeni od neovlaštenog pristupa. Neovlašten pristup ovim podatcima može prouzrokovati značajne posljedice kao što su naprimjer: financijski gubitak kompanije ili dobitak konkurentskoj kompaniji, smanjenje povjerenja korisnika usluga ili potrošača proizvoda. Primjeri ovih informacija su: podatci o plaćama, podatci o zaposlenima, projektna dokumentacija, računovodstveni podatci, povjerljivi ugovori.
- Tajni podatci - podatci kod kojih je neautoriziran pristup strogo zabranjen. Integritet podataka je na najvišem nivou. Broj ljudi koji može da pristupi ovim podatcima trebao bi da bude ograničen. Prilikom pristupa ovim informacijama moraju se poštovati veoma striktna pravila. Primjer ovih podataka su: vojni podatci, podatci o većim financijskim transakcijama, podatci od državnog značaja i slično. Ova vrsta podataka se treba čuvati u kriptiranom obliku ili u uređajima sa hardverskom zaštitom. Kada se govori o zaštiti podataka na mreži, uglavnom se misli na zaštitu povjerljivih i tajnih podataka koji se prenose putem računalne mreže.

Sve masovnija upotreba računalnih mreža iziskuje korištenje mehanizama i mjera za zaštitu podataka koji se tim putem prenose. Mjere za zaštitu podataka, zasnivaju se na tri principa:

- Prevencija - odnosi se na poduzimanje preventivnih aktivnosti za zaštitu podataka i računalnih sustava od mogućih napada.
- Detekcija - otkrivanje kako je narušena zaštita, kada je narušena i tko ju je narušio.
- Reakcija - poduzimanje aktivnosti koje dovode do restauracije podataka ili do restauracije računalnog sustava.

Najveća prijetnja podatcima koji se prenose putem računalne mreže javlja se usred slabosti komunikacijske opreme pomoću koje se vrši prijenos podataka. Ugrožavanje podataka u računalnim mrežama se odnosi na prisluškivanje, analizu, mijenjanje, uklanjanje informacija kao i lažno predstavljanje.

7.3. Vrste napada na podatke

Napadi preko mreže kojima je za cilj preotimanje podataka mogu se podijeliti u dvije grupe:

- Pasivni napadi - Pasivni napadi se odnose na sva prisluškivanja i nadgledanje informacija tijekom prijenosa, bez ikakvih izmjena. Ovom vrstom napada napadač na relativno jednostavan način dolazi do informacija. Pasivni napadi se teško otkrivaju. Kao najčešće korišteni mehanizmi zaštite od pasivnih napada primjenjuje se kriptiranje podataka koji se prenose putem komunikacijskih linija. Kriptiranje podataka se odnosi na modifikaciju istih tako da postanu nerazumljivi ili besmisleni za sve one korisnike kojima nisu namijenjeni. Kao takvo, kriptiranje predstavlja najvažniji element zaštite podataka u računalnim mrežama.
- Aktivni napadi - su svi napadi koji vrše promjenu sadržaja ili toka informacija. Ova vrsta napada je daleko kompliciranija i teža za otkrivanje nego pasivni napadi. U aktivne napade ubrajaju se modifikacije paketa informacija koji se kreću putem mreže, slanje lažnih paketa, prekidi toka informacija kao i razne vrste preusmjeravanja paketa na mreži. Zbog raznovrsnosti ove vrste napada, mehanizmi zaštite moraju biti daleko kompliciraniji i napredniji nego kod pasivnih napada. [14]

7.4. Sigurnosni servisi

Sigurnosni servisi predstavljaju skup pravila koja se odnose na aktivnosti korisnika koje doprinose sigurnosti podataka na mreži. Postoji šest vrsta osnovnih sigurnosnih servisa:

- Autentifikacija,
- Povjerljivost ili tajnost podataka,
- Nemogućnost negiranja poruka,
- Integritet podataka,
- Autorizacija i kontrola pristupa,
- Raspoloživost resursa,

Autentifikacija (identifikacija) se odnosi na potvrdu originalnosti poruka, odnosno na identifikaciju izvora poruke ili dokazivanje identiteta korisnika. Autentifikacija se odnosi na pametne (*smart*) kartice, kreditne kartice, biometrijske čitače i slično. [15]

Povjerljivost ili tajnost podataka osigurava zaštitu podataka od neovlaštenih lica. Podatke kroz mrežu treba slati u kriptiranom obliku, osim toga, podatci se, također, trebaju i čuvati u istom. Povjerljivost se ostvaruje kriptiranjem podataka ili fizičkom zaštitom komunikacijske linije. [15]

Servis nemogućnosti negiranja poruka pruža prevenciju od lažnog negiranja slanja date poruke/dokumenta. Servis također sprječava da primatelj izmjenjuje sadržaj primljenih poruka i da tvrdi da je takvu primio. Najčešće korišteni mehanizam koji osigurava zloupotrebu ove vrste je digitalni potpis. [15]

Autorizacija je servis koji vrši provjeru da li je identificiranom korisniku dozvoljen pristup određenim podatcima, a servis kontrole pristupa utvrđuje prava pristupa korisnika. Za realizaciju ovog servisa potrebno je omogućiti postavljanje privilegija objektima koji im pripadaju i spriječiti korisnike sustava da pristupaju korištenjem prava pristupa drugih korisnika. [15]

Raspoloživost resursa se odnosi na reakciju u cilju održavanja funkcionalnosti resursa u slučaju detekcije otkaza ili napada. [15]

Digitalni potpis je metoda koja se koristi za provjeru porijekla i utvrđivanje besprijekornosti informacije. Vrlo je bitno da digitalni potpis zadovoljava određene zahtjeve:

- vjerodostojnost potpisanog dokumenta (nepromjenjivost dokumenta),
- nemogućnost ponovnog korištenja jednom generiranog potpisa na drugom mjestu,
- nemogućnost krivotvorenja potpisa,
- nemogućnost izbjegavanja odgovornosti za potpisani dokument. [16]

7.5. Virusi i napadi

Virologija u računalnom području je znanost koja se ponajviše bavi virusima, a u manjoj mjeri drugim štetnim ili zlonamjernim programima. I ona kao i kriptografija ima dvije strane: stvaranje virusa i borba protiv njih. Virusi su samoumnažajući programi koji se šire sa zaraženog informacijskog sustava na druge, kopirajući svoj programski kod u druge programe ili dokumente.

Antivirusi su razvijeni kao rješenje za viruse i njihova glavna zadaća je prepoznati i onemogućiti viruse (ili druge zlonamjerne programe) prije nego što se oni aktiviraju. Oni rade najčešće na metodi prepoznavanja obrazaca ili dijelova nekog virusnog programa, takozvanih „potpisa“. [17]

7.6. Kriptovirologija

Dosad su spomenute samo „dobre“ strane kriptografije no ona se može koristiti i u štetne svrhe kao što je naprimjer slučaj kad napadač napada neki sustav i štiti svoj trag ili identitet kriptografijom.

Kriptovirologija je aktivnost koja se bavi proučavanjem primjenom kriptografskih i kriptoanalitičkih metoda i tehnika na stvaranje zlonamjernih programa i aktivnosti te borbu protiv njih.

