Kriptografija, kriptografski algoritmi i informacijska sigurnost

Beović, Ivan

SVEUČILIŠTE U SPLITU
SVEUČILIŠNI ODJEL ZA
FORENZIČNE ZNANOSTI

MODUL FORENZIKA I NACIONALNE SIGURNOSTI

DIPLOMSKI RAD

KRIPTOGRAFIJA, KRIPTOGRAFSKI ALGORITMI I INFORMACIJSKA SIGURNOST

IVAN BEOVIĆ

Split, srpanj 2023.

SVEUČILIŠTE U SPLITU
SVEUČILIŠNI ODJEL ZA
FORENZIČNE ZNANOSTI

MODUL FORENZIKA I NACIONALNE SIGURNOSTI

DIPLOMSKI RAD

KRIPTOGRAFIJA, KRIPTOGRAFSKI ALGORITMI I INFORMACIJSKA SIGURNOST

MENTOR: izv. prof. dr. sc. Marija Boban

IVAN BEOVIĆ

Matični broj studenta:
696/2021.

Split, srpanj 2023.

Rad je izrađen u Sveučilišnom odjelu za forenzične znanosti Sveučilišta u Splitu

pod nadzorom mentorice izv. prof. dr. sc. Marija Boban

u vremenskom razdoblju od siječnja do lipnja 2023. godine

Datum predaje diplomskog rada: 06. srpnja 2023.

Datum prihvaćanja rada: 10. srpnja 2023.

Datum usmenog polaganja 17. srpnja 2023.

Povjerenstvo: 1. Prof. dr. sc. Jozo Čizmić

2. Doc. dr. sc. Tonći Prodan

3. Izv. prof. dr. sc. Marija Boban

SADRŽAJ

1. UVOD

1.1. Informacijska (ne)sigurnost novog doba

Era suvremenog života i poslovanja dijelom je omogućena napretkom informacijskih tehnologija, a samim tim i razvoj i primjena sve većeg broja kompleksnih informacijskih sustava. Primjena novih softverskih rješenja i informatičkih tehnologija u poslovnim procesima, sustavima automatizacije obrade podataka, ujedno i kod donošenja odluka od strane menadžmenta, postaje neizostavni dio funkcioniranja institucija i pojedinaca (1).

S obzirom na funkcije sustava da vrše prikupljanje, čuvanje, obradu i analizu podataka, uređuju i kontroliraju procese automatizacije i elektronske transakcije, to su oni permanentno ugroženi sa aspekta zaštite sigurnosti podataka i funkcioniranja. Sigurnost podataka je od izuzetnog značaja za svaki poslovni sustav. Informacije, intelektualno vlasništvo, dokumentacija, sadržaj, mreže, podaci o zaposlenima i korisnicima itd., mogu se smatrati dijelom ključnih dobara korporacije. Svaki od ovih elemenata mora biti pažljivo čuvan u cilju osiguranja povjerljivosti poslovnih tajni jedne institucije (2). Postoji više vrsta ugrožavanja sigurnosti u informacijskim sustavima. Prema cilju napadača, prijetnje je moguće klasificirati na sljedeći način (3):

- prenamjena ili brisanje datotečnih sustava,
- ugroza aspekata privatnosti - razotkrivanje informacijskog sadržaja i
- neautorizirano korištenje računalskih resursa.

Prenamjena podataka je ugroza koja se prvenstveno tiče pristupa memorijskim izvorima računala sa sigurnosno kritičnim informacijskim sadržajima.

Ugroza privatnosti predstavlja neautorizirani pristup povjerljivim informacijama. Jedan od napada ove vrste je prisluškivanje (*eavesdropping*), koje je vrlo teško na vrijeme otkriti jer nema vidljivih izvanjskih manifestacija. Prisluškivanje je vrlo aktualan način prijetnje, budući se ogromna količina informacija razmjenjuje preko potencijalno nesigurnih kanala. Lažno predstavljanje (*masquerading*) je način prijetnje kada napadač pokušava iskoristiti nečiji identitet zbog upada u računalski sustav.

Neautorizirano korištenje računalskih resursa se najčešće očituje kroz odbijanje davanja usluga. Osnovni cilj ove vrste napada odnosi se na sprječavanje točnog funkcioniranja izvršnih programa sustava. Navedene ugroze ovog tipa upotrebljavaju zlonamjerne programe za

generiranje velikog broja zahtjeva za uspostavu konekcije, koji će se odbiti u izvršavanju. Ovim se opterećuj mrežni server koji kod uspješno napada prekida s radom odnosno odgovara zahtjevima iz napada i time je onemogućeno da mu legalni korisnici pristupe (4). Posebna prijetnja informacijskim sustavima podrazumijeva klasu napada koji se izvode bez naročitog cilja od strane napadača, tj. bez neke eksplicitne koristi.

Kriptoanaliza je napad kojim se ostvaruje prijetnja narušavanja privatnosti. Aktivnost napadača je usmjerena otkrivanju tajnih parametara zaštićene komunikacije Mogućnost kriptoanalize je definirana čuvanjem i razmjenom simetričnih i asimetričnih ključeva, dužinom ključa, mogućnošću primijenjenog kriptografskog sustava potencijalima izvršitelja napada (1).

Napad tipa trojanskog konja predstavlja distribuciju zlonamjernih programa unutar mreže. Ova vrsta napada se obično temelji na slabostima samog operativnog sustava. Trojanski konj se prikazuje kao izvorni program mada je projektiran na način da izvede neku ilegalnu radnju. Ova vrsta računalnog virusa se obično maskira u sustavne programe i briše tragove vlastite instalacije. Ostavlja jedino trag u izmijenjenoj funkcionalnosti programa (5).

U sustavima s tradicionalnom organizacijom, mjere sigurnosti se baziraju na ograničavanju neautoriziranog pristupa informacijama i zaštićenim dijelovima sustava. Međutim, ovaj model nije pogodan za distribuirano mrežno okruženje, imajući u vidu njegovu osnovnu karakteristiku da omogućava otvorenu i što dostupniju komunikaciju. Zato su, paralelno s razvojem računalskih sustava, razvijani i softversko - hardverski sustavi zaštite čija je uloga da onesposobe, otklone ili umanje prijetnje i potencijalne sigurnosne propuste. Neki od načina obrane su (6):

- šifriranje, za zaštitu tajnosti podataka,
- više stupanjska antivirusna zaštita,
- pravilna upotreba mrežnih barijera, koje vrše filtriranje IP paketa,
- primjena tehnologije digitalnog potpisa, koja omogućuje zaštitu integriteta poruke, provjeru identiteta pošiljaoca i osigurava izvornost sadržaja poslane poruke,
- postupak uzajamne autentifikacije subjekata komunikacije,
- korištenje digitalnih certifikata, kao parametara koji jedinstveno garantiraju identitet subjekta, i
- korištenje odgovarajućeg kriptografskog hardvera za čuvanje i generiranje ključeva i izvršavanje sigurnosno kritičnih postupak.

Širok je dijapazon sustava za zaštitu informacijskih sustava, i u većini slučajeva se koriste kriptografski mehanizmi zaštite. Suvremena rješenja sustava zaštite karakterizira višeslojna arhitektura, sa upotrebom hardverskih sigurnosnih modula (HSM - Hardware Security Module) kao što su smart kartice i kriptografski koprocesori, a baziraju se na infrastrukturi javnog ključa te primjeni tehnologija kriptografije, digitalnog potpisa i digitalnih certifikata (7).

1.2. Povijest, značaj i osnovni pojmovi kriptologije

Još od davnina kada su ljudi počeli pisati, pojavila se potreba da neke zapisane informacije ostanu tajne. Osmišljavanjem tehnika kojim bi se skrile zapisane informacije ustanovila se nova znanstvena disciplina – kriptografija. Kriptografija se bavi razvojem sustava za šifriranje informacija. Riječ kriptografija nastala je od grčih riječi *kryptós* (skriven, tajna) i *graphein* (pisati) (8).

Osnovni zadatak kriptografije je osigurati povjerljivost, dostupnost i integritet informacija. Povjerljivost (*Confidentiality*) podrazumijeva sprječavanje neovlaštenog pristupa informacijama. Integritet (*Integrity*) podrazumijeva sprečavanje neovlaštene izmjene informacija. Dostupnost (*Availability*) podrazumijeva stalnu dostupnost informacija ovlaštenim entitetima. Ova tri zadatka popularno se nazivaju CIA trojstvo (gdje je CIA skraćenica za *Confidentiality*, *Integrity*, *Authentication*, a ne za američku obavještajnu agenciju *Central Intelligence Agency*) (5).

Slika 1. CIA trojstvo – povjerljivost, integritet i dostupnost (5)

U početku, kriptografija se koristila prvenstveno u vojne svrhe. U spartanskoj vojsci, 650 godina prije nove ere, koristila sa skitala – traka obavijena oko štapa po kojoj se pisala poruka. Odmotana traka nudi slova koja s ispremještana i vidljiv je nerazumljiv tekst (5). Na primjer, ako bi pisalo FORENZIKAINACIONALNA u četiri reda skitale, po 6 znakova u svakom redu

F O R E N

Z I K A I

N A C I O

N A L N A

i odmotali skitalu, vidljiv tekst bio bi FZNNOIAARKCLEAINNIOA.

Slika 2. Skitala (5)

Jedan od vojskovođa koji je poznat po upotrebi šifriranih poruka je Julije Cezar. Kod slanja poruka vojskovođama, kodirao ih je tako da bi slova u tekstu bila ispremještala za neki određeni broj mjesta u abecedi. Primatelji poruke mogli su dekodirati jer su znali koji je to broj – ostali su vidjeli samo gomilu nerazumljivog teksta (5).

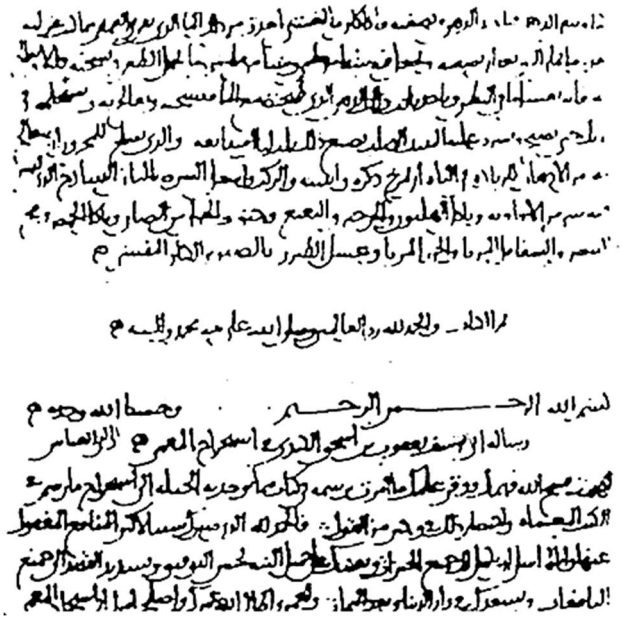
Na primjer, ako bi bilo napisano FORENZIKA i svako slovo u poruci pomaknuto tri mjesta u desno slovo F postalo bi I, slovo O postalo bi Š… i rezultat pomicanja bila bi šifrirana poruka IŠUHPBLMČ.

Slika 3. Dva rotirajuća diska za kodiranje Cezarovim kodom (5)

Steganografija je bliska kriptologiji, a bavi maskiranjem postojanja poruke. Također je prvi put evidentirana u drevnoj Grčkoj. Iz spisa Herodota, oko 500 godina prije nove ere, vidi se primjer tetoviranja poruke na obrijanoj glavi roba koja se ne vidi ispod sveže izrasle kose. Suvremeniji primeri steganografije uključuju upotrebu nevidljive tinte, vodenih žigova itd. (8).

U Indiji 2000 godina stari spisi govore o dva tipa šifriranja – prvi tip je zasnovan na zamjeni slova na osnovu njihovih fonetskih odnosa (npr. samoglasnici postaju suglasnici), a druga na šifriranom alfabetu uparivanjem slova i upotrebom recipročnih slova. U Perziji, današnjem Iranu, također su postojala dva tipa šifriranja – prvi kraljevski skript korišten je za službenu korespondenciju u kraljevstvu, a drugi za komunikaciju sa ostalim državama (5,8).

Prvu knjigu o kriptografiji pod nazivom „Knjiga kriptografskih poruka" napisao je arapski filozof Al-Khalil (717–786) u kojoj se po prvi put koriste permutacije i kombinacije arapskih riječi. Međutim, poruke dobivene klasičnim metodama šifriranja otkrivaju statističke podatke o originalnoj poruci, a ti podaci se često mogu zlouporabiti za razbijanje kodova. Nakon otkrića analize frekvencija pojave slova u poruci, arapski matematičar Al-Kindija je u devetom stoljeću napisao knjigu „Rukopis za dekodiranje kriptografskih poruka", u kojoj je prvi put opisana upotreba tehnika frekvencijske analize. Kriptoanaliza proučava načine i metode "razbijanja" kriptografskih sustava. Riječ kriptoanaliza nastala je od grčkih riječi *kryptós* (skriven, tajna) i *analýein* (analiza) (8–10).



Slika 4. Prva stranica iz Rukopisa za dešifriranje kriptografskih poruka

Prvu raspravu o kriptografiji napisao je Leone Batista Alberti, 1467. godine. On je također tvorac kodnog kruga i drugih rješenja dvostrukog prikrivanja teksta. Pola stoljeća nakon toga, u pet svezaka objavljeno je djelo Johanesa Trithemusa iz područja kriptografije. U XVI. stoljeću značajan doprinos daju talijani Girolamo Kardano, Batisto Porta te francuz diplomat Bleis de Vigener (8).

Slika 5. Kriptografska mašina u obliku knjige iz XVI stoljeća iz Francuske

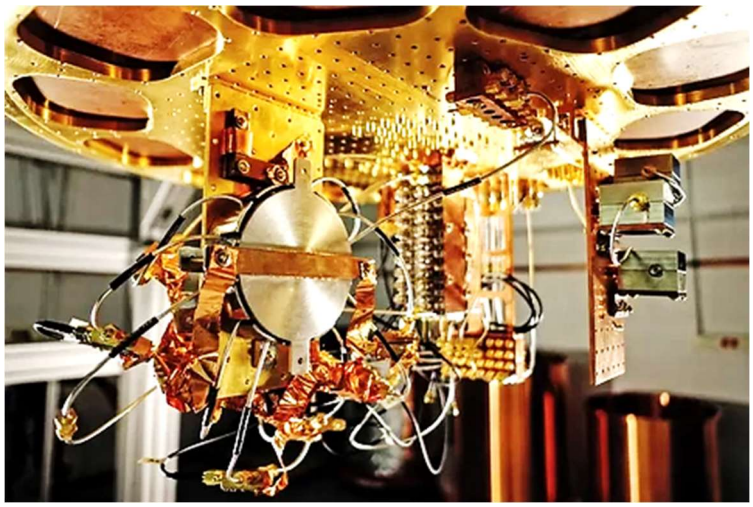
U XIX stoljeću došlo se do zaključka da se u kriptografiji ne smije oslanjati na tajnost algoritama za šifriranje, već na tajnost ključa. Tajnost ključa sama po sebi mora biti dovoljna da se šifrirana poruka ne može razbiti. Ovo je postao jedan od osnovnih principa kriptografije zapisan 1883. od strane Auguste Kerckhoffs (Kerkohov princip). Izričitije, to je naglasio i Claude Elwood Shannon, tvorac Teorije informacija i osnova teorijske kriptografije, kao Shannonov princip kriptologije: „neprijatelj poznaje sustav“ (5).

Tijekom drugog svjetskog rata Nijemci su napravili stroj nazvan Enigma koja je kodirala poruke na način koji do tada nije bio korišten. Međutim, uz pomoć kriptoanalitičkih metoda saveznici su uspeli razbiti kriptografski sustav Enigme (5,11).

