ЗАШТИТА ПОДАТАКА

Симетрични алгоритми заштите

увод у криптографију

Zadatak 1

- Osnovni kriptografski algoritmi. Šifrovati poruku “napadamo u podne ako ne bude vetra”, koristeći svaki od sledećih osnovnih kriptografskih algoritama:
  - Cezar (*Ceazar*) algoritam u originalnom obliku (pomeraj je 3),
  - monoalfabetski algoritam sa ključem: qwertzuiopasdfghjklyxcvbnm,
  - *Playfair* algoritam sa ključnom reči: vetrobran (i i j tretirati kao jedno polje matrice),
  - *Rail Fence* algoritam u tri reda,
  - *Row Transposition* algoritam sa ključem: 4312567
- Napomena: koristiti 26 slova engleske abecede.

Rešenje

- napadamo u podne ako ne bude vetra

```
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
```

Rešenje

- napadamo u podne ako ne bude vetra

  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

- **Q**

Rešenje

- napadamo u podne ako ne bude vetra

  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

- **QD**

Rešenje

- napadamo u podne ako ne bude vetra

  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

- **QDS**

Rešenje

- napadamo u podne ako ne bude vetra

```
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
```

- **QDSDGDPR X SRGQH DNR QH EXGH YHWUD**

Rešenje

- napadamo u podne ako ne bude vetra

  `abcdefghijklmnopqrstuvwxyz`

  `qwertzuiopasdfghjklyxcvbnm`

Rešenje

- napadamo u podne ako ne bude vetra

  abcdefghijklmnopqrstuvwxyz

  qwertzuiopasdfghjklyxcvbnm

- **f**

Rešenje

- napadamo u podne ako ne bude vetra

  abcdefghijklmnopqrstuvwxyz

  qwertzuiopasdfghjklyxcvbnm

- **fq**

Rešenje

- napadamo u podne ako ne bude vetra

  abcdefghijklmnopqrstuvwxyz

  qwertzuiopasdfghjklyxcvbnm

- **fqh**

Rešenje

- napadamo u podne ako ne bude vetra

  abcdefghijklmnopqrstuvwxyz

  qwertzuiopasdfghjklyxcvbnm

- **fqhqrqdg x hgrft qag ft wxrt ctykq**

Rešenje

- napadamo u podne ako ne bude vetra

Rešenje

- na pa da mo up od ne ak on eb ud ev et ra
- vetrobran

Rešenje

- na pa da mo up od ne ak on eb ud ev et ra
- vetrobran

v				

Rešenje

- na pa da mo up od ne ak on eb ud ev et ra
- vetrobran

V	E			

Rešenje

- na pa da mo up od ne ak on eb ud ev et ra
- vetrobran

V	E	T		

Rešenje

- na pa da mo up od ne ak on eb ud ev et ra
- vetrobran

V	E	T	R	O
B	A	N		

Rešenje

- na pa da mo up od ne ak on eb ud ev et ra

V	E	T	R	O
B	A	N	C	

Rešenje

- na pa da mo up od ne ak on eb ud ev et ra

V	E	T	R	O
B	A	N	C	D

Rešenje

- na pa da mo up od ne ak on eb ud ev et ra

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

Rešenje

- na pa da mo up od ne ak on eb ud ev et ra

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

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

- cn

Rešenje

- na pa da mo up od ne ak on eb ud ev et ra

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

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

- cn mn

Rešenje

- na pa da mo up od ne ak on eb ud ev et ra

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

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

- cn mn bn se xl dk

Rešenje

- na pa da mo up od ne ak on eb ud ev et ra

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

- cn mn bn se xl dk at dg td va zb te tr ec

Rešenje

- napadamo u podne ako ne bude vetra
- n d u n o u e
- a a a o p d e k n b d v t a
- p m o a e e r
- ndunoueaaaopdeknbdvtapmoaeer

