ZAŠTITA PODATAKA

Simetrični algoritmi zaštite

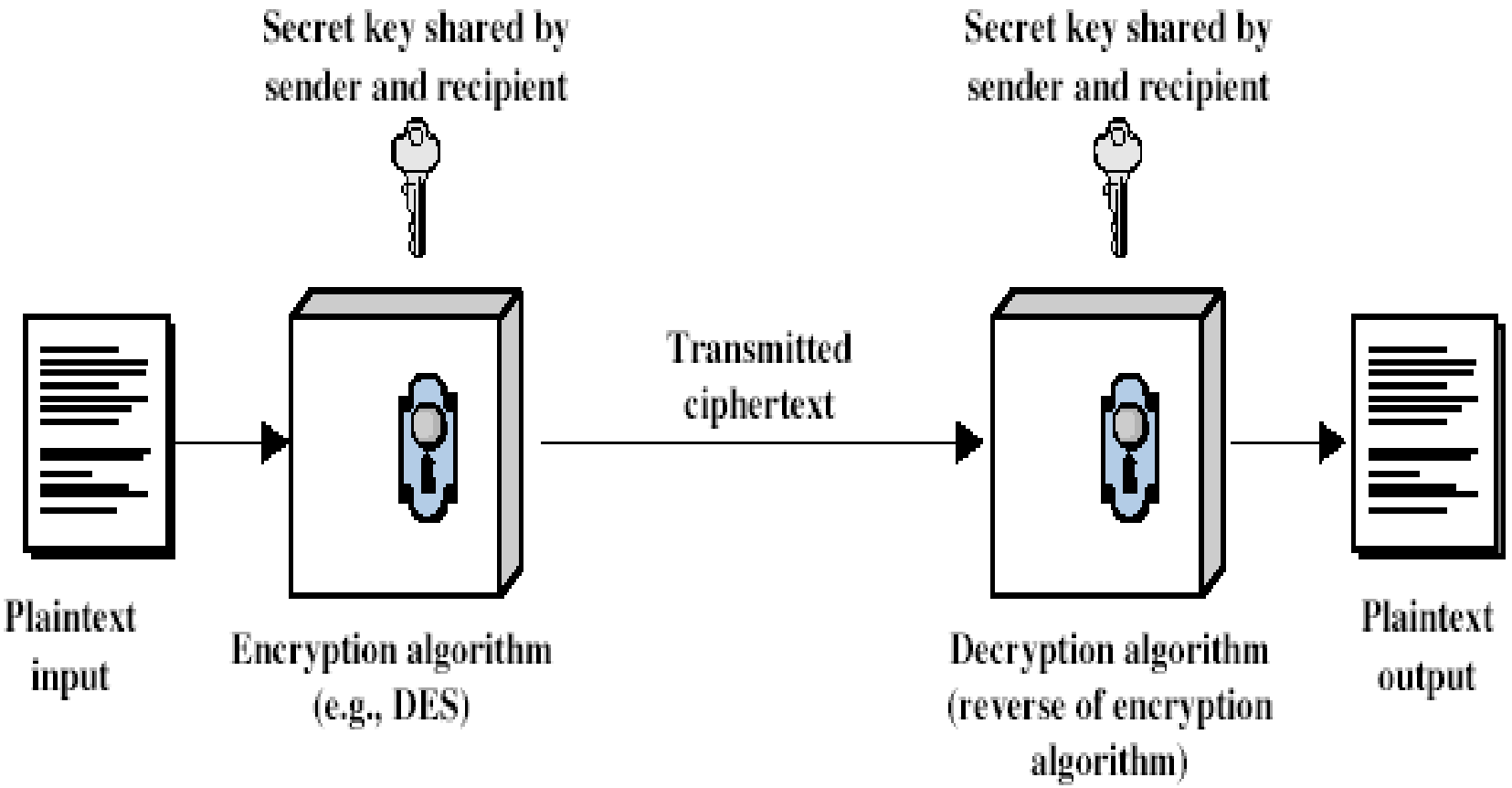
Kriptovanje (Šifrovanje)
Simetrično šifrovanje

- Konvencionalno / sa tajnim ključem / sa jednim ključem
- Pošiljalac i primalac dele zajednički ključ
- Svi klasični algoritmi šifrovanja su zasnovani na tajnom ključu
- Jedini tip šifrovanja do otkrića javnih ključeva u sedamdesetim godinama prošlog veka

