Vigenère-ova šifra

Kod supstitucijske šifre svakom slovu otvorenog teksta odgovara jedinstveno slovo šifrata. Takvi kriptosistemi se zovu *monoalfabetski*. Prikazaćemo sada Vigenère-ovu šifru koja spada u *polialfabetske kriptosisteme*. Naime, kod nje svako slovo otvorenog teksta može se preslikati u jedno od m mogućih slova (gde je m dužina ključa).

Sistem koji se danas naziva Vigenère-ova šifra definisan je na sledeći način:

Neka je m fiksan prirodan broj. Za ključ $K = (k_1, k_2, \dots, k_m)$, definišemo

$$\text{šifrovanje:} \quad e_K(x_1, x_2, \dots, x_m) = (x_1 + k_1, x_2 + k_2, \dots, x_m + k_m),$$
$$\text{dešifrovanje:} \quad d_K(y_1, y_2, \dots, y_m) = (y_1 - k_1, y_2 - k_2, \dots, y_m - k_m),$$

gde su svi numerički ekvivalenti (brojevi koji odgovaraju slovima) otvorenog teksta (x), šifrata (y), ključa (k) elementi skupa $\mathbf{Z_{26}}$ (tj. brojevi 0,1,...,25). Takođe, sve operacije su unutar skupa $\mathbf{Z_{26}}$ (znači da se sabiranje i oduzamnje vrši po modulu 26).

Vidimo da se kod šifrovanja m susednih slova šifruje Cezarovom šifrom, ali sa međusobno različitom dužinom ključa tj. pomeraja (za jedno slovo je pomeraj k_1 za drugo k_2 itd.). Kada se šifruje m slova dužina ključa se ponavlja, tako da je svako m-to slovo šifrovano sa istom dužinom ključa tj. istim pomjerajem.

Zadatak 1: Neka je $m = 4$ i ključna reč BROJ. Šifrovati otvoreni tekst KRIPTOLOGIJA.

Rešenje: Numerički ekvivalent za ključnu riječ BROJ je ključ $K = (1, 17, 14, 9)$. Šifrovanje se sprovodi na sledeći način:

K	R	I	P	T	O	L	O	G	I	J	A	- otvoreni tekst
10	17	8	15	19	14	11	14	6	8	9	0	- numerički ekvivalent otvorenog teksta
B	R	O	J	B	R	O	J	B	R	O	J	- ključna riječ
1	17	14	9	1	17	14	9	1	17	14	9	- ključ (numerički ekvivalent)
x+k mod 26												
11	8	22	24	20	5	25	23	7	25	23	9	- numerički ekvivalent šifrata
L	I	W	Y	U	F	Z	X	H	Z	X	J	- šifrat

Dakle, šifrat je LIWYUFZXHZXJ. Uočavamo da se prvo slovo O iz otvorenog teksta KRIPTOLOGIJA preslikalo u F, a drugo u X.

Postoje i druge varijante Vigenère-ove šifre kod kojih se ključ ne ponavlja u nedogled. Jedna takva (sigurnija od originalne) je ona s *autoključem*, u kojoj otvoreni tekst generiše ključ. Kod nje se za šifrovanje prvih m slova koristi ključna reč, a za šifrovanje ostalih slova koriste se redom slova od početka otvorenog teksta (npr. kao ključ za šifrovanje m+1-vog slova koristi se prvo slovo otvorenog teksta, za m+2-go slovo koristi se drugo slovo, itd.). Ova varijanta šifrovanja spada u tzv. protočne kriptosisteme.

Zadatak 2. Sve isto kao u Zadatku 1., ali sa autoključem.

Rešenje: U ovom primeru za šifrovanje ćemo iskoristiti tzv. Vigenère-ov kvadrat (Ako slovo K treba šifrovati ključem B, onda pogledamo kolonu koja počinje s K i red koji počinje s B. U preseku je šifrat L.)

