Matematičke metode u kriptografiji

Čokara, Danijel

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA

Stručni studij elektrotehnike: Informatika

MATEMATIČKE METODE U KRIPTOGRAFIJI

Završni rad

Danijel Čokara

Osijek, 2016.

Sveučilište Josipa Jurja Strossmayera u Osijeku

ELEKTROTEHNIČKI FAKULTET OSIJEK

Obrazac Z1S: Obrazac za imenovanje Povjerenstva za obranu završnog rada na stručnom studiju

Osijek,

Odboru za završne i diplomske ispite

Imenovanje Povjerenstva za obranu završnog rada na stručnom studiju

Ime i prezime studenta:	Danijel Čokara
Studij, smjer:	Stručni studij elektrotehnike, smjer Informatika
Mat. br. studenta, godina upisa:	AI4221, 2012. godina
Mentor:	Doc. dr. sc. Tomislav Rudec
Sumentor:	Doc. dr. sc. Alfonzo Baumgartner
Predsjednik Povjerenstva:	Izv. Prof. dr. sc. Dominika Crnjac Milić
Član Povjerenstva:	Doc. dr. sc. Alfonzo Baumgartner
Naslov završnog rada:	Matematičke metode u kriptografiji
Primarna znanstvena grana rada:	**Programsko Inženjerstvo**
Sekundarna znanstvena grana (ili polje) rada:	
Zadatak završnog rada	Pikaz uporabe matematičkih metoda u kriptografiji.
Prijedlog ocjene pismenog dijela ispita (završnog rada):	
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: Postignuti rezultati u odnosu na složenost zadatka: Jasnoća pismenog izražavanja: Razina samostalnosti:

Potpis sumentora:	Potpis mentora:

Dostaviti:

1. Studentska služba

U Osijeku, godine Potpis predsjednika Odbora:

ETFOS
ELEKTROTEHNIČKI FAKULTET OSIJEK
Sveučilište Josipa Jurja Strossmayera u Osijeku

IZJAVA O ORIGINALNOSTI RADA

Osijek,

Ime i prezime studenta:	Danijel Čokara
Studij :	Stručni studij elektrotehnike, smjer Informatika
Mat. br. studenta, godina upisa:	A|4221, 2012. godina

Ovom izjavom izjavljujem da je rad pod nazivom**: Matematičke metode u kriptografiji**

izrađen pod vodstvom mentora Doc. dr. sc. Tomislava Rudeca

i sumentora Doc. dr. sc. Alfonza Baumgartnera

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis studenta:

SADRŽAJ

1. UVOD **1**
2. MODULARNA ARITMETIKA **3**
2.1 UVOD U MODULARNU ARITMETIKU 3
2.1.1 Računanje ostatka 5
2.1.2 Klase ekvivalencije 6
2.2 OSNOVE ALGEBRE U MODULARNOJ ARITMETICI 8
3. KLASIČNA KRIPTOGRAFIJA **9**
3.1. POVIJEST KRIPTOGRAFIJE 9
3.1.1 Skital 10
3.2 PODJELA TAJNE KOMUNIKACIJE PISANJA KROZ POVIJEST 10
3.3 TRANSPOZICIJA 11
3.3.1 Izmjenična transpozicija 12
3.3.2 Transpozicija s obilaskom 12
3.3.3 Stupčasta transpozicija 13
3.4 SUPSTITUCIJA 13
3.4.1 Cezarova šifra 14
3.4.2. Afina šifra 14
3.4.3 Vigenerova šifra 15
3.4.4 Hillova šifra 18
3.5 KRIPTOANALIZA U KLASIČNOJ KRIPTOGRAFIJI 21
3.5.1 Provođenje kriptoanalize 22
3.5.2 Vrste kriptoanalize 23
4. MODERNA KRIPTOGRAFIJA **25**
4.1 SIMETRIČNI SUSTAV 25
4.1.1 Šifre toka 26
4.2 BLOKOVNE ŠIFRE 31
4.2.1 DES algoritam 31
4.2.2 AES algoritam 35
4.3 ASIMETRIČNI SUSTAVI 38
4.3.1 RSA algoritam 39
5. ZAKLJUČAK **41**
LITERATURA **42**
SAŽETAK **43**
ŽIVOTOPIS **44**

1. UVOD

Pomisao na riječ kriptografija nas uglavnom podsjeti na zaštitu elektroničke pošte, bankovne račune, sigurnost mreže odnosno interneta kojeg koristimo kod kuće. Iza tih misli o navedenoj znanstvenoj disciplini se krije niz od najjednostavnijih matematičkih metoda i algoritama do najsuvremenijih računalnih programa koji se koriste za postizanje kranjih ciljeva. Kriptografijom se prvenstveno koriste oružane snage te diplomatske službe, ali razvojem telekomunikacija i mnoge druge službe.

Kriptografija je znanost koja se bavi logičkom promjenom informacije podataka. Ona se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati. Drugim riječima, glavni zadatak kriptografije je omogućiti sigurnu i nesmetanu komunikaciju dvjema osobma preko nesigurnog komunikacijskog kanala. Današnja upotreba komunikacije, prijenosa podataka i informacije bila bi nezamisliva bez enkripcije. Sigurnu komunikaciju koristimo kao vlasnici mobilnog uređaja gdje svaki uređaj posjeduje šifriran prometni kanal do davatelja usluge. Korištenjem internet trgovanja upotrebljavamo šifriran kanal između računala te davatelja usluge u trgovine.

Kriptografija je podgrana znanstvene discipline pod nazivom kriptologija. Kriptologija se sastoji od dvije podgrane, to su kriptografija i kriptoanaliza. Ona se kroz kriptografiju, koristeći rezultate kriptoanalize, bavi otkrivanjem novih metoda za zakrivanje podataka, te uz obrnuti proces bavi oktrivanjem novih metoda za otkrivanje zakrivenih podataka. Za što bolje razumjevanje ovih grana potrebno je znati objasniti značenje riječi šifriranje, dešifriranje i ključa. Šifriranje predstavlja metodu transformiranja izvornog poznatog sadržaja u neprepoznatljiv sadržaj. Dešifriranje predstavlja obrnuti proces odnosnu konverziju neprepoznatljivog sadržaja u izvorni. Ključ u kriptologiji predstavlja parametar ili podatak koji korisniku omogučuje šifriranje ili dešifriranje sadržaja.

Tablica 1.1. Podjela kriptologije.

Kriptologija	
Kriptografija	Kriptoanaliza
- Simetrični algoritmi - Asimetrični algoritmi - Kriptografski protokoli	- *brute force* metoda - Analiza frekvencije slova - Ostale metode

Cilj završnog rada je da posluži kao materijal za učenje studentima, odnosno skripta predmeta koja će se baviti diskretnom matematikom ili informacijskim sustavima, i samim prikazom matematičkih metoda kojim se služimo unutar kriptografije.

2. MODULARNA ARITMETIKA

2.1 UVOD U MODULARNU ARITMETIKU

U ovom poglavlju će se koristiti nekoliko metoda šifriranja iz klasične kriptografije kako bi se upoznala primjena modularne aritmetike. Metode šifriranja iz klasične kriptografije danas nisu toliko u upotrebi. Unatoč tome modularna aritmetika se koristi u svim granama moderne kriptografije. Koristi se u simetričnim, a najviše asimetričnim algoritmima.

Kriptografija i kriptografski sustavi se baziraju računanjem u određenim matematičkim metodama. Jedno od glavnih pravila u modernoj kriptografiji je da se računanja izvode u konačnom iliti određenom skupu. Skupovi brojeva na koje smo uglavnom naviknuti, kao primjerice skup prirodnih brojeva ili skup realnih brojeva čine skup neograničenih brojeva. U sljedećem dijelu modularna aritmetika će biti predstavljena kroz životne primjere.

Primjer 1.1 Za ovaj primjer uzimamo prikaz sata u 12 satnom mjerenju vremena (24 sata su podijeljena na 2 perioda, prijepodne i poslijepodne)

Krenemo li s brojanjem sati dobijemo ovakav rezultat :

$$1h, 2h, 3h, 4h, 5h, 6h, 7h, 8h, 9h, 10h, 11h, 12h, 1h, 2h, 3h \ldots 10h, 11h, 12h$$

Zaključak: Dodavanjem brojeva nikada ne napuštamo određeni skup.

Slika 2.1. Prikaz skupa brojeva na satu (izvor: http://educationwithfun.com/pluginfile.php/881/mod_page/intro/ill2.PNG)

Primjer 1.2 Za ovaj primjer uzimamo skup brojeva:

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

Možemo izvoditi sve računske operacije sve dok je rezultat manji od 9. Primjerice:

$$2 + 1 = 3$$
$$7 - 4 = 3$$
$$3 \cdot 2 = 6$$
$$8/2 = 4$$

U suprotnome kada pokušavamo operaciju tipa 6 + 7 moramo koristiti određeno pravilo. Uzimamo dobiveni broj u ovome slučaju te ga dijelimo sa 9.
Pošto je 6 + 7 = 13, tada 13/9 i dobivamo ostatak 4. Matematički to zapisujemo na sljedeći način:

$$6 + 7 \equiv 4 \bmod 9$$

Definicija modulo iliti operatora ostatka se temelji na uređenoj trojci (a, r, m) za koje vrijedi :

- *a* je definiran brojem dobiven operacijskim radnjama unutar određenog skupa
- *m* definira broj određenog skupa
- *r* definira ostatak

Neka su *a*, *r*, $m \in \mathbb{Z}$, dok je $m > 0$
Tada zapisujemo: $a \equiv r \bmod 9$, AKO *m* dijeli *a-r* u matematičkom zapisu: $\frac{m}{a-r}$

Primjer 1.3

Uzmimo *a* koji iznosi 32 te *m* koji iznosi *24.*

$$32 \equiv 8 \, mod \, 24$$

Provjera: $m / (a - r) = 24 / (32 - 8) = 24 / 24 = 1$

Zaključak: zapis je ispravan i točan!

2.1.1 Računanje ostatka

Kada zapisujemo $a, m \in \mathbb{Z}$, a možemo definirati i na sljedeći način:

$a = q \cdot m + r$

Ovdje je q definiran kao kvocijent.

Primjer 1.4 U ovom primjeru su prikazani načini korištenja kvocijenta i ostatka

Neka su: $a = 42$, $m = 9$

$a = 4 \cdot 9 + 6$

$r = 6$

nakon čega slijedi provjera: $\frac{m}{(a-r)} = \frac{9}{36}$ gdje vidimo da je izračun moguč.

Neka su: a = 42, m = 9

$a = 3 \cdot 9 + 15$ Provjera: $\frac{m}{(a-r)} = \frac{9}{27}$ Ispravno!

$r = 15$

Neka su: a = 42, m = 9

$a = 5 \cdot 9 + (-3)$ Provjera: $\frac{m}{(a-r)} = \frac{9}{45}$ Ispravno!

$r = -3$

Iz navedenih primjera možemo zaključiti da promjenom kvocijenta u izračunu dobijemo različite ostatke.

2.1.2 Klase ekvivalencije

U prošlom poglavlju je pokazano kako promijenom kvocijenta dolazi do promjene ostatka ali da su svi načini matematički točni i ispravno zapisani. Iza toga se krije sustav koji dopušta takve iznimke u matematici, a to su klase ekvivalencije.

Za određeni modulo iliti operator ostatka, nije bitno koji element uzimamo za računanje sve dok spada u njegove klase ekvicalencije. Veliki dio tih klasa se koristi se koristi u računanju današnje primjenjene kriptografije. Ako računamo pomoću prepravljenog modulo što je u većini slučajeva u kriptografiji tada smo u mogučnosti izabrati element iz klase koji nam rezultiraju najlakši put računanja.