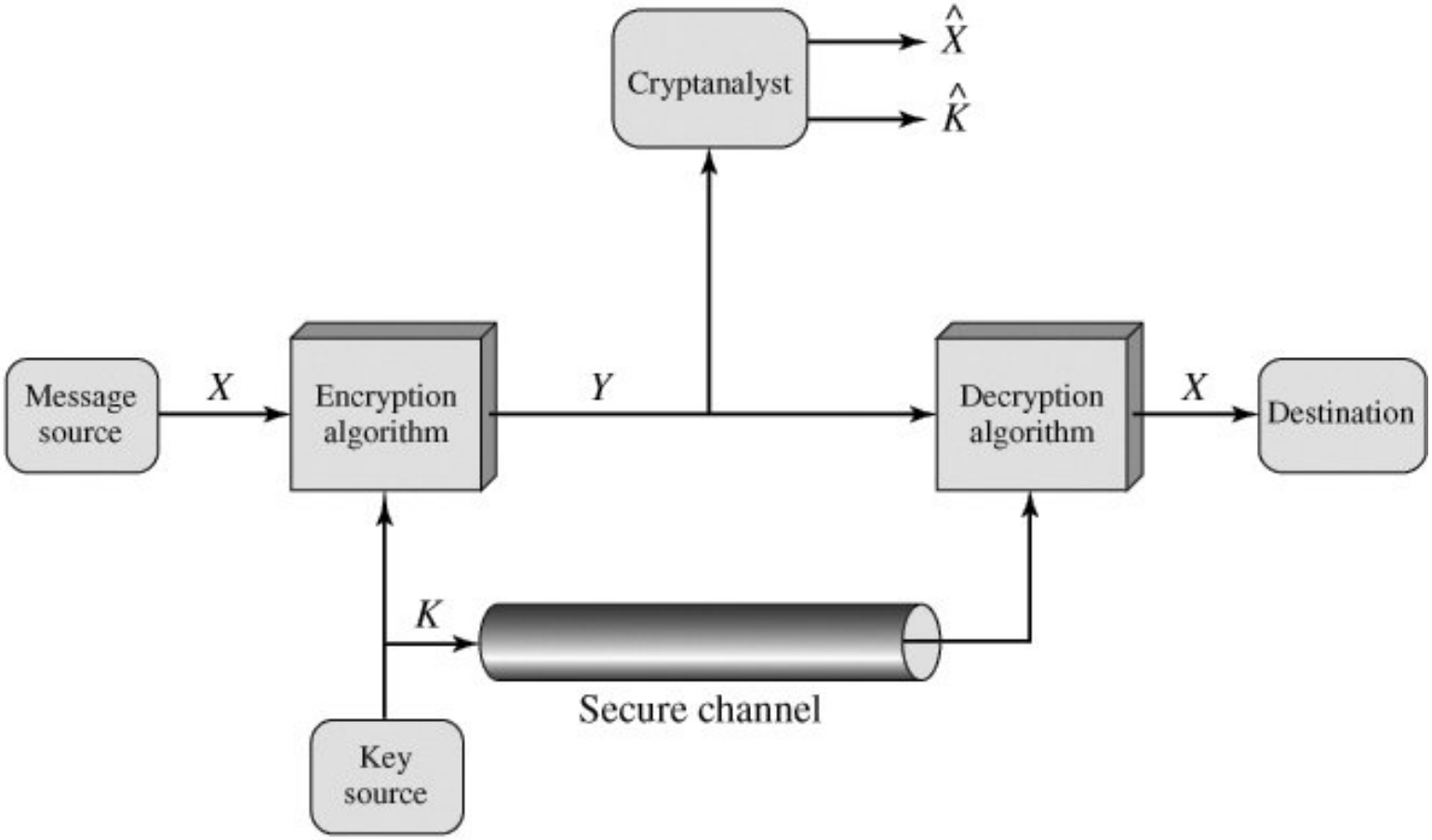
Osnovna terminologija

- **plaintext *otvoreni tekst*** - originalna poruka
- **ciphertext *šifrovana poruka*** – kodirana poruka
- **cipher *šifra*** – algoritam transformacije originalne u kodiranu poruku
- **key *ključ*** – informacija korišćena u šifri, poznata samo pošiljaocu/primaocu
- **encipher (encrypt) *šifrovanje (kriptovanje)*** – konverzija originalne poruke u kodiranu
- **decipher (decrypt) *dešifrovanje (dekriptovanje)*** – obnavljanje originalne poruke iz kodirane
- **cryptography *kriptografija*** – nauka o metodama i principima šifrovanja
- **cryptanalysis (codebreaking) *kriptoanaliza (razbijanje šifre)*** – nauka o metodama i principima dešifrovanja šifrovane poruke *bez* poznavanja ključa
- **cryptology *kriptologija*** – kriptografija + kriptoanaliza

Model simetričnog šifrovanja



Model kriptosistema



Zahtevi

- Dva zahteva za sigurnu upotrebu simetričnog šifrovanja:
  - Jak algoritam šifrovanja (čak i kada je poznat veći broj šifrovanih tekstova i njihovih otvorenih poruka, nije moguće dešifrovati novi šifrovani tekst)
  - Tajni ključ poznat samo pošiljaocu i primaocu

    $Y = E_K(X)$

    $X = D_K(Y)$
- Pretpostavlja se da je algoritam šifrovanja poznat
- Podrazumeva siguran kanal za distribuciju ključa

Kriptografija

- Određeno je:
  - Tipom korišćene operacije šifrovanja
    - Supstitucija / transpozicija / proizvod - ponavljanje
  - Brojem ključeva
    - Jedan ključ ili tajna / dva ključa ili javna
  - Načinom na koji se obrađuje originalni tekst
    - Block ***(blokovski)*** / stream ***(u toku ili sekvencijalno)***

Tipovi napada u kriptoanalizi

- **Poznata samo kodirana poruka**
  - Poznati samo algoritam, kodiran tekst i statistika i može da identifikuje originalan tekst
- **Poznat originalan tekst**
  - Poznati ili pretpostavljeni originalan tekst i kodirani tekst.
- **Izabran originalni tekst**
  - Izabere se originalan tekst da se dobije kodirani
- **Izabran kodirani tekst**
  - Izabran kodirani tekst da se dobije originalna
- **Izabrani tekst**
  - Izabere bilo originalni ili kodirani tekst

Napad grubom silom

- Proba se svaki ključ
- Osnovni napad, trajanje razbijanja proporcionalno dužini ključa
- Pretpostavlja se bilo poznat ili prepoznatljiv originalan tekst

Key Size (bits)	Number of Alternative Keys	Time required at 1 encryption/μs	Time required at 10^6 encryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\ \mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\ \mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\ \mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\ \mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26}\ \mu s = 6.4 \times 10^{12}$ years	6.4×10^{6} years

Dodatne definicije

- **Bezuslovna sigurnost**
  - Bez obzira na raspoložive računare, šifra se ne može razbiti, jer kodirana poruka nema dovoljno informacije da jedinstveno odredi odgovarajući originalan tekst
- **Računarska sigurnost**
  - Pri datim računarskim resursima, šifra se ne može razbiti u smislenom vremenu

Klasične supstitucione šifre

- Slova originalnog teksta se zamenjuju drugim slovima, brojevima ili simbolima
- Ako se originalan tekst posmatra kao niz bita, supstitucija obuhvata zamenu grupe bita originalnog teksta sa grupom bita kodiranog teksta

Cezarova šifra

- Najranija poznata
- Julije Cezar
- Upotreba u vojnim operacijama
- Zameniti svako slovo sa slovom koje je za 3 mesta dalje u azbuci
- primer:

```
danas duva jak vetar
GDQDV GXYD MDN YHWDU
```

Cezarova šifra

- Transformacija preko slova:

```
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
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
```

- Dodeliti svakom slovu broj:

```
a b c d e f g h i j k  l  m
0 1 2 3 4 5 6 7 8 9 10 11 12
n  o  p  q  r  s  t  u  v  w  x  y  Z
13 14 15 16 17 18 19 20 21 22 23 24 25
```

