Zadatak 2.1 *Dešifrirajte poruku*

$$AYCQY\ PAGNF\ CPGQR\ FCKMQ\ RDYKM\ SQQFG\ DRAFG\ NCP$$

šifriranu Cezarovom šifrom iz otvorenog teksta na engleskom jeziku.

Rješenje:

Napomenimo samo kako se zbog preglednosti kod duljih šifrata obično stavlja razmak nakon svakog petog slova. To naravno nema nikakve veze s razmacima u otvorenom tekstu, koje zanemarujemo kod šifriranja.

Potrebno je provesti osnovnu analizu frekvencije slova. Uočimo:

Q(5), F(4), C(4), G(4), A(3), Y(3), ...

Sada koristimo frekvenciju slova u engleskom jeziku i potrebno je kombinirati parove, dok ne dobijemo smisleni tekst. Ovdje je slovo C šifrat najfrekventnijeg slova engleskog alfabeta, tj. slova E, pa je funkcija dešifriranja dana s

$$d_K(y) = (y - 24) \bmod 26.$$

Zbog kongruencija, kvivalentno je gledati

$$d_K(y) = (y + 2) \bmod 26.$$

Slijedi otvoreni tekst

$$CAESAR|CIPHER|IS|THE|MOST|FAMOUS|SHIFT|CHIPER.$$

Zadatak 2.2 *Dešifrirajte poruku*

$$SEKHI\ UEVDK\ CRUHJ\ XUEHO\ QDTSH\ OFJEW\ HQFXO$$

šifriranu Cezarovom šifrom iz otvorenog teksta na engleskom jeziku.

Rješenje:

Uočimo:

H(5), E(4), U(3), O(3), S(2), ...

Ovdje je slovo E šifrat slova O (jedno od frekventnijih slova engleskog alfabeta), pa je funkcija dešifriranja dana s

$$d_K(y) = (y - 16) \bmod 26,$$

tj.

$$d_K(y) = (y + 10) \bmod 26.$$

Slijedi otvoreni tekst

$$COURSE|OF|NUMBER|THEORY|AND|CRYPTOGRAPHY.$$

Zadatak 2.3 *Dešifrirajte poruku*

$$KFGBP\ BQBPH\ LRPMF\ KGXQF\ XIFGB\ QBPHL$$
$$RPMFK\ GXQFP\ BFLPQ\ XQFPS\ LG$$

šifriranu Cezarovom šifrom iz otvorenog teksta na hrvatskom jeziku.

Rješenje:

Uočimo:

F(8), P(8), B(6), Q(6), G(5), ...

Ovdje je slovo F šifrat slova I (jedno od frekventnijih slova hrvatskog alfabeta), pa je funkcija dešifriranja dana s

$$d_K(y) = (y - 23) \bmod 26,$$

tj.

$$d_K(y) = (y + 3) \bmod 26,$$

pa dobivamo

$$NIJE|SE|TESKO|USPINJATI|ALI|JE|TESKO|USPINJATI|SE|I|OSTATI|SVOJ.$$

Na kraju, ovisno o značenju riječi dodajemo dijakritičke znakove. Dakle, otvoreni tekst je:

NIJE SE TEŠKO USPINJATI ALI JE TEŠKO USPINJATI SE I OSTATI SVOJ.

Zadatak 2.4 *Dekriptirajte šifrat*

$$TQCWT\ \ QCKIQ\ \ RWNOQ\ \ OBCEW\ \ OQVKB\ \ UKAPK$$
$$OQOQB\ \ CQPQA\ \ JGDUQ\ \ EQORW\ \ TSJGR\ \ WEQKY$$
$$WGTWC\ \ JKRBI\ \ KZGVO\ \ GBQ$$

dobiven supstitucijskom šifrom, ako je poznato da je otvoreni tekst na hrvatskom jeziku.