Primjer 1.5 Klase ekvivalencije modulo 5

$$\{\dots -25, -20, -15, -10, -5, 0, 5, 10, 15, 20, 25 \dots\} \text{ – Klasa A}$$
$$\{\dots -24, -19, -14, -9, -4, 1, 6, 11, 16, 21, 26 \dots\} \text{ – Klasa B}$$
$$\{\dots -23, -18, -13, -8, -3, 2, 7, 12, 17, 22, 27 \dots\} \text{ – Klasa C}$$
$$\{\dots -22, -17, -12, -7, -2, 3, 8, 13, 18, 23, 28 \dots\} \text{ – Klasa D}$$
$$\{\dots -21, -16, -11, -6, -1, 4, 9, 14, 19, 24, 29 \dots\} \text{ – Klasa E}$$

Primjenimo to sada na:
$13 \cdot 16 - 8 = 208 - 8 \equiv ? \bmod 5$ i odmah zaključujemo da ostatak možemo dobiti na lakši način. To možemo uraditi tako da svaki element u računanju zamjenimo s drugim elementom iz iste skupine gdje se nalazi. Na primjer:

$$3 \cdot 1 - 3 = 3 - 3 \equiv 0 \bmod 5 \ \ ili$$

$$8 \cdot 6 - (-7) = 48 + 7 \equiv 55 \bmod 5$$

Jedna od glavnih računskih operacija u praktički svim zapisima enkripcije javnog ključa je matematička metoda eksponencije u zapisu $x^e \bmod m$ gdje su x, e, m cijeli brojevi velikog iznosa, u

području oko 2048 bita svaki. Primjer upotrebe ove metode je korištenje u računalnom softveru, točnije internet pretraživaču. Povezivanjem na stranicu velike razine sigurnosti ona koristi enkripciju javnog ljuča koja je osnovana na ovoj matematičkoj metodi - ključa. Takve stranice mozemo prepoznati po kratici *https* odnosno *Hypertext Transfer Protocol*.

Primjer 1.6. Računanje eksponencijama

$$3^8 \; mod \; 7 \equiv ?$$

1. način $3^8 = 6561 \equiv 2 \bmod 7$

Postupak: $6561/7 = \; 937$ i ostatak 2

2. način $3^8 = 3^4 \cdot \; 3^4 = 81 \; \times 81$

sada 81 mijenjamo brojem iz iste klase ekvivalencije modulo broja 7, a to je 4 ($81/4 \; = 11$ i ostatak 4). Slijedi zapis:

$$3^8 = 4 \cdot 4 = 16 \bmod 7$$

Odakle možemo lagano izračunati i zapisati kao $16 \; \equiv 2 \; \bmod 7$

Zaključak je da su oba načina matematički ispravna, ali u kriptografiji postoji pravilo gdje se bira najmanji pozitivni broj iz određene klase ekvivalencije nekog modulo. Tim postupkom nema potrebe za korištenjem kalkulatora pri eskponenciranju, što smo u prvom načinu ovog primjera koristili.

2.2 OSNOVE ALGEBRE U MODULARNOJ ARITMETICI

Modularnu aritmetiku definiramo kao aritmetički sustav kod kojeg se elementi odnosno brojevi vračaju u krug nakon što dosegnu određenu vrijednost tj. modulo. U kriptografiji koristimo komutativne prstene cijelih brojeva. Što je prsten u teoriji algebre?

Prsten je definiran kao neprazan skup s dvjema binarnim operacijama, to su zbrajanje množenje elemenata prstena. Pošto se u ovom slučaju radi o skupu cijelih brojeva tada prsten možemo definirati na ovaj način:

Skup $\mathbb{Z}_m = \{0,1,2,3 \dots, m-1\}$

Operacije: 1. $a + b \equiv c \bmod m,\ c \in \mathbb{Z}$

2. $a \cdot b \equiv d \bmod m, c \in \mathbb{Z}$

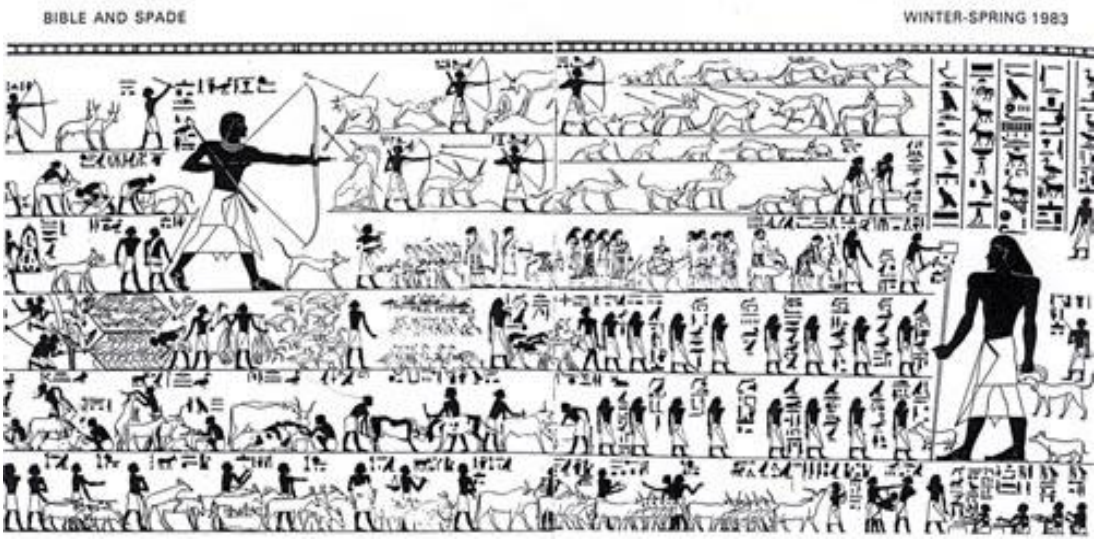
Takav prsten ima svojstva i pravila koja se poštuju kako bi rezultati ostali uvijek unutar vrijednosti skupa tog prstena. Ovo su najvažnija svojstva:

- asocijativnost zbrajanja: $(a + b) + c = a + (b + c)$
- suprotni element $-a \in \mathbb{Z}$ takav da je: $a + (-a) = (-a) + a = 0$
- komutativnost zbrajanja: $a + b = b + a$
- neutralni element za zbrajanje: $a + 0 = 0 + a = a$
- asocijativnost množenja: $(a \cdot b) \cdot c = b \cdot (a \cdot c)$
- zakon distributivnosti: $a \cdot (b + c) = ab + ac\ (a + b) \cdot c = ac + bc$

3. KLASIČNA KRIPTOGRAFIJA

3.1. POVIJEST KRIPTOGRAFIJE

Kada je u pitanju kriptografija, jedan od prvih primjera tajnog zapisa potječe iz Starog Egipta u periodu vladavine XII dinastije (1919. do 1783. godine p.n.e.). Pronađeni su u grobnici plemića Khnumhotepa II. Zapis je iscrtan slikama tadašnjeg plemićkog života. Za zapis su korišteni standardni hijeroglifi uz primjenu djelomične zamjene hijeroglifa drugima kako bi se dobio zakriveni zapis.

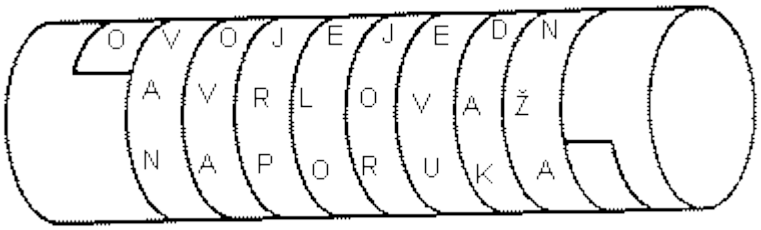


Slika 3.1. Šifrirani zapis u grobnici Khnumhotepa II. (izvor: http://www.biblearchaeology.org/image.axd?picture=2009%2F9%2FBeni-Hasan-Drawing.jpg)

Porijeklo riječi kriptografija dolazi od izvedenice grčkog pridjeva *kriptos* (što znači skriven) i glagola *grafo* (što znači pisati). Po tome možemo zaključiti da se najraniji zapisi o tajnom pisanju korišteni u ratne svrhe upravo nalaze s tog područja. Herodot je u svom dijelu „Historije“ pisao o sukobima Grčke i Perzije koji su se odvijali pet stoljeća prije Krista. U tome zapisu Herodot objašnjava kako je Grke spasilo tajno pisanje jer su tako bili obavješteni unaprijed o napadima Perzijanaca te su to iskoristili za svoju korist u bitci.

3.1.1 Skital

Kriptografski uređaj koji se koristio za šifriranje poruka je Skital. Skital je koristio metodu transpozicije odnosno slovima se mijenjao položaj u rečenici. Uređaj je se koristio na taj način da se oko štapa namota vrpca na kojoj bi bila ispisana poruka. Kako bi se poruka mogla ispravno pročitati potrebno je znati promjer štapa jer u protivnome vrpca ispada kao niz bezmislenih znakova.



Slika 3.2. Skital (izvor: http://e.math.hr/vigenere/skital.gif)

Primjer 1:

Orginalna poruka sa slike 2 je: OVO JE JEDNA VRLO VAŽNA PORUKA.

U slučaju da vrpca ne dođe do primatelja poruke već nekog stranca njemu će biti niz slova:

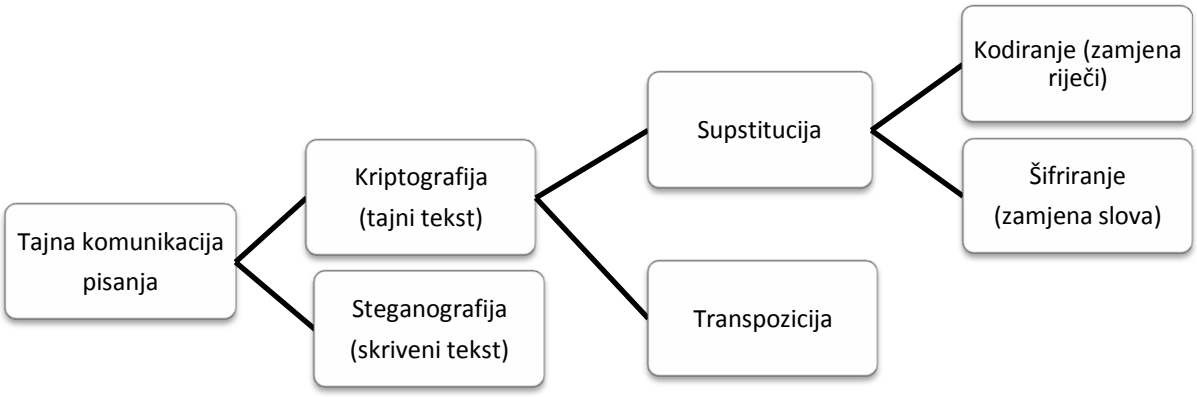
OVANO VAJRPELOJ OREVUDAKNŽA

3.2 PODJELA TAJNE KOMUNIKACIJE PISANJA KROZ POVIJEST

Tajnu komunikaciju kroz povijest djelimo na dvije glavne podjele. To su steganografija te kriptografija. Steganografija je definirana tako da se skriva sama postojanost poruke. Pod steganografiju spada pisanje takozvanom nevidljivom tintom. Steganografija je imala široku primjenu. Nevidljivu tintu moguće je bilo dobiti iz tekućine biljke mlječike. Tinta bi nestala kada se osuši, te bi se ponovno pojavila postepenim zagrijavanjem podloge.

Uz steganografiju se razvila kriptografija. Za kriptografiju je već navedeno objašnjenje u prijašnjem poglavlju. Kriptografiju dijelimo u dvije grane kroz metodu enkripcije, a to su kroz metodu transpozicije i metodu supstitucije.

Tablica 3.1. Podjela tajne komunikacije pisanja



3.3 TRANSPOZICIJA

U ovoj metodi šifriranja se jednostavno koristimo premještanjem slova otvorenog teksta te tako dobivamo anagram. U slučaju korištenja malog broja slova, ova je metoda nesigurna za slanje poruka zbog malog broja kombinacija kojim se orginalna poruka može probiti.

Primjer 1:
Otvoreni tekst: OVA
Broj mogućih transpozicija: 6 (3 faktorijela)
Moguće transpozicije: OVA, VAO, AVO, OAV, AOV, VOA.
Kod poruke s velikim brojem znakova ova metoda je sigurna za šifriranje, jer je teška za dešifriranje i željenom primatelju poruke. Zbog toga ova metoda nije bila najbolje rješenje. U slučaju korištenja poruke s 25 različitih znakova, broj kombinacija se može posložiti na 25 faktorijela što je otprilike 15^{24} načina zapisa. U tom slučaju potrebno je sa primateljem unaprijed dogovoriti transpozicijsku metodu kojom se koristi pošiljatelj. Jedan od primjera metode transpozicije je već navedeni uređaj Skital koji je opisan u jednom prošlih poglavlja.