7.7. Zaštita napadača uz pomoć kriptografije

Tipični napadač razvija alate za napade na svom, skrivenom računalu koje štiti lozinkama, kriptiranjem izvornog koda napadačkih programa i slično. No, svoje napada ne pokreče sa svog računala, već s nekog tuđeg računala u koje je prodro, iskoristivši njegovu ranjivost. Kako bi zameo tragove, u pravilu, do računala s kojeg će pokrenuti napad dolazi kroz nekoliko drugih računala čiju je sigurnosnu zaštitu također probio. Svoju prisutnost na tim računalima, a posebno na računalu s kojeg će pokrenuti napad također štiti lozinkama te kriptiranjem napadačkih programa i podataka koje on sakupi. Kriptirat će i komunikaciju umnoženih i raširenih napadačkih programa s izvorišnim računalom (s koje je pokrenut napad). Ovakvi bi se oblici korištenja kriptografije uvjetno mogli nazvati „normalnim“ (što ne znači i dozvoljenim) korištenjem u rukama napadača. [17]

7.8. Korištenje kriptografije protiv žrtve

Napadač može primijeniti kriptografiju na žrtvinim alatima, sustavu ili podatcima. Nakon što napadački program prodre u sustav žrtve, može potražiti točno određeni program i/ili podatke ili ih odabrati nasumce, te na njih primijeniti kriptografski postupak. Na računalu će ostati samo kriptirani podatci koje njihov vlasnik ili legitimni korisnik više ne može upotrijebiti. Napadač će se nekim komunikacijskim putem obratiti žrtvi te tražiti otkupninu u zamjenu za dekriptiranje žrtvinih podataka. Tu se za napadača pojavljuje tehnički izazov: kako dekriptirati podatke žrtve tako da to žrtva može prihvatiti, a da napadač ne otkrije svoj identitet. U praksi postoje dva modela:

- Osnovni - u kojem napadač stvori RSA ključ. Javni dio ključa pohrani u virus, a privatni čuva kod sebe. Kad virus prodre u sustav žrtve, kriptirat će njen sadržaj javnim ključem. Napadač od žrtve traži otkupninu i kad ju dobije šalje žrtvi privatni dio ključa kojim žrtva onda može vratiti svoje podatke.

- Hibridni - i ovdje se, kao i kod osnovnog, u virusu nalazi javni ključ napadača, ali se žrtvini podatci ne kriptiraju njime već jednim novim, slučajno izabranim ključem. Taj se ključ kriptira javnim ključem napadača i pohrani na sustavu ili pošalje napadaču. Kad je otkupnina plaćena, napadač samo treba dekriptirati ključ kojim su kriptirani žrtvini podatci i poslati ga žrtvi. [17]

8. ZAŠTITA RAČUNALNIH MREŽA ORUŽANIH SNAGA PRIMJENOM VIRTUALNOG HONEYBOTA

Proporcionalno s razvojem informacijsko-komunikacijske tehnologije (IKT) raste složenost sustava i široka primjena, ali i broj incidenata na javnim mrežama. Napadači vrlo brzo pronalaze propuste u zaštiti novih sustava, razvijaju svojstvene alate i tehnike kojima se zaobilaze definirane sigurnosne mjere. Vrijeme reagiranja pri upadu u računalni sustav znatno je skraćeno. Imajući u vidu ove prijetnje, pri razvoju novih računalnih mreža velika se posvećenost pridaje projektiranju sustava zaštite. Međutim, i pored svih poduzetih mjera, značajan je negativan učinak štetnih programa koji se svakodnevno pojavljuju – tipa virusa, crva, trojanaca itd. Svaki napad na bilo koji sustav karakteriziraju sljedeći elementi:

- Metoda: vještina, znanje, alat i druga sredstva kojima se vrši napad,
- Prilika: vrijeme i raspoloživost sustava za napad,
- Motiv: razlog zbog kojeg neko napada sustav.

Sa gledišta zaštite računalnih sustava izuzetno je bitno praćenje i poznavanje karaktera napada sa svim njegovim elementima. Mehanizmi za detekciju napada nisu uvijek u mogućnosti da preventivno djeluju na sve vrste napada. Česti su napadi koji nisu poznati sustavu obrane i predstavljaju novitet, te se nameće potreba za pravovremenim otkrivanjem i izučavanjem njihove prirode u fazi dok nisu kompromitirani ciljani sustavi. Tehnike, metode, sredstva i motivi svakodnevno poprimaju nove nepoznate dimenzije. Da bi se prikupili podatci i izučila priroda napada koji sigurno predstoji, primjenjuju se različite tehnike. Relativno nova, ali svakim danom sve popularnija tehnika na našim područjima, namijenjena prvenstveno svim vrstama napadača je upravo *honeypot.*

U računalnoj terminologiji, *honeypot* je računalni mehanizam koji je postavljen za otkrivanje, odbijanje ili, na neki način, suprotstavljanje pokušajima neovlaštene uporabe informacijskih sustava.

Pojam *honeypot* prvi je put predstavio osnivač *honeynet* projekta Lance Spitzner 1999. godine u radu nazvanom "Izgraditi *Honeypot*". [18]

Iako je Spitzner bio prvi koji je doveo riječ "*honeypot*" na područje računalne znanosti, idejno rješenje je predloženo sredinom 1980-ih.

Honeypot obuhvaća sve računalne resurse (sklopovski, aplikacijski te mrežni) koji služe kao mamac, a predviđeni su da budu napadnuti ili kompromitirani od neovlaštenih korisnika. Načini implementacije i primjena *honeypota* je raznolika, što ovaj sustav zaštite čini fleksibilnim i primjenjivim u različitim područjima zaštite računalnih sustava. Zaštita računalnih sustava je trajni proces cjelokupnog životnog ciklusa sustava, koja treba osigurati već prije spomenutu prevenciju, detekciju te nakraju, reakciju. *Honeypot* se može svrstati u sve tri faze zaštite. Mogućnost detekcije neovlaštenih aktivnosti, te prikupljanje novih spoznaja o tehnikama i alatima koje napadači koriste, a koji se kasnije koriste za razvoj novih sigurnosnih rješenja, karakteristike su koje to potvrđuju.

8.1. Pojam, definicija i arhitektura Honeypota

Svakako prvi korak u razumijevanju *honeypota* upravo je njegova definicija. Za razliku od svima poznatog vatrozida (*firewalla)* i mehanizma za prevenciju napada (*Intrusion Prevention System*, IPS), *honeypot* ne može spriječiti štetne aktivnosti u sustavu. Njegova svrha je, prvenstveno, da te aktivnosti registrira. Ovaj resurs može registrirati bilo koji nekriptirani napad u mrežama, što ga čini fleksibilnim, pa time i popularnim i sve češće primjenjivanim. Definicija da je "*honeypot* resurs informacijskih sustava namijenjen neovlaštenim korisnicima" ukazuje na mogućnost njegove široke primjene u svim tipovima distribuiranih informacijskih sustava s velikim mogućnostima detekcije. [14]

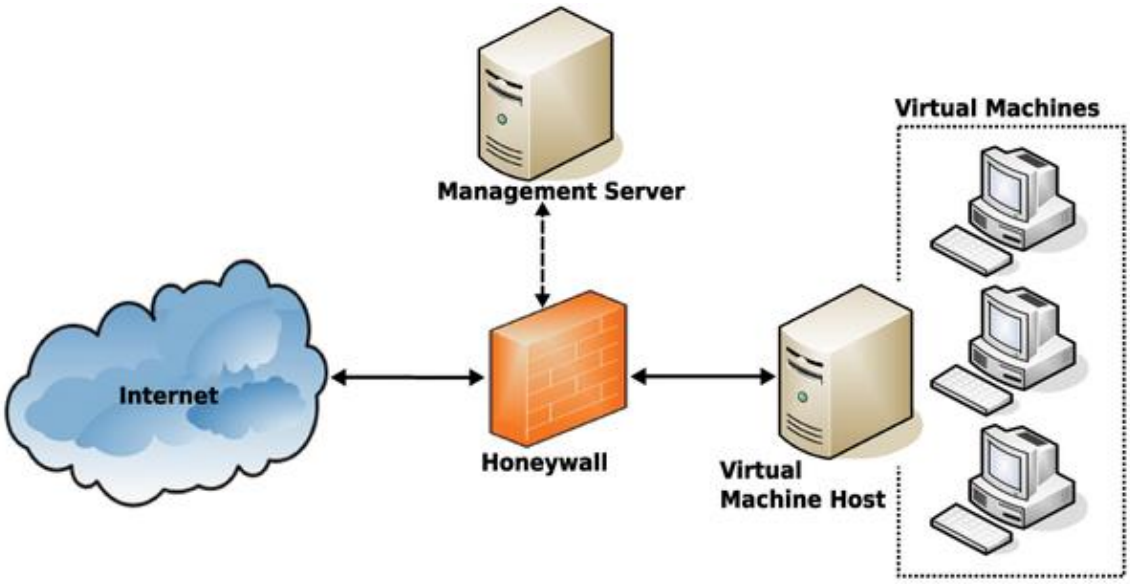
Postavlja se pitanje same prirode *honeypota* kao arhitekture koja bilježi samo neautorizirane aktivnosti na sebi ne smije imati korisne resurse za sam informacijski sustav na koji je postavljen. U teoriji *honeypot* ne bi trebao vidjeti promet u mreži, jer on nema legalnih aktivnosti. Svaka interakcija produkcijskih

