

Enkripcija

1. Osnovni pojmovi i terminologija u kriptografiji

Termin **originalni tekst** (eng. *plaintext*) odnosi se na tekst koji je moguće pročitati i razumeti bez primene nekih posebnih metoda. Ukoliko se taj tekst prenosi preko nekog komunikacionog kanala, on se naziva **poruka**. Poruka se može slati putem računarske mreže kako u originalnom obliku, tako da svima bude razumljiva, ili kao nerazumljiv sadržaj koji se naziva **šifrovan tekst ili šifrat** (eng. *ciphertext*).

Postupak pomoću koga se originalni tekst poruke transformiše u šifrovan tekst naziva se **šifrovanje** (eng. *encryption*). Šifrovanje se koristi da bi se obezbedilo da nijedan korisnik, osim korisnika kome je poruka namenjena, ne može da sazna sadržaj poruke. Ukoliko neki neovlašćeni korisnici dođu u posed šifrovanog teksta, oni ne mogu pročitati originalni tekst poruke. Šifrovanje originalnog teksta se obavlja pomoću određenog pravila za šifrovanje odnosno **algoritma šifrovanja**. Svaki algoritam šifrovanja kao ulazne podatke ima originalnu poruku i **ključ**, a kao izlaz daje šifrovanu poruku.

Cilj šifrovanja poruka je da se omogući:

- A. **Poverljivost podataka** – obezbeđivanje da neautorizovana (neovlašćena) strana ne dođe do poverljivih informacija.
- B. **Autentičnost podataka** – omogućava definisanje i proveru identiteta pošiljaoca.
- C. **Integritet podataka** – prevencija neovlašćene promene sadržaja poruke (izmena, brisanje, uništavanje) prilikom njenog slanja.

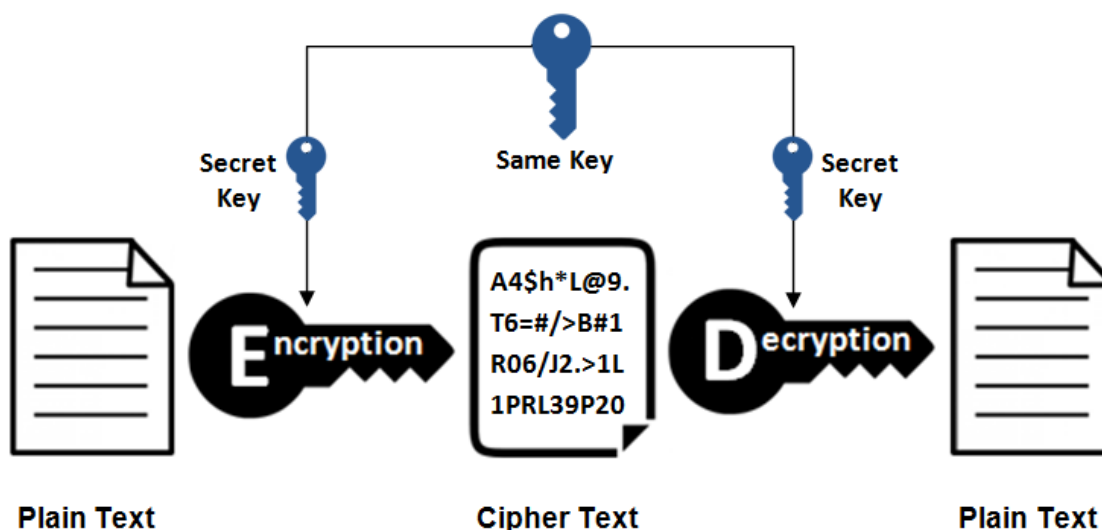
Postupak koji omogućava da se od šifrovane poruke dobije originalna poruka naziva se **dešifrovanje** (eng. *decryption*).