Vigenère-ov kvadrat:

```
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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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
```

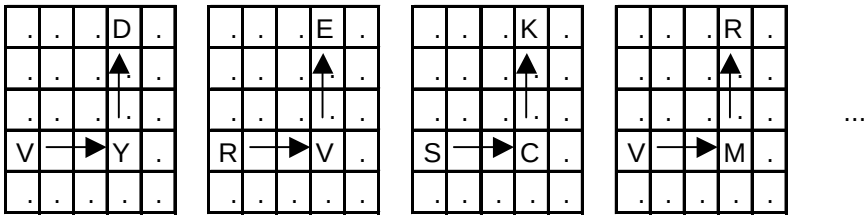
Dobijamo:

B	R	O	J	K	R	I	P	T	O	L	O
K	R	I	P	T	O	L	O	G	I	J	A
L	I	W	Y	D	F	T	D	Z	W	U	O

- ključna riječ
- otvoreni tekst
- šifrat

Zadatak 3. Dekriptujte šifrat YVCMZ HOFNV EBZ dobijen Vigener-ovom šifrom. Ključna reč je VRS.

Rešenje: Do rešenja možemo doći korišćenjem Vigenère-ovog kvadrata. Postupak je sledeći: nađemo prvo slovo ključne reči (slovo V) u prvoj koloni (vrsti) Vigenère-ovog kvadrata, a zatim u vrsti (koloni) koja sadrži to slovo tražimo prvo slovo u šifratu (Y). Odgovarajuće slovo otvorenog teksta je prvo slovo u koloni (vrsti) koja sadrži slovo šifrata (D). Na isti način dobijamo ostala slova otvorenog teksta:



...

,

tako da na kraju imamo:

Y	V	C	M	Z	H	O	F	N	V	E	B	Z
V	R	S	V	R	S	V	R	S	V	R	S	V
D	E	K	R	I	P	T	O	V	A	N	J	E

- šifrat
- ključna riječ
- otvoreni tekst

Drugi način za dešifrovanje je koristeći numeričke ekvivalente i matematičku definiciju za dešifrovanje ($x = y–k \bmod 26$):

Y	V	C	M	Z	H	O	F	N	V	E	B	Z
24	21	2	12	25	7	14	5	13	21	4	1	25
V	R	S	V	R	S	V	R	S	V	R	S	V
21	17	18	21	17	18	21	17	18	21	17	18	21

- šifrat
- numerički ekvivalent šifrata
- ključna riječ
- ključ

y–k mod 26

3	4	10	17	8	15	19	14	21	0	13	9	4
D	E	K	R	I	P	T	O	V	A	N	J	E

- numerički ekvivalent otvorenog teksta
- otvoreni tekst

Zadatak 4: Dekriptujte šifrat VLLOE EXEN dobijen Vigener-ovom šifrom sa autoključem. Ključna reč je VRS.

Rešenje: Do rešenja možemo doći na dva načina kao i u prethodnom primeru. Jedina razlika je što u početku znamo samo prva tri slova ključne reči, a ključnu reč postepeno dopunjavamo dešifrovanim slovima.
Rešenje korišćenjem Vigenère-ovog kvadrata:

V	L	L	O	E	E	X	E	N
V	R	S	A	U	T	O	K	L
A	U	T	O	K	L	J	U	C

- šifrat
- ključna riječ
- otvoreni tekst

Rešenje korišćenjem numeričkih ekvivalenata:

V	L	L	O	E	E	X	E	N
21	11	11	14	4	4	23	4	13
V	R	S	A	U	T	O	K	L
21	17	18	0	20	19	14	10	11

- šifrat
- numerički ekvivalent šifrata
- ključna riječ
- ključ

y–k mod 26

0	20	19	14	10	11	9	20	2
A	U	T	O	K	L	J	U	C

- numerički ekvivalent otvorenog teksta
- otvoreni tekst

Iako Vigenère-ova šifra na prvi pogled izgleda sigurna, nju je, uz pomoć kriptoanalize, relativno lako razbiti, čak i bez poznavanja uzorka šifrat – otvoreni tekst.