- Tada je Cezarova šifra:

  $C = E(\kappa,p) = (p + k) \bmod (26)$,

  $p = D(\kappa,C) = (C - k) \bmod (26)$,

  gde je *C*-šifrovani znak, *p*-originalni znak, a *k*-pomeraj

Kriptoanaliza Cezarove šifre

- Samo 26 različitih kodiranih tekstova
  - A se preslikava u A,B,..Z
- Može se probati svih 26 (25) preslikavanja
- **Metodom grube sile**
- Dat kodiran tekst, probati sa svim razmacima pomeranja
- Potrebno je prepoznati smislen tekst
- Npr. razbiti poruku “X NROLNR VDWL MH QDSDG"

Kriptoanaliza Cezarove šifre (2)

key	
1	W MQNKMQ UCVK LG PCRCF
2	V LPMJLP TBUJ KF OBQBE
3	U KOLIKO SATI JE NAPAD
4	T JNKHJN RZSH ID MZOZC
5	S IMJGIM QYRG HC LYNYB
6	R HLIFHL PXQF GB KXMXA
7	Q GKHEGK OWPE FA JWLWZ
8	P FJGDFJ NVOD EZ IVKVY
9	O EIFCEI MUNC DY HUJUX
10	N DHEBDH LTMB CX GTITW
11	M CGDACG KSLA BW FSHSV
12	L BFCZBF JRKZ AV ERGRU
13	K AEBYAE IQJY ZU DQFQT

key	
14	J ZDAXZD HPIX YT CPEPS
15	I YCZWYC GOHW XS BODOR
16	H XBYVXB FNGV WR ANCNQ
17	G WAXUWA EMFU VQ ZMBMP
18	F VZWTVZ DLET UP YLALO
19	E UYVSUY CKDS TO XKZKN
20	D TXURTX BJCR SN WJYJM
21	C SWTQSW AIBQ RM VIXIL
22	B RVSPRV ZHAP QL UHWHK
23	A QUROQU YGZO PK TGVGJ
24	Z PTQNPT XFYN OJ SFUFI
25	Y OSPMOS WEXM NI RETEH

Monoalphabetska Šifra

- Umesto samo pomeranja – promešati alfabet (permutacija svih slova alfabeta) i primeniti na otvoreni tekst
- Svako slovo originalnog teksta se preslikava u različito slovo kodiranog teksta
- Ključ je 26 slova dugačak, odnosno postoji 26! mogućih ključeva

```
Plain:  abcdefghijklmnopqrstuvwxyz
Cipher: QAZWSXEDCRFVTGBYHNUJMIKOLP
Plaintext: napad je u podne
Ciphertext: GQYQW RS M YBWGS
```

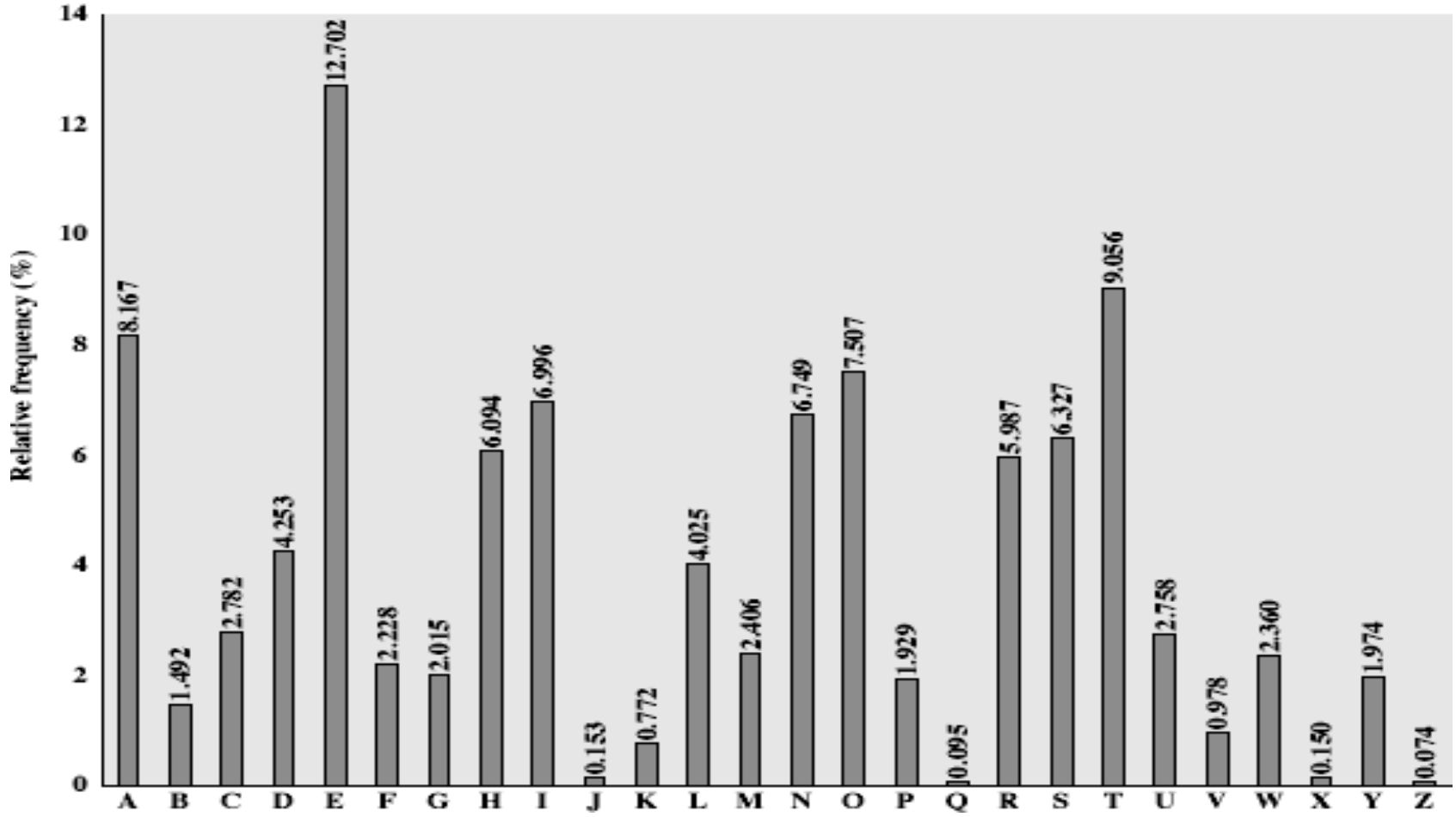
Sigurnost monoalfabetske šifre

- Ukupno 26! ključeva
- Možemo pomisliti da smo sigurni
- **!!!POGREŠNO!!!**
- Osobine jezika mogu pomoći kriptoanalizi