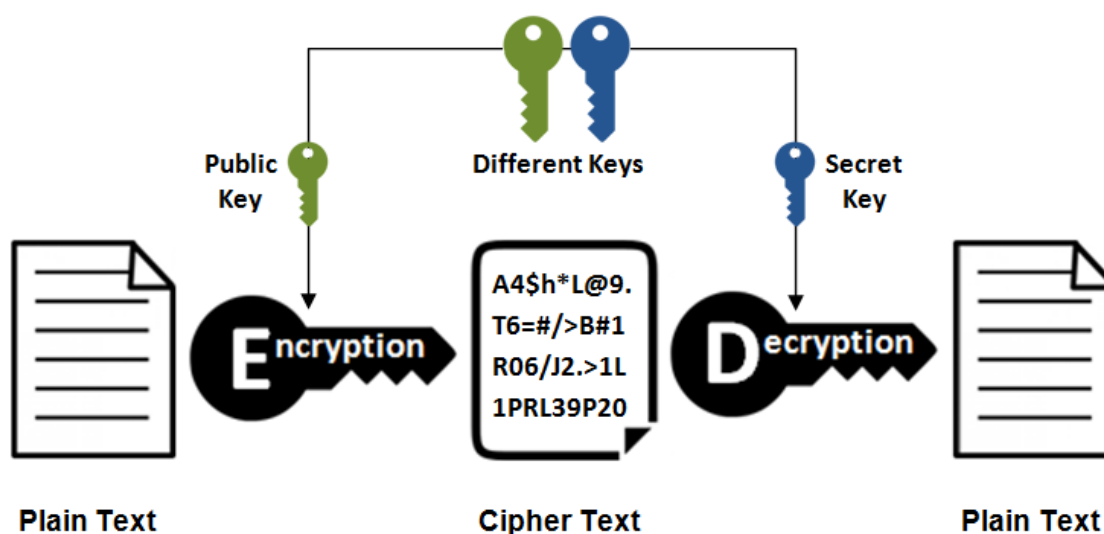
Slika 1. Enkripcija podataka

U kriptologiji postoje dva osnovna bezbednosna modela, a to su: **simetrični** (eng. *symmetric*) ili model sa tajnim ključevima i **asimetrični** (eng. *asymmetric*) ili model sa javnim i privatnim ključevima. Moderni kriptološki sistemi su najčešće kombinovani (eng. *hibrid*) u cilju postizanja kompletne zaštite, najčešće u više nivoa.

Symmetric Encryption



Asymmetric Encryption

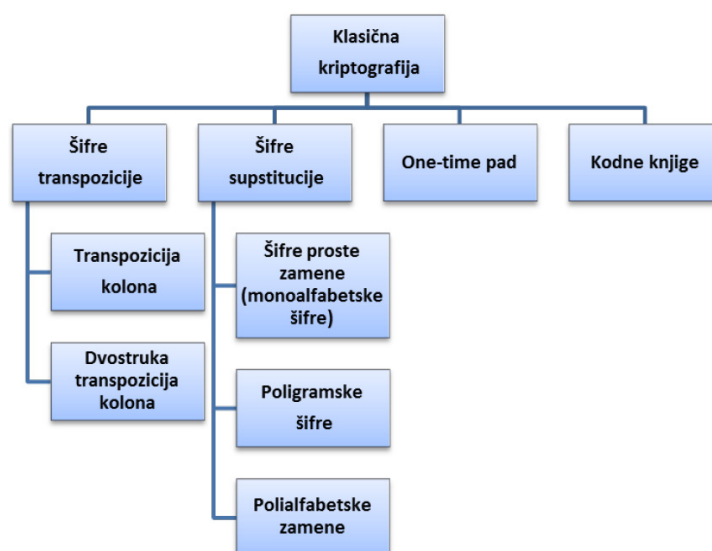


Slika 2. Simetrični i asimetrični model šifrovanja poruka

Bezbednost današnjih sistema definiše se u skladu sa trenutnim razvojem računara, čije performanse imaju veliku ulogu u razvoju kriptologije. Cilj je napraviti takav algoritam čija cena dešifrovanja bi bila veća od vrednosti same šifrovane poruke. Takođe, skup mogućih ključeva mora biti dovoljno velik da bi postupak potpune pretrage ključeva bio nemoguć u konačnom vremenu.

2. Klasična kriptografija

U nastavku vežbe ukratko će biti razmotrene klasične šifre koje su izabrane zbog svog istorijskog značaja i da bi se na njihovom primeru prikazali osnovni principi koji postoje i danas kod modernih šifara. Podela klasične kriptografije prema tipovima šifri prikazana je na Slici 3.



