KRIPTOGRAFIJA

SIGURNOST PODATAKA U ONLINE OKRUŽENJU

- Online trgovina? Plaćanje računa? Slanje poruka?
- Jesu li ovakve i slične radnje sigurne?
- podatci putuju mrežom kao paketi kojima svatko može pristupiti
- web-stranica HTTP/HTTPS (secure)
- prijava na webmail, društvenu mrežu, e-Dnevnik, prilikom slanja broja kreditne kartice, poruka i sl.
- podatci putuju **uglavnom kriptirani**
- kod računala – može se kriptirati cijeli disk računala (poslovna računala)

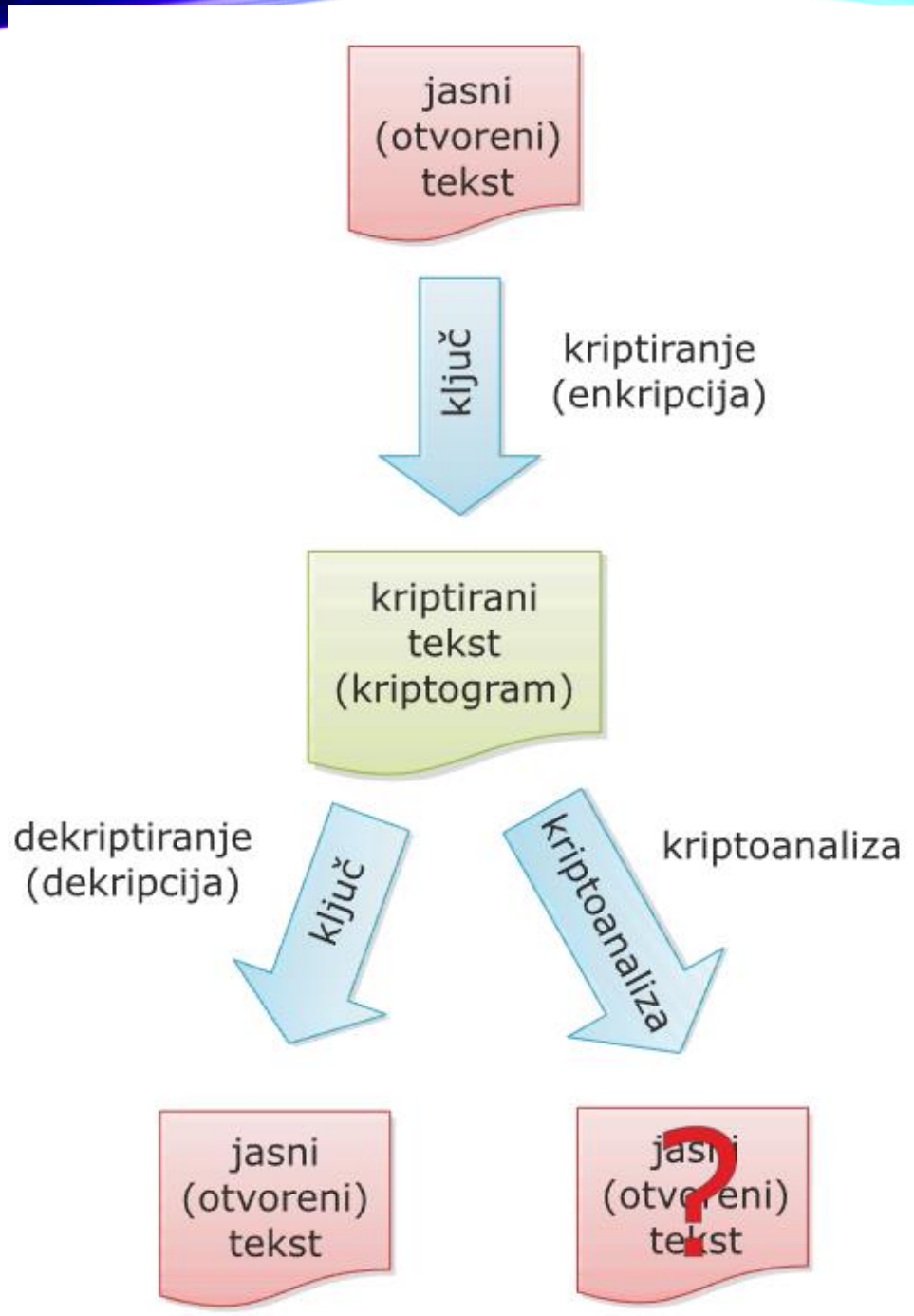
OSNOVNI POJMOVI

- kriptologija (grč. kryptos = skriven, tajan, logos = riječ) je znanost koja se bavi postupcima enkripcije, dekripcije i kriptoanalize tj. sigurnošću podataka
- **kriptografija** (grč. kryptos = tajan + grapheins = pisati) - pisanje "tajnih" poruka
- **jasni (otvoreni) tekst** – tekst koji šalje pošiljatelj
- **ključ** – pravila po kojima se jasni tekst pretvara u kriptogram i obrnuto po kojima iz kriptograma dobivamo jasan tekst
- **kriptirani tekst ili kriptogram** – tekst dobivem „skrivanjem" jasnog teksta
- **kriptiranje ili enkripcija** – postupak pretvaranja jasnog teksta u kriptogram

OSNOVNI POJMOVI

- **dekriptiranje ili dekripcija** – postupak dobivanja jasnog teksta iz kriptograma pomoću poznatog ključa
- **kriptoanaliza** – postupak dobivanja jasnog teksta iz kriptograma bez poznavanja ključa
- **kriptografski algoritam (šifra)** – skup kriptografskih funkcija koje s ključem pretvaraju izvorni tekst u šifrirani tekst i obrnuto

POSTUPAK ENKRIPCIJE I DEKRIPCIJE