3.3.1 Izmjenična transpozicija

Primječujemo da transpozicija osigurava visok postotak tajnosti poruke, ali je nedostatak što u većini slučajeva zadaje probleme u oktrivanju poruke i samom primaocu kome je poruka namjenjena. Kako bi se to izbjeglo pošiljatelj unaprijed dogovara matematičku metodu kojom će primaoc poruke lakše pročitati orginalni sadržaj poruke koji mu je namjenjen. Jedna od tih metoda je izmjenična transpozicija. Kod ove se metode slova poruke naizmjenice pišu u gornji i donji redak, pa se na kraju nadovežu jedan na drugi. Otvoreni tekst se transpozicionira u broj redaka određen ključem. U sljedečem primjeru ključ transpozicije iznosi 2 odnosno $K_T = 2$.

Primjer 2.

Otvoreni tekst: DISKRETNA MATEMATIKA

Transpozicija: D S R T A A E A I A
I K E N M T M T K

Skrivena poruka ili šifrat: DSRTNAAEAIAIKENMTMTK

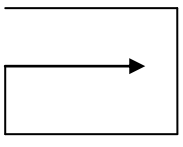
3.3.2 Transpozicija s obilaskom

Pri korištenju ove metode slova poruke se pišu u polje zadanih dimenzija, a šifrat dobivamo korištenjem ključa koji opisuje obilazak polja.

Primjer 3.

Otvoreni tekst: DISKRETNA MATEMATIKA

Tranpszicija: D K T M E T A
I R N A M I
S E A T A K



Ključ: u smjeru kazaljke na satu s početkom od lijevog desnog kuta, spiralno prema unutra

Šifrat: DKTMETAKATAESIRNAMI

3.3.3 Stupčasta transpozicija

Kao što sam naziv ove metode govori, slova otvorenog teksta zapisujemo u redke manjih duljina te iz čitamo stupac po stupac. Duljinu redaka određujemo ključnom riječi, a sami redoslijed čitanja stupca je određeno abecednim poredkom slova u ključnoj riječi.

Otvoreni tekst: THE ALCHEMIST BY PCOELHO
Ključna riječ: DREAM
Čitanje : 2 5 3 1 4
Transpozicija: T H E A L
A L C H E
M I S T B
Y P C O E
L H O

Šifrat: AHTOTAMYLECSCOLEBEHLIPH

3.4 SUPSTITUCIJA

Supstituciju definiramo kao matematičku metodu gdje svako slovo ili znak mijenja svoj identitet, ali zadržava svoje mjesto. Jedan od prvih zapisa ove knjige nalazimo u *Kama Sutri* koju je sabrao Mallanaga u 3. stoljeću. Taj zapis predstavlja određenu filozofiju u Indiskoj hinduističnoj religiji koja opisuje 64 vještine koje žene trebaju savladati a jedno od njih je i tajno pisanje, za prikrivanje detalja njihovih ljubavnih veza. Tehnika je jednostavno definirana nasumičnim povezivanjem slova abecede, nakon čega se sparuju (slova otvorenog teksta se zamjenjuju nasumično odabranim parovima).

Primjer 1.
Otvoreni tekst: MATEMATIKA
Supstitucija: M → G, A → R, T → N, E → O, I → P, K → L
Šifrat: GRNOGRNPLR

3.4.1 Cezarova šifra

Prva primjena supstitucijske šifre u vojne svrhe pojavljuje se u Galskim ratovima Gaja Julija Cezara. Njegova šifra nastaje pomicanjem abecede za 3 mjesta. Svakom slovu otvorenog teksta odgovara jedinstveno slovo abecede koje ga zamjenjuje, te zbog toga ovaj tip šifre nazivamo i monoalfabetska šifra.

Neka je otvoreni tekst označen oznakom *x*, dok je šifrirani tekst *y*, a ključ oznakom *k* tada možemo zapisati: $x,y,z \in Z_{26}$.

Iz toga možemo zaključiti: Enkripcija: e_k (x)≡ $x + k$ mod 26

Dekripcija: d_k (y)≡ $y - k$ mod 26

Tablica 3.2. Cezarova šifra

A 0	B 1	C 2	D 3	E 4	F 5	G 6	H 7	I 8	J 9	K 10	L 11	M 12
N 13	O 14	P 15	Q 16	R 17	S 18	T 19	U 20	V 21	W 22	X 23	Y 24	Z 25

Primjer 1.

Otvoreni tekst = DISKRETNA

Ključ k = 12

DISKRETNA = x_1, x_2, x_3 .... x_9 = 3, 8, 18, 10, 17, 4, 19, 13, 0.

Šifrat je tada izračunat kao:

y_1, y_2, y_3 .... y_9 = 15, 20, 4, 22, 3, 16, 5, 25, 12 = PUEWDQFZM

3.4.2. Afina šifra

Afina šifra je poseban slučaj supstitucijske šifre. Pošto su sve dotadašnje supstitucijske šifre 26! permutacija od 26 elemenata, potrebno je bilo razviti funkciju sigurnijeg sustava. To je postignuto

time da se u funkciju za šifriranje dodaje više od jednog parametra. Ovdje su to parametri a i b. Funkcija enkripcije i dekripcije Afine šifre:

neka su $x, y, a, b \in \mathbb{Z}_{26}$

Enkripcija: $e_k(x) = y \equiv a \cdot x + b \bmod 26$

Dekripcija: izvučemo iz enkripcije na sljedeči način:

$$d_k(y) = y \equiv a \cdot x + b \bmod 26$$

$$a \cdot x + b \equiv y \bmod 26$$

$$a \cdot x \equiv (y - b) \bmod 26$$

$$x \equiv (y - b) \bmod 26/a$$

$$x \equiv a^{-1} \cdot (y - b) \bmod 26$$

Najlakše odredimo broj b elemenata iz funkcije enkripcije, a to su: 0,1,2,3…25 $\#b$ = 26
Pogledom na Afinu funkciju enkripcije zaključujemo da nema uvjeta i ograničenja za elemente a te da ih možemo prebrojati kao b elemente. Razlika je što a nema istu funkciju u dekripciji odnosno koristimo inverzni a parametar što rezultira ograničenjem broja elemenata.
Uvjet za a elemente je korištenje NZD $(a, 26) = 1$. NZD označava največeg zajedničkog djelitelja argumenata u zagradi. Pošto je $2 \cdot 13 = 26$, a NZD $(a, 26) = 1$, za elemente parametra $a \in \mathbb{Z}$ vrijede sljedeči brojevi: $1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25$.

Uzmemo li za parametar b 26 brojeva iz skupa $\mathbb{Z}_{26}$ a za parametar mogućih 12 množenjem tih dvaju elemenata dobijemo Afinu šifru s 312 ključeva.

$$26 \cdot 12 = 312, \#k = 312$$

Zaključujemo da ključ s prostorom od 312 elemenata može zagorčati život nekome tko pokušava vršiti dekripciju *brute-force* napadom. Afina šifra se smatra poboljšanom verzijom Cezarove, ali u principu ima jednake slabosti jer je lako dešifrirati metodom učestalosti slova.

3.4.3 Vigenerova šifra

Pojavom korištenja metode analize frekvencija slova u kriptoanalizi šifriranje više nije bilo sigurno kao prije. Time su ljudi bili promorani naći nove metode šifriranja. Trebalo je osmisliti novu, jaču šifru, koja će nadmudriti kriptoanalitičare. Dotadašnje su supstitucijske šifre koristile samo jednu abecedu za enkripciju poruke, te je zbog toga predloženo korištenje više njih koje bi promiješale unutar jedne poruke.

Prva izrada ovog načina šifriranja poruke je bio Albertijev sustav te se vršio na sljedeći način kao u tablici 3.3 :

- gdje su u prvom redu obična abeceda, a u drugom i trečem šifrirane abecede

Tablica 3.3. Šifrirane abecede

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

Albertijev sustav se temeljio na tome da poruku možemo enkriptirati naizmjenice. Prvo slovo enkriptirano iz prve šifrirane abecede, sljedeće iz druge i tako naizmjenice. Primjerice želimo enkriptirati poruku „MATEMATIKA“ iz tablice 2.2. Šifrat poruke matematika glasi „WSDVWSDYUS“.

Albertijev sustav je kasnije razgrađen od Blaise de Vigenere, pa je nova šifra nazvana po njemu odnosno Vigenerova šifra. Pošiljatelj poruke bi korištenjem jedne abecede šifrirao poruku Cezarovom šifrom, ali ova metoda mu omogućuje šifriranje slova različitim abecedama. Postupak započinje izradom Vigenerovog kvadrata, odnosno prikaz otvorene abecede i 26 različito šifriranih abeceda, koje nastaju pomakom za jedno mjesto u desno. Ključ koristi niz od m znakova. Ključ se potpisuje ispod otvorenog teksta i to tako da se ponavlja sve dok ne dođemo do kraja riječi, koji se rasporedi u onoliko blokova koliko iznosi razlika broja slova otvorenog teksta i ključne riječi.

	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 3.3. Vigenerov kvadrat

Primjer 3.4 Enkripcija poruke DISKRETNAMATEMATIKA korištenjem Vigenerovog kvadrata s ključnom riječi OSIJEK.

Tablica 3.4. Enkripcija korištenjem Vigenerovog kvadrata

Otvoreni tekst:	D	I	S	K	R	E	T	N	A	M	A	T	E	M	A	T	I	K	A
Ključna riječ:	O	S	I	J	E	K	O	S	I	J	E	K	O	S	I	J	E	K	O
Šifrirana poruka:	R	A	A	T	V	O	H	F	I	U	E	D	S	E	I	C	M	U	O

Najveća prednost ovog način šifriranja što za razliku od prethodnih nije osjetljiv na metodu kriptoanalize odnosnu analizu frekvecije slova. Prednost je odabir broja ključeva. Ključ može biti sastavljen i odabran od nasumičnih slova sve do citata ili slično. U slučaju uzimanja ključne riječi koja je krača od otvorenog teksta, ponavljamo ključnu riječ sve dok svaki slovo iz otvorenog teksta ima svoje slovo ključne riječi. Ova vrsta šifriranja spada u polialfabetske jer koristi više šifriranih abecede, dok su dotašnje zbog korištenja samo jedne abecede bile zvane monoalfabetske šifre.

3.4.4 Hillova šifra

Polialfabetska šifra odnosno Vigenerova šifra pružala je daleko sigurniji način enkripcije i slanja poruke. Ljudi su se fokusirali na ravoju polialfabetskih šifra. Lester Hill je 1929. godine izumio kriptosustav kod kojeg se *m* slova otvorenog teksta zamjenjuje s *m* slova u šifratu. U slučaju da broj slova otvorenog teksta nije djeljiv s *m*, poruku treba nadopuniti kako bi mogla biti podjeljenja u blokove od *m* slova.

Ključ je u ovoj šifri definiran matricom K dimenzija $m \times m$. Element u matrici definiramo po njegovom položaju, odnosno ako je u *i*-tom redku i *j*-tom stupcu zapisujemo element kao $k_{(i,j)}$. Za elemente otvorenog teksta $x = (x_1, x_2)$ i elemente šifrata $y = (y_1, y_2)$ zapis u matrici vrijedi na sljedeči način: $(x_1, x_2, x_3 .. x_m) = (y_1, y_2, y_3 .. x_m)$

$$\begin{pmatrix} k_{1,1} & k_{1,2} & \cdots & k_{1,m} \\ k_{2,1} & k_{2,2} & \cdots & k_{2,m} \\ \vdots & \vdots & & \vdots \\ k_{m,1} & k_{m,2} & \cdots & k_{m,m} \end{pmatrix},$$

Primječujemo da se radi u linearnoj transformaciji, te da se *x* može izračunati iz *y*, odnosno obrnuto kako bi šifrat dešifrirali. Za dešifriranje poruke koristimo se linearnom algebrom, odnosno inverznom matricom ,K^{-1}..

Neka nam je *m* fiksan prirodan broj. Za *k* odnosno ključ možemo definirati uporabu $m \cdot m$ matrice. Primjerice neka nam je $m = 2$, elemente otvorenog teksta možemo zapisati $x = (x_1, x_2)$, a elemente šifrata $y = (y_1, y_2)$. Prepoznajemo da su elementi šifrata linearne kombinacije otvorenog teksta te onda ih možemo zapisati na sljedeči način:

$$y_1 = (4x_1 + 6x_2 \bmod 26)$$

$$y_2 = (7x_1 + 9x_2 \bmod 26)$$

Zapisujemo ih u obliku matrice: $(y_1, y_2) = (x_1, x_2) \begin{pmatrix} 4 & 7 \\ 6 & 9 \end{pmatrix}$

U sljedečih nekoliko primjera su objašnjene matematičke operacije u enkripciji i dekripciji Hillove šifre.