Rješenje:

Napravit ćemo (istovremeno) analizu frekvencija slova i bigrama tako da za svako slovo u alfabetu napišemo sve njegove sljedbenike u šifratu (za zadnje slovo u šifratu stavljamo *). Dobivamo sljedeću tablicu:

A | P, J
B | C, U, C, I, Q
C | W, K, E, Q, J
D | U
E | W, Q, Q
F |
G | D, R, T, V, B
H |
I | Q, K

J | G, G, K
K | I, B, A, O, Y, R, Z
L |
M |
N | O
O | Q, B, Q, Q, Q, R, G
P | K, Q
Q | C, C, R, O, V, O, B, P, A, E, O, K, *
R | W, W, W, B
S | J
T | Q, Q, S, W
U | K, Q
V | K, O
W | T, N, O, T, E, G, C
X |
Y | W
Z | G

Iz tablice iščitavamo kako su najfrekventnija slova

Q(13), K(7), O(7), W(7), B(5), C(5), G(5), R(4), T(4), E(3), J(3),

a najfrekventniji bigrami

OQ(4), QO(3), RW(3), BC(2), EQ(2), JG(2), QC(2), TQ(2), WT(2).

Logično je pretpostaviti da je $e(A) = Q$. Uočavamo također recipročne bigrame OQ i QO, što nas navodi na $e(N) = O$.

Nadalje, većina pojavljivanja slova R vezana je uz bigram RW, te da je W jedno od najfrekventnijih slova. To nas vodi na pretpostavku da je $e(J) = R$ i $e(E) = W$.

Pokušajmo otkriti šifrat čestog bigrama ST (jednostavno idemo redom - to je najčešći bigram od do sada neotkrivenih). Najozbiljniji kandidati su BC i JG. Možemo uzeti neki od njih, pa vidjeti što ćemo dobiti. Mi ćemo krenuti s BC, jer frekvencije od B i C odgovaraju očekivanim frekvencijama od S i T. Dakle, uzmimo da je $e(S) = B$ i $e(T) = C$. Od najfrekventnijih slova u hrvatskom jeziku, još nismo odgonetnuli šifrate od I i O. Glavni kandidati su K i G, i to upravo tim redoslijedom. Pa uzmimo da je $e(I) = K$ i $e(O) = G$.

Pogledajmo što smo do sada pretpostavili:

otvoreni tekst	*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*
šifrat	*q*				*w*				*k*	*r*				*o*	*g*				*b*	*c*						

.

Ubacimo ove pretpostavke u polazni šifrat:

T	*Q*	*C*	*W*	*T*	*Q*	*C*	*K*	*I*	*Q*	*R*	*W*	*N*	*O*	*Q*	*O*	*B*	*C*	*E*	*W*	*O*	*Q*	*V*	*K*	*B*	*U*	*K*	*A*	*P*	*K*
	a	*t*	*e*		*a*	*t*	*i*		*a*	*j*	*e*		*n*	*a*	*n*	*s*	*t*		*e*	*n*	*a*		*i*	*s*		*i*			*i*

O	*Q*	*O*	*Q*	*B*	*C*	*Q*	*P*	*Q*	*A*	*J*	*G*	*D*	*U*	*Q*	*E*	*Q*	*O*	*R*	*W*	*T*	*S*	*J*	*G*	*R*	*W*	*E*	*Q*	*K*	*Y*
n	*a*	*n*	*a*	*s*	*t*	*a*		*a*			*o*			*a*		*a*	*n*	*j*	*e*				*o*	*j*	*e*		*a*	*i*	

W	*G*	*T*	*W*	*C*	*J*	*K*	*R*	*B*	*I*	*K*	*Z*	*G*	*V*	*O*	*G*	*B*	*Q*
e	*o*		*e*	*t*		*i*	*j*	*s*		*i*		*o*		*n*	*o*	*s*	*a*

Sada već imamo dovoljno elemenata otvorenog teksta da možemo postupno odgonetavati čitave riječi (npr. prva riječ: *matematika*, zadnja riječ: *odnosa*). Konačno dobivamo otvoreni tekst

Matematika je znanstvena disciplina nastala
proučavanjem brojeva i geometrijskih odnosa.