Kriptografija i kriptoanaliza su znanstvene discipline kriptologije. Kriptologija se bavi raznim aspektima sigurnosti informacija. Riječ kriptologija nastala je od grčih riječi *kryptós* (skriven, tajna) i *logos* (nauka) (9).

Nakon drugog svjetskoga rata, razvojem informacijskih tehnologija, kriptologija i njene znanstvene discipline postale su izuzetno važne i permanentno se razvijaju. Suvremena računala mogu velikim brzinama razbiti primitivne kriptografske algoritme, pa zbog toga kriptografski algoritmi postaju sve kompleksniji. Kvantna kriptografija će vjerojatno u skorijoj budućnosti predstavljati temelj zaštite informacija.

Kvantna kriptografija je posljedica otkrića u području kvantnog računalstva. Zasniva se na Heisenbergovom principu neodređenosti. S druge strane, kvantna kriptoanaliza može pretpostaviti veliku opasnost za sigurnost informacija za sve kriptografske algoritme koje danas koristimo (9,10).



Slika 6. Kvantno računalo kompanije Google (8)

Značaj kriptologije u suvremenom društvu je ogroman počem od privatnost elektronske komunikacije omogućena je kriptografskim sustavima; cjelokupno poslovanje koje se danas obavlja elektronski (eCommerce), bilo u privatnom ili javnom sektoru, ne bi bilo moguće bez postojanja pouzdanih kriptografskih sustava; postojanje i upotreba kriptovaluta zasnovana je na kriptografskim sustavima; u pojedinim državama se čak i izbori i brojanje glasova birača implementiraju elektronskim putem uz pomoć kriptografskih sustava (2,11).

U navedenim primjerima moglo se uočiti da s jedne strane pošiljatelj na određeni način kodira poruku, a s druge strane primatelj kodiranu poruku dekodira. Između njih može postojati netko tko pokušava razbiti šifru kako bi došao do originalne poruke. Za sve navedene radnje u kriptologiji se koristi određena terminologija (3):

- **Otvoreni tekst** (plaintext) predstavlja poruku koja se treba zaštiti.
- **Kodiranje** (encryption) predstavlja skup metoda kojom se tekst transformira u kod (šifriran, nerazumljiv tekst).
- **Algoritam kodiranja** predstavlja skup pravila koja se koristi za kodiranje otvorenog teksta.
- **Kod** (ciphertext) predstavlja rezultat šifriranja.
- Rezultat izvršavanja algoritma šifriranja ovisi o vrijednosti **ključa** (key).
- **Dešifriranje** (decryption) predstavlja skup operacija kojom se kod transformira u otvoreni tekst.
- **Algoritam dešifriranja** predstavlja skup pravila koja se koristi za dešifriranje koda.
- Rezultat izvršavanja algoritma dešifriranja ovisi od vrijednosti **ključa** (key).

1.3. Klasična i moderna kriptografija

1.3.1. Klasična kriptografija

Klasični kriptografski sustavi dominirali su u dalekoj povijesti – danas su apsolutno nesigurni i podložni kriptoanalitičkim napadima. Izučavaju se samo zbog određenih ideja, odnosno, određenih osnovnih principa kriptografije definiranih tim sustavima. Šifre u klasičnoj kriptografiji možemo podijeliti na sljedeći način (3,8):

1.3.1.1. Šifre transpozicije

Šifre transpozicije zasnivaju se na principu transpozicije (premještanja) slova u otvorenom tekstu, popularno nazvano *skrembliranje* teksta. Kod predstavlja skremblirani tekst, a ključ primijenjenu transpoziciju. Način rada ovakvog sustava odgovara Shenonovom principu difuzije, odnosno širenje statistike otvorenog teksta i koda [5].

1.3.1.2. Transpozicija kolona

Najjednostavniji oblik transpozicije kolona je već spomenuta Skitala koja predstavlja jednostavan sustav transpozicije kolona. Otvoreni tekst ima odrađeni broj znakova koji se zapisuju u određeni broj redova definiranih ključem. Kod se dobije iščitavanjem kolona dobivene matrice. Za dešifriranje koda neophodno je poznavanje ključa (3).

Unaprijeđenje ovog sustava moguće je uvođenjem ključne riječi koja će odrediti redoslijed transpozicija po alfabetskom redu. Dužina ključne riječi treba biti manja od broja stupaca pa ako je manja onda se ponavlja (5).

Za sigurnost kriptografskog sustava neophodan je veliki prostor ključeva, ali to nije dovoljan uvjet. Veliki prostor ključeva može usporiti napadača izvrši napad u prihvatljivom vremenskom roku, ali ne može da ga spriječi da probije sustav (3).

1.3.1.3. Dvostruka transpozicija kolona

Dvostruka transpozicija kolona predstavlja još veće unapređenje transpozicija kolona pomoću ključnih riječi. Implementira se promjenom redoslijeda kolona i redoslijeda redova u matrici dimenzija [*n,m*]. Ključ predstavlja dimenziju matrice, odnosno broj kolona, a ključne riječi redoslijede permutacija po kolonama i redovima. Kod dobivamo iščitavanjem kolona nakon transpozicija (11).

1.3.1.4. Šifre supstitucije

Šifre supstitucije, odnosno šifre zamjene, zasnivaju se na zamjeni (vrijednosti) slova, a ne na zamjeni pozicije slova kao u prethodnom poglavlju. To znači da se jedno slovo npr. A preslikava u drugo slovo, npr. F.

Ako pogledamo samo mala slova alfabeta engleskog jezika kojih ima 26, prostor ključeva iznosi 26! što je jednako *403291461126605635584000000*. Ako nam je potrebna jedna sekunda da provjerimo jedan ključ, znači da nam za potpunu pretragu prostora ključeva treba *6721524352110093926400000* minuta, odnosno *112025405868501565440000* sati, odnosno *4667725244520898560000* dana, odnosno *12788288341153146740* godina.

Kako su računala danas izuzetno brza, recimo da možemo provjeriti milijun ključeva u sekundi. To bi značilo da za potpunu pretragu ključeva treba *12788288341153* godina (9).

1.3.1.5. Monoalfabetske šifre

Monoalfabetske šifre koriste fiksne zamjene tokom cijele poruke i jedan tip monoalfabetskih šifara– Cezarova šifra.

Ako se svakom velikom slovu u hrvatskom jeziku dodijeli broj od 0 do 29, tako da je A=0, B=1, C=2, …, Ž=29, onda se može formalizirati algoritme šifriranja i dešifriranja na sljedeći način:

$$C_i = P_i + K(\text{algoritam } 30)$$

$$P_i = C_i + (30 - K)(\text{algoritam } 30)$$

gdje je: P_i i-to slovo otvorenog teksta, C_i i-to slovo koda, K ključ odnosno pomak (5).

Ako pogledamo engleski alfabet, onda će se slovima dodjeljivati vrijednosti od 0 do 25, jer u engleskom alfabetu postoji 26 slova. Također će se prilikom formaliziranja algoritama koristiti operaciju algoritam 26. Ako se radi sa ASCII znakovljem, onda su slovima već dodijeljene dekadne vrijednosti prema ASCII tabeli u koloni „*Dec*“ (9):

Dec	Bin	Hex	Char	Dec	Bin	Hex	Char	Dec	Bin	Hex	Char	Dec	Bin	Hex	Char
0	0000 0000	00	[NUL]	32	0010 0000	20	space	64	0100 0000	40	@	96	0110 0000	60	`
1	0000 0001	01	[SOH]	33	0010 0001	21	!	65	0100 0001	41	A	97	0110 0001	61	a
2	0000 0010	02	[STX]	34	0010 0010	22	"	66	0100 0010	42	B	98	0110 0010	62	b
3	0000 0011	03	[ETX]	35	0010 0011	23	#	67	0100 0011	43	C	99	0110 0011	63	c
4	0000 0100	04	[EOT]	36	0010 0100	24	$	68	0100 0100	44	D	100	0110 0100	64	d
5	0000 0101	05	[ENQ]	37	0010 0101	25	%	69	0100 0101	45	E	101	0110 0101	65	e
6	0000 0110	06	[ACK]	38	0010 0110	26	&	70	0100 0110	46	F	102	0110 0110	66	f
7	0000 0111	07	[BEL]	39	0010 0111	27	'	71	0100 0111	47	G	103	0110 0111	67	g
8	0000 1000	08	[BS]	40	0010 1000	28	(	72	0100 1000	48	H	104	0110 1000	68	h
9	0000 1001	09	[TAB]	41	0010 1001	29	)	73	0100 1001	49	I	105	0110 1001	69	i
10	0000 1010	0A	[LF]	42	0010 1010	2A	*	74	0100 1010	4A	J	106	0110 1010	6A	j
11	0000 1011	0B	[VT]	43	0010 1011	2B	+	75	0100 1011	4B	K	107	0110 1011	6B	k
12	0000 1100	0C	[FF]	44	0010 1100	2C	,	76	0100 1100	4C	L	108	0110 1100	6C	l
13	0000 1101	0D	[CR]	45	0010 1101	2D	-	77	0100 1101	4D	M	109	0110 1101	6D	m
14	0000 1110	0E	[SO]	46	0010 1110	2E	.	78	0100 1110	4E	N	110	0110 1110	6E	n
15	0000 1111	0F	[SI]	47	0010 1111	2F	/	79	0100 1111	4F	O	111	0110 1111	6F	o
16	0001 0000	10	[DLE]	48	0011 0000	30	0	80	0101 0000	50	P	112	0111 0000	70	p
17	0001 0001	11	[DC1]	49	0011 0001	31	1	81	0101 0001	51	Q	113	0111 0001	71	q
18	0001 0010	12	[DC2]	50	0011 0010	32	2	82	0101 0010	52	R	114	0111 0010	72	r
19	0001 0011	13	[DC3]	51	0011 0011	33	3	83	0101 0011	53	S	115	0111 0011	73	s
20	0001 0100	14	[DC4]	52	0011 0100	34	4	84	0101 0100	54	T	116	0111 0100	74	t
21	0001 0101	15	[NAK]	53	0011 0101	35	5	85	0101 0101	55	U	117	0111 0101	75	u
22	0001 0110	16	[SYN]	54	0011 0110	36	6	86	0101 0110	56	V	118	0111 0110	76	v
23	0001 0111	17	[ETB]	55	0011 0111	37	7	87	0101 0111	57	W	119	0111 0111	77	w
24	0001 1000	18	[CAN]	56	0011 1000	38	8	88	0101 1000	58	X	120	0111 1000	78	x
25	0001 1001	19	[EM]	57	0011 1001	39	9	89	0101 1001	59	Y	121	0111 1001	79	y
26	0001 1010	1A	[SUB]	58	0011 1010	3A	:	90	0101 1010	5A	Z	122	0111 1010	7A	z
27	0001 1011	1B	[ESC]	59	0011 1011	3B	;	91	0101 1011	5B	[	123	0111 1011	7B	{
28	0001 1100	1C	[FS]	60	0011 1100	3C	<	92	0101 1100	5C	\	124	0111 1100	7C	|
29	0001 1101	1D	[GS]	61	0011 1101	3D	=	93	0101 1101	5D	]	125	0111 1101	7D	}
30	0001 1110	1E	[RS]	62	0011 1110	3E	>	94	0101 1110	5E	^	126	0111 1110	7E	~
31	0001 1111	1F	[US]	63	0011 1111	3F	?	95	0101 1111	5F	_	127	0111 1111	7F	[DEL]

Slika 7. ASCII sustav znakova (9)

1.3.1.6. Poligramske šifre

Poligramske šifre predstavljaju modernizirani kodni sustav sa šiframa supstitucije. Grupe slova šifriraju se zajedno, a ne kao pojedinačna slova. Na primjer, NIK može se može šifrirati s ABA, OLA se može šifrirati s KKA, itd. Dva primjera poligramskih šifara su *Playfeir* šifra i Hilova (*Hill*) šifra (9).

Playfeir šifra zasniva se na zamjeni blokova od dva znaka (bigrami). Ovaj postupak šifriranja opisao je Charles Wheatstone 1854. godine, a koristili ga je vojska Velike Britanije u I svjetskom ratu. Ključ je bila matrica dimenzija [5,5], sa 25 slova, bez slova J (3).

Matrica se kreirala na osnovu izabrane ključne riječi, a bigram P_1P_2 otvorenog teksta šifrira se u skladu sa sljedećim pravilima (9):

- Ako su p_1p_2 iz istog rada onda c_1c_2 postaju za dva slova desno od njih, gdje je prvi stupac susjedna desna kolona zadnjoj koloni.
- Ako su p_1p_2 u istome stupcu onda c_1c_2 dva slova ispod njih, tako da taj red bude susjedni onome u donjem zadnjem redu.
- Ako su p_1p_2 u različitim stupcima i kolonama onda c_1c_2 postaju ravnina dijagonale pravokutnika koji sadrži rubove p_1p_2, gdje je c_1 u istom redu kao p_1 dok je c_2 u istom redu kao p_2.
- Ako je $p_1=p_2$ tada se između njih vrši umetanje neutralnog (NULL) znaka.
- Ako otvoreni tekst sadrži neparan broj slova se dodaje neki neodređeni znak.

Kriptoanaliza *Playfeir* šifre ovisi prvenstveno od veličine otvorenog teksta koji se šifrira. Ako je kod velik primjenjuje se frekvencijska analiza bigrama. Ako je kod mali, frekvencijska analiza nije moguća pa se pogađaju moguće riječi, uspoređuju sa strukturom koda i postupno se rekonstruira matrica (10).

Hillova šifra kreirana od strane Lester Hilla i radi po principima linearne funkcije Ona radi s grupama s više od tri slova. Veličina matrice otvorenog teksta određuje veličinu matrice koja je zapravo ključ. Hill je uveo i invertiranje i množenje matrica u procesu skrembliranja[1] otvorenog teksta, i na kraju i sustave linearnih jednadžbi. Da bi dokazao da njegov sustav nije suviše kompliciran patentirao je i kodni stroj (12).

Na ovaj način Hill je zaštitio kodni sustav od frekvencijske analize slova i bigrama jer je prikrio strukturu otvorenog teksta u potpunosti. Međutim pomoću napada "poznati otvoreni tekst" i "izabrani otvoreni tekst" sustav se može razbiti, pa zato nije nikada doživio praktičnu primjenu (10,12).

[1] Skrembliranje je postupak kodiranja kojim se želi postići što slučajnija izmjena nula i jedinica, odnosno želi se postići statistička neovisnost izvora i toka podataka.

1.3.1.7. Polialfabetske šifre

Šifarski sustavi sa polialfabetskim šiframa eliminiraju preslikavanja izvornih frekvencija slova u otvorenom tekstu u zamjene u kodove korištenjem višestrukih zamjena. Najpoznatiji primjer polialfabetskih šifara predstavlja Vigenere šifra iz XIX. stoljeća Može se opisati kao multi-Cezarova šifru, jer se svako slovo preslikava u neko moguće slovo ovisno o poziciji u tekstu (polialfabetska zamjena) (7).

	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	V
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	W
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	X
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 8.Tabula recta –može se koristiti prilikom dešifriranja Vigenere šifrom (12)

Ovakav način šifriranja bio je inspiracija za razvoj mnogo kompleksnijih sustava za šifriranje poput Enigme u II svjetskom ratu – Enigma u osnovi koristi polialfabetske šifre zamjene.

Slika 9. Enigma – varijanta s tri rotora (12)

1.3.1.8. Idealne šifre

Pojam idealne (perfektne) šifre definirao je Claude Elwood Shannon. godine. Idealna šifra čini kriptografski mehanizam koji ne nudi nikakvu informaciju iz otvorenog teksta, niti o korištenom ključu. Matematički formulirano, ako se neki otvoreni tekst ***P*** i ***h*** pojavljuje s vjerojatnoćom ***p(x)***, onda postoji ključ kojim se preslikava svaka poruku u svaki kod s istom vjerojatnošću. Prosječna količina informacija u porukama mjeri se entropijom i ovisi od vjerojatnosti. Što je vjerojatnost poruke veća, količina informacija je manja i obrnuto. Funkcija koja ovo opisuje je binarni logaritam, što znači da količina informacija u poruci predstavlja potrebni broj bitova za opis poruke (3,7).