ZAŠTO ŠIFRIRATI PODATKE ODNOSNO KOJA SVOJSTVA KRIPTOGRAFSKA FUNKCIJA MORA IMATI?

- **očuvanje tajnosti podataka** (bez valjanog ključa „nemoguće" je dešifrirati tekst)
- **osiguranje integriteta podataka** (da se šifrirani tekst nije promijenio)
- **autentifikacija** (utvrđivanje indentiteta sudionika u komunikaciji)

PRIJE NEGO KRENEMO DALJE

- radi jednostavnosti koristit ćemo samo velika slova engleske abeceda

slovo	A	B	C	D	E	F	G	H	I	J	K	L	M
broj	0	1	2	3	4	5	6	7	8	9	10	11	12

slovo	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
broj	13	14	15	16	17	18	19	20	21	22	23	24	25

TRADICIONALNI KRIPTOSUSTAVI

ZAŠTO KRENUTI S KRIPTIRANJEM TEKSTA?

- ratovi – slanje poruka da ih neprijatelj ne može pročitati
- poruke su prenosili glasnici, golubovi pismonoše...
- cezarova šifra - Gaj Julije Cezar (1. st. pr. Kr.)

KRIPTIRANJE S POMAKOM (SUPSTITUCIJSKE ŠIFRE)

- **cezarovo kriptiranje** - svako slovo pomiče za tri mjesta udesno u latinskoj abecedi
  - npr. A bi zamijenio slovom D, slovo B slovom E itd.
- **pomicanje za proizvoljan broj slova u abecedi**
- kriptirani tekst bi se dekriptiralo na način da svako slovo pomaknemo za 3 slova ulijevo
- **simetrični ključevi** - ključ za dekriptiranje može dobiti iz ključa za kriptiranje
- (**asimetričnim ključevima** - ključ za dekriptiranje ne može dobiti iz ključa kriptiranja (RSA))
- **monoalfabetski sustav** – neki znak se uvijek kriptira u isti znak
- (**polialfabetski sustavi** - sustavi kod kojih se neki znak može kriptirati različitim znakovima)