Dakle, alfabet šifrata izgleda ovako,

q s u v w x y z k r i p t o g a f j b c d e h l m n

odnosno

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*
q	*s*	*u*	*v*	*w*	*x*	*y*	*z*	*k*	*r*	*i*	*p*	*t*	*o*	*g*	*a*	*f*	*j*	*b*	*c*	*d*	*e*	*h*	*l*	*m*	*n*

.

Uočavamo pojavljivanje riječi *kriptografija* unutar alfabeta šifrata. Radi se o varijanti supstitucijske šifre koja se naziva **Cezarova šifra s ključnom riječi**. U njoj ključ predstavlja ključna riječ (u ovom slučaju KRIPTOGRAFIJA), te broj (u ovom slučaju 8) koji označava poziciju između 0 i 25 na kojoj počinjemo pisati ključnu riječ, ali bez ponavljanja slova. Dakle, u ovom primjeru ključ je $K = (\text{KRIPTOGRAFIJA}, 8)$.

Zadatak 2.5 *Dekriptirajte šifrat*

A K F G H A W B N S Q S W B G S I R Y F O E B J Y I B U A K
E H O S T Y Q A K Q I S J S I R S O V R H W S T S J B F Y Q
I S I F G J Y I S X B F W B A V B I S O E B A G K S I S V B
Q S

dobiven Cezarovom šifrom s ključnom riječi. Poznato je da je otvoreni tekst pisan na hrvatskom jeziku, te da je ključna riječ jedan grad na hrvatskoj obali. Odredite ključ $K = (\textit{ključna riječ, broj})$*, gdje "broj" označava poziciju u alfabetu od koje počinje ključna riječ.*

Rješenje:

Analizom frekvencije slova dobivamo sljedeću tablicu:

A | K, W, K, K, V, G
B | N, G, J, U, F, F, A, I, A, Q
C |
D |
E | B, H, B
F | G, O, Y, W, G
G | H, S, J, K
H | A, O, W
I | R, B, S, R, S, F, S, S, S
J | Y, S, B, Y
K | F, E, Q, S
L |

M |
N |
O | E, S, V, E
P |
Q | S, A, I, I, S
R | Y, S, H
S | Q, W, I, T, J, I, O, T, J, I, X, O, V, I, *
T | Y, S
U | A
V | R, B, B
W | B, B, S, B
X | B
Y | F, I, Q, Q, I
Z |

Iz tablice iščitavamo kako su najfrekventnija slova

S(15), B(10), I(9), A(6), F(5), Q(5), Y(5), G(4), J(4), K(4), O(4), W(4),

a najfrekventniji bigrami

IS(5), SI(4), WB(3), AK(3), BF(2), BA(2), EB(2), FG(2), IR(2), JY(2), OE(2), QS(2), IR(2).

Logično je pretpostaviti da je $e(A) = S$. Uočavamo recipročne bigrame IS i SI pa iz toga možemo zaključiti da je $e(N) = I$. Na prvi pogled može nam se učinit da je JE šifrirano s WB, odnosno da je E šifrirano s B, ali to je kriva prepostavka. Sljedeće što možemo pretpostaviti je da je neki od druga dva česta samoglasnika (I ili O) šifriran s B. Mi ćemo prepostaviti da je $e(I) = B$ pa kada to ubacimo u tekst dobivamo:

A	*K*	*F*	*G*	*H*	*A*	*W*	*B*	*N*	*S*	*Q*	*S*	*W*	*B*	*G*	*S*	*I*	*R*	*Y*	*F*	*O*	*E*	*B*	*J*	*Y*	*I*	*B*	*U*	*A*	*K*
–	–	–	–	–	–	–	*i*	–	*a*	–	*a*	–	*i*	–	*a*	*n*	–	–	–	–	–	*i*	–	–	*n*	*i*	–	–	–
E	*H*	*O*	*S*	*T*	*Y*	*Q*	*A*	*K*	*Q*	*I*	*S*	*J*	*S*	*I*	*R*	*S*	*O*	*V*	*R*	*H*	*W*	*S*	*T*	*S*	*J*	*B*	*F*	*Y*	*Q*
–	–	–	*a*	–	–	–	–	–	–	*n*	*a*	–	*a*	*n*	–	*a*	–	–	–	–	–	*a*	–	*a*	–	*i*	–	–	–
I	*S*	*I*	*F*	*G*	*J*	*Y*	*I*	*S*	*X*	*B*	*F*	*W*	*B*	*A*	*V*	*B*	*I*	*S*	*O*	*E*	*B*	*A*	*G*	*K*	*S*	*I*	*S*	*V*	*B*
n	*a*	*n*	–	–	–	–	*n*	*a*	–	*i*	–	–	*i*	–	–	*i*	*n*	*a*	–	–	*i*	–	–	–	*a*	*n*	*a*	–	*i*
Q	*S*																												
–	*a*																												

.

Sada nas zadnji dio teksta navodi na riječ: *analiza*, odnosno da je $e(L) = V, e(Z) = Q$. Pogledajmo čime bi mogao biti šifriran bigram ST. Eliminacijom dobivamo da je ST šifriran s FG, odnosno da je $e(S) = F$ i $e(T) = G$. Pogledajmo kako sada izgleda otvoreni tekst:

A	*K*	*F*	*G*	*H*	*A*	*W*	*B*	*N*	*S*	*Q*	*S*	*W*	*B*	*G*	*S*	*I*	*R*	*Y*	*F*	*O*	*E*	*B*	*J*	*Y*	*I*	*B*	*U*	*A*	*K*
–	–	*s*	*t*	–	–	–	*i*	–	*a*	*z*	*a*	–	*i*	*t*	*a*	*n*	–	–	*s*	–	–	*i*	–	–	*n*	*i*	–	–	–
E	*H*	*O*	*S*	*T*	*Y*	*Q*	*A*	*K*	*Q*	*I*	*S*	*J*	*S*	*I*	*R*	*S*	*O*	*V*	*R*	*H*	*W*	*S*	*T*	*S*	*J*	*B*	*F*	*Y*	*Q*
–	–	–	*a*	–	–	*z*	–	–	*z*	*n*	*a*	–	*a*	*n*	–	*a*	–	*l*	–	–	–	*a*	–	*a*	–	*i*	*s*	–	*z*
I	*S*	*I*	*F*	*G*	*J*	*Y*	*I*	*S*	*X*	*B*	*F*	*W*	*B*	*A*	*V*	*B*	*I*	*S*	*O*	*E*	*B*	*A*	*G*	*K*	*S*	*I*	*S*	*V*	*B*
n	*a*	*n*	*s*	*t*	–	–	*n*	*a*	–	*i*	*s*	–	*i*	–	*l*	*i*	*n*	*a*	–	–	*i*	–	*t*	–	*a*	*n*	*a*	*l*	*i*
Q	*S*																												
z	*a*																												

.

Odavde je vidljivo da je $e(V) = J, e(E) = Y, e(D) = X, e(C) = W, e(P) = A, e(K) = O, e(R) = E$ i $e(O) = K$. Dakle, alfabet šifrata je

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
s	t	w	x	y	z	d	u	b	r	o	v	n	i	k	a	c	e	f	g	h	j	l	m	p	q

,

a otvoreni tekst glasi:

Postupcima za čitanje skrivenih poruka bez poznavanja ključa
bavi se znanstvena disciplina kriptoanaliza. Prema tome, ključ je $K = (\text{DUBROVNIK}, 6)$.