uređaja s *honeypotom* je nelegitimna aktivnost i tako se i registrira u njemu. Zamisao je da je potrebno zavarati napadača da radi na legitimnom sustavu iako je on na *honeypotu* koji samo simulira rad pravog. Tako napadač troši dragocjeno vrijeme i resurse, dok će *honeypot* pratiti i snimati sve njegove aktivnosti. Tako *honeypot* prikuplja dovoljno informacija o napadaču, a da u stvari ne raspolaže legitimnim podatcima tvrtke, odnosno ustanove. Složenija rješenja *honeypota*, koja simuliraju čitave mreže sa svim komponentama klasičnih računalnih mreža (server, vatrozid, preklopnik, mehanizmi za detekciju i prevenciju napada i dr.) nazivaju se *honeynetom* i prvenstveno su primijenjeni u svrhu istraživanja, tj. prikupljanja informacija o napadaču.

Potrebno je posebnu pažnju obratiti na sigurnosnu politiku vatrozida iza kojeg se nalazi *honeynet* sustav. Konfiguraciju je potrebno prilagoditi tako da se omogući prikupljanje što veće količine informacija o neovlaštenim korisnicima, a da se pritom neovlaštene aktivnosti ograniče isključivo na *honeynet* sustav. Površnom i nepažljivom konfiguracijom vatrozida situacija može vrlo lako izmaći kontroli, nakon čega kompromitirani *honeynet* sustav predstavlja ozbiljnu prijetnju i za legitimne računalne sustave. Ovu mogućnost uvijek treba svesti na minimum.

Honeynet nije proizvod, ne instalira se nikakav softver, to je arhitektura koja se sastoji od niza *honeypotova*. Ova arhitektura treba biti dobro kontrolirana kako bi se moglo pratiti što se dešava u mreži. Ovakva arhitektura postavlja se u ciljni sustav. Za uspješno postavljanje arhitekture *honeyneta* ključna su tri zahtjeva:

- Kontrola podataka - koja definira koje aktivnosti se kontroliraju *honeynetom*, kako bi se smanjio rizik,
- Snimanje podataka - koji su usmjereni prema *honeynet* aktivnosti napadača,
- Zbirka podataka - ovaj zahtjev svojstven je samo za organizacije koje imaju više *honeynet* platformi u distribuiranom okruženju, kao što je *Honeynet* istraživačko okruženje. Ove organizacije sve snimljene podatke prikupljaju na jedno mjesto, kako bi ih analizirali i poredali. [14]



Slika 11. Prikaz *Honeynet* arhitekture [19]

U prvoj generaciji *honeyneta* vatrozid je postavljen na trećem nivou gdje se lako detektira. Ovaj problem je riješen postavljanjem *gatewaya* s dva uređaja koji se teško detektira. Vatrozid radi u most (*bridge*) modu i kontrolira sve konekcije izvana i iznutra na prvoj generaciji *honeyneta*.

Prednost pristupnog računala u drugoj generaciji je ugradnja IPS-a (*Intrusion Preventions System)*, koji omogućava iste funkcije kao i mehanizama za detekciju napada (*Intrusion Detection System*, IDS), ali za razliku od IDS-a ima sposobnost da blokira i modificira napade. Ova osobina pomaže u razdvajanju legitimnih i štetnih aktivnosti. Ako napadač pokuša da napadne mrežne resurse van *honeypota* IPS će takav pokušaj blokirati ili modificirati. On registrira poznate napade, a nepoznati napadi prolaze. Ova generacija *honeyneta* je teža za detekciju s obzirom na to da realnije simulira računalne mreže. Virtualni *honeynet* sve funkcionalnosti *honeyneta* izvršava na jednom računalu. Razvijen je softver koji kreira više virtualnih računala i radi na različitim operativnim sustavima. Ova tehnologija je dobra ako su ograničeni resursi. Također, virtualni *honeynet* je lakše održavati u usporedbi s klasičnim,

jer se sve izvršava na jednom računalu. Virtualni *honeynet* ima nekoliko ograničenja u pogledu tipa arhitekture i operacijskog sustava koji se može koristiti, što je uvjetovano konkretnim rješenjem. [14]

8.2. Analiza stvarnog sustava

Ministarstvo obrane i vojska imaju razvijene informacijske sustave usklađene s organizacijskom strukturom. Pojedini dijelovi sustava funkcioniranju zasebno u organizacijskim cjelinama kao lokalne računalne mreže. Za razvoj opremanje i projektiranje računalnih mreža zadužena je uprava za telekomunikacije i informatiku. U skladu s materijalnim mogućnostima i raspoloživim sredstvima konstantno se poboljšavaju organizacijske cjeline kao i tehnologija. Najviše se ulaže upravo u zaštitu računalnih sustava. Primjenom svih poznatih hardverskih i softverskih rješenja sprječava se neovlašteni pristup računalnim mrežama unutarnjeg ili vanjskog karaktera. Obavezna je primjena vatrozida, mehanizma za detekciju i prevenciju napada, a prijenos podataka se vrši kriptirano. Prijetnje koje se nameću razvojem i otvaranjem pojedinih dijelova sustava prema javnoj mreži postaju svakim danom sve veće, posebno imajući na umu znanja i metode, a ponajviše želju napadača da se domognu korisnih informacija. Imajući na umu značaj tih informacija koje se nalaze u resursima Ministarstva obrane i Vojske, nameće se potreba kontinuiranog praćenja i dogradnja zaštite informacijskih sustava. [14]

8.3. Primjena virtualnog honeyneta u zaštiti računalnih sustava

Uvođenje virtualnog *honeyneta* predstavlja značajno unapređenje u smislu zaštite računalnih sustava ponajviše zbog mogućnosti da se *honeynet* s više operativnih sustava postavi na jednom računalu. Glavna prednost je relativno malo angažiranje resursa i jednostavna administracija.

Pošto je kod većine interna računalna mreža spojena preko usmjernika (*routera)* s internetom, preporuča se instalacija arhitekture virtualnog *honeyneta*

neposredno iza usmjernika i to preko preklopnika na jednom domaćin (*host*) računalu. Svi virtualni *honeypotovi* koriste VMWare sučelje.

VMWare je programski paket koji podržava kreiranje virtualnih komponenti mreže za zamišljenu računalnu mrežu. To je, u stvari, virtualna mreža koju će *honeynet* vidjeti nakon instalacije. *Honeynet* je konfiguriran tako da koristi tri sučelja; dva most (*bridge*) i jedan samo domaćin (*host-only)*. *Honeypot* 3 i 4 su konfigurirani preko jednog samo domaćin sučelja, dok napadač koristi most sučelje.