Redundantnosti jezika i kriptoanaliza

- Jezici su **redundantni**
- Npr. "th lrd s m shphrd shll nt wnt"
- Slova se ne upotrebljavaju sa istom učestanošću
- U Engleskom je najčešće E
- Zatim T,R,N,I,O,A,S
- Ostala su retka
- Postoje tabele učestalosti kombinacija od 2 i tri slova

Učestanost slova u engleskom



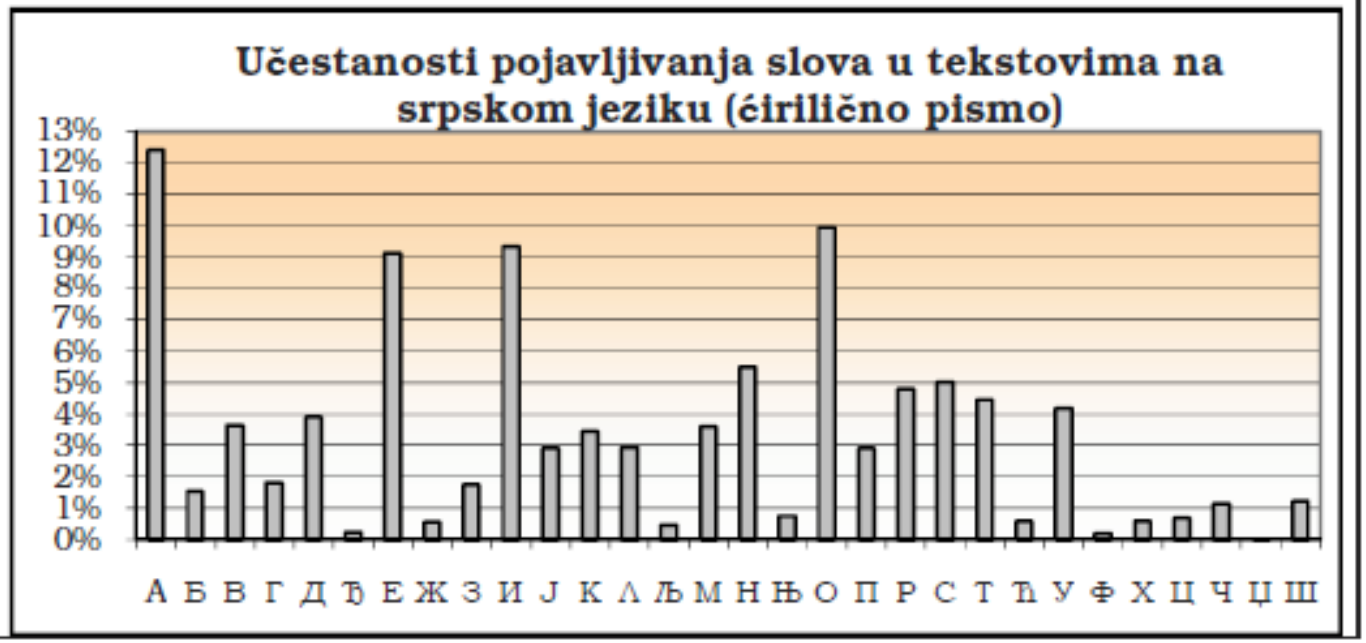
Učestanost slova u srpskom jeziku

PRIMENJENI JEZIK [српски (ћирилица)]

DUŽINA PISMA [30]

DUŽINA TEKSTA [100000]

BROJ TEKSTOVA [12]



А	0.1240	З	0.0177	Њ	0.0076	Ф	0.0020
Б	0.0156	И	0.0935	О	0.0996	Х	0.0061
В	0.0366	Ј	0.0291	П	0.0292	Ц	0.0069
Г	0.0181	К	0.0347	Р	0.0482	Ч	0.0115
Д	0.0393	Л	0.0294	С	0.0502	Џ	0.0003
Ђ	0.0023	Љ	0.0048	Т	0.0447	Ш	0.0125
Е	0.0913	М	0.0362	Ћ	0.0061		
Ж	0.0056	Н	0.0551	У	0.0421		

Koristimo u kriptoanalizi

- Osnovni koncept – šifre sa monoalfabetskom substitucijom ne menjaju relativnu učestalost slova
- Izračunati učestalost slova u kodiranom tekstu
- Uporediti učestalost sa poznatom statistikom jezika
- Tabele sa čestim parovima i trojkama slova pomažu

Primer kriptoanalize

- Dat kodirani tekst:

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
```

- Izračunati relativnu učestalost slova u tekstu
- Pretpostaviti da su P i Z, e i t
- Pretpostaviti ZW je “th” pa je ZWP “the”
- Produžavanjem sa pretpostavkama i ispravkama grešaka:

```
it was disclosed yesterday that several informal but
direct contacts have been made with political
representatives of the viet cong in moscow
```

Poboljšanje – Gausova metoda

- Slova koja se pojavljuju sa većom učestanošću kodovati sa više različitih kodova koji bi se ili ciklično ili slučajno menjali.
- Time se menja frekvencija pojavljivanja pojedinih slova u kriptovanom tekstu
- Problem – učestalosti dvoslovnih i troslovnih kombinacija ostaju i u ovakvom tekstu.

Playfair šifra

- Veliki broj ključeva u monoalphabetskoj šifri nije obezbedio sigurnost
- Jedan pristup popravljanju sigurnosti je šifrovanje većeg broja slova od jednom
- **Playfair šifra** je primer
- izmišljen je 1854. godine

Playfair matrica ključa

- 5X5 matrica slova zasnovana na ključu
- Napuni se po vrstama sa slovima ključne reči, uz izostavljanje duplikata
- Popuni se ostatak matrice sa ostalim slovima
- Ako izaberemo ključnu reč MONARCHY