U klasičnoj kriptografiji *One-time pad* (OTP) je jedina dokazana sigurna šifra. Definirali su je Gilbert Vernam i Major Joseph Mauborgne 1917. godine. OTP radi nad binarnim podacima. Kod se dobija primjenom ekskluzivne disjunkcije (XOR, simbol $\oplus$, u programskom jeziku S operator ^) nad otvorenim tekstom i ključem, a otvoreni tekst primjenom ekskluzivne disjunkcije nad kodom i ključem. Sigurnost se temelji na slučajnom izboru ključa te jednokratnoj upotrebi ključa. OTR je dokazano sigurna kada (3):

- Kod ne nudi informaciju o otvorenom tekstu
- Svaki otvoreni tekst je iste dužine i isto je "vjerojatan"
- Ključ je slučajan i korišten samo jednom
- Ključ poznaju isključivo pošiljatelj i primatelj
- Ključ je po dužini sloga jednak poruci
- Mehanizam provjere integriteta poruke ne postoji

1.3.1.9. Kodne knjige

Kodna knjiga (*codebook*) je knjiga koja uparuje riječi (otvoreni tekst) sa kodovima (kod). Sigurnost kodnih sustava s kodnim knjigama zasniva se na fizičkoj sigurnosti samih kodnih knjiga jer one predstavljaju ključ. Danas se u kriptografiji pojam kodna knjiga ne odnosi samo na fizički odštampane knjige, nego na bilo koji dokument, fizički ili elektronski, koji sadrži tablicu sa uparenim otvorenim tekstovima i kodovima. Najveći izazovi u šifarskim sustavima s kodnim knjigama odnose se na sigurnost distribucije i fizičku sigurnost kodnih knjiga (5).

1.3.2. Moderna kriptografija

U klasičnoj kriptografiji otvoreni tekst je stvarno bio tekst napisan slovima abecede, postupak šifriranja i dešifriranja bio je manualan, na papiru (u rijetkim slučajevima polu-automatiziran u vidu sprave za šifriranje/dešifriranje) i ključevi su bili simetrični. Razmjena ključeva između pošiljatelja i primatelja bila je manualna – usmena, pismena ili polu-automatizirana na neki unaprijed dogovoren način. Jedini sustav ispred svog vremena u klasičnoj kriptografiji bio je *One-time* pad. Naglim razvojem telekomunikacijskih i računalskih sustava, klasični kriptografski sustavi bili su osuđeni na propast, bez obzira na to koliko su bili sigurni ili nesigurni (10).

Kriptografu je bilo dovoljno pretpostaviti da kriptoanalitičar, odnosno napadač, posjeduje elektronski računalo i da može velikom brzinom da izvrši neki od adekvatnih napada. Zbog toga se u modernim šifarskim sustavima uvodi faza kodiranja otvorenog teksta – iz jezika ljudi u jezik računala, odnosno u bitove. Način kodiranja otvorenog teksta nije tajna, kao što ni algoritmi šifriranja i dešifriranja nisu tajna. Tako se često primjenjuje američki standardni kod ASCII (*American Standard Code for Information Interchange)* (13).

Iako je u modernoj kriptografiji uvedeno digitalno šifriranje i dešifriranje informacija i dalje se nastavilo sa korištenjem supstitucije/premještanja i transpozicije/zamjene. Međutim, primjenom računalskih sustava kriptografi su uvidjeli da mogu realizirati mnogo složenije algoritme, neusporedivo većom brzinom u odnosu na klasične (14).

Danas su neki moderni standardizirani kriptografski algoritmi realizirani čak i "hardverski" u vidu procesorskih instrukcija, pa zbog toga možemo šifrirati, dešifrirati i razmjenjivati ogromne količine informacija skoro u realnom vremenu. U okviru moderne kriptografije razmatraju se dvije vrste kriptografskih sustava – simetrične i asimetrične, a u okviru simetričnih, dva tipa šifara – sekvencijalne i blokovske (13).

1.3.2.1. Sekvencijske šifre

Kod sekvencijskih šifara (*stream cipher*), na osnovu ključa ***K*** inicijalizira se generator pseudo slučajnih brojeva (PRNG – *Pseudo-Random Number Generator*) koji generira pseudo slučajni niz. Pseudo slučajni niz je sličan pravom slučajnom nizu, ali se razlikuje po tome što generator pseudo slučajnih brojeva u nekom trenutku počinje da generira vrijednosti iz početka.

Proces šifriranja podrazumijeva primjenu operaciju XOR nad bitovima kodiranog otvorenog teksta i bitovima dobivenog pseudo slučajnog niza (sekvence). Dešifriranje koda vrši se obrnutim redoslijedom. Znači, svaki pseudo slučajni niz ***S*** dobija se od strane generatora pseudo slučajnih brojeva na osnovu ključa K. Dobiveni pseudo slučajni niz može se promatrati kao radni ključ (14).

$$S = PRNG(K)$$

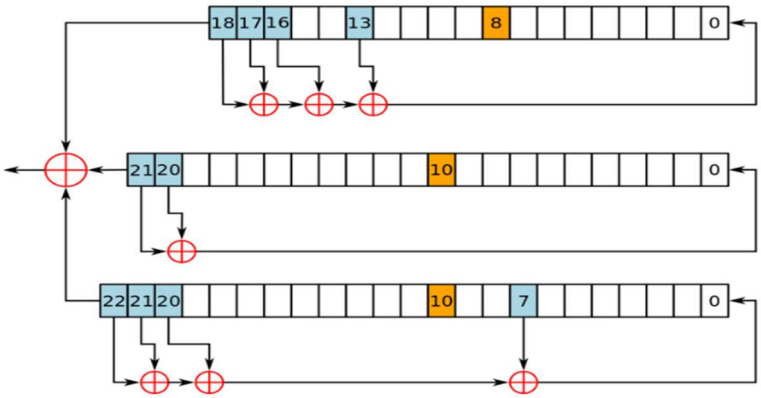
Za generirani pseudo slučajni niz dužine n bitova $S = \{s_0, s_1, s_2, \dots, s_{n-1}\}$ i kodirani otvoreni tekst dužine n bitova $P = \{p_0, p_1, p_2, \dots, p_{n-1}\}$ izračunava se kod dužine ***n*** bitova $C = \{c_0 = s_0 \oplus p_0, c_1 = s_1 \oplus p_1, c_2 = s_2 \oplus p_2, \dots, c_{n-1} = s_{n-1} \oplus p_{n-1}\}$ (13).

Može se zaključiti da je funkcioniranje generatora pseudo slučajnih brojeva jako važno, pa je vremenom osmišljeno više njegovih implementacija. Jedno od rješenja su linearni pomičući registri sa povratnom spregom (LFSR – *Linear-Feedback Shift Register*). LFSR predstavlja promicateljski registar čiji je sadržaj određen linearnom funkcijom njegovog prethodnog stanja. Inicijalno stanje LFSR-a zove se sjeme (*seed*) i ono ne smije biti nula jer se u tom slučaju neće nikada promijeniti. Pozicije bitova koje utiču na prethodno stanje zovu se tapovi (*taps*). LFSR na izlazu daje jedan bit – posljednji bit u registru – koji se zove izlazni bit (3).

1.3.2.2. A5/1

A5/1 je sekvencijski kodni sustav koji se koristi u GSM protokolu za zaštitu 2G prometa i SMS poruka između mobilnog telefona i bazne stanice. Tvorci algoritma i oni koji su ga implementirali u hardveru oslanjali su se na tajnost algoritma, suprotno osnovnim principima kriptografije, da algoritam nije tajna već samo ključ. Neizbježno je bilo da nacrt algoritma dospije u javnost (1994.), reverznim inženjeringom iz mobilnog telefona bude detaljno opisan (1999.) i kasnije potpuno razbijen tzv. Andersonovim napadom (A5/1 *cracking project*) (3,9).

A5/1 koristi tri LFSR od 19, 22 i 23 bita i 64-bitni ključ. Plavom bojom označeni su tap bitovi. Narančastom bojom su označeni takt bitovi. Registar se koristi ako se njegov takt bit slaže sa takt bitom u makar još jednom registru. Na izlazu se dobija po jedan bit radnog ključa u svakom taktu (7).

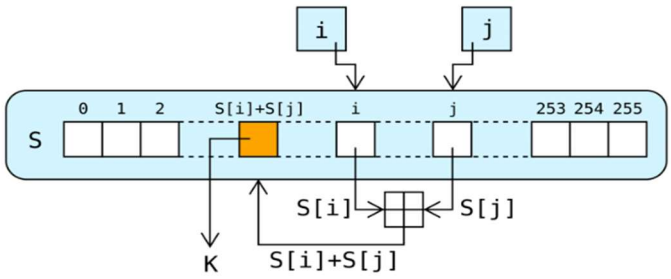


Slika 10. A5/1 LFSR (7)

Nasljednik, A5/2 objavljen je 1999. godine i razbijen istog mjeseca. Oba sustava zabranjena su za upotrebu u mobilnoj telefoniji od 2007. godine. Tek je KASUMI (UMTS, GSM (A5/3), GPRS (GEA3)) kodni sustav donio poboljšanu zaštitu – također je razbijen, ali napadi na njega "ne funkcioniraju" u mobilnoj mreži. Prvi Bluetooth standardni koristili su E0 protokol sa četiri LFSR registra i 128-bitni ključ – razbijen 2004/2005. godine (10).

1.3.2.3. RC4

A5/1 dizajniran je za implementaciju u hardveru, dok je RC4 (*Rivest Cipher 4*) dizajniran kao softverski algoritam. Kriptograf Ronald Rivest iz američke agencije RSA kreirao je ovaj algoritam 1987. godine. U javnost je dospio 1994. godine – objavljen anonimno. Pošto je RC4 zaštićen kao poslovna tajna zakonima o intelektualnoj svojini, prozvan je ARCFOUR ili ARC4 (skraćeno od *alleged RC4*). A5/1 u jednom taktu generira po jedan bit radnog ključa, dok RC4 u jednom taktu generira jedan bajt radnog ključa. Ključ u RC4 algoritmu može biti od 1 do 256 bajtova i upotrebljava se za inicijalizaciju permutacija. Permutacije su moguće kao sve permutacije svih mogućih vrijednosti sve od 0 pa do 255 bajtova. Svaki put kada se generira jedan bajt radnog ključa, mijenja se permutacija (15).



Slika 11. RC4 generiranje radnog ključa (*na slici je radni ključ označen sa K*) (15)

Zvanično je razbijen 2015. godine, a korišten je za sigurnost bežičnih računalskih mreža u WEP i WPA protokolima, za sigurnost transporta podataka u BitTorrent protokolu, u starijim verzijama aplikacija Skype, Opera… IETF je u dokumentu RFC 7465 zabranila je upotrebu RC4 u TLS protokolu, dok su kompanije Microsoft i Mozilla objavile slične preporuke, čime je RC4 dobrim dijelom povučen sa weba (12,15).

Do danas je standardizirano mnogo sekvencijalnih šifri: RC4, A5/1, A5/2, ChaCha, Chameleon, FISH, Helix, ISAAC, MUGI, Panama, Phelix, Pike, Salsa20, SEAL, SOBER, SOBER-128, WAKE… Među svim navedenim *ChaCha* se istakla kao najkorištenija sekvencijalna šifra u softverskom inženjeringu (15,16).

1.4. Kriptografski algoritamski sustavi

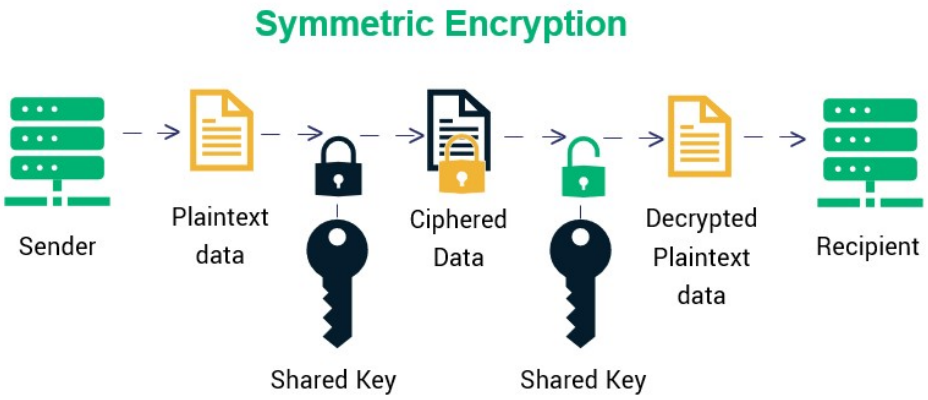
U kriptologiji postoje dva osnovna algoritamska sustavi: kodni sustav simetričnog ključa (*symmetric key cryptosystem*) i kodni sustav javnog ključa (*public key cryptosystem*). Kodni sustav sa simetričnim ključem koristi upravo identične ključeve, tj. uvijek se iz ključa šifriranja može jednoznačno izračunati ključ dešifriranja. Kodni sustavi s javnim ključem koristi javni ključ (*public key*) za šifriranje i privatni, tajni ključ (*private, secret key*) za dešifriranje, gdje poznavanje javnog ključa nije dovoljno za izračunavanje privatnog ključa. Moderni kodni sustavi su često vrlo kompleksni kombinirani (hibridni) kodni sustavi, ili kako se još nazivaju kriptografski sustavi (11).

1.4.1. Simetrični kriptografski algoritmi

Simetrični kriptografski algoritmi su se u kriptografiji počeli prvi koristiti. U početku su imali ulogu u poslovima državnih struktura, pa su iz tog razloga bili tajni, kreirani i korišteni upravo od strane odgovarajućih državnih organa. Razvojem informacijskih tehnologija i komunikacije, javila se potreba za javnim kriptografskim algoritmima. Danas se uglavnom koriste u distribuiranim sustavima elektronskih transakcija (7).

Kod simetričnih algoritama koristi se isti tajni ključ kod šifriranja i dešifriranja, pa se ova vrsta algoritama drugačije i naziva - algoritmi s tajnim ključem.

Pri upotrebi simetričnih kriptografskih algoritama, kao parametar u komunikaciji bira se odgovarajući algoritam koji će se koristiti tijekom transakcije. Algoritmi se najčešće primjenjuju u obliku liste implementiranih kriptografskih algoritama (15).



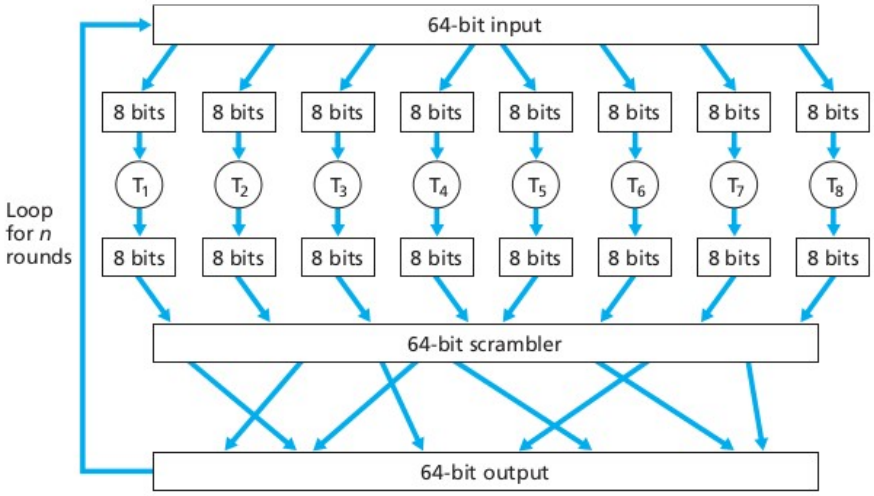
Slika 12. Simetrični kriptografski algoritmi (15)

Postoje dvije vrste simetričnih kriptografskih algoritama (15):

- blok kodni kripto sustavi,
- sekvencijski kodni sustavi,

Blok kodni sustavi vrše kriptiranje otvorenog teksta i šifrirane poruke u blokovima određene veličine. Sekvencijalni kodni sustavi vrše kriptiranje niza bita, bajtova ili riječi.