Prvi korak ka razbijanju šifre je određivanje dužine ključne riječi, a jedna metoda se zove *Kasiskijev test*. Metoda se zasniva na činjenici da će dva identična segmenta otvorenog teksta biti šifrovana na isti način ukoliko se njihove početne pozicije razlikuju za *m, 2m, 3m,...* mesta (*m* je dužina ključa). Obrnuto, ako uočimo dva identična segmenta u šifratu, dužine barem 3, tada je vrlo verovatno da oni odgovaraju identičnim segmentima otvorenog teksta. U Kasiskijevom testu tražimo u šifratu parove identičnih segmenata dužine barem 3 i zabeležimo udaljenosti između njihovih početnih položaja. Ako na takav način dobijemo udaljenosti d_1, d_2, ... , onda je razumna pretpostavka da *m* najmanji zajednički delilac ovih brojeva.

Spomenućemo i drugu metodu za određivanje dužine ključa koja koristi tzv. indeks koincidencije. Indeks koincidencije $I_c(x)$ niza *x* od *n* slova definiše se kao verovatnoća da su dva slučajna elementa iz *x* jednaka. Korišćenjem teorije verovatnoće moguće je izračunati vrednost indeksa koincidencije (zavisi od dužine niza *n* i statistički utvrđene frekvencije slova). Prilikom izračunavanja dužine ključa *m* koristi se činjenica da su, za slučajni otvoreni tekst i šifrat dobijen konstantnim pomeranjem svih slova otvorenog teksta, indeksi koincidencije statistički isti (npr. za engleski jezik iznose oko 0.065), dok je, za šifrat sa promenljivim vrednostima pomeraja, indeks znatno manji. Ova razlika je posledica postojanja većih razlika između pojedinačnih frekvencija slova kod otvorenog teksta, nego kod šifrata sa promenljivim pomerajem. Ako se kod šifrata dobijenog Vigenère-ovom šifrom pretpostavi da neki broj *m* ogovara dužini ključa, onda će, ako je pretpostavka tačna, nizovi: (y_1, y_{m+1}, y_{2m+1}, y_{3m+1}, ...), (y_2, y_{m+2}, y_{2m+2}, y_{3m+2}, ...) ,..., (y_m, y_{2m}, y_{3m}, ...), imati indekse koincidencije vrlo bliske indeksu otvorenog teksta (0.065). Ako pretpostavljeno *m* ne odgovara stvarnoj dužini ključa, indeksi koincidencije ovih nizova će biti znatno manji.

Nakon utvrđivanja dužine ključa *m*, određivanje samog ključa postiže se korišćenjem tzv. međusobnog indeksa koincidencije. *Međusobni indeks koincidencije* dva niza definiše se kao verovatnoća da je slučajni element iz jednog jednak slučajnom elementu iz drugog niza. Tu se koristi osobina da je međusobni indeks koincidencije dva niza otvorenog teksta znatno veći (oko 0.065) u odnosu na isti indeks između niza otvorenog teksta i niza kod kojeg je izvršen konstantan pomeraj slova otvorenog teksta (ispod 0.045). Vigenère-ov šifrat se rastavlja na *m* podnizova: (y_1, y_{m+1}, y_{2m+1}, y_{3m+1}, ...), (y_2, y_{m+2}, y_{2m+2}, y_{3m+2}, ...) ,..., (y_m, y_{2m}, y_{3m}, ...). Elementi nekog podniza šifrovani su istim delom ključa tj. svi imaju isti pomeraj u odnosu na odgovarajuća slova otvorenog teksta. Sada se, za svaki podniz posebno, vrši pomeranje slova redom za k=0,1,2,...,25 i računa međusobni indeks koincidencije sa nizom slova proizvoljnog otvorenog teksta. Pomeraj kod koga se izračuna najveći indeks koincidencije predstavlja vrednost dela ključa. Od *m* postojećih podnizova dobijamo svih *m* delova ključa i na taj način dobijamo ključnu reč.