```
MONAR
CHYBD
EFGIK
LPQST
UVWXZ
```

I i J SU JEDNO SLOVO!

Šifrovanje i dešifrovanje

- Originalni tekst se šifruje po dva slova odjednom, po sledećim pravilima:
  1. Ako je par ponovljeno slovo, ubaciti slovo za ispunu – npr. 'X', pa se reč "balloon" šifruje po parovima "ba lx lo on"
  2. Ako oba slova pripadaju istom redu, zameni sa slovima udesno u istom redu (ROR) – npr. “ar" se šifruje kao "RM"
  3. Ako su oba slova u istoj koloni, zameni sa slovom ispod (opet sa rotacijom) – npr “mu" se šifruje kao "CM"
  4. U svim ostalim slučajevima se slovo zamenjuje onim slovom iz iste kolone kojem odgovara kolona slova iz para (temena pravougaonika) – npr. “hs" se šifruje kao "BP", a “ea" kao "IM" ili "JM" (po želji)

Sigurnost Playfair šifre

- Sigurnost znatno popravljena u odnosu na monoalfabetsku šifru
- Postoje 26 x 26 = 676 digrama (parova slova)
- Potrebno je sada 676 tabela sa učestalošću pojave da bi se analiziralo (prema 26 za monoalfabetsku)
- Zbog statistike –uzorak kodiranog teksta mora biti odgovarajući broj puta veći
- Široko primenjena tokom dugog perioda (vojske SAD i Britanije u prvom svetskom ratu)
- Može se razbiti sa nekoliko stotina slova
- Još uvek sadrži mnoge elemente strukture originalnog teksta

Ćirilična Playfair matrica

- Probajte da kriptujete teskt
  - “заштитаподатака”

ШИФРАБ
ВГДЂЕЖ
ЗЈКЛЉМ
НЊОПСТ
ЋУХЦЧЏ

Polialfabetske šifre

- Drugi pristup popravljanju sigurnosti je upotreba višestrukih alfabeta šifara
- Naziv **polialfabetske substitucione šifre**
- Otežava kriptoanalizu jer treba pogoditi više alfabeta, a zaravnjuje distribuciju učestalosti
- Koristi se ključ da se izabere alfabet koji će se koristiti za svako slovo u originalnom tekstu
- Definisanim redom koristiti svaki alfabet
- Ponovo početi od početka kada je dostignut kraj ključa

Vigenère šifra

- Najjednostavnija polialfabetska šifra je **Vigenère šifra**
- U osnovi su višestruke Cezarove šifre
- Ključ je dugačak više slova $K = k_1 k_2 \ldots k_d$
- i-to slovo određuje i-ti alfabet koji se koristi
- Koristi svaki alfabet po redu
- Ponovi alfabet od početka, posle d-tog slova u poruci
- Dekriptovanje se obavlja inverzno (alfabet – slovo)

Vigenère tablica

Key	Plaintext	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

- Ispisati originalan tekst
- Ispisati ponovljeni ključ iznad originalnog teksta
- Iskoristiti svako slovo ključa kao ključ Cezarove šifre
- šifruje odgovarajuće slovo originalnog teksta
- Npr. upotrebom ključa *deceptive*

```
key:        deceptivedeceptivedeceptive
plaintext:  wearediscoveredsaveyourself
ciphertext:ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