U blok tehnici šifriranja, šifriranje se vrši u blokovima od ***k*** bita. Ako je ***k*** = 64, tada se poruka podijeli na 64-bitne blokove, a svaki je blok neovisno šifriran (11,15).



Slika 13. Primjer 64-bitnog (15)

Danas postoji niz popularnih blok šifra, DES (*Data Encryption Standard)* 3DES, AES (*Advanced Encryption Standard)* i drugi. DES koristi 64-bitne blokove s 56-bitnim ključem. Potrošnja resursa s algoritma DES-a je srednja i trebat će otprilike 6,4 dana da se probije DES ključ. 3DES je razvijen kao sigurnija alternativa zbog DES-ove male duljine ključa. U 3DES - u, DES algoritam prolazi kroz tri puta s tri ključa i trebat će 4,6 milijardi godina da se razbije trenutnom tehnologijom. AES koristi 128-bitne blokove i može raditi s ključem koji je dugačak 128, 192 i 256 bita. Potrošnja resursa ovog algoritma je niska i trebala bi otprilike 149 bilijuna godina da bi se probio 128-bitni AES ključ. Zbog većeg unosa fiksne duljine, blok šifre općenito su sporije od sekvencijskih šifra (13).

U sekvencijskom sustavu šifriranje se vrši jedan bit po jedan. Ova vrsta šifriranja nije tako uobičajena. Blok šifre koriste se mnogo češće za simetrično šifriranje.

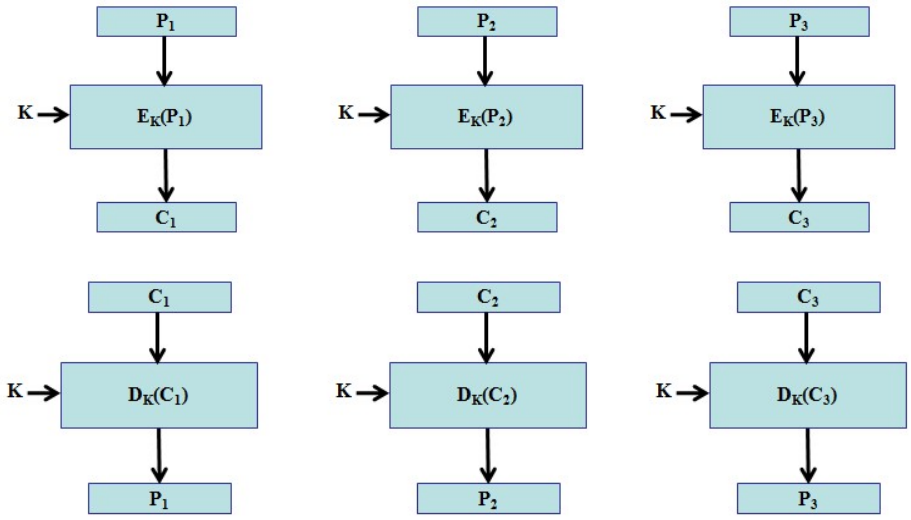
1.4.1.1. Vrste simetričnih kriptografski algoritama

Postoji veliki broj javnih simetričnih algoritama koji se primjenjuju kao standardi u suvremenim sustavima zaštite. Tijekom primjene uočene su izvjesne opće ranjivosti specifične kod upotrebe blok kodnih ustava u specifičnim uvjetima. Ove ranjivosti se otklanjaju kombiniranjem nekoliko kriptografskih modova.

Kriptografski algoritam predstavlja način upotrebe osnovnog kodnog algoritma. Najčešće se radi o kombinacijama povratne petlje i neke dopunske jednostavne aktivnosti. Aktivnosti koje se primjenjuju u kriptografskim algoritmima su jednostavne, jer je pouzdanost sustava uvjetovana pouzdanošću osnovnog algoritma, dok je primijenjena kriptografska moda tada manje značajna. Najčešći su sljedeći (3,15):

a) Algoritam koda elektronske knjige

Algoritam elektronske kodne knjige ECB (E*lectronic Codebook Mode*) čine i najbrži način upotrebe simetričnih algoritama. Primjenom ECB algoritma, pojedini blok otvorenog teksta se transformira u kod, bez kakve povratne informacije. (15).



Slika 14. Algoritam elektronske kodne knjige – enkripcije, dekripcije (15)

Opasnost u upotrebi ovog algoritma proizlazi iz činjenice ukoliko izvršitelj kriptoanalize ima otvoreni tekst i kod nekoliko poruka, može napraviti elektronsku knjigu kodova, i da ne poznaje kodni ključ. Iste otvorene poruke će imati identičan kod, pa se jednostavnom zamjenom blokova koda dobije otvoreni tekst (17). Ponavljanje određenih fragmenata poruka je realna pojava, a slabosti ECB algoritma nema ukoliko se uvijek šifriraju različite poruke.

Problem ove prirode se otklanja na nekoliko načina (15):

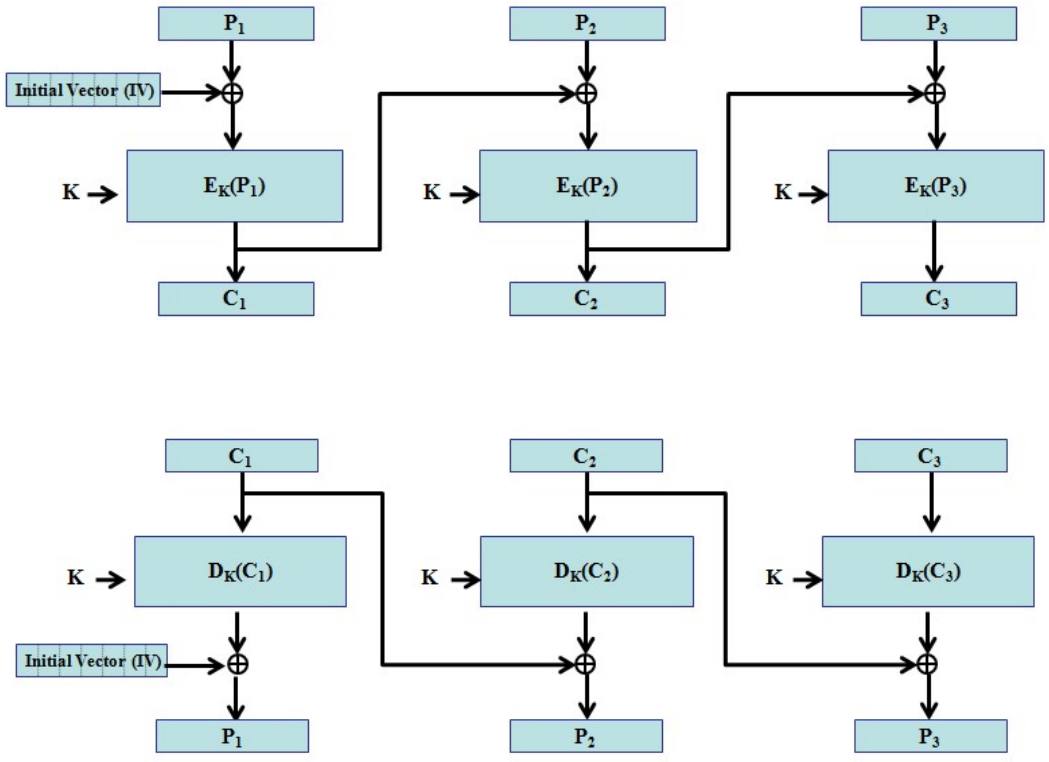
- primjenom kompresijskih metoda, bez umanjivanja informacijskog sadržaja (različite kompresivne metode se temelje na identifikaciji bit-nih ponavljajućih dijelova i uklanjanju ponavljanja),
- primjenom ostalih kriptografskih algoritama.

b) Algoritam ulančavanja blokova

Algoritam uvezivanja blokova CBC (*Cipher Block Chaining Mode*) vezuje blokove koda na način da se rezultati prethodno šifriranih blokova uporabljaju u kodnoj zamjeni tekućeg bloka. Navedenim postupkom se postiže da svaki blok koda nije ovisan o tekućem bloku, nego i o svim prije šifriranim blokova otvorenog teksta.

U CBC-u, blokovi se međusobno povezuju na taj način da se kodira „ekskluzivno ili“ (XOR - *Exclusive Or*) između bloka otvorenog teksta i šifriranog bloka, a potom se konačno dobiveni kod dobiveni blok šifrira. Proces dešifriranja se odvija na inverzan način: dobiveni blok podataka se dešifrira, a zatim se primjeni operacija XOR nad tako dobivenim skupom podataka i prijašnjim blokom (18).

Karakteristika CBC algoritma je u tome da identični blokovi otvorenog teksta budu šifrirani u različite blokove koda. U prvoj fazi šifriranja i dešifriranja neophodno je korištenje inicijalnog vektora, koji je po veličini identičan veličini šifriranog bloka, odnosno dešifrata. Inicijalni vektor ne treba biti tajan, iako je poželjno da se generira slučajno. Ovim još više dobiva na sigurnosti (7).

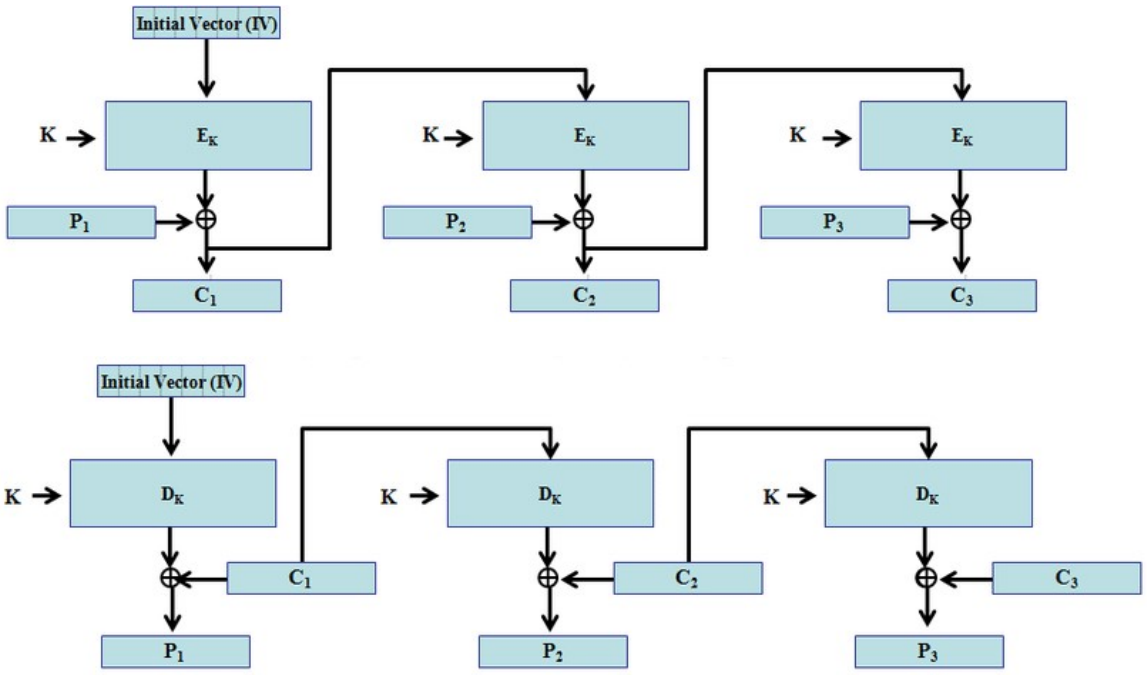


Slika 15. Algoritam ulančavanja blokova – enkripcije, dekripcije (15)

Postoji modifikacija ovog algoritma, tzv. algoritam ulančavanja blokova sa propagacijom (PCBC - *Propagating Cipher Block Chaining*), gdje se suština ogleda u primjeni ekskluzivne disjunkcije na tekući blok otvorenog teksta, prethodni blok koda, ali i na prethodni blok otvorenog teksta (14).

c) Algoritam povratnog šifriranja

U određenim primjenama potrebno je dijelove otvorenog teksta koji se šifriraju u jedinicama manjima od osnovne veličine koda, mijenjati što se realizira modom povratnog šifriranja - CFB (*Cipher Feedback Mode).* Ovaj algoritam obilježen je kao r-bit CFB algoritam, tako da je manji ili jednak bloku primijenjenog kodnog algoritma (14,15).



Slika 16. Algoritam povratnog šifriranja – enkripcije, dekripcije (15)

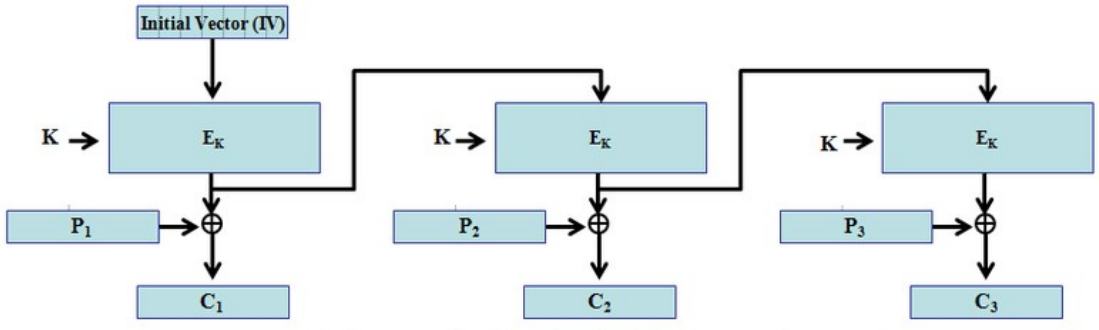
Operacija šifriranja se izvodi na sljedeći način (19):

- otvoreni tekst se podijeli na blokoveveličine r-bit, formira se inicijalizacijski vektor veličine n-bit i upiše u povratni registar i odabere se ključ kodne transformacije,
- formira se izlazni blok tako što se primjenom odabranog ključa izvrši šifriranje sadržaja povratnog registra,
- blok koda se formira tako što se primijeni ekskluzivna disjunkcije nad sadržajem tekućeg bloka otvorenog teksta,
- sadržaj povratnog registra se pomiče za r bita lijevo, a na mjesto r bita najmanje težine se upisuje formirani blok koda.

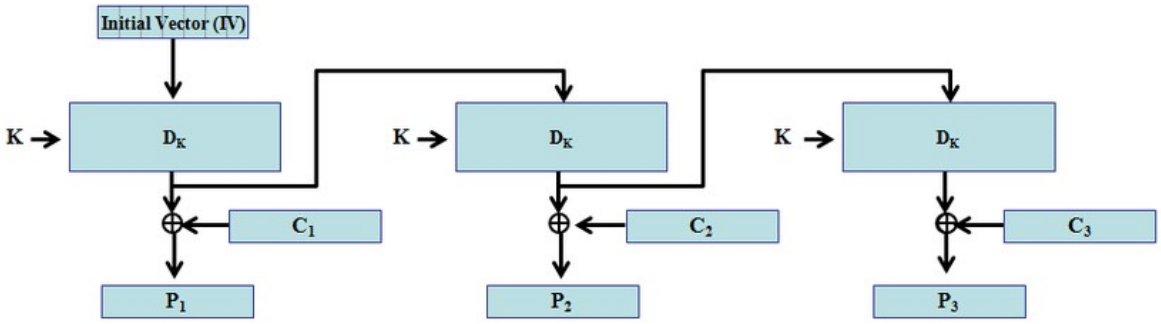
Dešifriranje se odvija slično. Temeljna karakteristika ovog algoritma je ta da prijemna i predana strana koristi osnovni kod u algoritmu šifriranja (15).

d) Izlazni povratni algoritam

Izlazni povratni algoritam OFB (*Output Feedback Mod)* je kombinacija ECB i CFB algoritma koji sprječava propagaciju[2] pogrešaka i dopušta prijenos podataka u jedinicama koje su manje od veličine samog bloka. Ukoliko se dogodi pogreška na jednom bitu prilikom šifriranja otvorenog teksta, primjenom izlaznog povratnog algoritma, neće biti propagacije greške, već će primjena kodnog algoritma za dešifriranje rezultirati u jednom pogrešnom bitu dešifriranog otvorenog teksta (15).