Mosno sučelje nam služi da *honeypot* spojimo na računalnu mrežu preko domaćin računala. Pomoću mosta vrši se spajanje virtualne mrežne kartice u virtualnom *honeypotu* na mrežnu karticu domaćin računala. U pravilu, na domaćin računalu se uvijek prvo instalira VMWare, a zatim različiti operativni sustavi za *honeypot* (3 koristi Linux, a 4 Windows platformu). Nakon instaliranja operativnog sustava instalira se *honeywall*, što uključuje razvoj, konfiguriranje i upravljanje *honeynetgatewayom*. *Honeynet* je na drugom nivou zaštite, a prima i kontrolira sve podatke koji pristižu od napadača. [14]

8.4. Prednosti primjene Honeypota

Za razliku od IDS-a koji prijavljuje kada i tko od napadača pristupa mreži, *honeypot* je odvojen od mreže, ne vodi računa o preopterećenju prometa na mreži niti razdvajanje legitimnih od nelegitimnih paketa podataka. *Honeypot* prati samo podatke koji pristižu na njega. Obično je ta količina podataka mala, ali vrlo važna, jer nosi informacije o napadaču. *Honeypot* daje mogućnost administratorima da brzo uoče o nedozvoljenim pristupima, a ako je *honeypot* napadnut i onesposobljen daje mogućnost administratoru da u realnom vremenu spriječi napad na računalne resurse kompanije, te može služiti i kao svojevrsni alarm.

Prednosti ove metode su:

- mogućnost prikupljanja informacija o tehnikama i alatima koje napadač koristi,
- mali broj lažnih upozorenja s obzirom na to da *honeypot* registrira samo neovlaštene aktivnosti,
- relativno mala količina prikupljenih podataka (bilježi male količine podataka, ali su to po prirodi vrlo korisni podatci),
- fleksibilnost brojne mogućnosti i vrlo široko područje primjene,
- skromni zahtjevi za računalnim resursima,
- mogućnost analize kriptiranih protokola,
- projektiranje arhitekture je jednostavno, ali sama implementacija je puno kompliciranija, imajući u vidu da je potrebno solidno znanje o principima zaštite računalnih sustava. Za implementaciju nisu potrebni složeni algoritmi ili tablice stanja i sl., kao što je to slučaj s drugim tehnologijama koje su namijenjene za detekciju i identifikaciju neovlaštenih korisnika.

9. e-HRVATSKA

Strategija e-Hrvatska je inicijativa napravljena s namjerom unapređenja kvalitete života građana u Republici Hrvatskoj podizanjem konkurentnosti gospodarstva pomoću informacijske i komunikacijske tehnologije, pružanjem visokokvalitetnih elektroničkih javnih usluga društvu, a u skladu s važećim Strategijama i zakonima Republike Hrvatske, direktivama Europske unije i preporukama struke. Svrha ove strategije je stvoriti koherentan, logičan i učinkovit informacijski sustav države pružanjem visokokvalitetnih i ekonomičnih elektroničkih usluga kako na nacionalnoj, tako i na europskoj razini. Osigurati interoperabilnost između postojećih i novih IKT sustava u javnoj upravi, ujedno eliminirajući dupliciranje njihovih funkcionalnosti, također je u fokusu ove Strategije. Ostvarenje njenih ciljeva mjerit će se na temelju postotka građana i tvrtki koje koriste javne e-usluge, kao i razinom zadovoljstva korisnika.

Glavna vizija je izvrsnost u pružanju pametnih, održivih i sigurnih elektroničkih javnih usluga (e-usluga) koje će osigurati višu kvalitetu života građana, poslovnih i znanstvenih subjekata, točnije horizontalno i vertikalno integriranih kompleksnih elektroničkih usluga okrenutih korisnicima, koje su dostupne putem različitih kanala 24/7, a koje brzinom i kvalitetom odgovaraju potrebama korisnika. Navedeno se osigurava pružanjem e-usluga, informatizacijom poslovnih/upravnih procesa i otvaranjem informacija javne uprave za ponovno korištenje u komercijalne i nekomercijalne svrhe. [19]

9.1. e-Usluge

Republika Hrvatska intenzivno radi na uvođenju e-uprave. Iako su mnoga područja jako dobro pokrivena e-uslugama, ipak i dalje postoji mogućnost unapređenja sustava. Ujedno su uspostavljeni ključni preduvjeti razvoja e-usluga: e-identitet, sigurni pretinac za komunikaciju s javnom upravom, jedinstveno mjesto pristupa i identifikacije/autentifikacije te sustav javnih i

osnovnih registara. Korištenje navedenog propisano je Zakonom o državnoj informacijskoj infrastrukturi. [20]

9.2. e-Građani

Sustav e-Građani uspostavljen je s ciljem modernizacije, pojednostavljenja i ubrzanja komunikacije građana i javnog sektora te povećanja transparentnosti pružanja javnih usluga.

Sustav e-Građani čine:

- Središnji državni portal
- Osobni korisnički pretinac i
- Nacionalni identifikacijski i autentifikacijski sustav.

Komponente predstavljaju sigurnu i naprednu elektroničku komunikaciju s javnim sektorom. Svaki od sustava rješava pojedini problem. Središnji portal rješava pitanje raspršenosti informacija i e-usluga, Nacionalni identifikacijski i autentifikacijski sustav (NIAS) rješava pitanje verifikacije elektroničkog identiteta i razvijena je mreža za izdavanje jedne vrste pristupnih elemenata, a osobni korisnički pretinac (OKP) predstavlja mehanizam za sigurnu dostavu personaliziranih informacija korisnicima. [20]

9.2.1. Zaštita osobnih podataka građana (GDPR)

GDPR (*General Data Protection Regulation*) je Opća uredba o zaštiti osobnih podataka koja se primjenjuje od 25. svibnja 2018. Zaštita osobnih podataka jedan je od osnovnih zadataka koje GDPR stavlja pred organizacije bilo da je riječ o osobnim podacima korisnika, klijenata ili zaposlenika. Organizacije u svakom trenutku moraju znati gdje su koji podaci te u koju svrhu se smiju koristiti. Isto tako, u slučaju da netko odluči povući privolu za korištenje njegovih osobnih podataka, organizacije moraju biti u mogućnosti učiniti to u zadanom roku. [21]

Svrha zaštite osobnih podataka je zaštita privatnog života i ostalih ljudskih prava, i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka.

Zaštita osobnih podataka u Republici Hrvatskoj osigurana je svakoj fizičkoj osobi bez obzira na državljanstvo i prebivalište te neovisno o rasi, boji kože, spolu, jeziku, vjeri, političkom ili drugom uvjerenju, nacionalnom ili socijalnom podrijetlu, imovini, rođenju, naobrazbi, društvenom položaju ili drugim osobinama.

Zakonom o zaštiti osobnih podataka osnovana je Agencija za zaštitu osobnih podataka kao samostalno i neovisno tijelo s temeljnom zadaćom provedbe nadzora nad obradom osobnih podataka u Republici Hrvatskoj.

Osobni podatci smiju se iznositi iz RH u druge države ili međunarodne organizacije ukoliko država ili međunarodna organizacija osigurava odgovarajuću zaštitu osobnih podataka, odnosno ako su ispunjeni drugi uvjeti određeni Zakonom o zaštiti osobnih podataka (npr. Privola ispitanika, ugovorne klauzule koje jamče zaštitu osobnih podataka itd.).

Zbirke osobnih podataka, odnosno osobni podatci sadržani u zbirkama osobnih podataka smiju se iznositi iz Republike Hrvatske u svrhu daljnje obrade samo ako država ili međunarodna organizacija u koju se osobni podatci iznose ima odgovarajuće uređenu zaštitu osobnih podataka, odnosno osiguranu adekvatnu razinu zaštite.

Razumijeva se da sve države članice EU imaju odgovarajuće uređenu zaštitu osobnih podataka kao i države za koje je Europska Komisija utvrdila da osiguravaju adekvatnu zaštitu osobnih podataka (ostale države svijeta). [22]

9.2.2. Izdavanje certifikata

Sustav za izdavanje certifikata sastoji se od korijenskog certifikacijskog tijela koje izdaje certifikate za subordinirana certifikacijska tijela koja onda izdaju certifikate krajnjim korisnicima.