Playfair-ova šifra

Jedna ideja za poboljšanje supstitucijskih šifara je uvođenje polialfabetskih šifara. Takvu jednu šifru videli smo u prethodnom poglavlju. Druga ideja je upotreba blokova slova kao osnovnih elemenata otvorenog teksta. Prikazaćemo najpoznatiju takvu šifru, tzv. *Playfair-ovu šifru*. To je bigramska šifra, u smislu da se šifruju parovi slova i to tako da rezultat zavisi i od jednog i od drugog slova. Algoritam za šifrovanje se bazira na 5 x 5 matrici slova, a prilikom njenog formiranja koristi se ključna riječ. Na primjer, ako je ključna riječ PLAYFAIR, onda matrica izgleda ovako:

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

S obzirom da imamo 25 slova, dogovor je da se slova I i J poistovjete. U slučaju da je otvoreni tekst na našem jeziku, mi ćemo poistovećivati V i W. Šifrovanje se sada vrši na sledeći način. Najprije podelimo otvoreni tekst na blokove od po dva slova. Pritom pazimo da se ni jedan blok ne sastoji od dva jednaka slova, kao i da je dužina teksta parna. I jedno i drugo postižemo umetanjem npr. slova X ukoliko je to potrebno.

Kod šifrovanja bloka od dva slova, mogu nastupiti tri slučaja:

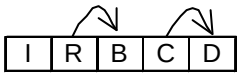
1. Oba slova se nalaze u istoj vrsti matrice. Tada ih zamenjujemo sa slovima koja se nalaze za jedno mjesto udesno (ciklično). Npr. EH →GK, ST →TN, FP→PL.
2. Slova se nalaze u istoj koloni. Tada ih zamenjujemo sa slovima koja se nalaze za jedno mesto ispod (ciklično). Npr. OV →VL, KY →SC, PI →IE.
3. U protivnom, pogledamo pravougaonik koji određuju ta dva slova, pa ih zamijenimo s preostala dva vrha tog pravougaonika. Redosljed je određen tako da najprije dođe ono slovo koje se nalazi u istom redu kao prvo slovo u polaznom bloku. Npr. OC →SR, RK →CG, PD →FI.

Dešifrovanje se vrši obrnutim postupkom.

Zadatak 1. *Šifrujmo otvoreni tekst* CRYPTOGRAPHY *pomoću Playfair-ove šifre sa ključem* PLAYFAIR.

Rešenje:

C i R pripadaju istom redu:

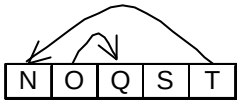


C R → D B

Y i P pripadaju istom redu:

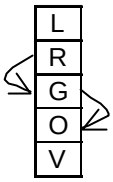
Y P → F L

T i O pripadaju istom redu:



T O → N Q

G i R pripadaju istoj koloni:

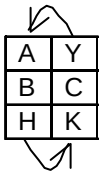


G R → O G

A i P pripadaju istom redu:

A P → Y L

H i Y pripadaju pravougaoniku:



H Y → K A

Rezultat: CR YP TO GR AP HY → DB FL NQ OG YL KA

Playfair-ova šifra ima brojne prednosti u odnosu na supstitucijsku šifru. Spomenimo neke. Kako je šifra bigramska, gube se u šifratu jednoslovne reči (npr. "a") koje dosta utiču na frekvencije. Dalje, bigramsko šifrovanje smanjuje na polovinu broj elemenata dostupnih analizi frekvencije. Na kraju, broj bigrama je puno veći od broja individualnih slova (26 slova - 676 bigrama), dok su frekvencije najfrekventnijih bigrama puno ujednačenije od frekvencija najfrekventnijih slova.

Ipak, kod dugih tekstova ova šifra postaje nesigurna, jer se može iskoristiti analiza frekvencija bigrama. Poznato je da i kod ove šifre deo strukture jezika ostaje sačuvan. Naime, slova u šifratu nisu jednako raspoređena. Dok u otvorenom tekstu na engleskom jeziku najfrekventnije slovo ima relativnu frekvenciju oko 13%, u šifratu dobijenom Playfair-ovom šifrom to iznosi oko 7%, dok recimo kod Vigenere-ove šifre imamo oko 6%. Takvi podaci mogu nam pomoći i kod određivanja koja je šifra u pitanju.