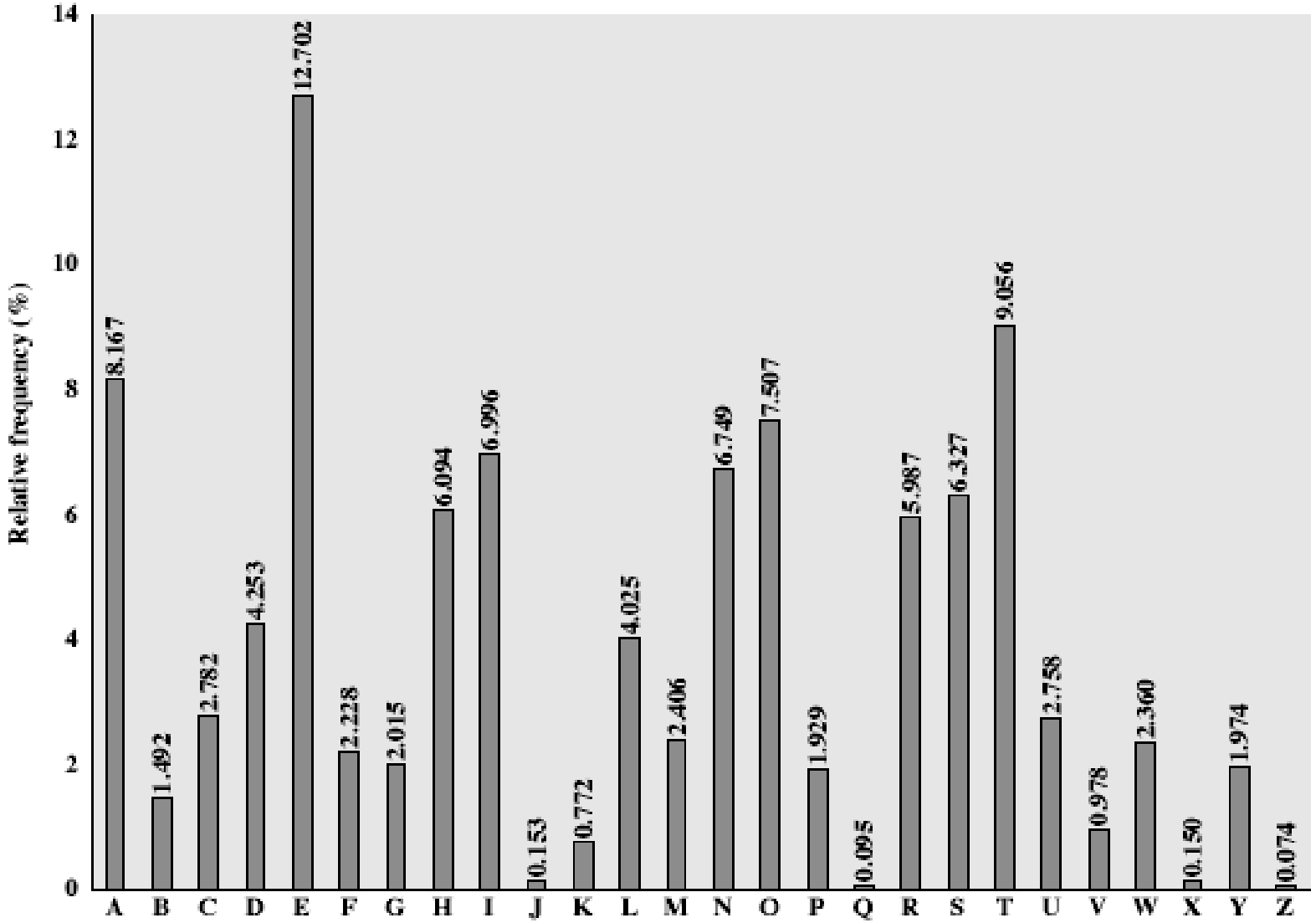
Rešenje

- napadamo u podne ako ne bude vetra
- 4 3 1 2 5 6 7
- n a p a d a m
- o u p o d n e
- a k o n e b u
- d e v e t r a
- ppovaoneaukenoadddetanbrmeua

Zadatak 2

- Prikazati postupak kriptoanalize monoalfabetske šifre nad porukom UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESX UDBMETSXAIZVUEPHZHMDZSHZOWSFPAPPDT SVPQUZWYMXUZUHSXEPYEPOPDZSZUFPOMBZ WPFUPZHMDJUDTMOHMQ