Fina koristi jedno korijensko certifikacijsko tijelo „Fina Root CA“, te dva subordinirana certifikacijska tijela „Fina RDC“ (registar digitalnih certifikata) te „Fina RDC –TDU“. (registar digitalnih certifikata - u tijelima državne uprave)

Fina RDC izdaje kvalificirane normalizirane i *lightweight* certifikate za:

- fizičke osobe – građane (osobni certifikati)
- fizičke osobe povezane s poslovnim subjektom (poslovni certifikati)
- IT opremu povezanu s poslovnim subjektom (poslovni certifikati za IT opremu).

Fina RDC-TDU CA izdaje te certifikate državnim dužnosnicima i zaposlenicima u tijelima državne uprave. [23]

9.2.3. Kriptografski algoritmi i duljine ključeva

Sukladno odredbama zakonske regulative iz područja elektroničkog potpisa, za izdavanje certifikata i vremenskih žigova Fina koristi propisane sigurne kriptografske algoritme i duljine kriptografskih ključeva.

Za izračun sažetka pri potpisivanju certifikata CRL i vremenskih žigova koristi se algoritam SHA-256,RSA.

Duljine kriptografskih RSA parova ključeva koje se koriste su sljedeće:

- CA parovi ključeva: duljina 4096 bitova, RSA
- Korisnički parovi ključeva: duljina 2048 bitova, RSA

Na taj se način ostvaruje sigurnost i povjerenje u izdane certifikate i kvalificirane vremenske žigove. [23]

9.3. e-Zdravstveno

Hrvatski zavod za zdravstveno osiguranje aktivacijom usluge e-Zdravstveno omogućuje registriranim korisnicima pokretanje postupka za utvrđivanje statusa osigurane osobe u obveznom zdravstvenom osiguranju elektroničkim putem

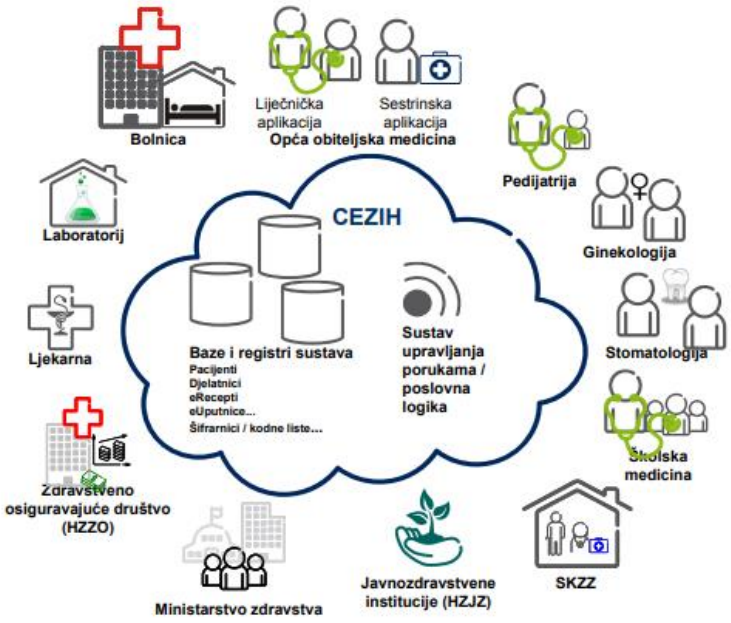
(podnošenje elektroničke prijave). Pod pojmom elektronička prijava podrazumijevamo: podnošenje prijave i odjave osiguranih osoba, te promjenu podataka osiguranih osoba elektroničkim putem. Usluga je namijenjena pravnim osobama (obveznicima uplate doprinosa), koji se vode u registru Zavoda, raspolažu odgovarajućom elektroničkom opremom i posjeduju elektronički potpis u skladu s odredbama Zakona o elektroničkom potpisu, te koje žele postati korisnici usluge e-Zdravstveno koristeći:

- FINA e-karticu (s naprednim digitalnim potpisom),
- Multifunkcionalnu karticu koja se korisnicima e-zabe izdaje prilikom ugovaranja B2G (*Business to Government*) usluga. [24]

9.3.1. Implementacija projekta CEZIH

CEZIH je Centralni zdravstveni informacijski sustav Republike Hrvatske koji povezuje niz aplikacija i sustava zdravstva u Republici Hrvatskoj. Operator središnjeg dijela integralnog informacijskog sustava CEZIH je Hrvatski zavod za zdravstveno osiguranje.

Koncepcija sustava je takva da klijentske aplikacije razmjenom poruka, a koristeći web servise sustava CEZIH mogu komunicirati međusobno ili prema drugim korisnicima koji imaju pristup podacima unutar sustava. Jedna od najpopularnijih usluga CEZIH sustava je eRecept, te kasnije uvedena eUputnica, koje su za razliku od ostalih usluga u velikoj većini doživjele nepodijeljene pohvale svih sudionika sustava: pacijenata, ljekarnika, liječnika, HZZO-a i drugih partnera uključenih u sustav i izvan njega. [25]



Slika 12. Načelna shema CEZIH sustava [25]

9.3.2. Problemi kod uvođenja CEZIH sustava

Jedan od temeljnih problema koji su se ispriječili na početku implementacije sustava bila je nepovjerljivost prema projektima koje forsira HZZO kao i stav liječnika da je to samo jedan u nizu uzaludnih pokušaja informatizacije hrvatskog zdravstva. [26]

Sam prijelaz na nove aplikacije, koje nisu nalik na prethodno korištena sučelja uzrokuje bitno usporenje rada timova zbog uhodavanja, a potrebno je i dopunjavati podatke zbog nepotpunog automatskog prijenosa podataka iz starijih aplikacija. Zbog kompleksnosti aplikacije javlja se i materijalni problem zbog nabavka nove ili dogradnje postojeće računalne i komunikacijske opreme. [26]

Jedan od glavnih i najčešće spominjanih prigovora na CEZIH bio je da sustav narušava povjerljiv odnos liječnik-pacijent te se „iznošenjem“ podataka iz ordinacije krši Ustav i zakone RH. Međutim, razlog tome bila je neupućenost korisnika u stvarni stupanj kriptološke zaštite u razmjene podataka. [26]

9.3.3. Ugroze za zdravstvene informacije

U posljednje vrijeme javlja se sve veći broj *cyber* - napada kojima je cilj doći do zdravstvenih podataka ili zdravstvenih kartona korisnika. Do te pojave dolazi zbog činjenice da podatci iz zdravstvenih kartona sada vrijede deset puta više od onih o nečijoj kreditnoj kartici jer se uz pomoć zdravstvenih podataka mogu stvoriti lažne kartice i podizati medicinska oprema, lijekovi i pomagala, te organizirati prijevare osiguravajućih kuća. Stoga se sve više hakera odlučuje upravo na ovu vrstu kriminala te smišljaju što inovativnije načine kako bi dobili detaljan uvidu u stanje stanovništva, segmenta državne uprave i slično. Na meti su najviše bolnice i druge institucije u kojima su pohranjeni zdravstveni podatci, a koje nisu dobro organizirane u aspektu čuvanja tih podataka.

Tvrtke za *cyber* - sigurnost otkrile su razne kriminalne skupine koje su slale viruse u rendgenske uređaje i aparate za analizu krvi kako bi došle do poslužitelja u kojem su pohranjeni osobni zdravstveni podatci.

Pošto se najviša sigurnost posvećuje upravo prije spomenutom ministarstvu, vojsci, te istraživačkim centrima, a ove ustanove su često uskraćene što za financijsku pomoć, što za stručnost osoba koji bi se bavili tim problemom pa bi se moglo reći da su klinički informatički sustavi puni sigurnosnih rupa.