Primjer 1. Matrica s računanjem operatora ostatka

$$\begin{pmatrix}3 & 7\\ 5 & 12\end{pmatrix}\cdot\begin{pmatrix}8\\ 5\end{pmatrix}=\begin{pmatrix}3\cdot 8+(7\cdot 5)\\ 5\cdot 8+(12\cdot 5)\end{pmatrix}=24+35-40+60=59-100=7-22 \bmod 26$$

Primjer 2. Želimo šifrirati otvoreni tekst HATS. Riječ dijelimo na 2 dijela HA koji odgovara numeričkom ekvivalentu [7,0], i TS koji odgovara ekvivalentu [19,18]. Pretpostavimo da je ključ matrica $K=\begin{pmatrix}3 & 3\\ 2 & 5\end{pmatrix}$

Enkripcija sloga HA: $\begin{pmatrix}3 & 3\\ 2 & 5\end{pmatrix}\cdot\begin{pmatrix}7\\ 0\end{pmatrix}=\begin{pmatrix}3\cdot 7+(3\cdot 0)\\ 2\cdot 7+(5\cdot 0)\end{pmatrix}=21-14 \bmod 26$

Enkripcija sloga TS: $\begin{pmatrix}3 & 3\\ 2 & 5\end{pmatrix}\cdot\begin{pmatrix}19\\ 18\end{pmatrix}=\begin{pmatrix}3\cdot 19+(3\cdot 18)\\ 2\cdot 19+(5\cdot 18)\end{pmatrix}=111-128=7-24 \bmod 26$

Šifrirana poruka iznosi brojeve redoslijedom $21, 14, 7, 24$ koji su ekvivalentni slovima VOHY

Primjer 3. Obrnutim postupkom želimo dešifrirati dobiveni šifrat DBBS iz prethodnog primjera

Za dešifriranje nam je potrebna inverzna matrica od $\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ odnosno $\begin{pmatrix}d & -b\\ -c & a\end{pmatrix}$

Tako ključ iz prethodnog zadatka zapisujemo ovako: $\begin{pmatrix}3 & 3\\ 2 & 5\end{pmatrix}$ postaje $\begin{pmatrix}5 & -3\\ -2 & 3\end{pmatrix}$

Formula za računanje determinante je $(a\cdot d)-(b\cdot c)$

Determinanta ključa iznosi $\begin{pmatrix}3 & 3\\ 2 & 5\end{pmatrix}=3\cdot 5-3\cdot 2=15-6=9$

Sada nam je potreban umnožak ključa i inverzne matrice ključa odnosno ,k^{-1} pa množimo:

$$9\cdot\frac{1}{9}=1$$

Sada je pitanje kojim brojem trebamo pomnožiti 9 da bi dobili 1 mod 26. Odgovor:

$$9 \cdot 3 = 27 \bmod 26, \text{ odnosno } 1 \bmod 26$$

Izračunamo mod 26 inverzne matrice ključa: $\begin{pmatrix} 5 & -3 \\ -2 & 3 \end{pmatrix} \bmod 26 = \begin{pmatrix} 5 & 23 \\ 24 & 3 \end{pmatrix}$

Zatim dobivanu matricu množimo s 3 jer smo 3 koristili kao kvocijent u dobivanju inverzne matrice.

$$\begin{pmatrix} 5 & 23 \\ 24 & 3 \end{pmatrix} \cdot 3 = \begin{pmatrix} 15 & 69 \\ 72 & 9 \end{pmatrix} = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \bmod 26$$

Napokon smo dobili ključ dešifriranja poruke k^{-1}.= $\begin{pmatrix} 5 & 23 \\ 24 & 2 \end{pmatrix} \bmod 26$.

Ponovno dijelimo šifrat na 2 sloga i dodajemo im numeričke ekvivalente [V,O] – 21,14 i

[H,Y] – 7, 24.

Dekripcija sloga VO: $\begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \cdot \begin{pmatrix} 21 \\ 14 \end{pmatrix} = \begin{pmatrix} 15 \cdot 21 + (14 \cdot 17) \\ 21 \cdot 20 + (14 \cdot 9) \end{pmatrix} = \begin{pmatrix} 553 \\ 546 \end{pmatrix} = \begin{pmatrix} 7 \\ 0 \end{pmatrix} \bmod 26$

Dekripcija sloga HY: $\begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 24 \end{pmatrix} = \begin{pmatrix} 15 \cdot 7 + (24 \cdot 17) \\ 24 \cdot 20 + (24 \cdot 9) \end{pmatrix} = \begin{pmatrix} 513 \\ 356 \end{pmatrix} = \begin{pmatrix} 19 \\ 18 \end{pmatrix} \bmod 26$

Dešifriranjem poruke VOHY dobijemo brojeve 7, 0, 19, 18 koji su ekvivalentni poruci HATS što smo i u prethodnom primjeru šifrirali. Zaključak je da su primjeri točni.

3.5 KRIPTOANALIZA U KLASIČNOJ KRIPTOGRAFIJI

Kriptoanaliza je znanstvena disciplina i dio kriptologije koja proučava metode otkrivanja značenja kriptiranih informacija bez pristupa tajnim informacijama za dekripciju odnosno ključa, te metode otkrivanja samog ključa uz poznavanje otvorenog teksta. Zbog rasta složenosti kriptografije su se tehnike i metode kriptoanalize mijenjale tijekom povijesti. Probijanje kriptografskog algoritma označava da je poznata metoda otkrivanja tajne poruke odnosno ključeva koji se koriste za dekripciju šifriranog teksta. Kriptografija i kriptoanaliza su međusobno povezane grane, jer kako bi se kreirala sigurna kriptografija, potrebno je bilo napraviti dizajn i sustav koji je prilagodljiv kriptoanalizi.

Kriptoanaliza kao pojam se smatra poprilično novim, no prve metode probijanja skrivenih poruka su puno starije. Prvo poznato objašnjenje kriptoanalize dao je u 9. stoljeću arapski matematičar Al-Kindi u djelu „Rukopis o dešifriranju kriptografskih poruka“. Knjiga najviše uključuje opis metode analize frekvencije slova. Ta metoda je najbolja za probijanje praktički svih šifriranih sustava koji su se javljali u klasičnoj kriptografiji. Uz metodu analize učestalosti, metoda koja se je najviše koristila je *brute-force* ili u prijevodu probijanje na silu koja definira metodu probijanja na taj način da je kriptoanalitičar pokušao sve kombinacije transpozicije ili supstitucije dok ne rezultira samim probijanjem. Nakon analize učestalosti je u Europi tijekom 15. Stoljeća razvijena metoda korištenja više šifriranih abeceda odnosno polialfabetski šifrat. Blaise de Vigenere je razvio tu ideju i primjenio je provođenjem uz vlastito osmišljeni sustav tj. Vigenerov kvadrat. U tom sustavu je za ključ korištena proizvolja riječ koja je uz kombinaciju šifriranih abeceda rezultirala sigurnu metodu prijenosa tajnih poruka. Ta metoda je dugo vremena smatrana potpuno sigurnom, sve dok Charles Babbage i Friedrich Kasiski nisu uspjeli probiti taj sustav. Tijekom Prvog svjetskog rata 20. stoljeću dolazi do velike potrebe tajnog prijenosa poruka najviše u vojne i političke svrhe. Izumitelji u Europi su razvili kružne mehanizme šifriranja kako bi spriječili ponavljanje koje je dovelo do probijanja Vigenerovog šifrata. Kako je kriptografija postala sve složenija, matematika je postala jako važna za razvijanje metode enkripcije i dekripcije. Važnost kriptografije i kriptoanalize najviše dolazi do izražaja za vrijeme Drugog svjetskog rata. Smatra se da su to grane koje su rezultirale samim ishodom rata. Najbolji primjer za to je razvoj stroja za šifriranje pod nazivom Enigma. Enigma danas predstavlja najzanimljiviji mehanički uređaj korišten

u povijesti za enkripciju i dekripciju poruka. Princip rada Enigme se temeljio na spojenim rotorima i razvodnim pločama. Njemačka je za vrijeme Drugog svjetskog rada koristila Enigmu za vojne svrhe te tako imala veliku taktičku prednost od neprijatelja. Dekripcija rada Enigme je uspješno je provedena od strane Britanaca pod vodstvom matematičara Alana Turinga.

Slika 3.4. Enigma (izvor: http://users.telenet.be/d.rijmenants/pics/hires-wehr3.jpg)

3.5.1 Provođenje kriptoanalize

Osnovna pretpostavka da se u kriptoanalizi zna koji se kriptosustav koristi pri probijanju. To se zove Kerckhoffovo načelo. Kriptoanaliza se provodi nagađanjem ključa ili korištenjem informacija o sustavu kojeg se pokušava enkriptirati. Razlikujemo nekoliko razina kriptoanalitičkih napada.

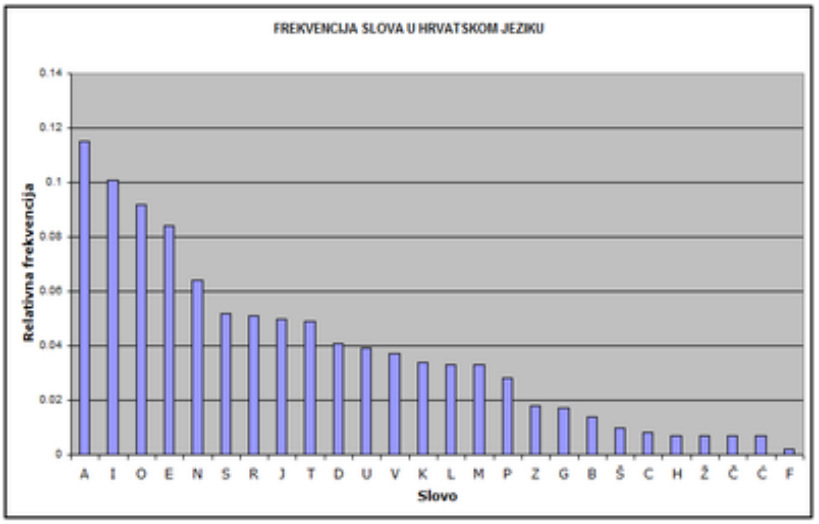
- Samo šifrirani tekst - napadač posjeduje pristup samo šifriranom tekstu
- Poznat otvoreni tekst – napadač posjeduje pristup šifriranom ali i otvorenom tekstu
- Izabrani otvoreni tekst - napadač je u mogučnosti odabira otvorenog teksta, te tako može dobiti njegov šifrat. Ova metoda je jača od prethodnih.
- Izabrani šifrirani tekst – napadač ima pristu alatu za dešifriranje, te teko bira šifrat kako bi otkrio otvoreni tekst

- Napad odgovarajućim ključem – kao prethodna metoda osim što napadač šifrirani tekst otkriva kombinacijom dvaju ključa
- Socijalni napad – ova metoda podrazumijeva: ucjene, potkupljivanje, krađe te slične metode kako bi se došlo do rezultata

3.5.2 Vrste kriptoanalize

Brute force odnosno napad silom je metoda uzastopnim pokušavanjem. To je jednostavna metoda koja se sastoji od sustavnog pronalaženja svih mogućih kandidata za rješenje i isprobavanja svakog od njih. Ova metoda je za probijanje zaporki, osim što je ova metoda jednostavna uvijek je i uspješna ako postoji rješenje. Najveći nedostatak i razlog zbog kojeg se ova metoda rijetko koristi su vrijeme i resursi potrebni za uspješnost. Ono proporcionalno raste s brojem mogučnosti za rješenje sustava.

Analiza učestalosti ili analiza frekvencije slova predstavlja proučavanje učestalosti pojave određenih slova ili grupe slova u šifriranom tekstu. Temelji se na tome da se u svakom dijelu šifriranog teksta određena slova i kombinacije pojavljuju s provjerenom vjerojatnošću. Za svaki jezik postoji određena distribucija pojave slova.



Slika 3.5. Distribucija slova u Hrvatskom jeziku (izvor: https://upload.wikimedia.org/wikipedia/commons/thumb/c/c2/Frekvencija_slova_hr.png)

Kasiski ispitivanje ili Kasiski metoda predstavlja metodu napada na šifru abecedne zamjene poput Vigenerove šifre. Temelji se na određivanju duljine ključne riječi te podijeli šifriranog teksta u n stupaca (gdje n predstavlja duljinu kodne riječi).

Računanje podudaranja je metoda usporedbe dva teksta uz računanje koliko se puta određeno slovo pojavljuje na istom mjestu u oba teksta. Rezultat koji se pokazuje kao ukupan broj ili normalizira dijeljenjem s očekivanim rezultatom, naziva se indeksom podudaranja.