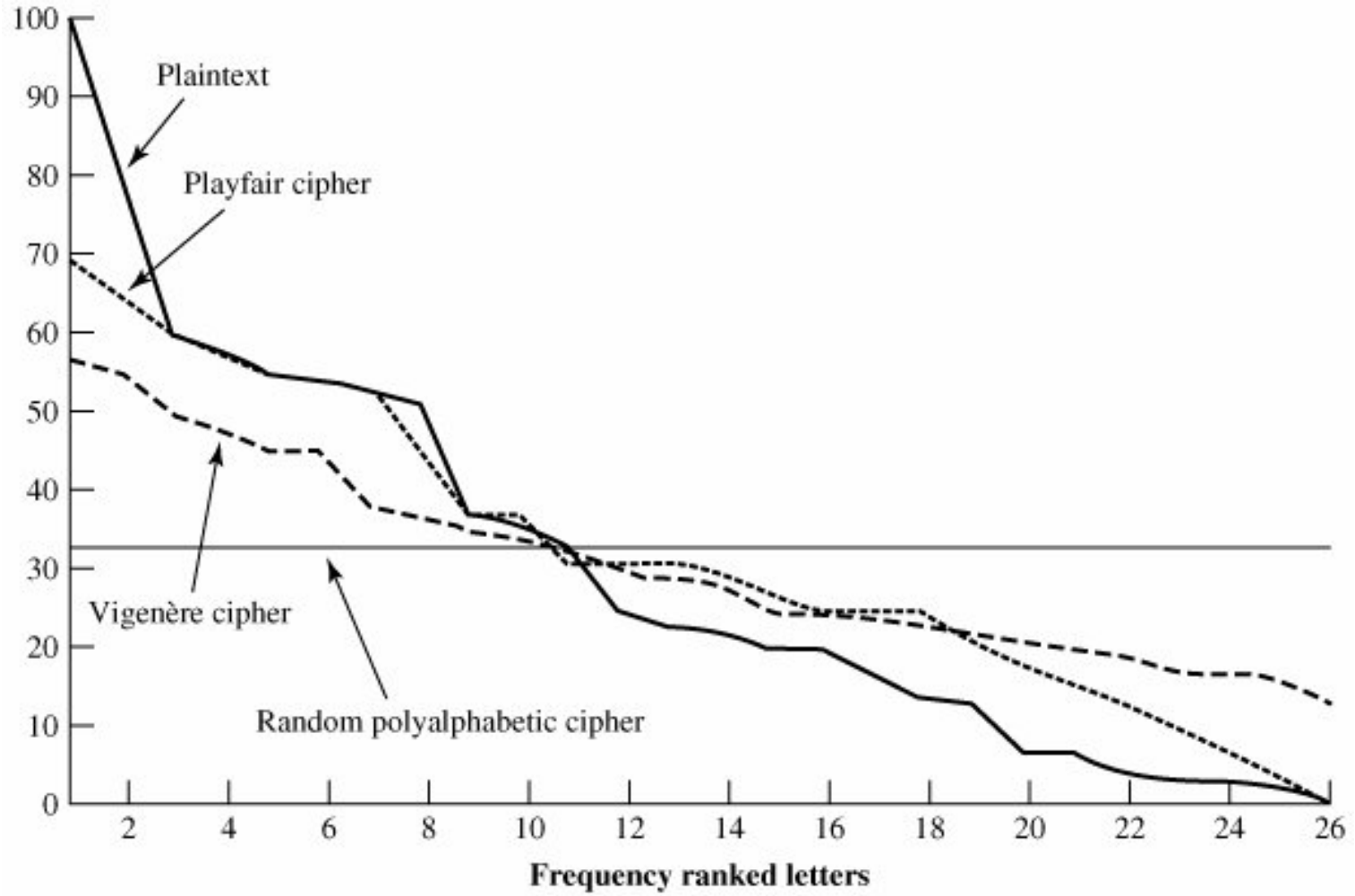
Pomoćna sredstva

- Pomoćni alati pomažu u šifrovanju i dešifrovanju
- **Saint-Cyr klizač** je jednostavno pomagalo
  - Klizač sa ponovljenim alfabetima
  - Poravnaj slovo originalnog teksta sa odgovarajućim ključem i pročitaj kodirano slovo
- Može se presaviti na disk za šifrovanje

Sigurnost Vigenère šifre

- Više slova u kodiranom tekstu za svako slovo originalnog teksta
- Učestalost slova narušena, ali nije potpuno izgubljena
- Ideja za kriptoanalizu: početi sa učestalošću slova
  - Da li je monoalfabetska
  - Pokušati odrediti broj alfabeta i tada napadati kao monoalfabetski

Statističke osobine kriptovanog teksta



Kasiski Metod

- Ponavljanja u kodiranom tekstu daju sugestiju o dužini perioda
- Pronađi nekoliko ponovljenih sekvenci u šifrovanoj poruci
- Izračunaj rastojanja između ovakvih sekvenci i traži zajednički faktor
- Dalje posmatraj šifru kao sekvencu monoalfabetskih šifara i koristi frekvenciju slova za kriptoanalizu

Autokey šifra

- Želimo **ključ dužine poruke** - Vigenère predložio **autokey** šifru
- Ključ (ključna reč) koji prethodi originalnom tekstu odsečenom na kraju je celokupan ključ
- Poznavanjem ključne reči se otkriva prvih nekoliko slova otvorenog teksta pa se onda ta slova koriste za dešifrovanje daljih slova poruke
- Još uvek postoje karakteristike učestalosti
- Npr. ključ *deceptive*

```
key:        deceptivewearediscoveredsav
plaintext:  wearediscoveredsaveyourself
ciphertext:ZICVTWQNGKZEIIGASXSTSLVVWLA
```

Hill-ova šifra

- *m* sukcesivnih slova originalnog teksta se zamenjuje sa *m* slova kriptovanog teksta. Dobija se *m* linearnih jednačina (m=3):
  - $c_1 = (k_{11}P_1 + k_{21}P_2 + k_{31}P_3) \bmod 26$
  - $c_2 = (k_{12}P_1 + k_{22}P_2 + k_{32}P_3) \bmod 26$
  - $c_3 = (k_{13}P_1 + k_{23}P_2 + k_{33}P_3) \bmod 26$
- $\mathbf{C} = \mathbf{PK} \bmod 26$
- $\mathbf{P} = \mathbf{PKK^{-1}} \bmod 26 = \mathbf{CK^{-1}} \bmod 26$, K^{-1} je inverzna matrica (po modulu 26)

Enkripcija Hill trigram

$$K = \begin{Vmatrix} 3 & 25 & 4 \\ 23 & 6 & 15 \\ 13 & 17 & 21 \end{Vmatrix}$$

P=YOU (24|14|20)

c1=3*24+14*23+13*20 mod 26 = 654 mod 26 = 4 (E)
c2=25*24+14*6+17*20 mod 26 = 1024 mod 26 = 10 (K)
c3=4*24+14*15+21*20 mod 26 = 726 mod 26 = 24 (U)

C=EKY (4|10|24)

Dekriptovanje Hill algoritam

- Određivanje K^{-1}:
  - det(K) mod 26 = -6335 mod 26 = 9 mod 26
  - $\det(K)^{-1} = 9^{-1} \bmod 26$
  - Pošto je 9*3=27, a 27=1 mod 26, $\det(K)^{-1} = 9^{-1} \bmod 26 = 3$
  - Odrediti adjungovanu matricu
  - $K^{-1} = \det(K)^{-1} \text{adj}(K) \bmod 26 = 3\ \text{adj}(K) \bmod 26$

$$K^{-1} = \begin{Vmatrix} 3 & 7 & 13 \\ 20 & 7 & 11 \\ 3 & 16 & 19 \end{Vmatrix}$$

Dekriptovanje

$$K^{-1} = \begin{Vmatrix} 3 & 7 & 13 \\ 20 & 7 & 11 \\ 3 & 16 & 19 \end{Vmatrix}$$

C= EKY (4|10|24)

p1= 4*3+10*20+24*3 mod 26 = 284 mod 26 = 24 (Y)
p2= 4*7+10*7+24*16 mod 26 = 482 mod 26 = 14 (O)
p3= 4*13+10*11+24*19 mod 26 = 618 mod 26 = 20 (U)

P=YOU (24|14|20)

Dekriptovati poruku:

EKYIMBHKXVNAZYUELMVPBJVS

Vernam-ova šifra

- 1918 godina.
- Radi nad binarnim podacima
- $c_i = p_i \text{ XOR } k_i$
- $p_i = c_i \text{ XOR } k_i$
- Vernam je predložio dugačku traku sa ključem koja se ponavlja
- I dalje ostaje mogućnost statističke analize teksta sa dovoljnom količinom kriptografskog materijala