Hill-ova šifra

Lester Hill je 1929. godine izumio šifru kod koje se m uzastopnih slova otvorenog teksta zamenjuje s m slova u šifratu. Dakle, radi se o *poligramskoj* šifri. Sva slova otvorenog teksta i šifrata definišu se brojevima iz skupa Z_{26} (tj. brojevima od 0 do 25). Ključ K je definisan matricom m x m čiji su svi elementi takođe iz skupa Z_{26}. Matrica K mora invertibilna tj. mora postojati njena inverzna matrica K^{-1} sa elementima iz skupa Z_{26}. Šifrovanje i dešifrovanje vrši se na sljedeći način:

$$\text{šifrovanje:} \quad e_K(x) = xK,$$

$$\text{dešifrovanje:} \quad d_K(y) = yK^{-1},$$

gdjđe su sve operacije u skupu Z_{26} (po modulu 26).

Hill je preporučio da se za ključ koriste matrice kod kojih je $K^{-1} = K$. To teoretski smanjuje sigurnost, jer je prostor ključeva manji, ali olakšava postupak šifrovanja i dešifrovanja.

Zadatak 1: Šifrovati otvoreni tekst UTORAK pomoću ključa

$$K = \begin{vmatrix} 5 & 8 & 22 \\ 2 & 5 & 24 \\ 10 & 20 & 17 \end{vmatrix},$$

Rešenje: Numerički ekvivalent otvorenog teksta je (20, 19, 14, 17, 0, 10). Računamo:

$$(20\ \ 19\ \ 14)\begin{vmatrix} 5 & 8 & 22 \\ 2 & 5 & 24 \\ 10 & 20 & 17 \end{vmatrix} = (278\ \ 535\ \ 1134) \bmod 26 = (18\ \ 15\ \ 16) = \text{SPQ},$$

$$(17\ \ 0\ \ 10)\begin{vmatrix} 5 & 8 & 22 \\ 2 & 5 & 24 \\ 10 & 20 & 17 \end{vmatrix} = (185\ \ 336\ \ 544) \bmod 26 = (3\ \ 24\ \ 24) = \text{DYY}.$$

Dakle šifrat je SPQDYY.

Ako prilikom šifrovanja u nizu od m slova promenimo samo jedno slovo šifrat će biti potupuno drugačiji. Na primjer, ukoliko bi u prethodnom primeru tekst umesto sa UTO počeo sa STO, onda bi šifrat umesto sa SPQ započeo sa IZY:

$$(18\ \ 19\ \ 14)\begin{vmatrix} 5 & 8 & 22 \\ 2 & 5 & 24 \\ 10 & 20 & 17 \end{vmatrix} = (8\ \ 25\ \ 24) = \text{IZY}.$$

Hill-ov kriptosistem s matricama dimenzije 3 x 3 skriva ne samo sve informacije o frekvencijama slova, već i o frekvencijama bigrama. Stoga, već za $m \geq 5$ možemo Hill-ov kriptosistem smatrati gotovo potpuno sigurnim na napad "samo šifrat". Međutim, ovu šifru je vrlo lako razbiti pomoću napada "poznat otvoreni tekst", a pogotovo pomoću napada "odabrani otvoreni tekst". To je i razlog zašto ovaj sistem gotovo uopšte nije bio u praktičnoj upotrebi (osim za šifrovanje pozivnih signala radio-stanica).

Zadatak 2. Šifrovati otvoreni tekst: VISA RACUNARSKA SKOLA (bez razmaka) pomoću koristeći isti ključ kao i u Zadatku 1. i programski jezik MATLAB.

Rešenje: Nakon ulaska u Matlab prvo ćemo definisati ključ unošenjem:

```
>> kljuc=[5 8 22; 2 5 24; 10 20 17]

kljuc =

    5    8   22
    2    5   24
   10   20   17

>>
```

Pošto je matrica ključa dimenzije 3x3 delimo otvoreni tekst na nizove od po 3 slova: VIS ARA CUN ARS KAS KOL AXX. Komandom «double» dobijamo ASCII kodove za niz slova. Kako je ASCII kod slova A broj 65 (za B je 66, za C je 67, itd.), to numeričke ekvivalente slova otvorenog teksta dobijamo kad rezultate dobijene komandom «double» umanjimo za 65. Na primer, za prva tri slova (VIS) dobijamo:

```
>> x=(double('VIS')-65)

x =

   21    8   18

>>
```