PRIMJER 1.

a) Koji ćemo tekst dobiti ako tekst INFORMATIKA kriptiramo kriptiranjem s pomakom pri čemu nam je pomak 5 udesno?

b) Koji ćemo tekst dobiti ako tekst KRIPTOGRAFIJA kriptiramo kriptiranjem s pomakom pri čemu nam je pomak 7 udesno?

c) Dekriptiraj tekst GIXZVXM koji smo kriptirali kriptiranjem s pomakom pri čemu nam je pomak 4 udesno?

PRIMJER 2.

Napišite funkcije u Pythonu koje će šifrirati i dešifrirati otvoreni tekst koristeći Cezarovu šifru (pomak za 3 udesno). Koristit ćemo samo velika slova engleske abecede (ukupno ih je 26).

RJEŠENJE PRIMJERA 2.

```
def sifriraj(tekst):
    novi = ""
    for z in tekst:
        indeks = ord("a")+(ord(z) - ord("a") + 3)%26
        novi += chr(indeks)
    return novi
def desifriraj(tekst):
    otvoreni = ""
    for z in tekst:
        indeks = ord("a") + (ord(z) - ord("a") - 3)%26
        otvoreni += chr(indeks)
    return otvoreni
def main():
    s = input().lower()
    print(sifriraj(s))
    x = input().lower()
    print(desifriraj(x))
main()
```

PRIMJER 3.

Napišimo program koji će kriptirati tekst s pomoću kriptiranja s pomakom, ali s proizvoljnim pomakom. Pomak neka bude manji od 27 jer u hrvatskoj abecedi imamo upravo 27 slova koja se zapisuju jednim znakom. Tekst će biti napisan slovima hrvatske abecede. Slova dž, lj i nj koja se zapisuju dvama znakovima, kodirat će se kao dva znaka.

RJEŠENJE PRIMJERA 3.

```
def kriptiraj(z, p):
    slova = "ABCČĆDĐEFGHIJKLMNOPRSŠTUVZŽ"
    indeks = (slova.index(z)+p)%len(slova)
    znak = slova[indeks]
    return znak
def main():
    s = input().upper()
    p = int(input())
    kript = ""
    for z in s:
        kript += kriptiraj(z, p)
    print(kript)
main()
```

AFINO KRIPTIRANJE

- poopćenje kriptiranja s pomakom
- kriptirani znak y dobiva se pomoću funkcije y = x*a + b, gdje je x broj slova jasnog teksta, a a i b prirodni brojevi (ključ)

PRIMJER 4.

a) Koji ćemo tekst dobiti ako tekst *AFINO* kriptiramo afinim kriptiranjem pri čemu je ključ kriptiranja $a = 3$, $b = 2$?

Rješenje:

A - (3*0+2)%26 = 2 - C

b) Koji ćemo tekst dobiti ako tekst *PROGRAM* kriptiramo afinim kriptiranjem pri čemu je ključ kriptiranja $a = 2$, $b = 7$?

PRIMJER 5.

Napišite funkciju u Pythonu koja će šifrirati i zadani tekst koristeći afino kriptiranje pomoću zadanih ključa. Koristit ćemo samo slova engleske abecede te unositi parametre ključa a i b.

RJEŠENJE PRIMJERA 5.

```
def sifriraj(s, a, b):
    novi = ""
    for z in s:
        indeks = ord("a") + ((ord(z)-ord("a"))*a+b)%26
        novi += chr(indeks)
    return novi

def main():
    s = input().lower()
    a = int(input())
    b = int(input())
    print(sifriraj(s, a, b))

main()
```

VIGENÈREOVO KRIPTIRANJE

- polialfabetski kriptosustav
- postupak
  - zapišemo otvoreni tekst, a ispod njega (od prvog do zadnjeg slova) redom pišemo slova ključa ponavljajući ključ do kraja teksta
  - svako slovo iz otvorenog teksta šifriramo slovom iz ključa ispod njega i to tako da ga pomičemo za k mjesta pri čemu je k pozicija odgovarajućeg slova iz ključa
- Primjer: (ALGORITAM, PYTHON)