Slika 3. Podela klasične kriptografije na tipove šifri

A. Šifre transpozicije

Šifre transpozicije rade na principu premeštanja slova originalne poruke. Tako dobijeni skremblovani tekst predstavlja šifrovanu poruku, a primenjena transpozicija ključ šifrovanja. Prva šifra ovog tipa poznata je pod imenom *Skitala* i koristili su je Spartanci još 500. godine pre nove ere. Princip rada šifre je vrlo jednostavan. Obavijala se kožna traka oko štapa i zatim se poruka pisala na tako dobijenom omotaču duž štapa. Kada je poruka bila napisana, kožna traka se razmotavala i dobijao se ispremeštan (skremblovan) tekst. Znakove je mogao pročitati samo onaj ko je imao štap jednake debljine. Može se zaključiti da je kompletna tajnost ove šifre određena debljinom štapa, tj. debljina štapa zapravo predstavlja ključ šifrovanja.



Slika 4. Skitala

A1. Transpozicija vrsta i kolona

Dvostruka transpozicija predstavlja moderniju verziju Skitale koja se realizuje tako što se menja redosled kolona i redosled redova u izabranoj dimenziji matrice $[n \times m]$. U ovom slučaju ključ je dimenzija matrice i permutacije po kolonama i redovima.

kolone	0	1	2	3	4	5	6
red 0	U	N	I	V	E	R	Z
red 1	I	T	E	T	U	N	O
red 2	V	O	M	S	A	D	U

kolone	1	0	6	2	4	3	5
red 1	T	I	O	E	U	T	N
red 0	N	U	Z	I	E	V	R
red 2	O	V	U	M	A	S	D

Slika 5. Transpozicija vrsta i kolona

Originalna poruka: UNIVERZITET U NOVOM SADU

Ključ: dimenzija matrice $[3 \times 7]$, permutacije kolona (1,0,6,2,4,3,5)
permutacije vrsta (1,0,2)

Šifrovana poruka: TIOEUTNNUZI E VROVU MASD

B. Šifre zamene (supstitucije)

Kod šifri supstitucije, raspored slova originalne poruke ostaje nepromenjen, ali slova teksta menjaju svoju vrednost, tj. preslikavaju se u druga slova. Postoji više tipova šifara zamene: monoalfabetske, homofone, poligramske i polialfabetske šifre.

B.1 Monoalfabetska šifra - Najstariji primer predstavlja šifra koju je Julije Cezar koristio za razmenu poruka sa svojim generalima. To je tip šifre proste zamene u kome se svako slovo originalne poruke menja odgovarajućim slovom azbuke, pomerenim za određeni broj mesta koji definiše ključ. Na primer, sa pomakom 3, A se zamenjuje slovom G, B sa D itd.

A	B	V	G	D	Đ	E	Ž	Z	I	J	K	L	U	M
G	D	Đ	E	Ž	Z	I	J	K	L	U	M	N	NJ	O

N	NJ	O	P	R	S	T	Ć	U	F	H	C	Č	DŽ	Š
P	R	S	T	Ć	U	F	H	C	Č	DŽ	Š	A	B	V

Slika 6. Monoalfabetska šifra

Originalni tekst: FAKULTET TEHNIČKIH NAUKA

Šifrovani tekst: ČGMCNFIF FIDŽPLAMLJLDŽ PGCMG

B.2 Homofone šifre – Homofone šifre predstavljaju unapređenje šifre prostih zamena, uvodeći element slučajnosti. Svako slovo se predstavlja sa jednim ili više brojnih kodova.

A	A	B	V	G	D	Đ	E	E	Ž	Z	I
12	14	16	18	20	22	24	26	28	30	32	34

I	J	K	L	LJ	M	N	N	NJ	O	O	P
11	10	09	08	07	06	05	04	03	02	01	00

R	R	S	T	Ć	U	F	H	C	Č	DŽ	Š
13	15	17	19	21	23	25	27	29	31	33	35

Slika 7. Homofone šifre

Originalni tekst: MEĐURAČUNARSKE KOMUNIKACIJE I RAČUNARSKE MREŽE

Šifrovani tekst: 06 26 24 23 13 12 31 23 04 14 15 17 09 28 09 02 06 23 05 11 09 14 29 34 10 26 34 15 12 31 23 04 14 15 17 09 28 06 15 26 30 28