Rešenje


Relative frequency (%)
0
2
4
6
8
10
12
14
A 8.167
B 1.492
C 2.782
D 4.253
E 12.702
F 2.228
G 2.015
H 6.094
I 6.996
J 0.153
K 0.772
L 4.025
M 2.406
N 6.749
O 7.507
P 1.929
Q 0.095
R 5.987
S 6.327
T 9.056
U 2.758
V 0.978
W 2.360
X 0.150
Y 1.974
Z 0.074

Rešenje

- Analiza frekvencije pojavljivanja karaktera
- Poruka:
  UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBM
  ETSXAIZVUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYM
  XUZUHSXEPYEPOPDZSZUFPOMBZWPFUPZHMDJUDT
  MOHMQ
- Pojavljivanje pojedinačnih karaktera:

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
2	2	0	6	6	4	2	7	1	1	0	0	8	0	9	16	3	0	10	3	10	5	4	5	2	14

Rešenje

- P i Z -> E i T
- Osim pojedinačnih frekvencija, analiza se sprovodi i na osnovu frekvencije digrama ili sekvence od više sukcesivnih karaktera
- najčešće TH -> Z = T, P = E i W = H
- *T**********E**E*TE****TH*T*E*E**********
  T***E*T***T**T*H**E*EE****E**TH****T*****E**
  E*E*T*T**E***THE**ET**********
- TH*T -> THAT ZWSZ, odatle je S = A

Rešenje

- Nakon dekripcije dobija se sledeća poruka:

IT WAS DISCLOSED YESTERDAY THAT SEVERAL INFORMAL BUT DIRECT CONTACTS HAVE BEEN MADE WITH POLITICAL REPRESENTATIVES OF THE VIET CONG IN MOSCOW

Zadatak 3

- Upotrebom ključa K šifrovati poruku *pay more money* *korišćenjem* Hill cipher algoritma

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

Rešenje

- Karakteri se kodiraju numeričkim vrednostima a = 0, b = 1, ... , z = 25
- **C** = **PK** mod 26
- Bira se m sukcesivnih karaktera plaintext-a i rešava se sistem jednačina:

  $c1 = (k11p1 + k21p2 + k31p3) \bmod 26$

  $c2 = (k12p1 + k22p2 + k32p3) \bmod 26$

  $c3 = (k13p1 + k23p2 + k33p3) \bmod 26$

Rešenje

plaintext: paymoremoney

m = 3

pay ⇔ 15 0 24

(15 0 24)**K** = (303 303 531) mod 26 = (17 17 11) = RRL

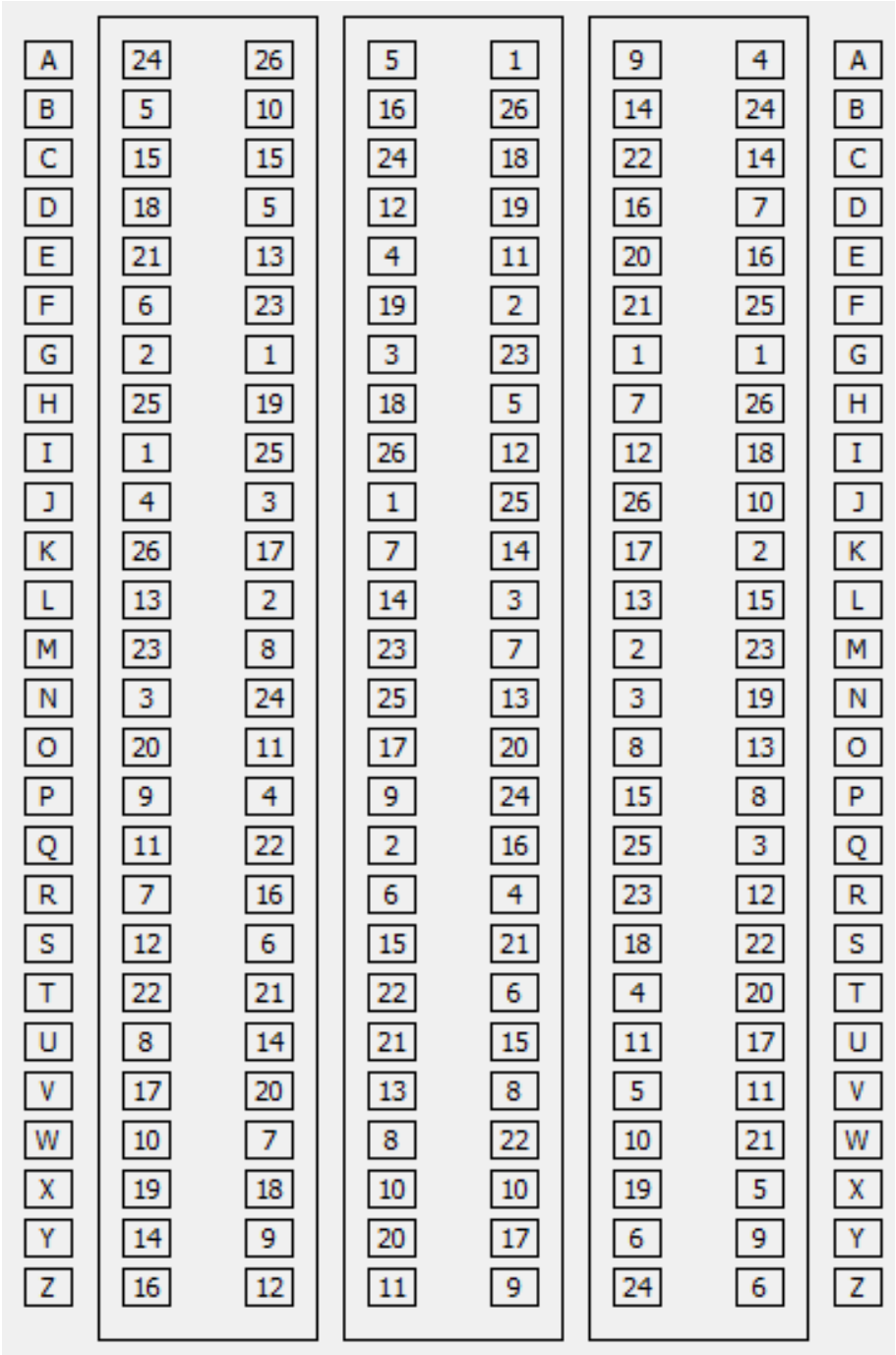
- ciphertext: RRLMWBKASPDH

- Dešifrovanje koristi inverznu matricu ključa
- **P** = D(**K**, **C**) = **CK**-1 mod 26 = **PKK**-1 = **P**

$$K^{-1} = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$$

Zadatak 4

- Prikazati postupak šifrovanja poruke *this is rotor machine algorithm* korišćenjem Rotor mašine.
- Početna konfiguracija



A	24	26	5	1	9	4	A
B	5	10	16	26	14	24	B
C	15	15	24	18	22	14	C
D	18	5	12	19	16	7	D
E	21	13	4	11	20	16	E
F	6	23	19	2	21	25	F
G	2	1	3	23	1	1	G
H	25	19	18	5	7	26	H
I	1	25	26	12	12	18	I
J	4	3	1	25	26	10	J
K	26	17	7	14	17	2	K
L	13	2	14	3	13	15	L
M	23	8	23	7	2	23	M
N	3	24	25	13	3	19	N
O	20	11	17	20	8	13	O
P	9	4	9	24	15	8	P
Q	11	22	2	16	25	3	Q
R	7	16	6	4	23	12	R
S	12	6	15	21	18	22	S
T	22	21	22	6	4	20	T
U	8	14	21	15	11	17	U
V	17	20	13	8	5	11	V
W	10	7	8	22	10	21	W
X	19	18	10	10	19	5	X
Y	14	9	20	17	6	9	Y
Z	16	12	11	9	24	6	Z