A	L	G	O	R	I	T	A	M
P	Y	T	H	O	N	P	Y	T
P	J	Z	V	F	V	I	Y	F

PRIJE NEGO KRENEMO DALJE

- radi jednostavnosti koristit ćemo samo velika slova engleske abeceda

slovo	A	B	C	D	E	F	G	H	I	J	K	L	M
broj	0	1	2	3	4	5	6	7	8	9	10	11	12

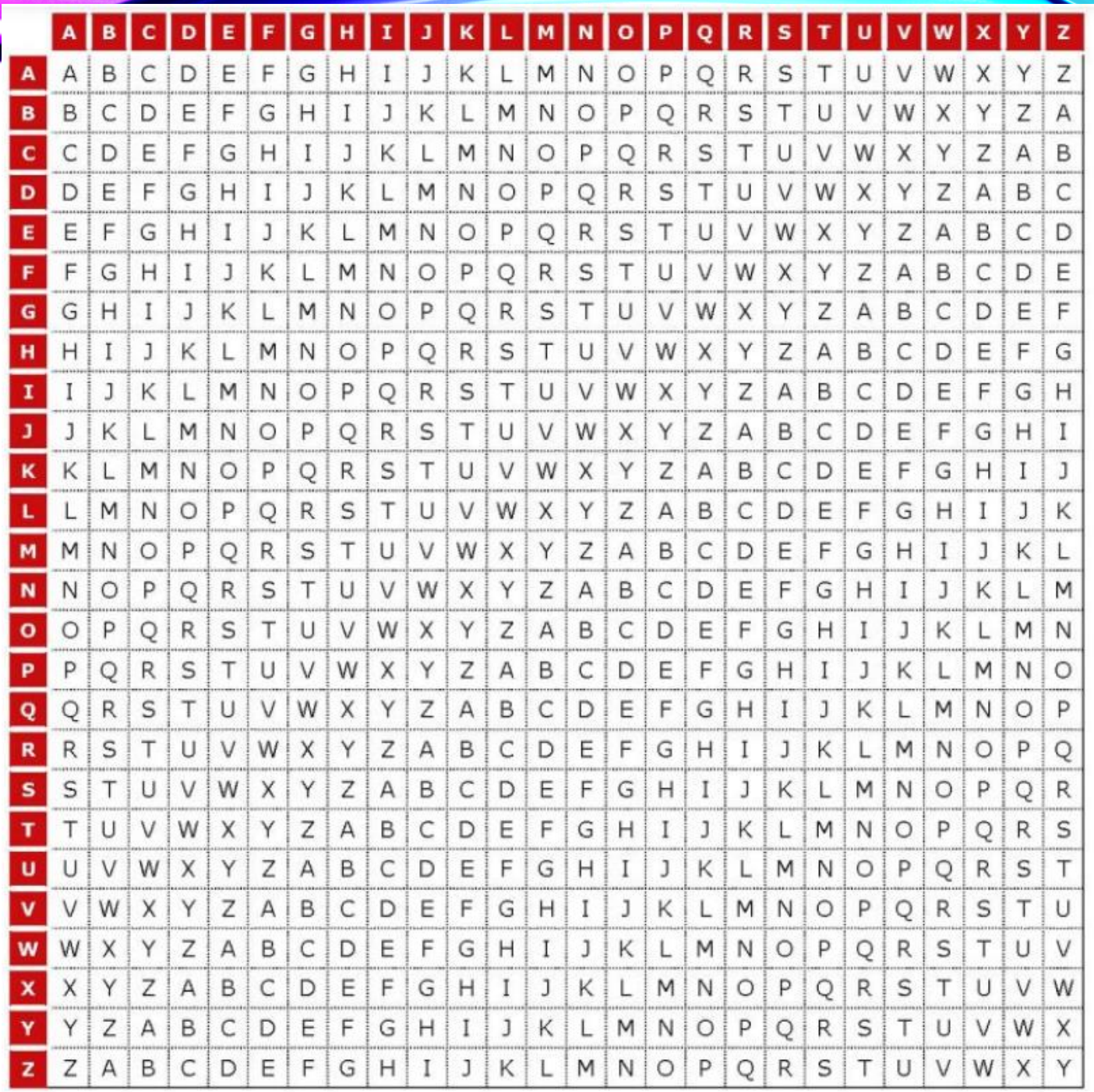
slovo	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
broj	13	14	15	16	17	18	19	20	21	22	23	24	25