One-Time Pad

- Stvarno slučajan ključ
- Ne može se razbiti, jer kodirani tekst nema statističku zavisnost sa originalnim tekstom
- Može se iskoristiti samo jednom
- problem distribucije ključeva
- Number radio stations?

```
ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
key:        pxlmvmsydofuyrvzwc tnlebnecvgdupahfzzlmnyih
plaintext:  mr mustard with the candlestick in the hall

ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
key:        mfugpmiydgaxgoufhklllmhsqdqogtewbqfgyovuhwt
plaintext:  miss scarlet with the knife in the library
```

Transpozicioni algoritmi

- ne radi se zamena slova u originalnoj poruci
- već se vrši promena redosleda slova u originalnoj poruci
- šifrovana poruka ima identičnu frekvenciju korišćenja slova kao i originalna poruka

Rail Fence algoritam

- ispisuje se poruka dijagonalno u nekoliko redova
- krajnja šifra se piše red po red

- npr. za: `VOZ IDE PO PRUZI`
- u tri reda (što predstavlja ključ)

```
V...d...p...i
.o.i.e.o.r.z.
..z...p...u..
```

- dobijemo šifru

```
VDPIOIEORZZPU
```

- trivijalno za kriptoanalizu

Row Transposition algoritam

- kompleksniji od prethodnog
- originalna poruka se ispisuje u obliku matrice, red po red
- šifrovana poruka se čita kolonu po kolonu
- kolone se permutuju po određenom redosledu koji predstavlja ključ

```
Plaintext: ZANIMLJIVA INFORMACIJA
Key:       4 3 1 2 5 6 7
           z a n i m l j
           i v a i n f o
           r m a c i j a
Ciphertext: NAAIICAVMZIRMNILFJJOA
```

Transpozicioni algoritam

- lako se prepoznaju, zbog identične frekvencije slova kao u originalnoj poruci
- za prethodni algoritam kriptoanaliza je pravolinijska
- mogu se učiniti znatno sigurnijim ukoliko se algoritam ponovi više puta
- za prethodni primer:

```
Plaintext: NAAIICAVMZIRMNILFJJOA
Key:       4 3 1 2 5 6 7
           n a a i i c a
           v m z i r m n
           i l f j j o a
Ciphertext: AZFIIJAMLNVIIRJCMOANA
```

Transpozicioni algoritam

- da bi prepoznali efekat dvostruke transpozicije, numerišimo redosled slova u originalnoj poruci
- Z A N I M L J I V A I N F O R M A C I J A
- 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21
- nakon prve transpozicije imamo:
- N A A I I C A V M Z I R M N I L F J J O A
- 3 10 17 4 11 18 2 9 16 1 8 15 5 12 19 6 13 20 7 14 21
- nakon druge transpozicije imamo:
- A Z F I I J A M L N V I I R J C M O A N A
- 17 1 13 4 8 20 10 16 6 3 9 19 11 15 7 18 5 14 2 12 21
- druga permutacija za razliku od prve je mnogo manje struktuirana, samim tim i teža za kriptoanalizu

Produkcioni algoritmi

- algoritmi bazirani na zameni ili transpoziciji nisu dovoljno sigurni zbog jezičkih karakteristika
- zato se koristi više algoritama uzastopno da bi se učinili sigurnijim, ali:
  - dva algoritma zamene, čine kompleksniju zamenu
  - dva transpozicije, kompleksniju transpoziciju
  - ali algoritam zamene, praćen algoritmom transpozicije čini novu, mnogo komplikovaniju šifru
- ovo je most između klasičnih i modernih šifri

Rotor mašine

- pre modernih šifara, rotor mašine su bile najpopularnije produkcione šifre
- korišćene su u Drugom svetskom ratu
  - Nemačka Enigma, Japanska Purple
- korišćen je niz nezavisno rotirajućih cilindara
- svaki cilindar ima 26 ulaznih i 26 izlaznih tačaka, koje su interno međusobno povezane tako da je svaki ulaz povezan sa jedinstvenim izlazom