[2] Propagacija domene je vrijeme potrebno da izmjene koje izvršiš na DNS-u postanu vidljive svima na internetu.



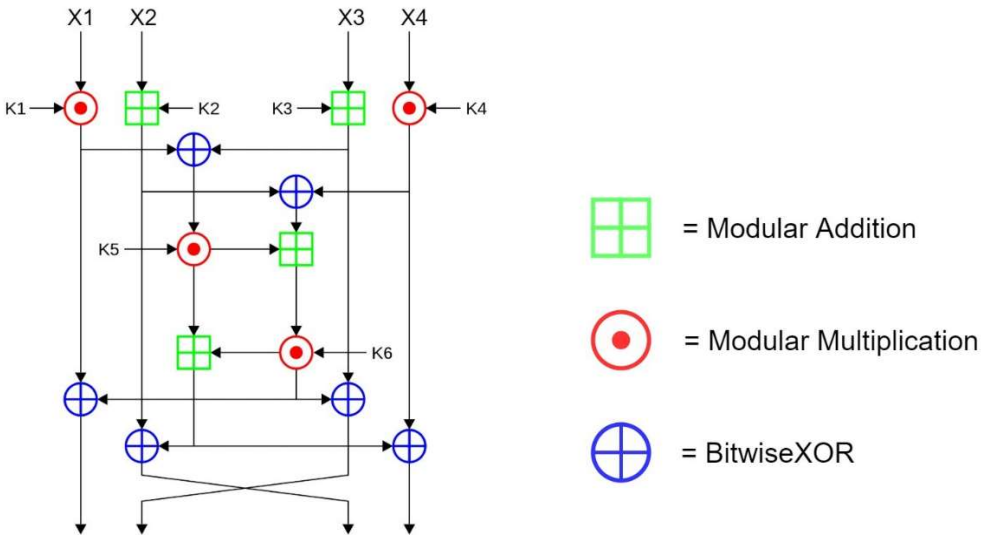
Slika 17. Izlazni povratni algoritam – enkripcije, dekripcije (15)

Kodna transformacija otvorenog teksta odvija se identično kao u CFB algoritmu. Razlika je ta što se povratna sprega omogućava korištenjem sadržaja izlaznog bloka. Kod CFB algoritma ostvaruje korištenjem bloka koda (20).

Izbor konkretnog algoritma primjene simetričnog kriptografskog algoritma u najvećoj mjeri ovisi od zahtjeva korisnika. Uobičajeno je da se za aplikacije gdje je imperativ brzina koristi ECB algoritam. Ovaj algoritam se sigurno koristi i prilikom razmjene kratkih poruka, jer pri tom ne dolaze do izražaja njegove slabosti. CBC algoritam se najčešće koristi za šifriranje datoteka. Algoritam CFB se često koristi za šifriranje nizova znakova gdje svaki znak individualno tretira. OFB kriptografski algoritam se često koristi u sustavima velikih brzina, gdje se ne dozvoljava propagacija grešaka. Primjenu najčešće nalaze niže nabrojani (20):

a) IDEA algoritam

Najviše primjenjivan, suvremenih simetričnih algoritama u aplikacijama široke upotrebe je IDEA algoritam (*International Data Encryption Algorithm).* Podatci koji se šifriraju dužine su 64-bit, a ključ primijenjen u šifriranju je dužine 128-bit. Dopuštena granica sigurnosti za korištenje simetričnih kriptografskih algoritama u suvremenim uvjetima je upravo 128-bit. Transformacija otvorenog teksta teče kroz osam ciklusa i na kraju posljednjeg se dobije šifrirani tekst (15,20).



Slika 18. IDEA algoritam (20)

IDEA kriptografski algoritam je optimiziran za izvršavanje na 16-bit procesorima. Sve osnovne operacije se izvode nad 16-bit podacima. Proces dešifriranja se izvršava isto kao proces šifriranja, mada priprema ključa za dešifriranje traje znatno duže za IDEA algoritam, a zasniva se na inventivnom sprezanju algebarskih operacija u različitim domenama, pogodnim za softversku implementaciju (5).

b) AES standard i Rijndael algoritam

Tijekom 2001. godine, američki nacionalni institut NIST (*National Institute of Standards and Technology*) je za simetrične algoritme objavio AES standard (*Advanced Encryption Standard*), koji je trebao zamijeniti prethodni standard DES (*Data Encryption Standard*), iz razloga jer su se poruke šifrirane prema DES standardu mogle lako dešifrirati zbog nedostataka u samom algoritmu, male dužine ključa i povećane procesne moći računala. Nakon selekcijske postupci, za realizaciju AES standarda izabran je Rijndael algoritam koji su realizirali Daemen i Rijmen (5).

Rijndael je blok kodni algoritam koji podržava transformaciju bloka otvorenog teksta promjenljive dužine (128/192/256-bit), primjenom ključa promjenljive dužine (128/192/256-bit). Za realizaciju AES standardnog algoritma izabran je oblik Rijndael algoritma koji podržava transformaciju bloka podataka od 128-bit, sa promjenljivom dužinom ključa. Algoritam AES realizira operacija šifriranja i dešifriranja bloka podataka u promjenljivom broju ciklusa. Broj ciklusa ovisi od dužine ključa i iznosi 10/12/14 za veličinu ključa od 128/192/256-bit, respektivno (20).

U okviru jednog ciklusa, transformacija se sastoji od četiri koraka (15):

- ByteSub - nelinearna supstitucija bajtova,
- ShiftRow - ciklični pomak vrsta matrice,
- MixColumn - množenje kolona matrice fiksnim polinomom po modulu i
- RoundKey - sabiranje ključa runde sa matricom.

1.4.2. Asimetrični kriptografski algoritmi

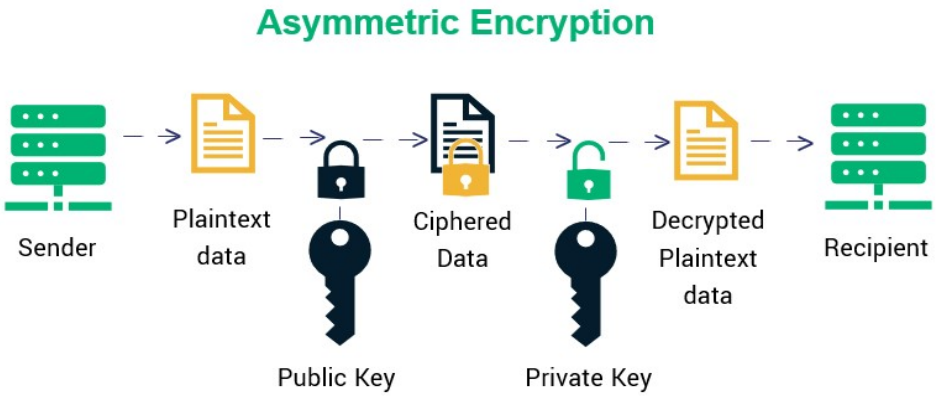
Asimetrični kriptografski algoritmi čine suvremeni oblik primjene kriptografije. Kriptografija asimetričnog ključa koristi različite ključeve za enkripciju i dekripciju, pa su algoritmi iz te grupe poznati i kao kriptografski algoritmi javnog ključa. Potrebno je istaknuti značajne karakteristike ovih algoritama (14):

- ukoliko se izvrši šifriranje poruke primjenom javnog ključa nekog korisnika, njeno dešifriranje se može uvjetno izvršiti primjenom privatnog ključa,
- ukoliko se izvrši šifriranje poruke primjenom privatnog ključa određenog korisnika, njeno dešifriranje se može izvršiti jedino primjenom odgovarajućeg javnog ključa, i
- poznavanjem tajnog ključa moguće je odrediti javni, dok je na temelju poznatog javnog ključa nemoguće odrediti tajni ključ.

Ova vrsta kriptografskih algoritama je proizašla iz potrebe distribucije kriptografskih ključeva, koji je bio glavni sigurnosni problem prilikom upotrebe simetričnih kriptografskih algoritama, pa su prvobitno razvijeni za zaštitu tajnosti (21). Sigurnost ovih algoritama temelji se na kompleksnosti matematičkih operacija koje se primjenjuju u određenim sustavima. Međutim, visoka računalska zahtjevnost ovih postupaka utječe na performanse sustava u kojima se koriste, pa nije preporučena primjena za zaštitu tajnosti informacija u sustavima s velikim protokom informacija (13).

U suvremenoj kriptografiji asimetrični algoritmi često se nalaze primjenu za realizaciju razmjene simetričnih ključeva aplikacijama koje primjenjuju simetrične kriptografske algoritme.

Primjenom asimetričnih kriptografskih algoritama mogu se ostvariti aktivnosti provjere integriteta, autentičnosti i izvornosti. Također, najčešće se primjenjuju u tehnologiji digitalnog potpisa i digitalnog omotnica (15).



Slika 19. Asimetrični kriptografski algoritam (15)

S gledišta kvalitete, otpornosti na različite vrste napada i načina implementacije, algoritmi sa javnim ključem nisu podjednako efikasni.

Najčešće korištena algoritma iz ove grupe su (13):

- RSA (*Rivest, Shamir, Adleman Algorithm*) i
- Diffie-Hellman - Poznat je kao *key-agreement algorithm* s obzirom da se ne može koristiti za enkripciju javnog ključa. Algoritam se koristi kako bi omogućio dvjema stranama da generiraju tajni ključ dijeleći informacije kroz javni medij. Taj ključ se onda može koristiti za enkripciju algoritmom tajnog ključa (3).

a) RSA algoritam

RSA algoritam je najpoznatiji predstavnik grupe asimetričnih kriptografskih algoritama. Potječe iz osamdesetih godina prošlog stoljeća, a naziva se prema inicijalima svojih autora: Rivest, Shamir, Adleman (13).

RSA algoritam se zasniva na problemu faktorizacije velikih brojeva na prim faktore. Prvi korak u realizaciji algoritma je izbor brojeva p i q. Prema željenom stupnju sigurnosti i namjeni sustava, određuje se veličina brojeva p i q. Potom se na slučajan način bira broj p_1 za koji se vrši provjera je li je prim. Ukoliko se utvrdi da je broj prim tada je $p = p_1$, u protivnom se bira novi broj p_1.Postupak se opetovano ponavlja. Kada se realizira selekcija broja p na isti način se utvrđuje vrijednost q. Nakon odabira navedenih veličina izabire se javni i tajni ključa, e i d (15).

Problem generiranja slučajnih brojeva u svojoj osnovi je problem generiranja slučajnih bita, pri čemu se izdvajaju dva osnovna pristupa.

Prvi način se bazira na generatorima pseudo slučajnih nizova (CSPRNG – *Cryptographically Secure Pseudo-Random Number Generator*) implementiranih u računalskim sustavima koji kao inicijalni izvor slučajnosti koriste određena stanja u sustavu. Najčešće su to informacije vezane za vrijeme između dva otkucaja na tastaturi, sadržaj vremenskog registra, tekuće pozicije pokazivačkih uređaja, sadržaji promjenljivih tablica unutar operativnog sustava itd. Karakteristika navedenog načina generiranja pseudo slučajnih nizova je da njegova bitska neodređenost nije veća od bitske veličine inicijalnih podataka (13).

Ukoliko inicijalni podaci nisu u dovoljnoj mjeri slučajni, kao što je proces mjerenja vremena intervala između otkucaja na tastaturi, bitska neodređenost se smanjuje i mogu se degradirati pretpostavljene slučajne karakteristike izvora, te izlazni niz učiniti predvidivim (5).

Drugi način se bazira na korištenju specijaliziranog hardvera za generiranje slučajnih bita. Ovi uređaji su bazirani na prirodnim pojavama za koje se smatra da se odvijaju na slučajan način. Jedan od primjera „nepredvidivosti“ je termalni šum poluprovodne diode. Slučajnost ovih procesa se često usložnjava kombiniranjem više slučajnih izvora (14).

Za sigurnost sustava s bazom RSA algoritma osnovno je sačuvati tajnosti parametra *d.* Jedan od načina da se dođe do tajnog eksponenta *d f*aktorizacija broja *n*. Pri tome treba voditi računa o izboru brojeva p i q tako da se ne omogući laku faktorizaciju. RSA algoritam se pokazao prilično robusnim i koristi se u većini suvremenih sustava zaštite (15).

b) Digitalna omotnica

Digitalna omotnica (*Digital Envelope*) je kombinacija simetričnih i asimetričnih kriptografskih algoritam koja je pomogla u rješavanju poteškoća distribucije ključeva. Karakteristična je za simetrične kriptografske sustave (15).

Postupkom stvaranja DE vrši se šifriranje sadržaja poruke primjenom određenog simetričnog algoritma (DES, 3DES, RC2, RC4, IDEA, AES ili nekog namjenskog tajnog algoritma) (21). Ključ simetričnog algoritma se šifrira javnim ključem primaoca poruke, primjenom odgovarajućeg asimetričnog algoritma. Šifriran sadržaj poruke simetričnom transformacijom i šifriran simetrični tajni ključ asimetričnog algoritma čine digitalnu omotnicu. Ključ kojim je šifrirana poruka može biti dešifriran jedino primjenom tajnog ključa subjekta kome je poruka upućena (14,15).

Ključevi simetričnih kriptografskih algoritama mogu se čuvati na vanjskim memorijskim uređajima (npr. *smart* kartice), što zahtjeva korištenje centraliziranog sustava upravljanja ključevima i sustavom zaštite (6).

c) Sesijski simetrični ključevi

Alternativni sustav upravljanja ključevima čini korištenje sesijskih simetričnih ključeva. Pri uspostavljanju veze između učesnika u komunikaciji, generiraju se slučajne vrijednosti, što čini tajni ključ odgovarajućeg simetričnog algoritma (sesijski ključ). Na taj način se koriste različiti simetrični ključevi, tako se ne trebaju čuvati na vanjskim memorijskim uređajima. Sesijski ključevi se najčešće kreiraju primjenom generatora pseudo slučajnih brojeva, što smanjuje njihov stupanj sigurnosti, te su manje sigurni od centraliziranih sustava za upravljanje ključevima. Primjenom sesijskog ključa realizira se postupak transformacije poruka koje se prenose ka prijemnoj strani. Šifrirana poruka zajedno sa sesijskim ključem, primjenom mehanizma digitalne omotnice, šalje se prijemnoj strani. Dešifriranje sesijskog ključa može izvršiti isključivo korisnik kojemu je poslana poruka, primjenom operacije privatnog ključa važećeg asimetričnog algoritma (18).

Moguće je realizirati kombinirani sustav upravljanja ključevima kod kojih se simetrični ključ dobije kombinacijom ključa s vanjskog memorijskog uređaja (*smart* kartice) i sesijskog ključa. Navedenom kombinacijom dobija se „ključ poruke“ (*message key*) (7,18).

d) Kriptografske kompresivne funkcije

Kriptografske kompresivne funkcije su poznate kao jednosmjerne *hash* ili *message digest* funkcije. Cilj ovih funkcija je u određivanju otiska određene poruke, odnosno provjere integriteta podataka (7).

Najjednostavniji primjer upotrebe *hash* funkcije je određivanje bita parnosti otiska poruke. Postupak upotrebe kriptografske kompresivne funkcije se ogleda u uspoređivanju dobivenog otiska poruke i ponovno generiranog otiska (3).