što znači da je 21 numerički ekvivalent slova V, 8 slova I, a 18 slova S.
Numerički ekvivalent šifrata (y) za niz VIS dobijamo na osnovu definicije Hill-ove šifre pomoću sledeće komande:

```
>> y=mod(x*kljuc,26)

y =

   15   22   24

>>
```

Šifrat za niz VIS dobijamo pomoću komande «char» koja kao rezultat daje slova koja odgovaraju unetim ASCII kodovima:

```
>> sifrat=char(y+65)

sifrat =

PWY

>>
```

Ponavaljanjem postupka za ostale podnizove dobijamo šifrat:

otvoreni tekst: VIS ARA CUN ARS KAS KOL AXX
šifrat: PWY IHS YMR GDM WYG GGP QDH

Naravno šifrat za pojedine podnizove može se dobiti direktno koristeći jednu formulu. Npr. za VIS:

```
>> sifrat=char(mod((double('VIS')-65)*kljuc,26)+65)

sifrat =

PWY
```

Takođe, moguće je napraviti program koji direktno daje rezultat za ulazni tekst.
Napomena: u sličaju korišćenja malih slova u prethodnoj formuli umesto oduzimanja i dodavanja broja 65 potrebno je koristiti broj 97 (to je ASCII kod slova *a*). Na primer:

```
>> sifrat=char(mod((double('vis')-97)*kljuc,26)+97)

sifrat =

pwy

>>
```

Zadatak 3: Dešifrujte šifrat: NAVMA AOIQF YF, dobijen istim ključem kao i u Zadatku 2. Koristiti MATLAB.

Rešenje: Najprije je potrebno naći ključ za dešifrovanje K^{-1}. Ovaj ključ je inverzna matrica matrice ključa za šifrovanje. Međutim, ovu matricu ne možemo dobiti prostom komandom "inv", jer su operacije po modulu 26. Matricu ključa za dešifrovanje K^{-1} (kinv) možemo dobiti po definiciji:

$$kinv=det(kljuc)^{-1}\ adj(kljuc)$$

množenjem inverzne vrednosti determinante matrice ključa (matrica "kljuc" je definisana u Zadatku 2.) sa adjungovanom matricom kjuča, gdje su operacije po modulu 26.

Adjungovanu matricu naći ćemo korišćenjem funkcije "inv" pomoću sledeće komandne linije:

```
> adj=mod(det(kljuc)*inv(kljuc),26)

adj =

   21.0000   18.0000    4.0000
   24.0000   21.0000    2.0000
   16.0000    6.0000    9.0000

>>
```

Determinantu ključa naći ćemo pomoću sledeće komande:

```
>> mod(det(kljuc),26)

ans =

   25

>>
```

Znači, determinanta ključa je 25. Inverzna vrednost ove determinante je inverzni broj broju 25 iz skupa Z_{26}. To je takođe broj 25. Sada matricu ključa za dešifrovanje (kinv) dobijamo množenjem broja 25 sa matricom adj:

```
>> kinv=mod(25*adj,26)

kinv =

    5.0000    8.0000   22.0000
    2.0000    5.0000   24.0000
   10.0000   20.0000   17.0000

>>
```

Vidimo da je *kinv=kljuc* tj. $K^{-1}=K$, što znači da se isti ključ koristi za šifrovanje i dešifrovanje. Sada delimo šifrat na podnizove od 3 slova (NAV MAA OIQ FYF), a za dešifrovanje koristimo istu formulu kao i u prethodnom primeru za šifrovanje. Na primjer za podniz NAV imamo:

```
>> char(mod((double('NAV')-65)*kinv,26)+65)

ans =

PET

>>
```

Ubacivanjem redom sva 4 podniza u formulu dobijamo:

šifrat: NAV MAA OIQ FYF

otvoreni tekst: PET ISE MES TAR,

što znači da je otvoreni tekst: PETI SEMESTAR.