4. MODERNA KRIPTOGRAFIJA

Danas je život bez kriptografije teško zamisliv. Koristimo se kriptografijom u svakodnevnim radnjama a da tog nismo ni svjesni. Kriptografija danas je primjenjena u elektroničkoj pošti, povezivanju na internet stranice, bankovne kartice, SIM kartice, trgovanje putem interneta, *online* putovnice i jedna popularna primjena danas su *Itunes* i *Kindle* koje zastupaju autorska prava pjesama odsnosno knjige te štite od zloupotrebe tuđeg materijala.

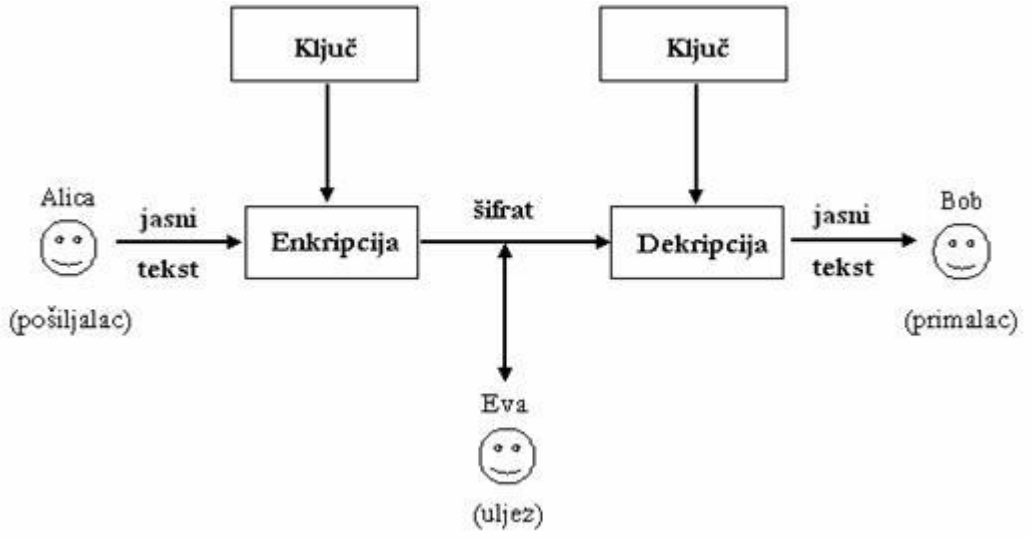
Pojavom računala i njihove široke uporabe završila je uporaba metoda klasične kriptografije. Najveća razlika između metoda klasične kriptografije i moderne je što su se metode klasične kriptografije temeljile na tajnom pisanju, odnosno matematičkim metodama tj. algoritmima kako bi se neka poruka šifrirala dok se metode moderne kriptografije temelje na tajnosti ključa. U modernoj kriptografiji je važnija tajnost ključa od tajnosti metode šifriranja. Postoje dvije metode koje definiraju kako ključ funkcionira u nekom kriptostustavu. Razlikujemo simetrične i asimetrične algoritme. Simetrični algoritam koristi jedan odnosno privatni ključ u kriptosustavu dok asimetrični koristi dva različita (javni i privatni) ključa.

4.1 SIMETRIČNI SUSTAV

Simetrični sustav u kriptografiji u slučaju enkripcije i dekripcije koristi jednak ključ. Sustav se bazira na tajnosti upotrebljenog ključa. Simetrični sustav u kriptografiji se koristi još zamjenskim nazivima kao što su: sustav s dijeljenim ključem, sustav s privatnim ključem i sustav s jednim ključem. U prošlosti se je razmišljalo na taj način kada imamo dvije funkcije, jednu za enkripciju i jednu za dekripciju da je siguran način prijenosa poruke jedino ako način šifriranja i dešifriranja držimo u tajnosti. To pravilo je vrijedilo sve dok Kerckhoff 1883. godine nije promijenio način djelovanja kriptografije. Kerckhoffov princip se temeljio na tome da je sustav u kriptografiji siguran i u slučaju kada su uljezu ili nekoj trečoj osobi poznati svi detalji sustava gdje se misli na algoritam enkripcije i dekripcije, osim ključa kriptografskog sustava.

Simetrična sustav u kriptografiji se ne bavi samo kriptiranjem, već i autentifikacijom. Najpoznatiji primjer takve tehnike su kodovi autentifikacije porukom (*message authentification codes,* ili skraćeno MAC). Problem u simetričnom sustavu kriptografije je što se i sam ključ prenosi, tu nastaje opasnost da uljez otkrije ključ. Stoga je negativna strana što je potreban dogovor između

pošiljatelja i primaoca poruke o ključu koji se koristi a da ga se ne domogne treča osoba. Simetrični sustav u kriptografiji isto tako ima i pozitivnu stranu, a to je puno veća brzina prijenosa od asimetričnog sustava. U raznim kriptografskim literaturama je u simetričnom sustavu pošiljatelj poruke nazvan Alice, primaoc Bob, dok je uljez ili neovlašteni korisnik nazvan Eve. Sustav je prikazana na slici 4.1.



Slika 4.1 Shematski prikaz simetričnog sustava (izvor: http://web.zpr.fer.hr/ergonomija/2005/rebac/images/simetrCrypto.gif)

Simetrične kriptografske algoritme dijelimo na:

- Algoritme koji kriptiraju blokove podataka
- Algoritme koji kriptiraju tokove podataka
- Kodovi autentifikacije poruke (MAC)

4.1.1 Šifre toka

Šifre toka (engl. *Stream Ciphers*) šifriraju svaki bit zasebno odnosno bit po bit. Za ključ ove šifre se koristi nizovni ključ koji je stvoren od niza bitova.

Prikaz osnovnih funkcija u šifri toka:

$$\text{Enkripcija: } y_i = e(x_i) = x_i + s_i \bmod 2$$

$$\text{Dekripcija: } x_i = e(y_i) = y_i + s_i \bmod 2$$

Prvo što možemo zaključiti iz funkcije enkripcije i dekripcije je da zbrajamo u obje funkcije. U

dosadašnjim primjerima kriptografije uvijek je postojala razlika odnosno u dekripciji se koristio suprotni operator od enkripcije.

Prikaz jednakosti funkcija tako da koristimo funkciju dekripcije:

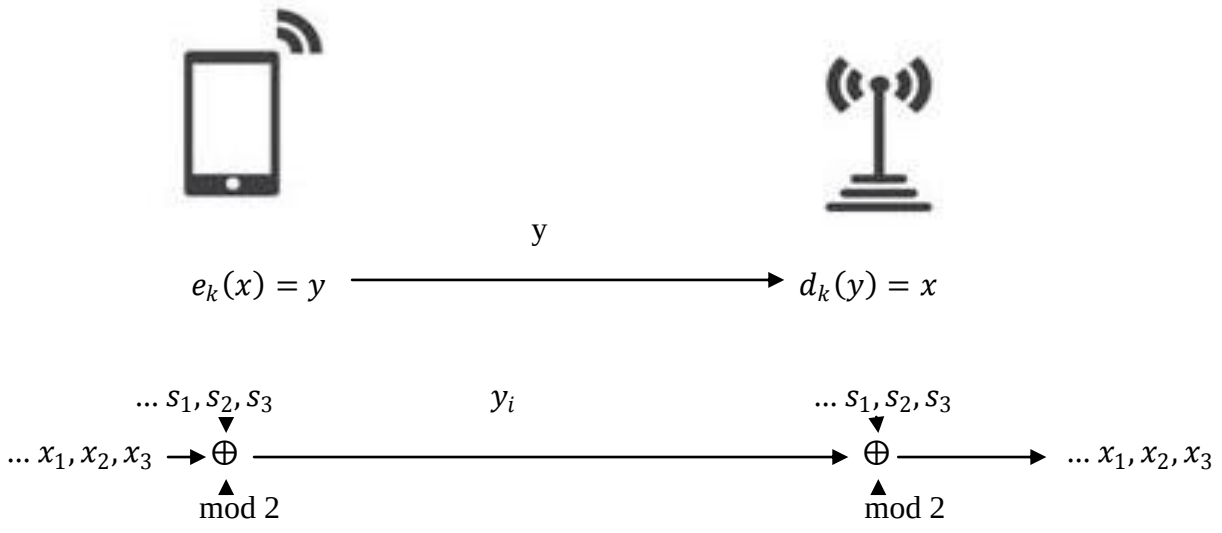
$$d(y_i) = y_i + s_i \bmod 2$$
$$d(y_i) = (x_i + s_i) + s_i \bmod 2$$
$$d(y_i) = x_i + 2s_i \bmod 2$$
$$d(y_i) = x_i$$

Objašnjenje: y_i se u prvom koraku zamijeni metodom supstitucije odgovarajućem ekvivalentu iz funkcije enkripcije. Uvijek će nam ispasti da imamo 2 nizovna ključa odnosno $2s_i$ što s modulo od 2 rezultira 0 i tako nam funkcija dekripcije ispada jednaka kao funkcija enkripcije.

Iz prethodnog prikaza zaključujemo sljedeće: $x_i, y_i, s_i \in \mathbb{Z}_2 = \{0,1\}$ - bitovi.

Primjenu šifre toka možemo objasniti u telefonskom pozivu s jednog mobilnog uređaja ka drugom. Poziv se ostvari tako da se mobilni uređaj prvo spoji preko vlastitog kanala na najbližu centralu pokrovitelja mreže. Tom kanalu nema nitko pristup osim samog pozivatelja. Kada se komunikacija između centrale uspostavi vrši se enkripcija nizom ključeva te se tako glas pozivatelja kvantizira po vremenskoj amplitudi na taj način da se ostvari kanal između njega i osobe koju je nazvao.

Primjer 4.1 Shematski prikaz komunikacije mobilnog uređaja i centrale gdje je znak $\oplus$ = mod 2.



Sada ćemo objasniti princip rada dodavanja mod 2 na niz bitova i nizovne ključeve.

Primjer 4.2. Zbrajanje mod 2

Tablica 4.1 Princip rada mod 2

x_i	s_i	y_i
0	0	0
0	1	1
1	0	1
1	1	0

Zaključak: Kada se u nizu ključeva s_i javlja bit 1 n on rezultira promjenom ulaznog bita odnosno 0 postaje 1, a 1 postaje 0 u tom slučaju. Uočavamo da dodavanje mod 2 funkcije djeluje isto kao logički sklip NILI (XOR) u elektrotehnici.

Primjer 4.2. Zbrajanje mod 2 u ASCII tablici

Tablica 4.2 Enkripcija ASCII znaka „A“

x_i	s_i	y_i	
1	0	1	
0	1	1	
0	0	0	
0	1	1	≡ mod 2 = NILI
0	1	1	
0	0	0	
1	1	0	

Enkripcijom šifre toka ASCII znaka „A“ smo dobili na izlazu niz bitova: 1101100 što u ASCII tablici predstavlja znak “*l*“.

Zaključujemo da dekriptirani niz ovisi o nizu ključeva koji koristimo. Glavno pitanje je koje nizove ključeva koristiti ? Kako bi se spriječilo nagađanje niza ključa napadom prisilne metode koristi se uređaj odnosno generator prividno slučajnih brojeva (engl. *random generator number).*

Generator slučajnih brojeva dijelimo na 3 tipa:

- Primjenjeni generator slučajnih brojeva
- Generator prividno slučajnih brojeva
- Kriptografski generator privodno slučajnih brojeva

U primjenjeni generator slučanih brojeva (engl. *True random number generator*) svrštavamo sve slučajne procese iz života gdje se fizički vrši takva radnja. Primjeri takvih slučajnih procesa su: bacanje kovanice, lutrija, rulet, posebni alati za enkripciju u računalu kao PGP alat (pokret miša, vrijeme između tipkanja) koji takve radnje koristi za generiranje slučajnih brojeva. Ovaj tip generiranja nije toliko bitan u kriptografiji, ali je primjenjen svaki dan u životu.

Generator prividno slučajnih brojeva (engl. *Pseudo random number generator*) sadrži kao što sam naziv otkriva privid ili nešto ne stvarno, odnosno generator slučajnih brojeva nije slučajan već je određen u stvarnosti. U ovom slučaju slučajni niz bitova je dobiven izračunom što znači da je određen i da netko ponovnim računanjem može dobiti jednak niz bita. U šifri toka su generatori prividno slučajnih brojeva imali razvijenu složenost i gledano s matematičke strane najbolje su razvijeni sustav, ali nedostatak je što nisu imali svojstvo nepredvidljivosti.