Pri upotrebi kriptografskih kompresivnih funkcija moraju biti zadovoljeni sljedeći kriteriji (3):

- moguće je kreiranje kriptografskog otiska poruke,
- nemoguće je rekonstruirati izvornu poruku na osnovu kriptografskog otiska i
- postoji zanemariva vjerojatnost kreiranja identičnih kriptografskih
- otisaka sa istim karakteristikama za različite poruke.

Osnovna podjela kriptografskih kompresivnih funkcija je:

- kriptografske kompresivne funkcije s tajnim ključevima
    - o blok MAC i
    - o sekvencijalni MAC.
- kriptografske kompresivne funkcije bez tajnih ključeva:
    - o MD4 i MD5 i
    - o RIPEMD-128 i RIPEMD-160.

Kriptografske kompresivne funkcije sa primjenom tajnog ključa temelje se i funkcijama za provjeru autentičnosti poruke (MAC - *Message Authentication Code*). Osim kontrole integriteta poruka, provjerava i autentičnost pošiljatelja. Zasnivaju se na upotrebi standardnih kriptografskih kompresivni funkcija, uz primjenu tajnih parametara. Kriptografske kompresivne algoritme bez upotrebe tajnog ključa MD4 i MD5 (MD - *Message Digest*) prvi je Ronald Rivest. Algoritam SHA1 (*Secure Hash Algorithm*) razvio je NIST u postupak definiranja standarda za digitalni potpis (DSS - *Digital Signature Standard*).U okviru projekta zaštite Europske unije pod nazivom *Race Integraty Primitives Evaluation* (RIPE), razvijen je algoritam za kreiranje kriptografskog otiska poruke RIPEMD (*RIPE Message Digest*) (14).

e) MD5 algoritam

Algoritam MD5 obrađuje poruke dužine do maksimalno 2^{64}-bit dajući kao rezultat kriptografsku kompresivnu vrijednost od 128-bit. U MD5 algoritmu, nakon inicijalizacije parametara, obrađuje se ulazna poruka u blokovima od 512-bit. Ukoliko bitska dužina ulazne poruke po modulu 512 nije jednaka 448, proširuje se data poruka s najmanjim brojem bita potrebnim za realizaciju prethodno navedenog zahtjeva. Proširivanje se realizira tako što se na kraj date poruke dodaje jedan bit jedinice s potrebnim brojem binarnih nula. Nakon izvršenja ovog procesa, vrši se povezivanje 64-bit reprezentacije dužine ulazne poruke na kraj posljednjeg bloka. Navedenim postupkom formira se poruka čija je dužina umnožak od 512-bit. Prilikom obrade u MD5 algoritmu, 512-bit blokovi poruke dijele se u 16 pod blokova dužine 32-bit nad kojima se ostvaruju sve operacije. Rezultirajuća vrijednost algoritma predstavlja skup od četiri 32-bit bloka, koji se povezuju tako da jednoznačno formiraju 128-bit vrijednosti otiska poruke (14).

f) SHA1 algoritam

SHA1 algoritam procesira poruke u blokovima od 512-bit, podijeljenih u 16 blokova od 32-bit. Postupak je sličan kao i kod MD5 algoritma. Poruka se proširuje do dužine koja je za 64-bit kraća od 512-bit. Na kraju se dodaje jedinica praćena odgovarajućim brojem nula. Potom se 64-bit reprezentacija poruke dodaje rezultatu. Izlaz iz algoritma predstavlja skup od pet 32-bit blokova, tako da zajedno formiraju 160-bit *hash* vrijednosti (14).

1.5. Kriptoanaliza

Kriptoanaliza je znanstvena disciplina koja izučava metode "razbijanja" kriptografskih sustava. Razbijanje se vrši bez poznavanja ključa, obično u cilju dobivanja otvorenog teksta. Međutim, nekada cilj ne mora biti dobivanje otvorenog teksta – cilj može biti identifikacija ključa, identifikacija skupa loših ključeva i dr. Prema količini i kvaliteti otkrivenih informacija, rezultate kripto analitičkog napada možemo klasificirati na sljedeći način (20):

- Potpuno probijanje (*total break*) – napadač je otkrio ključ
- Globalna dedukcija (*global deduction*) – napadač je otkrio funkciju ekvivalentnu algoritmu dešifriranja, ali ne i ključ

- Lokalna dedukcija (*instance/local deduction*) – napadač je otkrio dodatne otvorene tekstove ili kodove koji ranije nisu bili poznati.
- Informacijska dedukcija (*information deduction*) – napadač je otkrio određene informacije o otvorenim tekstovima ili kodovima koji prije bili nepoznati
- Algoritam razlikovanja (*distinguishing algorithm*) – napadač razlikuje kod od slučajne permutacije

Napadač može napasti kodni sustav tako što će isprobati sve ključeve, gdje nakon svakog dešifriranja provjerava željeni rezultat. Ovakav napad naziva se potpuna pretraga ključeva. Da bi ovakva pretraga postala besmislena, kodni sustav treba posjedovati veliki broj ključeva, odnosno veliki prostor ključeva (*keyspace*). U velikom prostoru ključeva napadač ne može isprobati sve ključeve u realnom vremenu, odnosno u nekom razumnom periodu. Veliki prostor ključeva je neophodan uvjet za sigurnost kodnog sustava, ali nije dovoljan. Povijest kriptologije je to pokazali više puta kroz vjekovnu intelektualnu borbu kriptografa i kriptoanalitičara (10).

Kaže se da je kodni sustav siguran ukoliko najbolji poznati napad uključuje potpunu pretragu ključeva, odnosno nesiguran ako postoji bilo koji oblik kratkog napada. Veličina prostora ključeva je temelj za pretpostavku stupnja sigurnosti kodnog sustava – sigurnost nije egzaktna nego se zasniva na pretpostavkama (7,18).

U pretpostavci da kodni sustav ima ključ dužine 100 bita, što znači da je prostor ključeva 2100. Ako napadač može testirati 230 ključeva/sekundi onda može pronaći pravi ključ za oko 19 trilijuna godina (19 x 1012 godina). Ako postoji kratki napad, pa napadač ne mora testirati čitavi prostor već samo 280 ključeva istom brzinom pronaći će pravi ključ za 36 milijuna godina. Kraće nego u prvom slučaju, ali i dalje besmisleno (18).

Neki od osnovnih modela, odnosno tipova napada su (2):

Poznat samo kod (*ciphertext-only attack*, COA): Ako napadač ima samo kodove poruka šifriranih istim algoritmom i posjeduje znanje o otvorenom tekstu u vidu općih znanja o statistici jednog jezika, onda može uspješno napasti klasične kodne sustave koji koriste šifre zamjene (supstitucije) i dođe do ključa.

Potpuna pretraga ključeva (*exhaustive key search – brute-force attack*): Ako napadač ima samo kodove poruka, onda može pokušati da ih dešifrira pomoću svih ključeva iz prostora ključeva dok ne nađe pravi ključ.

Poznat otvoreni tekst (*known-plaintext attack*, KPA): Ako napadač ima kod određene poruke otvoreni tekst koji mu odgovara, onda može, na osnovu ovih informacija, pokušati da dođe do ključa.

Poznat odabran otvoreni tekst (*chosen-plaintext attack – CPA*): Ako je napadač uspio dobiti privremeni pristup sustavu za šifriranje, onda može kreirati kod odabranog otvorenog teksta (može da šifrira otvoreni tekst po vlastitom izboru). Na osnovu para otvoreni tekst/kod, napadač može, poznavajući algoritme šifriranja, pokušati doći do ključa.

Poznat prilagodljivi odabrani otvoreni tekst (*adaptive chosen-plaintext attack – CPA2*): Ako je napadač uspio dobiti pristup šifarskom sustavu, onda može kreirati kodove sekvenci otvorenog teksta. Na osnovu prethodne sekvence može pretpostaviti sljedeću sekvencu.

Poznat odabrani kod (*chosen-ciphertext attack CCA*): Ako je napadač uspio dobiti pristup sustavu za dešifriranje, onda može kreirati otvoreni tekst od odabranih koda (može dešifrirati kodove koje posjeduje). Na osnovu para kod/otvoreni tekst, napadač može, poznavajući algoritme dešifriranja, pokušati doći do ključa.

Modeli napada se mogu opisati i pomoću resursa koje zahtijevaju (3):

- Vrijeme – broj koraka računanja koji se moraju izvršiti.
- Memorija – količina prostora za skladištenje potrebno za izvođenje napada.
- Podatci – količina i vrsta otvorenih tekstova i koda potrebnih za određenu vrstu napada.

Ne postoje precizni brojevi o ovim parametrima, ali se u teoretskoj kriptoanalizi često navode pretpostavke.

1.6. Informacijska sigurnost i kritična infrastruktura

Potreba dinamičkog, proaktivnog i strateškog pristupa nužna je u procesu planiranja zaštite kritične infrastrukture i u uvjetima različitih oblika kriznih i izvanrednih situacija. Prije nego što je pojam „kritična infrastruktura" postao predmet interesa u brojnim analizama koje istraživale terorizam i unutrašnju sigurnost, pojam „infrastruktura" osamdesetih godina bio je referentna točka izvršitelja javne politike i sigurnosti (22).

Ekspanzijom opasnosti od terorizma, u suvremenim analizama, sve je prisutniji izraz kritična infrastruktura. Kritična infrastruktura postala temeljni dio nacionalne sigurnosti, a njena zaštita

predstavlja jednu od glavnih zadaća svake države, kao i svake zasebne institucije u sklopu države (1).

Kao primjer navodi se nekoliko definicija kritične infrastrukture, koje su zastupljene kao modeli u nekim od navedenih država. U Sjedinjenim Američkim Državama (SAD) kritična infrastruktura u osnovi se odnosi na širok opseg različitih sredstava i imovine koji su neophodni za svakodnevno funkcioniranje društvenih, ekonomskih, političkih i kulturnih sustava (9).

Svaki prekid sadržaja kritične infrastrukture ocjenjen je kao ozbiljna prijetnja za pravilno funkcioniranje ovih sustava i može dovesti do umanjenja imovine, civilnih žrtava i značajnih ekonomskih gubitaka (2). U Australiji je definicija za izraz kritična infrastruktura određena preciznije i podrazumijeva: fizičku infrastrukturu, lance opskrbe, informacijske tehnologije i komunikacijske mreže, koje bi, ukoliko budu uništeni na duže vrijeme onesposobe, mogle značajno utjecati na društveno ili ekonomsko blagostanje nacije, odnosno na sposobnost države u održivosti obrane i osiguranja nacionalne sigurnost (23).

Prema strategiji Europske unije, kritična infrastruktura predstavlja imovinu, sustav ili njegov dio koji se nalazi na području zemlje članice, a neophodan je za održavanje temeljnih društvenih funkcija, zdravstvenog sustava i sustava sigurnosti, ekonomskog ili socijalnog blagostanja, a čije bi ometanje ili uništenje imalo značajan utjecaj na zemlju članicu. Europska kritična infrastruktura - *EKI*, obuhvaća kritičnu infrastrukturu na teritoriji zemlje članice čije bi ometanje ili uništenje imalo bitan utjecaj na bar dvije zemlje članice. Značajnost utjecaja negativnih čimbenika u funkcioniranju elemenata kritične infrastrukture mora se procijeniti na osnovu kriterija međuovisnosti. To podrazumijeva učinke nastale kao rezultat međuovisnosti od drugih tipova infrastrukture (24).

U praksi, definiranje okvira kritične infrastrukture u mnogim zemljama je različito. Ono ovisi o specifičnostima, počevši od političkih prilika do geografskih karakteristika. Od ogromnog je značaja dobro razvijen informacijsko komunikacijski sustav koji bi olakšao sakupljanje, selektiranje, čuvanje, prosljeđivanje i zaštitu osjetljivih poslovnih i privatnih podataka, kako u mirnodopskim, tako i u vanrednim situacijama (25).

1.7. Sigurnosne prijetnje informacijsko-komunikacijskim sustavima

Pojam informacija znači znanje, uputstvo, ili obavijest u ovisnosti od toga u koje svrhe se koristi. Informacija ukazuje na poruku koja sadrži činjenice – podatke iz kojih se mogu izvesti zaključci. Ona može biti govorna, pisana, štampana ili elektronski zapisana. S gledišta suvremenih informacijskih tehnologija, kvaliteta informacijsko-komunikacijskih sustava određuje na koji način će podaci biti kreirani, obrađivani, skladišteni i prenošeni, kao i kako će biti osigurana njihova zaštita i uništavanje. Informacijsko-komunikacijski sustavi predstavljaju skup metoda, postupaka i resursa uobličenih tako da bi se lakše došlo do nekog cilja (26).

Informacijski sustav definira integrirani sustav koji obuhvaća ljudske i tehnološke resurse za osiguravanje informacija za podršku funkcioniranja institucije. Osnovni cilj svakog informacijskog sustava je omogućavanje prikupljanja podataka i njihovo prikazivanje na najbolji način (6).

Informacijska sigurnost predstavlja svaku aktivnost koja osiguravaju zaštitu informacija s ciljem da bude omogućen kontinuitet u radu i smanjen, na najmanju moguću mjeru, utjecaj rizika i prijetnji po informacijski sustav. Informacijska sigurnost podrazumijeva zaštitu povjerljivosti, integriteta i dostupnosti podataka od neovlaštenog pristupa, promjene ili uništenja uz primjenu kontrolnih mehanizama koji trebaju biti unaprijed određeni, ugrađeni, nadgledani, provjeravani i poboljšavani u realnom vremenu. Postoje mnogobrojne definicije sigurnosti podataka ovisno od nivoa potrebe (2).

Na nivou države štite se nacionalni interesi u informacionoj sferi, koji su određeni skupom osobnih, poslovnih i državnih interesa. Kako se sigurnost podataka osigurava zaštitom, može se definirati i kao zaštićenost podataka od slučajnih ili namjernih aktivnosti koji mogu nanijeti neprihvatljivu i nemjerljivu štetu bazi podataka (6).

Sigurnost informacijskih i tehnoloških sustava je objektivna mjera rizika odnosno sigurnosti pouzdanog funkcioniranja sustava u odnosu prema sebi i svom okruženju. Sustav se smatra sigurnim ako je zaštićen od svih faktora rizika. Sigurnost sustava zaštite najbliže odgovara značenju engl. termina *Security assurance* (garantirana sigurnost) (22).

U praksi se sigurnost informacija najčešće očituje u sigurnosnom radu bez otkazivanja informacijskog sustava, interneta, malicioznih programa, prisluškivanja, te u sigurnoj komunikaciji i zaštiti privatnosti. Sigurnost informacija je proces, kontinuiranog održavanja zaštite informacija i potrebno ga je planirati, implementirati, izvršavati, održavati i poboljšavati

kroz uspostavljeni sustav za upravljanje zaštitom informacija – ISMS (*Information security management system*) (1). Najveći problem je manjak svijesti o potrebi procjene rizika, koji često uvodi tehnologije zaštite bez prethodne procjene rizika, odnosno koji nedovoljno shvaćaju nužnost kontrole (1,22).

Informacijsko komunikacijski sustavi su kritični segmenti ljudskog društva u 21. stoljeću. Poseban problem je taj što se zbog ubrzanog razvoja informacijsko-komunikacijske tehnologije i nezaustavljivog rasta njene primjene u svim sferama društvenog života uvećava njegova ranjivost i izloženost vrlo ozbiljnim potencijalnim opasnostima (27).

Suvremeni sigurnosni izazovi, koji se javljaju u područjima politike, ekonomije, financija, energetike, ekologije, religije, kulture, informatike i drugih područja društvenog života, nameću potrebu uključivanja većeg broja državnih i društvenih organizacija u poslove kojima se osigurava nacionalna sigurnost. Pored povećanja broja organizacija koje se bave pitanjima nacionalne sigurnosti, postoji potreba da se na sigurnosne izazove i prijetnje odgovori na jedinstven i usklađen način (26).