Zabrinjavajuća je činjenica da je svaki četvrti napad hakera, napad upravo na zdravstveni sustav. Napadi na isti iznimno su opasni jer kad se, primjerice, kompromitira sustav banke te se ukradu podatci klijenata, čim se napad otkrije on postaje bezopasan jer se promjene PIN-ovi. No kada se kompromitira sustav zdravstva, ukradene se informacije ne mogu mijenjati, stoga posljedice krađe podataka pacijenata mogu biti nesagledive. Ukradenim se podatcima o zdravstvenom stanju pacijenta, terapijama koje je primao i slično, mogu poslužiti, primjerice, privatne poliklinike, razni oglašivači, a činjenica je da medicinske podatke mogu zloupotrebljavati i privatne osiguravajuće kuće te poslodavci. Nimalo manje zabrinjavajuća je činjenica da bi provalom u zdravstveni sustav, hakeri mogli nanijeti ozbiljnu štetu jer sve podatke o

pacijentu, koji se nalaze u bazi podataka, mogu vrlo lako promijeniti. Zamislimo samo što bi se dogodilo kada bi iz kartona pacijenta izbrisali podatak da je alergičan na penicilin ili kada bi promijenili doze lijeka koje je liječnik propisao i slično.

Kao i sve što se prvobitno pojavi u Americi, ova vrsta kriminala našla je put i do naših prostora. Postavlja se pitanje ako se to događa na svjetskoj razini kakve šanse ima Hrvatski zavod za zdravstveno osiguranje (HZZO) protiv hakerskih napada?

Niti jedan sustav pa tako niti sustav HZZO-a, nije apsolutno siguran. Unatoč ogromnim ulaganjima upravo u zaštitu, čak su i giganti, kao što su Pentagon, NASA, CIA i FBI, bili kompromitirani. Nerealno je stoga, pretpostaviti da je sustav HZZO-a, sigurniji, kada znamo da se od hakerskih napada ni napredniji američki zdravstveni sustav nije uspio adekvatno zaštiti.

9.3.4. Zaštita zdravstvenih informacija u Republici Hrvatskoj

Osiguranje zaštite podataka u sustavu zdravstvene zaštite se ostvaruje pomoću sljedećih metoda:

- Korištenje pametnih kartica s certifikatom za sve zdravstvene djelatnike uz koju se omogućava provjera vjerodostojnosti korisnika,
- Specifična arhitektura baze podataka osigurava nemogućnost povezivanja pacijentovih medicinskih i administrativnih podataka od strane neovlaštene osobe (medicinski i administrativni podatci pacijenta nalaze se u dvije fizički odvojene baze podataka),
- Električno potpisivanje poruka i šifriranje komunikacijskih kanala kojim iste putuju osigurava integritet i privatnost informacija koje razmjenjuju različiti korisnici Informacijskog sustava primarne zdravstvene zaštite,
- Konfiguracija sigurnosnih postavki mrežnih uređaja i poslužitelja osigurava autorizirani pristup mrežnim resursima i poslužiteljima,

- Implementacija sustava na dvije fizički udaljene lokacije osigurava integritet podataka u slučaju prirodnih katastrofa ili velikih kvarova na hardveru,
- Svi podatci se osim u baze podataka pohranjuju i na trajne medije.

Privatnost podataka prilikom komunikacije između različitih entiteta u sustavu primarne zdravstvene zaštite osigurava se šifriranjem komunikacijskih kanala.

Sigurnosni mehanizmi u središnjem informacijskom sustavu primarne zdravstvene zaštite (ISPZZ) implementirani su na nekoliko razina:

- Na fizičkoj odnosno mrežnoj razini kontrola pristupa i zaštita samog sustava je osigurana korištenjem virtualne privatne mreže za kontrolu pristupa samoj mreži i vatrozidom koji štiti sustav od neovlaštenog upada i onesposobljavanja sustava,
- Na razini prijenosa podataka, sustav i podatci koji se prenose zaštićeni su enkripcijom komunikacijskog kanala između sustava i klijenata koji ga koriste,
- Na aplikativnoj razini sustav je zaštićen kontrolom pristupa podatcima i uslugama zasnovanim na upotrebi infrastrukture koja se koristi javnim ključem te pametnim karticama,
- Poruke koje se šalju kriptiraju se pomoću *HCAgent.dll* programa koji poruke kriptira uz pomoć privatnog ključa pohranjenog na prije spomenutim pametnim karticama. [27]

Svim osiguranicima dodjeljuje se matični broj osiguranika jer je JMBG u potpunosti zabranjen. Radi se na tome da se taj matični broj dodjeli i osobama koje nisu osigurane u HZZO-u. Tu ulogu u RH preuzela je FINA koja dodjeljuje osobne certifikate na temelju podataka o osobama dobivenim od MUP-a RH, Državnog zavoda za statistiku, te tijela opće uprave. [26]

10. KRIPTOGRAFSKE METODE U DOLASKU

Godine 1990., kriptograf Xuejia Lai te kriptograf i informacijski tehničar James Massey objavljuju „Prijedlog za novi Standard za šifriranje blokova podataka“ koji je prijedlog za Međunarodni algoritam šifriranja podataka (*International Data Encryption Algorithm* (IDEA)) koji je bio predviđen kao zamjena DES-u. IDEA za razliku od DES-a koristi 128 - bitni ključ te su same operacije lako implementarne na računalu što je u praksi vrlo efikasno.

Iste godine objavljuju se rezultati eksperimenata vezanih za kvantnu kriptografiju koja osim sigurnosti pruža i mogućnost detektiranja uljeza u komunikaciji i mjeru koliko je najviše bitova taj isti uljez mogao dohvatiti. Za to istraživanje ponajviše je zadužen fizičar i informacijski teoretičar koji radi u IBM-ovom istraživačkom centru Charles Henry Bennett. [28]

10.1. Kvantna kriptografija

Klasična fizika dopušta da se svako fizikalno svojstvo objekta ili fenomena može izmjeriti, a da se pritom ne utječe na sam objekt odnosno fenomen. Budući da su sve informacije, uključujući i ključ šifre, kodirani u nekom mjerljivom fizikalnom svojstvu nekog objekta ili signala, klasična fizika ostavlja potpuno otvorena vrata mogućnostima pasivnog „prisluškivanja“ jer dopušta mogućnost mjerenja fizikalnih svojstava bez remećenja, odnosno traga. No, to nije slučaj u kvantnoj fizici koja je temelj kvantne kriptografije. Kvantna teorija vrijedi za sve objekte: velike i male, ali su njezine posljedice najizraženije u mikroskopskim sustavima posebice na razini pojedinačnih molekula, atoma i subatomskih čestica. U takvim sustavima je čin mjerenja integralni dio kvantno-mehaničkog sustava, a ne samo pasivni vanjski proces kako to opisuje klasična fizika. Mjerenje na kvantnoj razini uvijek utječe na sustav i prestaje biti puki pasivni neinteragirajući proces. Zato je moguće dizajnirati kvantni kanal, dakle kanal koji nosi signale temeljene na kvantnim fenomenima tako da svaki pokušaj da se taj kanal „prisluškuje“ ometa signal na uočljiv način. To je moguće zato jer su u kvantnoj teoriji stanoviti parovi fizikalnih svojstava

(veličina) komplementarni u smislu da mjerenje jednog svojstva nužno mijenja (remeti) drugo. [28]

Kvantni kanal najčešće se realizira pomoću fotona, jer se on može jednako uspješno opisati i za bilo koji drugi kvantni sustav s dva stanja. Foton može biti polariziran pomoću jedne od tri ortogonalne baze polarizacije:

- linearna horizontalna – linearna vertikalna
- linearna pod kutem od 45 stupnjeva – linearna pod kutem od 135 stupnjeva
- cirkularna lijeva – cirkularna desna

Pošto su dvije polarizacije iz različitih baza međusobno konjugirane one se ne mogu razlikovati samo jednim mjerenjem. Kod korištenja dvije baze polarizacije detektor fotona ima na raspolaganju samo jedno mjerenje kojim utvrđuje dvije varijable. No u ovome kvantnome sustavu, kod mjerenja jedne varijable nepovratno se gube informacije o vrijednostima druge varijable zbog čega ne možemo napraviti kopiju fotona i biti 100% sigurni da će ona biti identična originalu. Na toj se činjenici temelji cjelokupna kvantna kriptografija. [29]

10.2. BB84 protokol

Najraširenija primjena kvantne kriptografije do sada leži u kvantnoj distribuciji ključeva, koja služi kao zamjena asimetričnim protokolima. U toj skupini najznačajniji je upravo BB84 protokol koji podrazumijeva dva komunikacijska kanala kod kojih je jedan jednosmjerni kvantni kanal, a drugi dvosmjerni javni kanal.