B.3 Poligramske šifre - rade na principu zamena nad većim grupama slova u originalnoj poruci. Jedna od najpoznatijih šifara je **Plejfer** šifra, koju su koristili Britanci tokom Prvog svetskog rata. Ključ Plejfer šifre bila je matrica dimenzija [5 x 5] sa 25 slova, karakter "J" se nije koristio ili je bio prisvojen nekom drugom slovu. Matrica se konstruiše na osnovu izabrane ključne reči. Prvi znakovi (sa levo na desno) u matrici će biti ključne reči, sa

uklonjenim duplim slovima. Par slova originalne poruke $m1$ i $m2$ šifruje se u skladu sa sledećim pravilima:

1. Ako su $m1$ i $m2$ u istom redu (ili koloni), tada su $c1$ i $c2$ dva slova koja se nalaze desno (ili ispod) od $m1$ i $m2$. Usvojeno je da je prva kolona susedna poslednjoj koloni, a prvi red susedan poslednjem redu.

2. Ako su $m1$ i $m2$ u različitim kolonama i redovima, tada su $c1$ i $c2$ ostale dve ivice (temena) pravougaonika koji sadrži ivice $m1$ i $m2$, gde je $c1$ u istom redu kao i $m1$ dok je $c2$ u istom redu kao i $m2$.

3. Ako je $m1 = m2$, slovo se prepisuje i umesto drugog slova se dodaje slovo "x".

4. Ukoliko originalna poruka ima neparan broj slova tada se na kraj poruke dodaje neutralni karakter "z".

PRIMER

Ključ je generisana matrica [5x5] za izabranu ključnu reč "FTN".

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

Originalan tekst: NO VI SA D

Šifrovan tekst: BL FP YG HW

B.4 Polialfabetске šifre - koriste veliki broj zamena na različitim pozicijama u poruci, u kojoj se slovo iz originalne poruke preslikava u jednu od nekoliko mogućnosti u šifrovanu poruku.

Najpoznatija šifra je Vižnerova šifra koja šifruje tekst korišćenjem tablice koja predstavlja serije Cezarovih šifara, zasnovanih na slovima ključa. Sastoji se od alfabeta napisanog 26 puta u novom redu, svaki red rotiran ulevo u odnosu na prethodni, odgovarajući svim mogućim kombinacijama (26) Cezarove šifre. U pojedinoj tački procesa šifrovanja, šifra koristi drugi alfabet iz jednog od redova. Koji će se red koristiti zavisi od ponavljajućeg ključa.

Na primer, recimo da je originalni tekst koji treba da se šifruje:

ATTACKATDAWN

Osoba koja šalje poruku bira ključ i ponavlja ga onoliko puta koliko je potrebno da odgovara dužini originalnog teksta, npr, ključ LEMON:

LEMONLEMONLE

Prvo slovo otvorenog teksta A se šifruje koristeći alfabet iz reda L, koje je prvo slovo ključa. To se radi tako što se traži slovo u redu L i koloni A Vižnerove tablice, odnosno traženo slovo je L. Za sledeće slovo originalnog teksta se koristi sledeće slovo ključa, slovo u preseku reda E i kolone T je traženo slovo X. Po tom sistemu se nastavlja do kraja originalnog teksta.

	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

PRIMER

Originalan tekst: ATTACK AT DAWN

Šifra: LEMON

Produžena šifra: LEMON LEMON LE

Šifrovan tekst: LXFOVP EF RNHR

C. Jednokratne šifre

Jednokratne šifre koriste ključ koji se samo jednom može upotrebiti i predstavljaju jedinu šifru za koju postoji matematički dokaz o savršenoj bezbednosti. Poruka se predstavlja binarnim nizom u kome je svako slovo zamenjeno odgovarajućim binarnim kodom i kodovanje ne mora biti tajno. Za šifrovanje se koristi ključ koji predstavlja slučajan niz bita iste dužine kao i sama poruka. Šifrovana poruka se iz originalne poruke dobija tako što se primeni **xor** operacija originalnog teksta i ključa, $c = a \oplus b$.