Društvena ovisnost od informacijsko-komunikacijskih sustava uvećava posljedice napada, kao i padova dotičnih sustava. Pod informacijsko-komunikacijskim sustavom podrazumijeva se svaki uređaj ili grupa međusobno povezanih uređaja, kojima se vrši automatska obrada podataka ili bilo kojih drugih funkcija. Napad je prijetnja koja je izvršena i, ako je uspješan, dovodi do kompromitiranja računalnog sustava, odnosno, narušava njegovu sigurnost. Svaki sustav ima svoje slabe točke (1).

Kompleksniji sustavi imaju potencijalno veću mogućnost ranjivosti i propusta. Napad u suštini predstavlja eksploatiranje gore spomenutih ranjivosti i propusta, a sastoji se od namjernih koraka koje poduzima napadač da bi se postigao određeni cilj. Nezgode predstavljaju širok spektar slučajno nastalih i potencijalno štetnih radnji i događaja, kao što su npr. prirodne, tehničke i druge nepogode. Pad sustava je štetni događaj koji dovodi do mana susta ili vanjskim elementima o kojima sustav ovisi. Padovi sustava su uzrokovani greškama u izradi softvera, sastavljanju hardvera, ljudskim greškama i sl. Napadi na računalske sustave se mogu klasificirati prema više kriterija (2).

Prema porijeklu napada dijele se na (6):

- Unutrašnji napad, realiziran od strane napadača unutar sustava – insajdera koji imaju mogućnost pristupa resursima, ali u neovlaštenim dijelovima.

- Izvanjski napad, realiziran je od strane napadača izvan sustava. Prema posljedicama po sustavne resurse, napad može biti:

    - Aktivni napad, tj. pokušaj da se promjene sistemski resursi ili da se utiče na njihove operacije.
    - Pasivni napad je pokušaj da se neovlašteno pristupi podacima u sustavu, ali bez utjecaja na sustavne resurse (preuzimanje, nadgledanje prijenosa podataka, prisluškivanje i sl., npr. *sniffing*). U praksi je čest slučaj da neželjeni događaji sa aspekta sigurnosti u informacijsko-komunikacijskim sustavima predstavljaju kombinaciju različitih vrsta napada.

Vrste napada su (1):

- *DDoS,*
- *Phishing,*
- *Botnet,*
- *Spam,*
- *Social Engineering,*
- *Sniffing,*
- *Spoting*
- *i Malware.*

Napad uskraćivanjem usluga (*Denial of service*) je tip napada koji pokušava da spriječi legitimne korisnike da pristupe mrežnim uslugama. To se ostvaruje preopterećenjem mrežnih servisa ili prekomjernom konekcijom, što uzrokuje pad konekcije ili servera. Infrastruktura umreženih sustava i mreža, ograničenih je resursa. DDoS alati su namijenjeni da pošalju veliki broj zahtjeva ciljanom serveru (obično e-mail, *web* ili *ftp* server), s ciljem da preplave resurse servera i učine ga neupotrebljivim. Napad uskraćivanjem usluga je organiziran tako da ometa ili potpuno obustavlja normalno funkcioniranje web sajta, servera ili drugih mrežnih resursa.

Jedan od najčešćih korištenih načina za učinkovito zagušenje servera ostvaruje se slanjem prevelikog broja imputa i zahtjeva (1).

To onemogućava normalno funkcioniranje servera i web stranice će se otvarati mnogo sporije, a u nekim slučajevima može dovesti do potpunog obaranja servera (prouzrokovati pad svih baza podataka i „sajtova“ na serveru). Svaki sustav na internetu opremljen mrežnim protokolima s TCP (*Transmission Control Protocol*) protokolom je moguća žrtva ugroze (18).

Tijkom DDoS napada, određeni server ili mreža prima zahtjeve iz kompromitiranih sustava. Usljed pretjeranog slanja zahtjeva server usporava i postaje beskoristan, sve dok napad traje (5).

Najčešći DDoS napadi su (5):

- Volumetric Attack
- Application Level Attack

Kada u napadu sudjeluje Volumetric Attack, ciljani web sajt ili mreža dovijaju veliku količinu zahtjeva sa botnet-a i inficiranih zombi sustava. Tu spadaju (5):

- *Connection flood*
- *TCP SYN flood (reset napadi)*
- *ICMP/UDP flood,* i oni uglavnom ciljaju treći i četvrti nivo, odnosno *Network Layer i Transport Layer.*

Ovakvi modeli napada iskorištavaju inficirane sustave da stvore veliki protok prometa. Sistemi se distribuiraju geografski i to sa protokom koji prelazi čak 10TB/s. Ovakvi napadi vremenom napreduju i postaju sve složeniji. Najraniji oblik DDoS napada, svakako predstavlja SYN flood koji se pojavio 1996. godine i eksploatira slabosti u TCP (*Transmission Control Protocol*). Ostali napadi eksploatiraju slabosti u operativnim sustavima i aplikacijama, što dovodi do nedostupnosti mrežnih usluga ili čak do pada servera. Mnogi alati su razvijeni za izvršenje takvih napada i postali su slobodno dostupni na internetu (*Bonk, LAND, Smurf, Snork, Teardrop*). TCP napadi su još uvijek najpopularniji oblik DDoS napada (6). Razlog je što ostali tipovi napada, kao što je upotreba (potrošnja) cjelokupnog prostora na hard disku, modificiranje tablice rutiranja na ruteru i sl., prvo zahtijevaju upad na mrežu, što može predstavljati problem za potencijalnog napadača, ako je sustav dobro zaštićen.

Postoje tri osnovna načina izvršavanja DDoS napada (6):

- Potrošnja svih resursa kao što je propusni opseg, što onemogućava legitimni promet, *SYN flooding attacks* – veliki broj zahtjeva da se otvori TCP konekcija, tj. veliki broj otvorenih konekcija, *smurf napadi* – veliki broj paketa usmjerenih ka mreži; - Uništenje ili oštećenje konfiguracijskih informacija (npr. rutera);
- Fizička oštećenja komponenti mreže da bi se spriječio pristup uslugama (računala, rutera, stanica za napajanje električnom energijom...)
- Klasični DDoS napadi su jedan na jedan napadi u kojima moćan host generira promet koji zatrpava konekciju ciljanog hosta što ometa ovlaštena osobe da pristupe mrežnim uslugama. Prvi put su se pojavili 1999. godine, a masovni DdoS napadi, počeli su 2000. godine, kada su oboreni popularni serveri, kao što je Amazon, CNN, eBay, YAHOO i dr.

Najbolji način za obranu od takvih napada je promjena konfiguracija rutera kod provajdera internet usluga. DDoS napadi koriste veliki broj računala zaraženih crvima ili trojancima, da realiziraju jednovremeni napad na ciljani sustav za vrlo kratko vrijeme. Daljinski kontrolirani zaraženi računalo naziva se „Zombi". Računala zombiji mogu, recimo, poslati na tisuće mailova izazivajući prekid usluga na email serveru. DDoS napad koji se dogodio u Estoniji 2007. godine bio je najveći napad ikada viđen. U tom napadu bilo je uključeno više različitih *bot* mreža (28).

Svaka je imala više desetina tisuća zombija. Često se u informatičkim krugovima događaji u Estoniji nazivaju „Prvi rat na mreži" (Web War I). Posljednji i najveći dosadašnji ransomware napad u svetu, otpočeo je 12.5.2017. godine. Novi ransomware je napravio pometnju širom sveta. Pogođen je NAS (Nacionalni zdravstveni sustav Velike Britanije), bolnice, kao i institucije povezane sa njima, te je zavladao potpuni kaos. 13 Zabilježeno je više od 145.000 napada u 74 zemlje, a najveći broj u Rusiji. Pored Velike Britanije i Rusije, teško su pogođene Turska, Kazahstan, Indonezija, Vijetnam, Japan, Španija, Njemačka, Ukrajina i Filipini (5).

Krivac za ove napade je v2.0 WCRY ransomware koji je poznat i pod nazivima Wannacry, Wannacryptor ransomware. Ransomware koristi NSA exploit koji je dospio u javnost zahvaljujući hakerskoj grupi *The Shadow Brokers*. Ima na desetine tisuća žrtava širom svijeta uključujući i rusko Ministarstvo unutarnjih poslova, kineski univerzitet, mađarsku telekomunikacijsku kompaniju, dijelove američke Fedex korporacije itd. (16)

Ne postoji sigurnosno rješenje koje će nekome pružiti stopostotnu zaštitu od postojećih i novih, sve kompleksnijih prijetnji. Kod IT sigurnosti postoje dva osnovna problema. Prvi je stalni rast broja i kompleksnosti cyber prijetnji, koji je objektivan problem i na njega se ne može mnogo

utjecati. Drugi problem, na koji može se može utjecati, su greške i pogrešno percipiranje situacije. Institucije prave greške kada su u pitanju neke jednostavne operacije, a koje čine instituciju ranjivom na različite napade (10).

Iako ne postoji jedno rješenje ili pristup za potpunu zaštitu, postoje jednostavne stvari koje je potrebno učiniti da bi se povećao nivo sigurnosti i da bi se osigurali uvjeti za obranu od narastajućih prijetnji. Prijetnja koja stiže u vidu *dropper* trojanca koji ima dvije komponente: Komponenta koja pokušava eksploatirati *SMB Ethernal Blue* ranjivost drugih računala – *ransomware wanna crypt*. Ukoliko uspješno uspostavi konekciju, prijetnja ne nastavlja dalje da inficira sustav ransomware-om, ili da se širi u druge sustave. Jednostavno, prijetnja se prestaje izvršavati, a ukoliko ne uspije, nastavit će sa kriptiranjem i širenjem. Drugim riječima, blokiranje ovog domena na zaštitnom zidu je vrlo loša ideja, jer će samo izazvati dalje širenje ransomware i dalje kriptiranje datoteka (6).

Ransomware također provjerava da li se koristi *proxi* (server posrednik) ili ne, te ako vidi da se nalazi iza *proxia*, nastavlja sa radom, ne provjeravajući postojanje navedene domene. *Wanna cry* ransomware je zaustavljen „*kill switch*" mehanizmom (28).

Problem predstavljaju otpornost i stalna mutacija ovog cyber parazita. Korisnici operativnog sustava Windows trebali bi primjenjivati sljedeće mjere (6):

- Ažuriranje (update) Windows-a. Ključno je instaliranje MS 17010 patch.
- Install patch AB 2871997
- Ažuriranje antivirusa
- Blokiranje dolaznog sadržaja TCP port 445
- Osigurati da se sve šifre za lokalne administratorske naloge na računarima u mreži razlikuju
- Napraviti rezervnu kopiju podataka (*back up*) sa računala i servera i sačuvati na vanjskim memorijskim jedinicama sve relevantne datoteke.

Iako nije dokazano da se širi putem elektronske pošte, važno je obavijestiti sve koji rade sa računarima da ne otvaraju linkove unutar poruka prispjelih elektronskom poštom od nepoznatih pošiljatelja, posebno ako su u pitanju arhivirane datoteke *(.zip, .rar)*, izvršne *(.com, .exe)* ili datoteke s ekstenzijom *(.jz)* (6)

2. CILJ RADA

Cilj je ovoga rada istraživanje, definiranje i analiza informacijske sigurnosti, ključnih sigurnosnih problema i mogućih potencijalnih rješenja prijetnjama, kao i kriptografski algoritmi za potrebe generiranja kriptografskih ključeva koji se primjenjuju u tehnologijama zašite informacijsko-komunikacijskih sustava.

Pridodano tome, namjera je istaknuti važnost informacijske sigurnosti osobito u odnosu na kritične infrastrukture institucija.

3. MATERIJALI I METODE

U radu su korištene osnovne znanstvene metode.

Metoda deskripcije je korištena pri objašnjavanju osnovnih pojmova i sustava funkcioniranja.

U teorijskim segmentima su primijenjene metode indukcije, dedukcije i analize, a u izvođenju zaključaka metode sinteze i generalizacije.

4. RASPRAVA

Informacijska sigurnost podrazumijeva skup tehničkih, logističkih, normativnih i administrativnih rješenja te postupaka koje se izvode u namjeri zaštite od neovlaštenog uvida, otuđenja ili uništenja, kao i zbog zaštite funkcionalnosti informacijskog sustava (2).

Termini sigurnost informacija ili informacijska sigurnost primarno podrazumijevaju sigurnost podataka IKTS, a sekundarno sigurnost objekata računalnog sustava (RS) i računalske mreže (RM), čime se posredno štite informacije. Ovakav pristup navodi da je konačni cilj sigurnosti i zaštite – zaštita informacija i podataka, koja se postiže zaštitom informacijske imovine (24).

Informacijska imovina u ISO/IEC 27001 obuhvaća informacije, hardver, softver i ljudske resurse. Misija, tj. ciljevi sustava zaštite informacija je da održanjem IKTS-a (informacijsko kompjuterskog tehnološkog sustava) na prihvatljivom nivou rizika osigura pouzdanost rada poslovnog IKTS-a i poveća efektivnost poslovnog procesa (1).

Primarni ciljevi zaštitite su zaštita informacijske imovine institucije. Ovi ciljevi se najčešće navode kao dostatan korpus relativno nezavisnih ciljeva zaštite u adekvatnim standardima zaštite (ISO/IEC 27001, NIST). U nekim standardima i elementima zaštite, spominju se i ciljevi zaštite kontrolirane odgovornosti (*Accountability*), izvornosti, autentifikacije i garantirane sigurnosti (*Security Assurance*) (6).

Ciljevi zaštite su međusobno ovisni. Na primjer, cilj zaštite integriteta obuhvaća zaštitu izvornosti i autentifikaciju, a cilj zaštite raspoloživosti – kontroliranu odgovornost, koja ovisi o mehanizma za osiguravanje izvornosti. Garantiranu sigurnost osiguravaju sva tri primarna sigurnosna cilja zajedno. sigurnosni zahtjev za raspoloživost informacija osigurava ovlaštenim korisnicima pouzdan rad i raspoloživost podataka i informacija sustava, i aplikacija, prema potrebi. Ovaj cilj štiti sustav od namjernog ili slučajnog kašnjenja podataka, odbijanja servisa ili isporuke podataka (DDoS) i od neovlaštene upotrebe sustava te informacija i uvijek je najvažniji sigurnosni cilj (1,6).

Sigurnosni zahtjevi za zaštitu integriteta, uključujući i zaštitu stabilnosti podataka i informacija (skladišnih, procesuiranih i prenesenih), konfiguracije (RS i RM i integriteta sesije) imaju za cilj da spriječe otkrivanje neovlaštenim osobama spremljenih, procesuiranih i prenošenih povjerljivih ili osobnih podataka (22).

Zahtjev za kontroliranu odgovornost entiteta i pojedinaca u instituciji traži da se akcije svakog entiteta i pojedinca mogu pratiti po jednoznačno registriranim tragovima. Servis za ostvarivanje ovog zahtjeva očituje se u sustavu politike zaštite i direktno uključuje normativni okvir, odvraćanje napadača, otkrivanje i sprječavanje upada i oporavka sustava (26).

Navedeni sigurnosni ciljevi su međusobno ovisni i rijetko se može ostvariti jedan, bez utjecaja drugih. Cilj zaštite povjerljivosti ovisi o zaštiti integriteta, zato što nije smisleno očekivati da informacija nije otkrivena, ukoliko je narušena cjelovitost sustava. Cilj zaštite integriteta ovisi o zaštiti povjerljivosti jer je opravdano vjerojatno da je mehanizam zaštite integriteta zaobiđen i cjelovitost informacija narušena, ako je narušena povjerljivost (npr. lozinka administratora) (2).