Osim spomenutog BB84 postoje i mnogi drugi protokoli kvantne razmjene ključeva koji se svi temelje na sličnim osnovama.

10.3. Kvantna kriptografija u primjeni

Sva praksa o kvantnoj kriptografiji daleko je od teorije koja se na papiru čini savršena. Postoji još mnogo neriješenih problema koji narušavaju teoretsku apsolutnu sigurnost kvantne kriptografije.

Godine 2002. na tržištu se javlja prvi komercijalni sustav za kvantnu distribuciju ključeva proizveden od tvrtke idQuantique. [30]

Testiranjima su otkrili da udaljenost na kojoj se može međusobno komunicirati iznosi preko 60 km dok je brzina prijenosa oko 1000 bit/s.

Iako je očito da ona u odnosu na klasičnu kriptografiju pruža više mogućnosti i prednosti kvantna kriptografija iziskuje stupanj tehnologije koji još nije dostignut. Za sada je ona najsigurniji način razmjene podataka no na umu treba imati i sva ograničenja vezana uz nju, a ponajviše udaljenost na kojoj je moguće komunicirati.

Uspiju li se ti problemi u skoroj budućnosti riješiti upravo bi kvanta kriptografija mogla označiti kraj borbe između šifrotvoraca i šifrolomaca iz koje bi šifrotvorci prvi put u povijesti izišli kao pobjednici jer je kvantna kriptografija zaista neprobojan sustav enkripcije.

10.4. Prvi sklopovski kriptografski uređaj razvijen u RH

Nedavno je Zavod za sigurnost informacijskih sustava (ZSIS) proveo postupak certificiranja kriptografskog uređaja TelSec razvijenog u Pomorskom centru za elektrotehniku u Splitu. [31]

Sam uređaj udovoljava svim zahtjevima za zaštitu nacionalnih klasificiranih podataka. Sukladno tome tvrtka TelSec je izdala Uvjerenje o sposobnosti kriptografskih uređaja za zaštitu nacionalnih klasificiranih podataka, te je samim time ovaj uređaj uvršten u Registar odobrene oprema za zaštitu klasificiranih podataka u RH.

TelSec uređaj je namjenski sklopovski uređaj koji služi za kriptografsku zaštitu govornog, podatkovnog, i video prometa. Sam uređaj je projektiran tako da se integrira u postojeću komunikacijsku infrastrukturu instalacijom između krajnjeg uređaja i centrale te je prvi sklopovski uređaj razvijen u RH koji je zadovoljio sve zahtjeve nužne za stjecanje Uvjerenja o sposobnosti za zaštitu nacionalnih klasificiranih podataka. [31]

10.5. Poznatiji hakerski napadi na području RH

Iako je bilo više manjih napada na neke poznatije i manje poznate tvrtke, ustanove te institucije, u novije vrijeme izdvojio bih samo jedan, a to je onaj koji se dogodio u svibnju 2017. godine. Tada je 75 tisuća računala u stotinama zemalja svijeta, među kojima je i Hrvatska jednostavno usporilo, zbog rapidnog kriptiranja sadržaja i lančanih napada prema ostatku mreže čime je započeo do sada najveći *cyber* napad u povijesti. Uz pomoć računalnog crva neovlašteno otuđenog od jedne američke obavještajne agencije koji je služio kao transportno sredstvo, distribuiran je r*ansomware* maliciozni kod (vrsta virusa, koja korisniku blokira pristup računalu i od njega zahtjeva plaćanje otkupnine) pod nazivom „*WannaCry*“ (u slobodnom prijevodu "želim plakati"), blokirana su računala tisuća tvrtki i institucija diljem svijeta s jasnom porukom koja se pokazivala na zaslonu: „Platite 300 dolara u *bitcoinima* (elektronička valuta) i računalo će biti ponovno pokrenuto.“. Ako u roku od šest sati nije uplaćena svota cijena bi se povećala. Virus se proširio tako da je iskoristio sigurnosnu rupu u operativnom sustavu Windows za koju je Microsoft izdao „zakrpu“ još u ožujku, no veliki broj tvrtki i organizacija jednostavno nije ažurirao svoja računala ostavivši ih tako ranjivim na napade.

Ciljana računala u ovom kriminalnom napadu nalazila su se većim dijelom u bolnicama, državnim institucijama i velikim tvrtkama, a Avast, jedan od vodećih proizvođača programa za računalnu sigurnost, kaže kako u povijesti još nije bilo napada ovog obujma. Iako se zaraza proširila diljem svijeta i pogodila države u različitim ustanovama i djelatnostima, što se tiče zdravstva, najveća šteta je učinjena u Velikoj Britaniji gdje su blokirana gotovo sva računala u

zdravstvenom sustavu, što je uzrokovalo opći kaos u bolnicama. Svi zakazani pregledi otkazani su, baš kao i operativni zahvati. Iako će se šteta mjeriti u milijunima, ipak, najveća šteta zasigurno se mjeri u ljudskim životima onih čiji operativni zahvati nisu mogli biti izvedeni. [32]

11. ZAKLJUČAK

Kriptografija se u 20. stoljeću uvelike promijenila u odnosu na prijašnje godine upravo zbog pojave računala koja su u stanju provjeravati algoritme puno brže nego što to može čovjek.Kako je kriptografija jedna od najpoznatijih grana u području sigurnosti, uopće ne začuđuje što se počela upotrebljavati, osim u području obrane i državne uprave, i šire u cilju zaštite života i zdravlja građana, zaštite materijalnih dobara i okoliša, te tako i u kritičnim područjima ljudske djelatnosti. No, pojavom računala i novih tehnologija, raste i broj mogućih prijetnji kao i upotreba kriptografskih metoda za zaštitu samih napadača na prije spomenute djelatnosti, pa se može reći da se borba između kriptografa i kriptoanalitičara i dalje svakodnevno nastavlja.

Zbog učestalih napada na institucije iz kritičnih područja ljudske djelatnosti vrlo je važno imati dobar informatički tim koji sprječava pokušaje neovlaštenog upada u sustav, te osigurati razne oblike edukacije i stručnog osposobljavanja djelatnika u pogledu sigurnosti cjelokupnog sustava i osoba koje rade u tim tvrtkama, institucijama ili postrojenjima kako ne bi upravo njihovom pogreškom procurili podatci ili bili nenamjerno izloženi. Fina, kao naša krovna agencija za dodjelu kvalificiranih ključeva i certifikata, također u svrhu zaštite građana i podataka u sustavu e-građani, svake godine izdaje novi RDC koji je ažuriran u odnosu na prethodni te je u potpunosti kvalificiran za uspješnu obranu sustava od novih vrsta napada.

Rješenje u kojem bi kriptografi konačno mogli odnijeti pobjedu nagoviješta se u budućnosti kriptografije u obliku paradigme nazvane kvantna kriptografija.

Nadam se da sam ovim radom postigao zadani cilj i svrhu te ukazao na važnost kriptografije u cilju zaštite života, zdravlja, okoliša i materijalnih dobara u kritičnim područjima ljudske djelatnosti kao i na važnost konstantnog usavršavanja u području kriptografije, jer osim aktualnih nagovještaja i obećanja kvantne kriptografije teško je predvidjeti što će nam ovaj dinamični tehnološki razvoj donijeti u budućnosti.