Kriptografski generator slučajno prividnih brojeva (engl. *Cryptograhycally Secure pseudo random number generator*) su u stvarnosti generatori slučajno prividnih brojeva sa dodatnim svojstvom nepredvidljivosti.

Šifriranje jednokratnim ključem

Definicija: Šifrat je bezuvjetno siguran i neprobojan (teorijski siguran), i u slučaju kada koristimo neograničen broj resursa za računanje odnosno probijanje.

Cilj je napraviti savršen i neprebojan šifrat. U ovom slučaju je to uspješno napravljeno. Ovakvo šifriranje je izimno jednostavno za formirati ali je nemoguće za dešifrirati. Uzmimo za primjer nizovnog ključa bacanje kovanice 1000 puta. Zanima ma nas redoslijed kojim je kovanica padala na određenu stranu. Tih 1000 slučajeva odnosno strana na koju je kovanica pala zna samo osoba koja je kovanicu i bacila što ovu radnju ćini tajnom. Nemoguće je odrediti redoslijed odnosno niz ključa. Šifriranje jednokratnim ključem spada u šifre toka.

Ono ima sljedeća svojstva:

- Niz ključa je iz primjenjenog generatora slučajnih brojeva
- Svaki niz ključa je upotrebljen samo jednom odnosno jednokratno

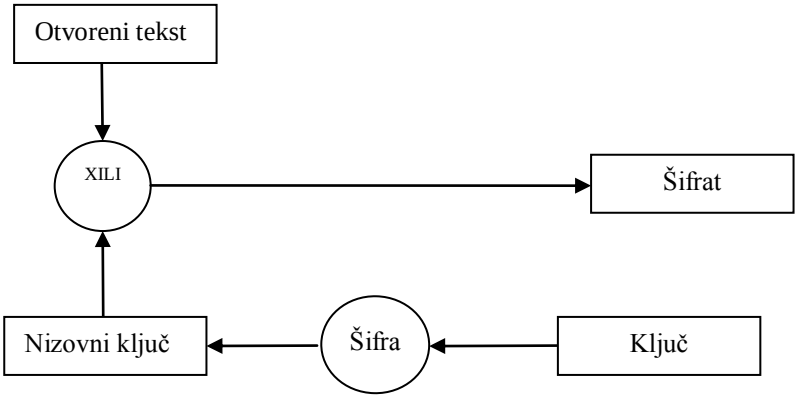
Pitanje: Zašto je bio potreban daljni razvoj šifriranja ako je ovaj sustav savršeno siguran?
Šifriranje jednokratnim ključem ima veliki nedostatak; niz ključa je jednake veličine kao i sama poruka.
Primjer 4.3 Enkripcija memorije veličine 400 MB
Rješenje: vrijednost pretvaramo u bite

$$400 \text{ MB} \cdot 8 = 3.2 \text{ Gbit niza ključa}$$

Šifriranje jednokratnim ključem u teoriji je savršen sustav, ali primjenimo li to u stvarni život jako su komplicirani i nisu korisni u praksi. Problem je što je ključevni niz bita jako dugačak i trebamo tako velik sadržaj poslati samo određenoj osobi, s tim da se niz ne može ponovno upotrijebiti. Takav sustav se danas koristi samo u ekstremnim vojnim svrhama.

Šifre toka danas

Zbog svih nedostataka šifriranja jednokratnim ključem kriptografi su došli na ideju da promjene dotadašnji sustav kako bi ga doradili i poboljšali rezultate funkcije. To je napravljeno tako da su primjenjeni generator slučajnih brojeva zamjenili s generatorom prividno slučajnih brojeva. Najbolji primjeri upotrebe dns ovog sustava je algoritam A5 u GSM mreži, te RC4 i SEAL.



Slika 4.2 Dijagram funcije šifre toka (izvor: osobna izrada)

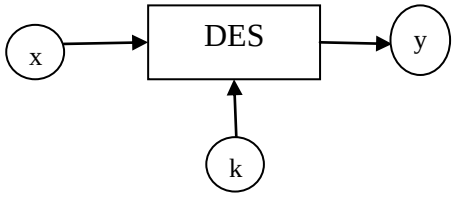
4.2 BLOKOVNE ŠIFRE

Blokovne šifre (engl. *Block Ciphers*) po samom nazivu možemo zaključiti imaju različit princip šiframa toka. Dok se u šiframa toka uzimao bit po bit za enkripciju u blokovnim šiframa enkriptiramo dio otvorenog teksta po blokovima odnosno manjim komadima otvorenog teksta, po određenoj duljini. U slučaju kada se radi o DES sustavu blokovi su duljine 64 bita, a u slučaju AES sustava 128 bita. Ovi sustavi koriste matematičku metodu permutacije, pa ćemo u sljedečem dijelu prikazati princip rada ovih sustava.

4.2.1 DES algoritam

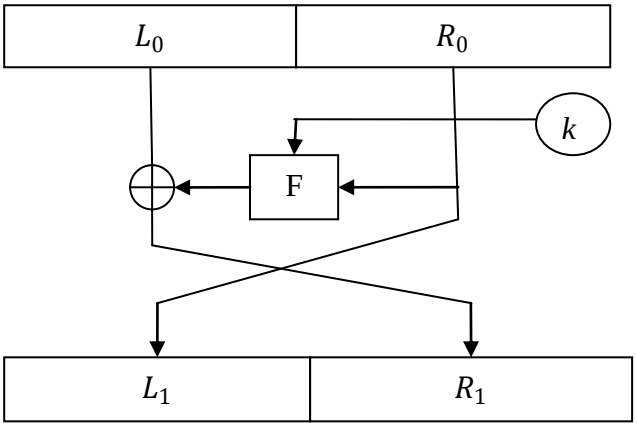
DES (engl. *Data encryption standard*) algoritam je među najraširenijim i poznatijim algoritmima simetričnog sustava. Ovaj algoritam spada u moderne i novije sustave jer se koristi još u današnje svrhe. Krajem šezdesetih prošlog stoljeća dolazi naglog razvoja financijskih transakcija, te i sama potreba za zaštitu tog sadržaja kriptografijom. Tijekom sedamtesetih sustav napokon razvija IBM tvrtka. Sustav je kroz neko vrijeme još dorađen u sklopu Agencija za nacionalnu sigurnost, NSA (*National Security Agency*), te 1976. biva prihvačen standardom pod današnjim nazivom *Data encryption standard.*

DES šifrira ulaznu poruku blokom duljine 64 bita, na izlazu dobijemo blok šifrata duljine 64 bita, dok je ključ *k* koji koristimo blok duljine 56 bita. Ključ se često pojavljuje u bloku duljine 64 bita, tada se svaki osmi bit zanemaruje, odnosno otpada i koristimo ga za provjeru partiteta.



Slika 4.3 Pojednostavljeni dijagram DES algoritma (izvor: osobna izrada)

Zanima nas što se događa unutar samog DES sustava u prijašnjem dijagramu. Pojednostavljeni dijagram ćemo sada prikazati u detalje kako izgleda u potpunosti. Točan naziv takvog prikaza algoritma je Feistelova mreža.



Slika 4.4 Dijagram 1. koraka DES algoritma (izvor: osobna izrada)

Princip rada 1. koraka: Algoritam pri prvom koraku izvodi inicijalnu permutaciju. Posljednji korak algoritma je definiran s konačnom permutacijom iz koje slijedi dobiveni šifrat. Otvoreni tekst odnosno poruku bloka duljine 64 bita dijelimo na 2 jednaka dijela (32 bita svaki). Lijevi nazivamo L (*left*), dok nam je desni dio R (*right*). Desni dio provlačimo kroz F blok iliti funkciju. U funkciju također uključujemo dio ključa odnosno podključ *k.* Na izlazu funkcije dobijemo operator modulo 2 odnosno logički sklop NILI. U taj logički sklop nam ulazi lijevi dio duljine bloka. Nakon što se izvrši matematički izračun iz sklopa NILI izlaz vodi ka suprotnom desnom R izlazu, dok izlaz s uvodnog desnog dijela završava u lijevom izlaznom. Ova metoda križanja vodova se još zove *Crossover.* Izlazi L_1 i R_1 će za sljedeći korak služiti kao uvodni podjeljeni dio bloka. Algoritam je završen kad se izvedu svi koraci odnosni svih 16.

Funkciju u inicijalnoj permutaciji algoritma definiramo po sljedećem pravilu:

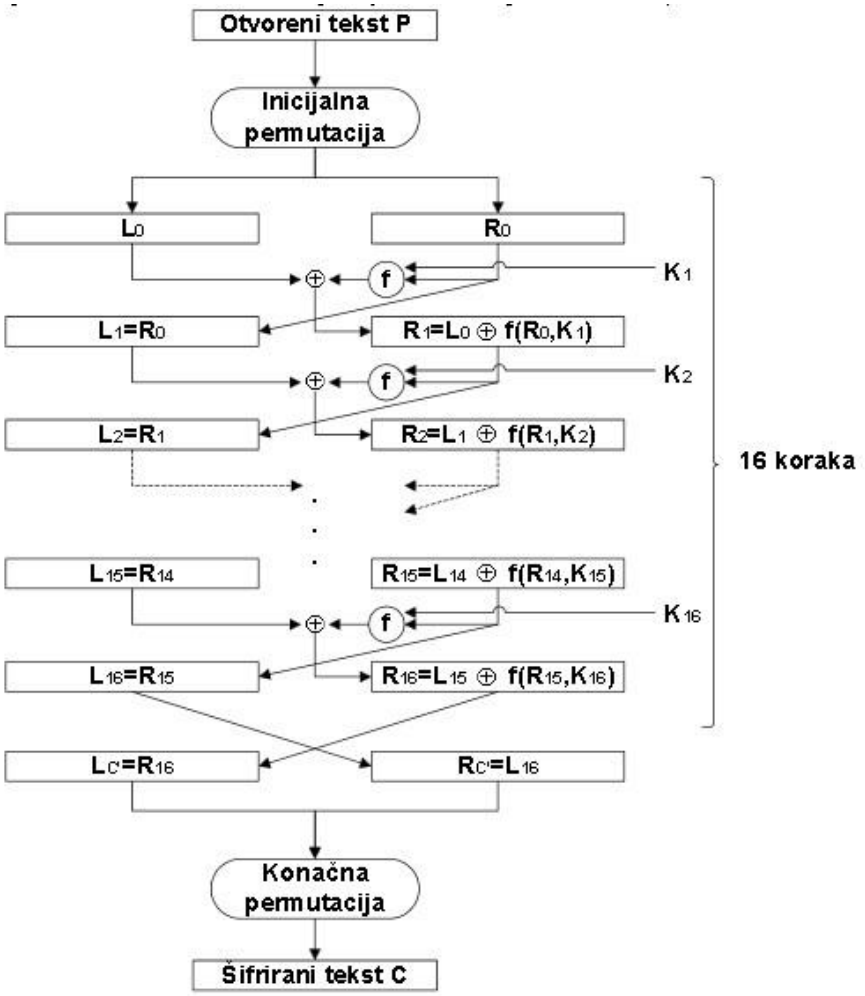
$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

Funkciju u završnoj permutaciji algortima definiramo po sljedećem pravilu:

$$C' = (L_{16}, R_{16})$$

$$C = C^{-1}$$



Slika 4.5 Dijagram 16 koraka DES algoritma (izvor: http://www.ieee.hr)

Primjer 4.4 Inicijalna permutacija bloka 64 bita. Ako vrijedi $i = 0$, do $i = 7$ (prvih sedam koraka)

$$P_i^T = P_{58-i\cdot 8}$$
$$P_{8+i}^T = P_{60-i\cdot 8}$$
$$P_{16+i}^T = P_{62-i\cdot 8}$$
$$P_{24+i}^T = P_{64-i\cdot 8}$$
$$P_{32+i}^T = P_{57-i\cdot 8}$$
$$P_{40+i}^T = P_{59-i\cdot 8}$$
$$P_{48+i}^T = P_{61-i\cdot 8}$$
$$P_{56+i}^T = P_{63-i\cdot 8}$$

Kraj inicijalnog permutacijskog zapisa. Sada to prenosimo u tablični zapis. Prvi bit se nalazi u gornjem lijevom kutu, dok se posljednji nalazi u donjem desnom kutu.