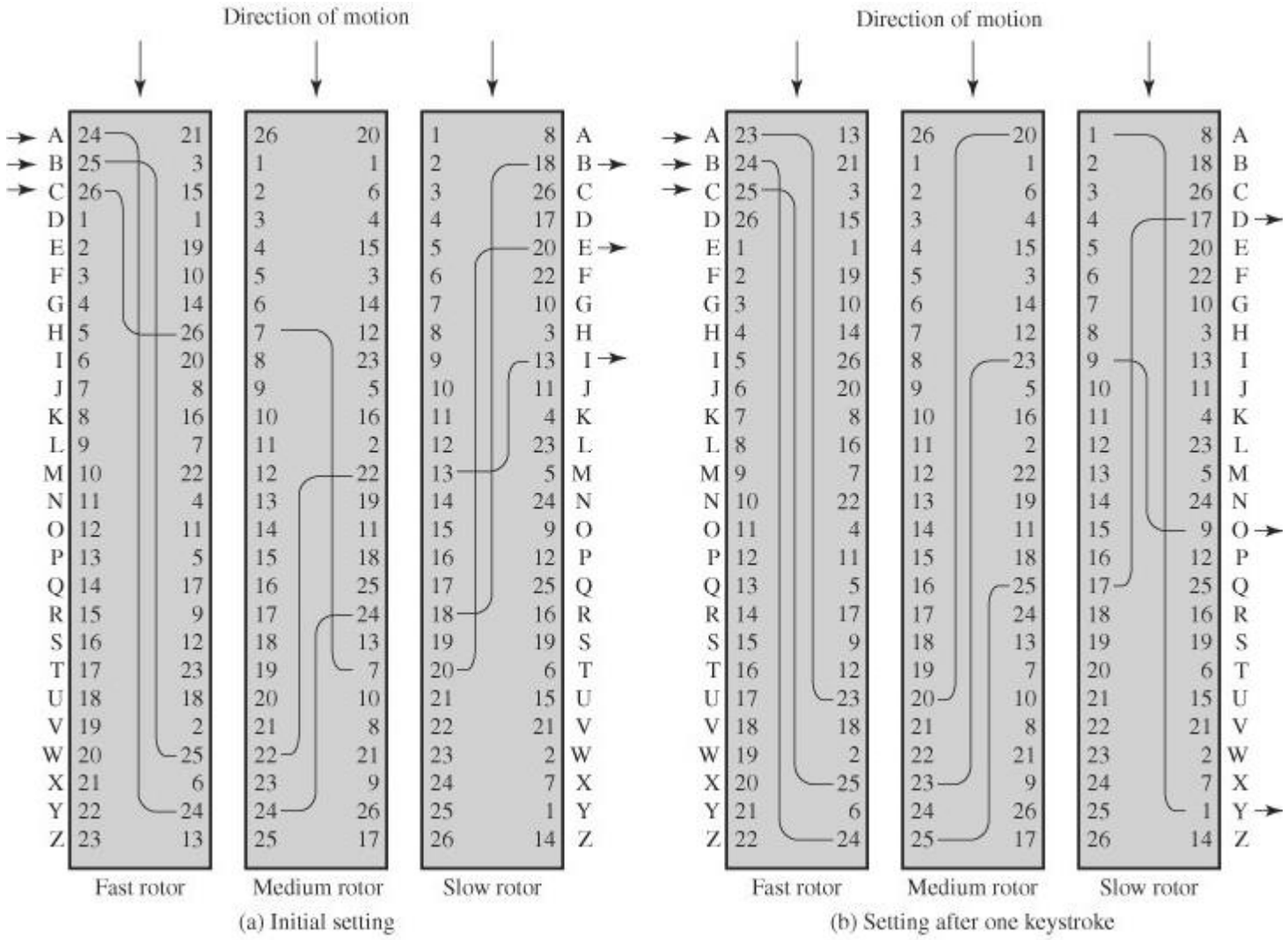
Rotor mašine

- ako se svakoj ulaznoj i izlaznoj tački dodeli po jedno slovo engleskog alfabeta, tada jedan cilindar definiše jedan monoalfabetski algoritam zamene
- ako posmatramo mašinu sa samo jednim cilindrom i ako cilindar rotira nakon šifrovanja jednog slova, imali bismo polialfabetski algoritam zamene sa periodom 26
- mašina sa jednim cilindrom ne proizvodi složene šifre, ali kada se upotrebi veći broj cilindara situacija se menja

Rotor mašine (3)

- ako posmatramo mašinu sa 3 cilindra, koji su redno vezani, tako da su izlazi prvog povezani na ulaze drugog, a izlazi drugog povezani na ulaze trećeg cilindra
- sada se prvi cilindar rotira za 1 nakon svakog šifrovanog slova, drugi cilindar se rotira za 1 svaki put kada prvi cilindar završi kompletan ciklus (26 rotacija), treći cilindar se rotira za 1 svaki put kada drugi cilindar završi kompletan ciklus (26 rotacija)
- sada postoji 17576 različitih algoritama zamene koji se koriste pre nego što dođe do ponavljanja
- ako se doda četvrti cilindar period je 456976, a sa pet cilindara 11881376

Rotor mašine (4)



Enigma

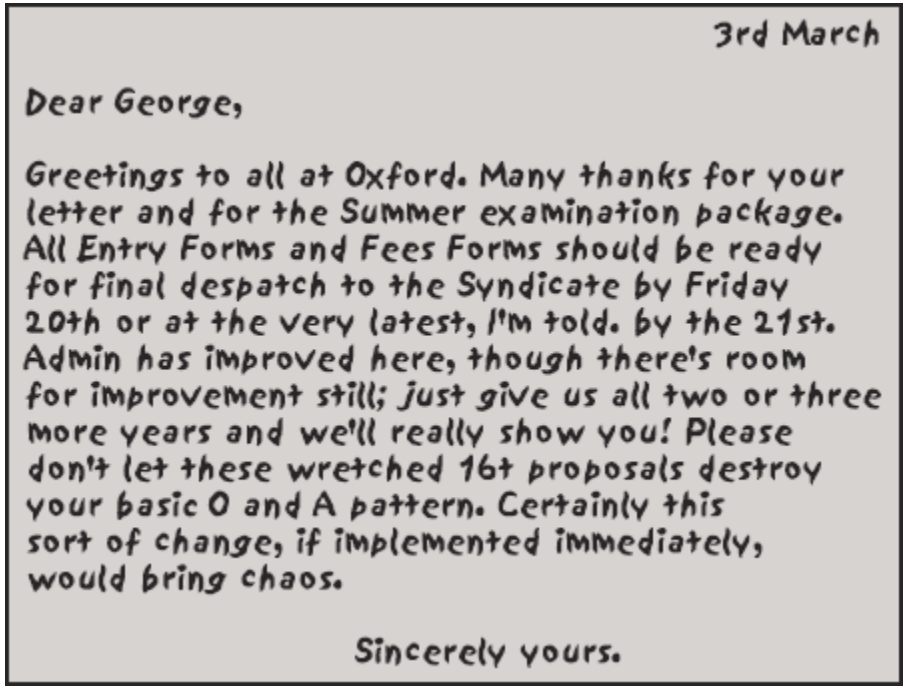
- 65 x 45 x 35cm, 50kg
- Ključ – knjiga kodova
- Postupak:
  - podešavanje prema ključu
  - kucanje slova po tastaturi
  - paljenje lampice koja odgovara šifrovanom slovu
  - slanje poruke radio vezom

Bomba

- 2.1m x 1.98m x 0.61m
- poznata originalna poruka
- na osnovu prevoda pronaći sva moguća podešavanja Enigme

Steganografija

- Steganos (gr): Zaštićen
- Što je danas lep dan. Iako je povremeno oblačno. Fali malo viša temperatura. Rekli su da će otopliti od sutra. Ako bude tako, biće dobro.
- ŠIFRA



3rd March

Dear George,

Greetings to all at Oxford. Many thanks for your letter and for the Summer examination package. All Entry Forms and Fees Forms should be ready for final despatch to the Syndicate by Friday 20th or at the very latest, I'm told. by the 21st. Admin has improved here, though there's room for improvement still; just give us all two or three more years and we'll really show you! Please don't let these wretched 16t proposals destroy your basic O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

Sincerely yours.

Steganografija

- alternativa za šifrovanje
- sakriva postojanje poruke
  - koristi se samo podskup slova/reči u dužoj poruci na neki način označenoj
  - koristi se nevidljivo mastilo
  - sakrivanje poruke u nekoj sličici ili zvuku
- ima mane
  - velika poruka da se sakrije relativno mali broj bita

Radio:Milutin Milosavljevic