Svako smanjivanje ovog skupa ciljeva zahtjeva odgovarajuću aproksimaciju i razumijevanje ove međuzavisnosti. S ciljem garantirane sigurnosti u međuovisnoj vezi su svi ciljevi zaštite. Kada se projektira sustav zaštite, projektant uspostavlja graničnu vrijednosti garantirane sigurnosti koji se postiže ispunjavanjem zahtjeva u svakom od četiri cilja, temeljeno na postupcima i standardima dobre prakse. Također, ističe činjenicu da se za garantiranu sigurnost nekog sustava moraju ispuniti projektirani funkcionalni zahtjevi za tehničku pouzdanost sustava (vjerojatnost ili srednje vrijeme rada bez otkaza sustava), ali i spriječiti neželjeni procesi i steći povjerenje u sustav zaštite (1).

Problem ranjivosti informacijske infrastrukture potakao je rasprave o adekvatnim sigurnosnim politikama i, uopće, adekvatnim politikama zaštite cyber prostora. Već tijekom 2006. godine, Europski parlament uputio je preporuku Savjetu Europe i Europskom Savjetu za zaštitu kritičnih infrastruktura. U okviru preporuke sadržani su i stavovi da kritične infrastrukture u Europskoj uniji postale su visoko povezane i međusobno ovisne, što ih čini posebno ranjivim na poremećaje i uništenje (6).

Usljed toga, potaknuta je potreba da se izgradi Europski program zaštite kritičnih infrastruktura (*European Programme for Critical Infrastructure Protection)*, koji bi bio financiran od strane država članica, i/ili vlasnika infrastruktura i operatera.” Na Svjetskom samitu o informacijskom društvu donijeta je Deklaracija o principima (2003.), u kojoj je naglašena potreba za razvijanjem koncepta cyber sigurnosti (23).

U odjeljku Deklaracije, posvećenom izgradnji povjerenja i sigurnosti u korištenju IKT, navodi da se jačanje povjerenja, uključujući sigurnost informacija i mreže, autentičnost, privatnost i zaštitu korisnika, neophodno je za razvoj informacijskog društva i stvaranje povjerenja između korisnika IKT. Potrebno je promovirati, razvijati i uvoditi globalnu kulturu cyber sigurnosti kroz saradnju svih dionika u donošenju odluka te međunarodnih ekspertnih tijela. Ovaj napor bi trebalo biti podržan kroz povećanje međunarodne saradnje. U okviru globalne kulture cyber sigurnosti važno je povećati sigurnost i osigurati zaštitu podataka i privatnosti, paralelno s povećanjem mogućnosti i pristupa i trgovine. Također, moraju se uzeti u obzir i stupanj socijalnog i ekonomskog razvoja svake zemlje i poštovati razvojno orijentirani aspekti informacijskog društva (25).

Mnoge državne institucije, ustanovljuju i uvode različite oblike informacijskih sustava i sustava elektronske dokumentacije. Sastavni dio nabave ili vlastitog razvoja tih sustava je i postupak osiguravanja zaštite informacija, kao i postupak definiranja načina smanjenja rizika i sprječavanja negativnih posljedice koje su moguće uslijed neadekvatne zaštite podataka (22).

Privatnost podataka tiče se namjere pojedine osobe da kontrolira javno iznošenje osobnih i nekih drugih izabranih informacija. Povjerljivost se odnosi na informacije i na mogućnost pojedinca da ih kontrolira način na koji pružatelj neke usluge (organizacija ili pojedinac) upotrebljava osobne informacije, kao i dalje širenje takvih informacija. Zaštita pruža privatnost i povjerljivosti izborom odgovarajućih strategija, postupaka i metoda zaštite (2).

Informacijska sigurnost stoga se adekvatno ogleda u svojoj definiciji po tome da se obuhvaća niz tehničkih i drugih postupaka utvrđenih s ciljem da se podaci zaštite od neovlaštenog ili nenamjernog uvida i krađe ili uništenja, kao i radi zaštite funkcionalnosti samog informacijskog sustava (27).

5. ZAKLJUČAK

Sigurnosne prijetnje informacijskom društvu raznovrsne su i specifične po tome što su primarno usmjerene na zlonamjerno destabiliziranje informacijskih sustava. Onemogućavanje normalnog funkcioniranja informacijskih sustava u društvu koje je od njih postalo ovisno može imati vrlo ozbiljne posljedice na sve aspekte društvenog života. Posljedice mogu biti čak i fatalne ukoliko se ugroze pojedine infrastrukture, kao što su, npr. sustavi za kontrolu kopnenog i zračnog prometa, hidrocentrala, nuklearnih elektrana, sigurnosnih i zdravstvenih službi ili, pak, za distribuciju električne energije. Napredak umrežavanja informacijskih sustava proširio je, u odnosu na koncept informacijske sigurnosti, listu svojstava informacija pred koje se postavljaju sigurnosni zahtjevi tj. ciljevi. S gledišta informacijske sigurnosti značajno je zadovoljavanje sljedećih svojstava informacijskih sustava: privatnost ili povjerljivost (engl. *privacy, confidentiality*), integritet (*engl. integrity*) i raspoloživost (*engl. availability*). Njima se ponekad dodaju još dva, a to su: autentičnost (*engl. authentication*) i neopozivost (*engl. nonrepudiation*).

Svrha privatnosti je da se dozvoli pristup informaciji isključivo autoriziranim osobama ili programima. Povjerljivost podataka može biti vezana za razloge nacionalne sigurnosti (npr. informacije o naoružanju), industrijske sigurnosti (npr. projekti nekog novog proizvoda) ili osobne privatnosti korisnika (npr. u zdravstvu određena oboljenja). Integritet je cilj kojim se teži osigurati podatke i resurse koji njima upravljaju (hardver i softver) tako da mogu biti modificirani ili uništeni samo uz posebnu i prethodno definiranu autorizaciju.

Svrha raspoloživosti se sastoji u tome da podaci budu u svakom trenutku dostupni autoriziranim korisnicima. Drukčije rečeno, sustav koji daje takve usluge treba funkcionirati samo kada se to od njega zahtjeva i to u ograničenom i unaprijed određenom vremenu. S gledišta informacijske sigurnosti, raspoloživost predstavlja sposobnost zaštite od štetnog događaja ili sposobnost očuvanja sustava u slučaju kada se neželjeni događaj već dogodio. Raspoloživost suvremenih informacijskih sustava, koji su stanju neprekidne aktivnosti, neophodna je kako za normalno izvršavanje aktivnosti informacijskog društva tako i za sigurnost ljudskih života.

Autentičnost je mjera sigurnosti koja ima za cilj odrediti vrijednosti i validnost prijenosa, poruke ili onoga tko je šalje. Ovom mjerom se kontrolira i autorizacija korisnika u primanju specifične kategorije informacija.

Neopozivost je mjera sigurnosti čiji je cilj osigurati tijek komunikacije. Ovom mjerom sigurnosti se postiže da pošiljatelj informacije ima dokaz o njenoj isporuci, ali i da primatelj informacije ima podatak o identitetu pošiljaoca. To ima za cilj da nijedan od učesnika u prijenosu ne može negirati izvršenu transakciju.

Stupanj važnosti navedenih svojstva informacija varira u ovisnosti od konteksta u kojem se razmjena informacija izvršava.

Zaštita podataka te jednostavan pristup često su oprečni zahtjevi: jednostavan pristup može ugroziti sigurnost ako aplikacija nije pomno i adekvatno kriptografski projektirana i implementirana, dok previše kompleksni kriptografski mehanizmi zaštite obično narušavaju jednostavnost korištenja aplikacije s gledišta korisnika. Veliki dio običnih ljudi, a među njima i informatičkih stručnjaka često ne uvažavaju složenost zaštite informacija pa i onda kad shvaćaju njen značaj i objektivno stanje. Faktori rizika se mogu svesti na minimum, ali nikada ukloniti u potpunosti.

6. LITERATURA

1. Bačić R. Tajnost podataka, kriptografija i informacijska sigurnost. University of Split. Faculty of Law; 2020.

2. Čizmić J. Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost. 2016;

3. Katz J, Lindell Y. Introduction to modern cryptography. CRC press; 2020.

4. Aung MAC, Wai MS. Study on Symmetric and Asymmetric Cryptographic Techniques. MERAL Portal; 2015.

5. Bauer C. Secret history: The story of cryptology. CRC Press; 2021.

6. Akrap G. Suvremeni sigurnosni izazovi i zaštita kritičnih infrastruktura. Strategos: Znanstveni časopis Hrvatskog vojnog učilišta" Dr Franjo Tuđman". 2019;3(2):37–49.

7. Marancina S. Kriptografija na osnovi kodiranja. Univerza v Ljubljani; 2018.

8. Menezes AJ, Van Oorschot PC, Vanstone SA. Handbook of applied cryptography. CRC press; 2018.

9. Forouzan BA, Mukhopadhyay D. Cryptography and network security. Vol. 12. Mc Graw Hill Education (India) Private Limited New York, NY, USA:; 2015.

10. Stinson DR, Paterson M. Cryptography: theory and practice. CRC press; 2018.

11. Klima R, Klima RE, Sigmon N, Sigmon NP. Cryptology: classical and modern. CRC Press; 2018.

12. Maqsood F, Ahmed M, Ali MM, Shah MA. Cryptography: A comparative analysis for modern techniques. International Journal of Advanced Computer Science and Applications. 2017;8(6).

13. Abood OG, Guirguis SK. A survey on cryptography algorithms. International Journal of Scientific and Research Publications. 2018;8(7):495–516.

14. Joseph DP, Krishna M, Arun K. Cognitive analytics and comparison of symmetric and asymmetric cryptography algorithms. Int J Adv Res Comput Sci. 2015;6(3):51–6.

15. Bisht N, Singh S. A comparative study of some symmetric and asymmetric key cryptography algorithms. International Journal of Innovative Research in Science, Engineering and Technology. 2015;4(3):1028–31.

16. Chinnasamy P, Padmavathi S, Swathy R, Rakesh S. Efficient data security using hybrid cryptography on cloud computing. In: Inventive Communication and Computational Technologies: Proceedings of ICICCT 2020. Springer; 2021. p. 537–47.

17. Sharma R, Bollavarapu S. Data security using compression and cryptography techniques. International Journal of Computer Applications. 2015;117(14).

18. Žufić I. Kriptografija u računalnim mrežama. University of Rijeka. Department of Informatics; 2016.

19. Hercigonja Z. Comparative analysis of cryptographic algorithms. International Journal of Digital Technology & Economy. 2016;1(2):127–34.

20. Aung MAC, Wai MS. Study on Symmetric and Asymmetric Cryptographic Techniques. MERAL Portal; 2015.

21. Kumar P, Rana SB. Development of modified AES algorithm for data security. Optik. 2016;127(4):2341–5.

22. Boban M. The right to privacy and the right to access information in the modern information society. Zb Radova. 2012;49:575.

23. Boban M. Pravo na privatnost i pravo na pristup informacijama u suvremenom informacijskom društvu. Zbornik radova Pravnog fakulteta u Splitu. 2012 Sep 17;49(3):575–98.

24. Boban M, Radalj J. Regulativa i primjena blockchain tehnologije i pametnih ugovora u suvremenom elektroničkom poslovanju. 2023;

25. Boban M. INFORMATION AND DISINFORMATION: IMPACT ON NATIONAL SECURITY IN THE DIGITAL AGE. Economic and Social Development: Book of Proceedings. 2022;309–17.

26. Gorica VV, Gorica V, Gorica-student V. INTEGRACIJA ZAŠTITE KRITIČNE INFRASTRUKTURE U PROCESU EVALUACIJE–METODOLOŠKI PRISTUP. Dani kriznog upravljanja. :269.

27. Boban M, Weber M. Internet of Things, legal and regulatory framework in digital transformation from smart to intelligent cities. In: 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE; 2018. p. 1359–64.

28. Cosic Z, Boban M. Information security management—Defining approaches to Information Security policies in ISMS. In: IEEE 8th International Symposium on Intelligent Systems and Informatics. IEEE; 2010. p. 83–5.

7. SAŽETAK

U ovom radu obuhvaćene su tehnologije s ciljem rješavanja različitih sigurnosnih problema u funkcioniranju suvremenih informacijskih sustava. Težište je na objašnjavanju dometa u slučaju moguće ugroze kritične infrastrukture. Dat je opis strukture i funkcionalnosti kriptografskih algoritama koji se trenutno primjenjuju u zaštiti informacija i izneseni su mogući pravci daljeg razvoja. Obuhvaćeni su opći pojmovi iz kriptografije i kriptografije te metodologije funkcioniranja kriptografskih algoritama uz objašnjenja prednosti i sigurnosnih problema vezanih uz njihovu primjenu, kao i moguća rješenja. Sigurnosne prijetnje informacijskom društvu raznovrsne su i specifične po tome što su primarno usmjerene na zlonamjerno destabiliziranje informacijskih sustava. Onemogućavanje normalnog funkcioniranja informacijskih sustava u društvu koje je od njih postalo ovisno može imati vrlo ozbiljne posljedice na sve sfere društvenog života. Posljedice mogu biti čak i fatalne ukoliko se ugroze pojedine infrastrukture.

Ključne riječi: informacijska sigurnost, kriptografija, kriptologija, kriptoanaliza, kritična infrastruktura

SUMMARY

This paper includes technologies with the aim of solving various security problems in the functioning of modern information systems. The emphasis is on explaining the range in the event of a possible threat to a critical infrastructure of a state. The description of the structure and functionality of the cryptographic algorithms, which are currently applying in the protection of information and the possible directions of further development have been presented. General terms in cryptography and cryptography and the methodology of the functioning of cryptographic algorithms are covered, with explanations for the benefits and security problems related to their application, as well as possible solutions. Information society safety threats are varied and specific in that they are primarily focused on malicious destabilization of information systems. Disabling the normal functioning of information systems in a society that has become dependent can have very serious consequences on all spheres of social life. The consequences can even be fatal if individual infrastructure is threatened.

Keywords: information security, cryptography, cryptology, cryptoanalysis, critical infrastructure

8. ŽIVOTOPIS

Osobni podaci	
Ime / Prezime	**Ivan Beović**
Adresa(e)	Put vile rustike 9, Ostrvica, 21253 Gata
Telefonski broj(evi)	095 549 8026
E-mail	ibeovic@gmail.com
Državljanstvo	Hrvatsko
Datum rođenja	03.09.1991.
Spol	Muški
Obrazovanje i osposobljavanje	Policijska akademija (2014-2015) Visoka škola Logos centar Mostar, prvostupnik kriminalistike (2018-2021) Sveučilište u Split, Diplomski studije forenzike i nacionalne sigurnosti (2021-2023)
Radno iskustvo	MUP, Temeljna i prometna policija (2015-2018) MUP, Specijalna policija (2018-2023)
Hobiji	Kickboxing (16 godina) juniorska reprezentacija Hrvanje (slobodni stil), Jiu jitsu
Osobne vještine i kompetencije	Vozačka dozvola A i B kategorija
Materinski jezik	**Hrvatski jezik**
Drugi jezik(ci)	**Engleski jezik (govor i čitanje)**

9. IZJAVA O AKADEMSKOJ ČESTITOSTI

SVEUČILIŠTE U SPLITU

Sveučilišni odjel za forenzične znanosti

Izjava o akademskoj čestitosti

Ja, Ivan Beović, izjavljujem da je moj diplomski rad pod naslovom KRIPTOGRAFIJA, KRIPTOGRAFSKI ALGORITMI I INFORMACIJSKA SIGURNOST rezultat mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na izvore i radove navedene u bilješkama i popisu literature. Nijedan dio ovoga rada nije napisan na nedopušten način, odnosno nije prepisan bez citiranja i ne krši ničija autorska prava.

Izjavljujem da nijedan dio ovoga rada nije iskorišten u nijednom drugom radu pri bilo kojoj drugoj visokoškolskoj, znanstvenoj, obrazovnoj ili inoj ustanovi.

Sadržaj mojega rada u potpunosti odgovara sadržaju obranjenoga i nakon obrane uređenoga rada.

Split, _____

Potpis studenta: _____