Tablica 4.3. Inicijalna permutacija bitova bloka od 64 bita

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Primjer 4.5 Konačna permutacija bloka 64 bita ako vrijedi $i = 0$, do $i = 3$ (prva tri koraka)

$$C^T_{16\cdot i+1} = C'_{40-i\cdot 2}; \quad C^T_{16\cdot i+2} = C'_{8-i\cdot 2};$$
$$C^T_{16\cdot i+3} = C'_{48-i\cdot 2}; \quad C^T_{16\cdot i+4} = C'_{16-i\cdot 2};$$
$$C^T_{16\cdot i+5} = C'_{56-i\cdot 2}; \quad C^T_{16\cdot i+6} = C'_{24-i\cdot 2};$$
$$C^T_{16\cdot i+7} = C'_{64-i\cdot 2}; \quad C^T_{16\cdot i+8} = C'_{32-i\cdot 2};$$
$$C^T_{16\cdot i+9} = C'_{39-i\cdot 2}; \quad C^T_{16\cdot i+10} = C'_{7-i\cdot 2};$$
$$C^T_{16\cdot i+11} = C'_{47-i\cdot 2}; \quad C^T_{16\cdot i+12} = C'_{15-i\cdot 2};$$
$$C^T_{16\cdot i+13} = C'_{55-i\cdot 2}; \quad C^T_{16\cdot i+14} = C'_{23-i\cdot 2};$$
$$C^T_{16\cdot i+15} = C'_{63-i\cdot 2}; \quad C^T_{16\cdot i+16} = C'_{31-i\cdot 2};$$

Kraj konačnog permutacijskog zapisa. Sada to prenosimo u tablični zapis. Prvi bit se nalazi u gornjem lijevom kutu, dok se posljednji nalazi u donjem desnom kutu.

Tablica 4.4. Završna permutacija bitova bloka od 64 bita

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Sigurnost DES algoritma je rizična zbog duljine ključa. Tijekom izrade algoritma je od strane IBM predložena duljina bloka od 112 bita za ključ sustava, no u konačnici su ostali pri 56 bita.

Način generiranja podključeva u DES algoritmu također pridonosi ne prihvatljivosti. Zbog strukture algoritma i duljine ključa smatramo da ovaj algoritam ne spada u kompletno sigurne sustave u kriptografiji, no s malim izmjenama se može smatrati dovoljno sigurnim.

4.2.2 AES algoritam

AES (engl. *Advanced encryption standard*) odnosno napredni kriptografski standard također spada u simetrične algoritme. Ono što je bio nedostatak DES algoritmu, odnosno duljina ključa je sada izmjenjeno. U ovom slučaju duljina blokova otvorenog teksta i šifrata iznosi 128 bita dok duljina bloka ključa može biti 128, 192, ili 256 bita. AES algoritam je najpopularniji i najkorišteniji kriptografski simetrični sustav današnjice. Iza funkcionalnosti AES algoritma stoji niz pravila i matematičkih metoda koje se koriste, pa ćemo prvo objasniti podlogu samog algoritma.

Na samom početku rada objašnjena je primjena modularne aritmetike u kriptografiji. U AES algoritmu također koristimo određene skupove.

Osnovne algebarske sktukture možemo podijeliti na sljedeči način:

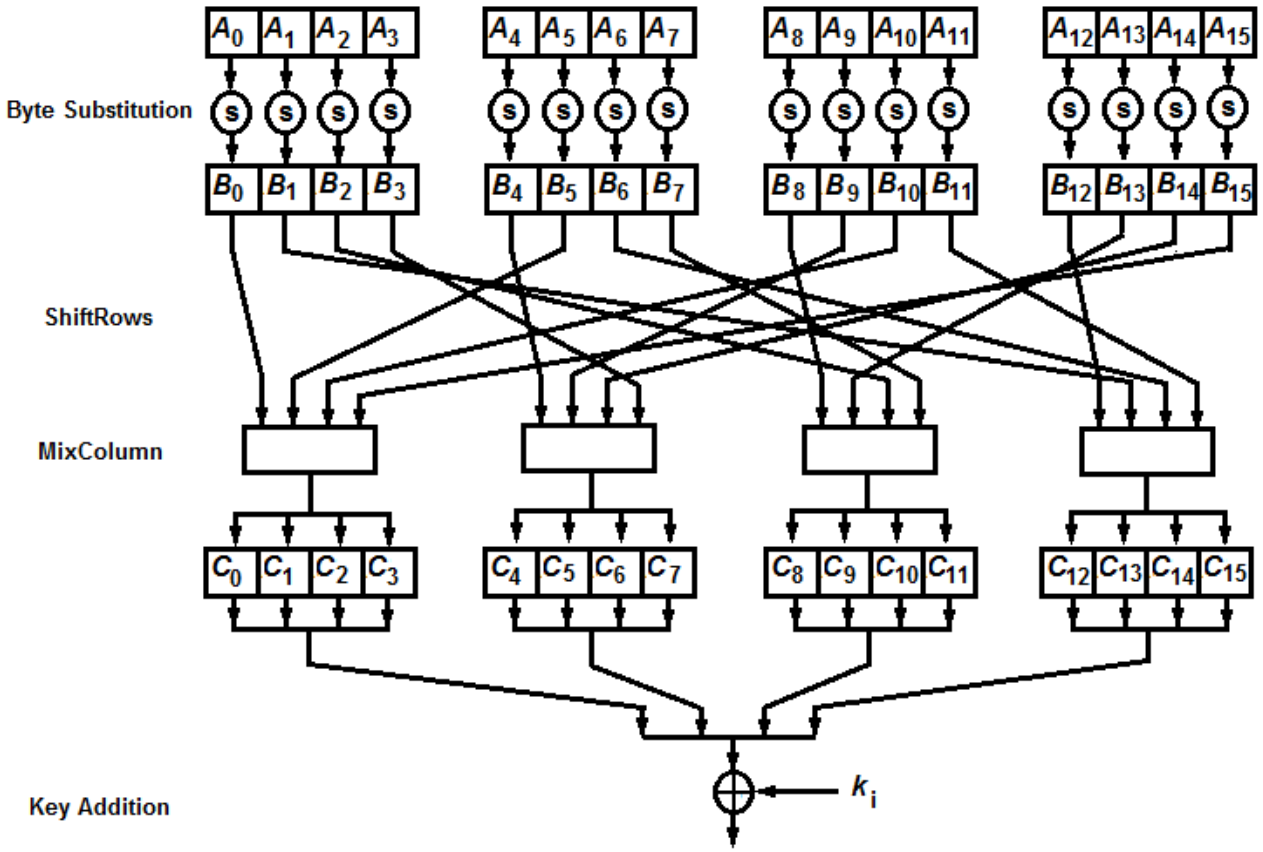
- grupa – koristimo operacije $+, -$
- prsten – koristimo operacije $+, -, \cdot$
- polja – koristimo operacije $+, -, \cdot, \frac{x}{y}$

U AES algoritmu koristimo polja što znači da su nam na raspolaganju sve računske operacije. Za postizanje navedenih izmjena u DES algoritmu potrebni su bili polinomi. Kao i u DES algoritmu imamo broj koraka u sustavu, u ovom slučaju broj koraka ovisi o duljini bloka ključa.

Podjela broja koraka u strukturi algoritma:

- 128 bita – 10 koraka
- 192 bita – 12 koraka
- 256 bita – 14 koraka

Unutar AES algortima sve operacije se vrše na dvodimenzionalnom nizu okteta, odnosno matricama. Enkripcija kao i dekripcija se provodi na taj način tako da se ulazni blok informacije kopira u matricu stanja nad kojom se provode razne operacije. Nakon toga, matrica stanja se transformira 10, 12, ili 14 puta ovisno o duljini ključa. Svaki od navedenih duljina ključa odnosno okteta ima svoje korake, a svaki od koraka predstavlja funkciju koja sadrži četiri transformacije.



Slika 4.6 Dijagram koraka AES algoritma (izvor: http://www.ieee.hr)

Primjer 4.6 Množenje u Galoisovom polju

$$A_i = 1100\ 0010$$

$$A_i(x) = x^7 + x^6 + x$$

$$B_i(x) = x^5 + x^2 + 1 = A_i(x)^{-1}$$

$$\downarrow$$

$$B_i = 0010\ 1111$$

$$(x^7 + x^6 + x) \cdot (x^5 + x^3 + x^2 + x + 1) = 1 \bmod x^8 + x^4 + x^3 + x + 1$$

$$\downarrow$$

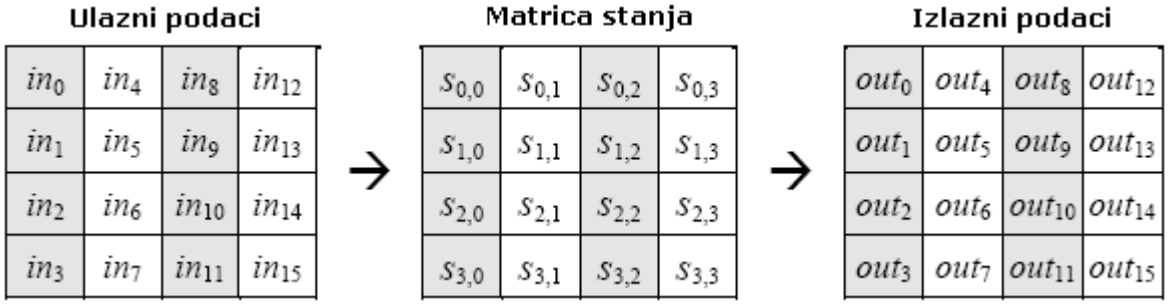
nedjeljivi polinom AES algoritma

Primjer 4.7 Množenje okteta $57\times 83 = c1$, gdje je nedjeljivi polinom $x^8 + x^4 + x^3 + x + 1$

$$(x^6 + x^4 + x^2 + x + 1) \cdot (x^7 + x + 1)$$
$$= x^{13} + x^{11} + x^9 + x^8 + x^7 + x^7 + x^5 + x^3 + x^2 + x^6 + x + x^4 + x^2 + x + 1$$
$$= x^{13} + x^{11} + x^8 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$$
$$= x^{13} + x^{11} + x^8 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \bmod (x^8 + x^4 + x^3 + x + 1)$$
$$= x^7 + x^6 + 1$$

Transforimacije koje se provode nad oktetima smo razvrstali u četiri podijele. Dijelimo ih na: zamjenu bloka na temelju suptstitucijske tablice, posmak redaka u matrici stanja, mješaje podataka unutar svake stupca matrice stanja, dodavanje podključa u matricu stanja.

Ulazno stanje odnosno bitovi otvorenog teksta, izlazno stanje odnosno bitovi šifrata te matrica stanja se prikazuju u 4×4 formatu:



Slika 4.7 Ulazno/izlazni podaci te matrica stanja (izvor: http://sigurnost.zemris.fer.hr/ns/wireless)

U svakom stupcu se formiraju četiri okteta koji formiraj 32-bitnu riječ. Matricu stanja je tada moguće interpretirati kao dvodimenzionalni niz od 32-bitnih riječi.

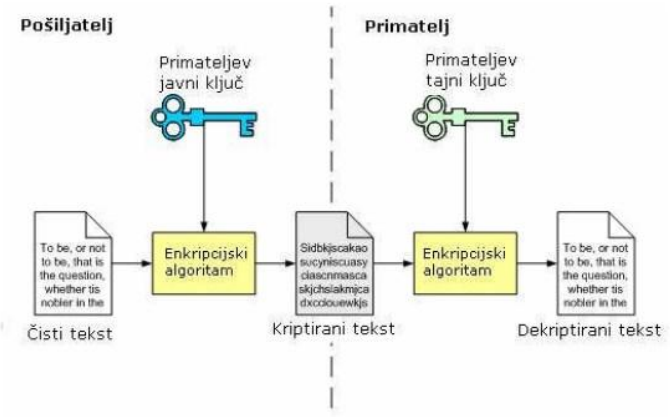
Nakon što smo formirali matricu oktetima vršimo transformaciju posmak redaka. Tu se okteti zadnja tri reda se pomiču za određeni broj elemenata (posmak). Ovakav posmak zapravo pomiće oktete na niže pozicije u redu. Sljedeći korak je mješanje podataka u stupcima matrice stanja. Stupci koji se inače smatraju polinomom četvrtog stupnja, se multipliciraju konstantom polinoma $a(x)$. Posljednji korak koji radimo je dodavanje podključa u matricu stanja. Pri dodavanju podključa zapravo izvodimo XILI operaciju nad bitovima.