PRIMJER 6.

a) Vigenèreovim kriptiranjem kriptirajmo jasni tekst INFORMATIKA, pri čemu je ključ za kriptiranje PROGRAM.

b) Vigenèreovim kriptiranjem kriptirajmo jasni tekst KOCKA JE BACENA, pri čemu je ključ za kriptiranje CEZAR.

TABLICA VIGENÈREOVA KRIPTIRANJA



	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

PRIMJER 7.

a) Vigenèreovim kriptiranjem kriptirajmo jasni tekst PYTHON, pri čemu je ključ za kriptiranje KOD.

b) Vigenèreovim kriptiranjem kriptirajmo jasni tekst JASNI TEKST, pri čemu je ključ za kriptiranje VIGENER.

c) Dekriptiraj tekst UVXTUGWW koji smo kriptirali Vigenereovim kriptiranjem pri čemu je ključ za kriptiranje ONLINE?

PRIMJER 8.

Napišimo funkciju čiji će parametri biti jasni tekst i ključ (pisani velikim tiskanim slovima). Funkcija treba vratiti tekst koji se dobije kriptiranjem jasnog teksta i danim ključem ako se koristi Vigenèreovo kriptiranje.

RJEŠENJE PRIMJERA 8.

```
def vigenere(t, k):
    k = k.upper()
    t = t.upper()
    k = k*(len(t)//len(k)+1)
    t2 = ""
    for i in range(len(t)):
        indt = ord(t[i]) - ord("A")
        indk = ord(k[i]) - ord("A")
        n = (indt + indk)%26 + ord("A")
        t2 += chr(n)
    return t2

t = input()
k = input()
print(vigenere(t, k))
```

TRANSPOZICIJSKO KRIPTIRANJE

- slova jasnog teksta permutiraju se prema zadanom ključu
- odredimo prirodan broj n – znakovi se zapišu u matricu koja se sastoji od n stupaca
- nepopunjeni dijelovi popune se proizvoljnim tekstom
- n različitih slučajnih prirodnih brojeva do n – ključ
- stupci matrice permutiraju se prema zadanom ključu – stupčasta transpozicija
- tekst pročita po stupcima (prvo se pročitaju svi znakovi koji se nalaze u prvom stupcu, zatim oni iz drugog...)

PRIMJER 9.

a) Transpozicijskim kriptiranjem kriptirajmo sljedeći tekst: TEKST KOJI CEMO KRIPTIRATI. Primijenimo ključ kriptiranja 2 4 1 3

b) Transpozicijskim kriptiranjem kriptirajmo sljedeći tekst: TRANSPOZICIJSKO KRIPTIRANJE. Primijenimo ključ kriptiranja 3 1 2 4

c) Transpozicijskim kriptiranjem kriptirajmo sljedeći tekst: SIGURNOST PODATAKA. Primijenimo ključ kriptiranja 2 3 1

d) Koji ćemo jasni tekst dobiti ako je kriptogram ETNTAONTIAVSSRROAKKGJEEOAJIAPM dobiven kriptiranjem primjenom stupčaste transpozicije i ključem kriptiranja 5 3 2 1 6 4.