Originalan poruka:

K	I	L	L	C	A	L	L	Y
011	010	100	100	001	000	100	100	111

Ključ:

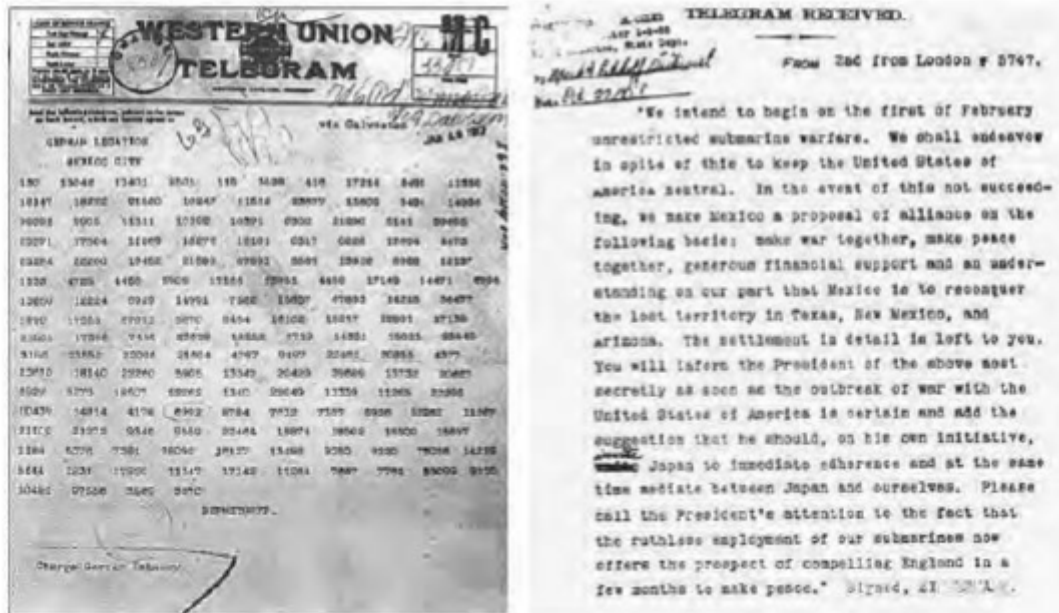
L	U	C	K	Y	L	O	O	K
100	110	001	011	111	100	101	101	011

Šifrovana poruka:

Y	L	O	Y	U	L	C	C	L
111	100	101	111	110	100	001	001	100

D. Kodne knjige

Kodne knjige predstavljaju moćan mehanizam za šifrovanje poruka i imale su veliku primenu u Drugom svetskom ratu. Najčešće su implementirane u vidu dva rečnika, od kojih se jedan koristi za šifrovanje, a drugi za dešifrovanje poruka. Ovi rečnici omogućavaju prevođenje fraza u kodne oznake i obrnuto. Sigurnost ovakvog šifarskog sistema se zasniva na fizičkoj bezbednosti kodne knjige.



Slika 8. Cimermanov telegram, šifrovana poruka i njen prevod

ZADATAK

Implementirati funkciju za šifrovanje poruka koja koristi metodu transpozicije redova i kolona.

1) Definirati ključ koji će se koristiti za šifrovanje poruka:

- Dimenzija tabele: 3 reda i 7 kolona
- Transpozicija redova: { 1, 0, 2 }
- Transpozicija kolona: { 1, 0, 6, 2, 4, 3, 5 }

2) Ispisati originalnu poruku (aplikacione podatke iz paketa) u formatu tabele.

3) Kreirati kopiju originalnog paketa tako što se iz originalnog paketa kopiraju sva zaglavlja (do aplikacionog sloja), a aplikacioni deo u kopiji paketa inicijalizuje sa nulom. Predlažemo korišćenje funkcija *memcpy()* i *memset()*.

```
void* memcpy (void * dst, const void* src, int bytes);  
void* memset (void* ptr, int value, int bytes);
```

4) Implementirati funkciju koja omogućava da se određenom redu (ili koloni) iz originalne tabele pronađe odgovarajuće mesto u transponovanoj matrici koristeći ključ u kome je definisana transpozicija redova (kolona).

Na primer, red 1 će u novoj matrici da se nalazi na poziciji 0, a red 0 na poziciji 1.

5) Omogućiti šifrovanje poruke (aplikacionih podataka) tako što će se slova iz originalne poruke premestiti na odgovarajuće pozicije u kopiranoj poruci.

6) Ispisati šifrovanu poruku u formatu tabele.

7) Za razmišljanje:

- Da li bi postojeća implementacija programa mogla da se koristi i za dešifrovanje poruka?
- U kakvom su odnosu ključ za šifrovanje i ključ za dešifrovanje poruka?
- Da li dužina poruke utiče na definiciju ključa šifrovanja?