Način na koji se AES razvio fascinira još dan danas. Tražio se nasljednik DES-a zbog nedostatka duljine ključa, te je napravljen javi natječaj za prijavu kako bi se napravio novi kriptografski sustav. Pobjednik natječaja su bili belgijanci Joan Daemen i Vincent Rijmen, a ime

algoritma je složeno od početna tri slova njihovih prezimena, odnosno Rijendael. U praksi se može reči da današnji AES nije jednak Rijendalu ali da poprima strukturu i većinu inačice. Danas AES koristimo u svakom pretraživaču, elektronskoj pošti, raznim softver inačicama koje koriste enkripciju kao štu su BitLocker, WinRAR, WinZip, Windows Office 2007, te sigurnost bežičnih mreža standarda 802.11 ili WPA2. Teoretski su pronađene metode za razbijanje AES enkripcije primjenom sile, ali trenutno takve napade još nije moguće izvesti. Dobra strana AES algoritma što uvijek postoji produljenje duljine ključa, što bi otežalo još više kriptoanalizu. Očekuje se da će u budućnosti biti predstavljena novija verzija nekog drugog standarda koji će ispunjavati sve uvjete današnje kriptografije.

4.3 ASIMETRIČNI SUSTAVI

Asimetrični sustavi za razliku od simetričnih koji koriste samo jedan ključ, imaju dva ključa (tajni i javni). Kod simetričnih sustava smo imali problem distribucije ključa, kod asimetričnih sustava tog problema nema. Princip rada asimetričnog sustava je takav da je tajni ključ poznat samo onoj osobi koja primi poruku i dešifrira ju. Ta je osoba u kriptografskoj literaturi opisana kao primatelj Bob. Ono što je posebno u ovom sustavu da Bob od privatnog iliti tajnog ključa izvede javni ključ koji je svima dostupan za enkripciju, ali jedino Bob ima odgovarjući privatni ključ za dekripciju. Jedan od primjera takvog sustava u životu je primopredaja u poštanskom sanduku. U prijevodu svatko od nas može staviti pismo u sandučić (šifrirati), ali samo osoba tj vlasnik sandučića može otvoriti s tajnim ključem (dešifrirati).



Slika 4.8 Prikaz asimetričnog sustava (izvor: http://www.ieee.hr)

Kao što smo rekli velika prednost asimetričnog sustava nad simetričnim je ta što nije potreban dogovor oko rješavanje situacije jednog ključa. Pošto je javni ključ izvedenica od privatnog postoji mogućnost izračuna privatnog preko javnog, ali ta je mogućnost minimalna pa skoro i ne moguća. Za takav izračun kriptoanalitičarima bi bilo potrebno vrijeme više od dvije godine za probijanje privatnog ključa. Osim mogućnosti enkripcije, velika prednost asimetričnog sustava nad simetričnim je ta što pruža mogućnost autentifikacije. Tu spadaju digitalni potpis, hash funkcije, te digitalni certifikat. Najpoznatiji i najkorišteniji asimetrični algoritam je RSA kojeg ćemo posebno obraditi u sljedećem poglavlju.

4.3.1 RSA algoritam

Istraživač računalnih znanosti Ron Rivest u MIT-ovom laboratoriju 1977. sa svojim kolegama Adi Shamirom, i Leonard Adlemanom razvijaju sustav koji su nazvali po inicijalima svojim prezimena odnosno RSA (Rivest, Shamir, Adleman). Kao što je navedeno u prošlom poglavlju RSA je najpopularniji i najkorisniji algoritam u asimetričnom sustavu kriptografije.

Dok smo u simetričnim sustavima koristili generatore brojeva, za razliku kao kod simetričnih sustava (AES, DES) , RSA algoritam zahtjeva računanje para ključeva (k_{pub} , k_{priv}).

Postupak izračuna ključeva:

1. Odabir dva velika prosta broja*: p i q*
2. Množimo ih*:* $n = p \cdot q$
3. $\varphi(n) = (p-1) \cdot (q-1)$
4. Biramo javni ključ $k_{pub} = e \in \{1, 2, 3 \dots, \varphi(n) - 1\}$, dok vrijedi $\left(e,\ \varphi(n)\right) = 1$
5. Računamo privatni ključ $k_{priv} = d$, tako da vrijed$i\ d \cdot e \equiv 1\ mod\ \varphi(n)$

Nakon što smo smo izdefinirali pripremu odnosno izračun ključa, sada je potrebno definirati enkripciju i dekripciju.

Enkripcija: $k_{pub} = (n, e), x \in \mathbb{Z}_n = \{0, 1, 2 \dots, n-1\}$

$$y = e_{kpub}(x) = x^e \bmod n$$

Dekripcija: $k_{priv} = d, y \in \mathbb{Z}_n$

$$x = d_{kpriv}(y) = y^d \bmod n$$

Primjer 4.8 Postupak izračuna parametra ključa

Bob nasumično bira dva velika prosta broja (inače oko 100 decimalnih mjesta) ali zbog jednostavnosti ćemo izabrati manje brojeve p = 3, i q = 11.

Pratimo korake kao u postupku:

1. Izabrani $\mathrm{p} = 3,\ \mathrm{i}\ \mathrm{q} = 11$
2. $n = p \cdot q = 33$
3. $\varphi(n) = (p-1) \cdot (q-1) = 2 \cdot 10 = 20$
4. Izaberemo javni ključ $e = 3$
5. $d \equiv e^{-1} \equiv 7 \bmod 20$

Kada smo odradili svu pripremu možemo krenuti s enkripcijom i dekripcijom:

Alice šalje poruku Bobu i poruku pretvara u broj x u ovom slučaju 4

$$x = 4$$

$$y = x^e \bmod n = 4^3 \bmod 33 \ = 64 \bmod 33 \equiv 31$$

$$\downarrow$$

Ovime je izvršena enkripcija, odnosno poslana je poruka preko nesigurnog kanala. Sada je potrebna dekripcija kako bi poruku mogao pročitati samo namijenjeni primatelj poruke.

$$x = y^d = 31^7 \equiv 4 \bmod 33$$

Iz primjera možemo zaključiti da su parametri koji definiraju sigurnost RSA sustava p i q. U praksi su oni definirani veličinom $p, q \geq 2^{512}$. Po tome kriptoanalitičaru nije moguće odgonetnuti te parametre zbog njihove decimalne duljine.

Zaključujemo da je princip funkcionalnosti ovog sustava jednostavan i da je ključ uspjeha i neprobojnosti i veličini prostih brojeva. Za izračun odnosno pretvorbu prostih brojeva u manje koje možemo koristiti koristimo modularnu aritmetiku koju smo obradili na početku ovog rada. Mnogi smatraju da modularna aritmetika nije najbolji princip računanja velikih prostih brojeva, te da postoje uspješni napadi zbog nje na ovaj sustav, ali ovaj sustav već desetljećima ostaje ne probojan. Razvojem računalne industrije dolazi i do mogućnosti korištenja ključeva većih duljina. RSA sustav je u današnjici najmanje 80% korišten od sveukupnih algoritama u asimetričnim sustavima.

5. ZAKLJUČAK

Kriptografija ima dugu i bogatu povijest. Tako se je kroz povijest i mijenjala svrha odnosno razlog slanja skrivenih poruka. Od prvih hijeroglifskih zapisa Egipćana, pa do zapisa Indijskog porijekla koji su opisivali načine života tadašnjeg naroda. Kako bi poruke ostale tajne, korištena je matematika i matematičke metode koje bi zbunile i obeshrabrile svakog ne željenog primatelja poruke. Najviše su utjecaja u klasičnoj kriptografiji imale matematičke metode supstitucije i transpozicije. Kriptografija je postala toliko bitna, da je u određenim trenucima povijesti koji su utjecali na cijeli svijet, kao štu su svjetski ratovi u 20. stoljeću bila razlog samog ishoda takvih bitki.

Razvojem računala u 20. stoljeću stvara se mogućnost implementacije novih matematičkih metoda u grani kriptografije. Kako bi sustavi bili sigurni, a sebi olakšali život pri računanju i stvaranju strukture algortima, kriptografi se koriste modularnom aritmetikom u svim novijim sustavima. Tako su u mogućnosti izbjeći matematičke operacije s velikim prostim brojevima, dok se kriptoanalitičari zbog tajnosti određenih matematičkih parametara moraju suočiti s njima. Uz modularnu aritmetiku matematička područja koja susrečemo u modernoj kriptografiji su računanje s matricama, ekspnencije, polinomi, permutacije, te se javlja kombinacija matematike i elektrotehnike jer se svi sustavi vrše i stvaraju preko računala.

Danas razvojem tehnologije u svakom koraku koristimo kriptografiju. Najviše se to odnosi na civilnu uporabu pametnih telefona i računala. Korištenjem pametnog telefona u svrhu poziva uvijek koristimo enkripciju. Druga svrha može biti bežično spajanje na zaštićenu mrežu. Ostale primjene su u medicini, audio i video idustriji, digitalnoj komunikaciji, internet bankarstvo i slično. Najbrži razvoj sigurnosnih sustava kriptografije i kriptoanalize su i dalje u vojnim svrhama. Najviše se odnosi na vojne velesile SAD-a, Rusije, Kine, Japana te neke manje zapadne sile. Većina algoritama koji oni koriste su i dalje nepoznanica javnosti, te je potrebno dugo vremena da i Hrvatska može uživati u mogućnostima takvog razvoja kriptografije.

Razvoj tehnologije je sve brži. Takvim razvojem dolazi i do mogućnosti kvalitetnijeg i bržeg učitavanja sadržaja neovisno o vrsti zaštite neke informacije ili duljine ključa. Potrebno je predočiti mladima od perioda srednje škole ili studija informacijskih znanosti o važnosti i rasprostranjenosti kriptografije.

LITERATURA

[1.] C. Paar, J. Pelzi., Understanding Cryptography., Bochum 2010.

[2.] A. Đuraković., Klasična kriptografija., Sveučilište J.J. Strossmayera u Osijeku, Osijek 2014.

[3.] T. Horvatek., Računalna kriptografija u nastavi., Visoka škola za infromacijske tehnologije Zagreb., Zagreb 2011.

[4.] A. Dujella, M. Maretić., Kriptografija, Zagreb 2007.

[5.] http://www.cis.hr/ - Centar informacijske sigurnosti

[6.] https://www.youtube.com/channel/UC1usFRN4LCMcfIV7UjHNuQg - predavanja

[7.] https://en.wikipedia.org

Matematičke metode u kriptografiji

SAŽETAK

Završni rad prikazuje razvoj kriptografije od samog početka do današnje uporabe. Opisane su sve matematičke metode koje su korištene pri kriptografiji. Prvo poglavlje je uvod u rad gdje je opisan pojam kriptografije. U drugom poglavlju je detaljno opisana matematička grana odnosno modularna aritmetika koja se koristi u većini matematičkih operacija u kriptografiji. U trećem poglavlju je opisana klasična kriptografija. Od samih temelja kako se kriptografija rodila, pa do korištenja supstitucije i transpozicije u metodama šifriranja. U četvrtkom poglavlju je opisan razvoj kritpografije nakon izuma računala, DES i AES algoritmi u simetričnim sustavima i RSA algoritam u asimetričnim sustavima. Posljednje poglavlje je zaključak gdje se opisuje i sažima osobno mišljenje autora rada o primjeni matematike u kriptografiji i utjecaj kriptografije na današnjicu.

Ključne riječi: kriptografija, matematičke, metode, razvoj, DES, AES, RSA, poglavlje

Mathematical methods in cryptography

ABSTRACT

This graduation thesis is showing the development of cryptography from the early days until today's use. All the mathematical methods that are used in crypto are well described. The first chapter is the introduction in the thesis where the meaning of cryptography is explained. In the second chapter the mathematical field called modulo arithmetic is explained in details. In the third chapter, classic cryptography has been described in details. From the days where crypto has been born, until the using of substitution and transposition in the encryption methods. In the fourth chapter the development after the invention of the computer has been explained. DES and AES algorithms in simetric systems and RSA in asimetric systems. The last chapter is the conclusion part where the toughts from the author are described, about the application of mathematics in cryptography and the influence that cryptography has on our lives.

Key words: Cryptography, mathematics, methods, development, DES, AES, RSA, chapter

ŽIVOTOPIS

Ime i prezime: Danijel Čokara

Datum i mjesto rođenja: 15.01.1994., Čapljina, BIH

Adresa: Zdenčac 21, Garešnica 43280

e-mail adresa: dcokara@etfos.hr, totalldc1@gmail.com

Strani jezici: engleski i njemački

Srednja škola: Tehnička škola Daruvar, smjer: Tehničar za računalstvo 2012.

Godina upisa studija: 2012.