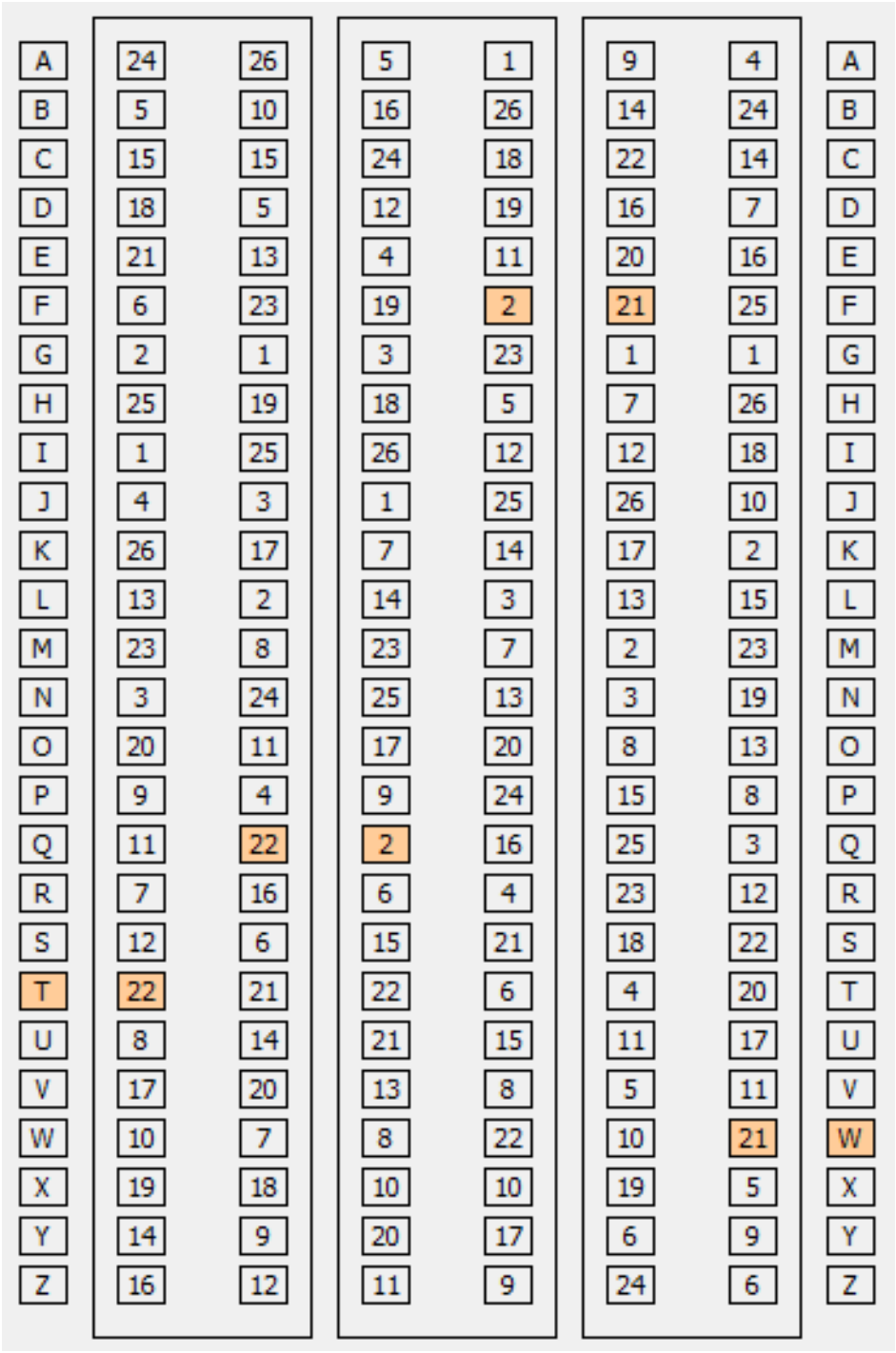
Rešenje

- Plaintext:

this is rotor machine algorithm

- Ciphertext:

w



Rešenje

- Plaintext:

this is rotor machine algorithm

- Ciphertext:

wghfnzkbgfvzsumendpvtuofcei