12. LITERATURA

[1] CARNet: Steganografija, CCERT-PUBDOC-2006-04-154 https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-04-154.pdf, pristupljeno 13.06.2018.

[2] Antolović A.: "Naprave za šifriranje“, Osijek 2015., http://www.mathos.unios.hr/~mdjumic/uploads/diplomski/ANT21.pdf, pristupljeno 13.06.2018.

[3] Wikipedia: Glosar kriptologije https://hr.wikipedia.org/wiki/Dodatak:Glosar_kriptologije, pristupljeno 13.06.2018.

[4] Asecuritysite: Mary, Queen of Scots, polyalphabet cipher https://asecuritysite.com/coding/mary, pristupljupljeno 14.06.2018.

[5] Bestcodes: CracktheCodes, http://bestcodes.weebly.com/vigenere-cipher.html, pristupljeno 15.06.2018.

[6] ČavrakH.: Enigma, http://e.math.hr/enigma/index.html,pristupljeno 15.06.2018.

[7] Dempsey R.: How can statistics be applied to cryptography?, https://www.quora.com/How-can-statistics-be-applied-to-cryptography, pristupljeno 16.06.2018.

[8] Wikipedia: Letter frequency, https://en.wikipedia.org/wiki/Letter_frequency, pristupljeno 16.06.2018.

[9] Dujella A.: Teorija brojeva i kriptografija, https://bib.irb.hr/datoteka/870211.novigrad-dujella-rev2.pdf, pristupljeno 17.06.2018.

[10] Wikimedia: Symmetric key encryption, 2014., https://commons.wikimedia.org/wiki/File:Symmetric_key_encryption.svg, pristupljeno 17.06.2018.

[11] Atorwithme: Kvantna kriptografija, 2013.,https://atorwithme.blogspot.com/2013/03/kvantna-kriptografija.html, pristupljeno 18.06.2018.

[12] Katedra za Automatizaciju i Metrologiju: Hibridni kriptosustavi, 2014.,http://www.am.unze.ba/rg/2007/zastita%20digitalnih%20podataka/HTML/hibridni%20kriptosistem.html, pristupljeno 18.06.2018.

[13] Zavod za sigurnost informacijskih sustava: Kriptografska zaštita, https://www.zsis.hr/default.aspx?id=55, pristupljeno 18.06.2018.

[14] Bobar Z.: Zaštita računarskih mreža Ministarstva odbrane i vojske srbijeprimenomvirtuelnoghoneyneta“, Vojnotehnički glasnik 3/09, UDC: 004.7.056.53, Beograd, 2009., https://cyberleninka.ru/article/n/za-tita-ra-unarskih-mre-a-ministarstva-odbrane-i-vojske-srbije-primenom-virtuelnog-honeyneta, pristupljeno 19.06.2018.

[15] Wikipedia: Information security, https://en.wikipedia.org/wiki/Information_security,pristupljeno 19.06.2018.

[16] CARNet: Korištenje eliptičnih krivulja u kriptografiji CCERT-PUBDOC-2006-09-169, https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-169.pdf, pristupljeno 30.06.2018.

[17] CARNet: Kriptografija u službi napadača CCERT-PUBDOC-2008-04-226, https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-04-226.pdf, pristupljeno 30.06. 2018.

[18] Wikipedia: Honeypot (computing), https://en.wikipedia.org/wiki/Honeypot_(computing), pristupljeno 30.06.2018.

[19] Researchgate: Virtual Honey Proposed Design, https://www.researchgate.net/figure/Virtual-Honeynet-Proposed-Design_fig2_224138278, pristupljeno 01.07.2018.

[20] Ministarstvo uprave: Strategija e-Hrvatska 2020, 2015., http://europski-fondovi.eu/sites/default/files/dokumenti/Strategija%20e-Hrvatska%202020.%20%2820.01.2016.%29.pdf, pristupljeno 02.07.2018.

[21] GDPR2018: https://gdpr2018.eu/sto-je-gdpr/, pristupljeno 02.07.2018.

[22] Azop: Zaštita osobnih podataka, http://azop.hr/, pristupljeno 02.07. 2018.

[23] Fina: Digitalni certifikati fina PKI sustav, https://www.fina.hr/Default.aspx?sec=1799, pristupljeno 02.07.2018.

[24] HZZO: Usluga e-Zdravstveno, 2010., http://www.hzzo-net.hr/dload/e_zdravstveno/Uputa_za_korisnike_HZZO_e-Zdravstveno_aplikacije.pdf, pristupljeno 02.07.2018.

[25] CEZIH: Centralni zdravstveni informacijski sustav Republike Hrvatske (CEZIH) - Koncept sustava, 2/15517-FCPBA 101 24/8 Uhr Rev B 2013., http://www.cezih.hr/pzz/dokumentacija/01_00_CEZIH_koncept_sustava.pdf, pristupljeno 02.07.2018.

[26] Kralj Da., Kralj Di.:Analiza primjenjivosti e-Health i M-Health rješenja u ordinacijama obiteljske medicine na području Županije karlovačke, Zagreb: HUOM, 2008. str. 224-240,https://www.bib.irb.hr/428654, pristupljeno 03.07.2018.

[27] Ericsson Nikola Tesla: Informacijski sustav primarne zdravstvene zaštite Republike Hrvatske, 2015., http://www.cezih.hr/pzz/dokumenti_pzz/HR_PHCIS_FunctionalSpecification.pdf, pristupljeno 03.07.2018.

[28] Singh S.: „Šifre Kratka povijest kriptografije", Zagreb, 2003.

[29] Risovic D.: Kvantna kriptografija, Časopis - Hrvatski vojnik, broj 12. godina VI. 1996. str. 26-31.,https://hrvatski-vojnik.hr/pdfmagazin/hv_012_95-04.pdf, pristupljeno 04.07.2018.

[30] Stipčević M.: Kvantna kriptografija, FER, Zagreb 2003., https://www.irb.hr/users/stipcevi/download/fer171203.pdf, pristupljeno 04.07.2018.

[31] Knezović G.: Prvi sklopovski kriptografski uređaj razvijen u RH, 2018., https://mreza.bug.hr/prvi-sklopovski-kriptografski-uredaj-razvijen-u-rh/, pristupljeno 04.07.2018.

[32] Karakaš B.: Vecernji, 2017., https://www.vecernji.hr/vijesti/najveci-hakerski-napad-u-povijesti-1169605, 07.07.2018.

[33] Lomonaco S.J.: A Quick Glance at Quantum Cryptography,University of Maryland Baltimore County, 1998., http://www.cs.umbc.edu/~lomonaco/lecturenotes/9811056.pdf, pristupljeno 07.07.2018.

[34] Radić D.: Informatička abeceda, Split, https://informatika.buzdo.com/pojmovi/gpg-1.htm, pristupljeno 11.07. 2018.

[35] Dujella A.: Kriptografija, https://web.math.pmf.unizg.hr/~duje/kript/-kriptografija.html, pristupljeno 11.07.2018.

[36] Antolović A.: Naprave za šifriranje, Osijek, 2015., http://www.mathos.unios.hr/~mdjumic/uploads/diplomski/ANT21.pdf, pristupljeno 12.07.2018.

[37] Rani R., Yadav S.,Choudhary S.,Kakran M.: „Steganography“ , Department of Information technology Meerut institute of Engineering & technology, 2012.

[38] Schneier B.: „Applied Cryptography, SecondEdition: Protocols, Algorthms, andSourceCodein C (cloth)“ 1996.

[39] Choudhury F.A.,Das H., Bharali P., Chakraborty T.: „Analysisofvariousssteganographyalgorithms and theirimplementation“, Umshing, Shillong, Meghalaya, 2012.

PRILOZI:

Popis slika: