Viženerov algoritam – Vigenere cipher

Enkripcija

K = (a_1, a_2, a_3,…), 0 ≤ a ≥ 25 – Karaktere za ključ uzimamo iz alfabeta koji koristimo, u ovom slučaju je to engleski lafabet koji ima 26 karaktera, npr. K=(10, 4, 24) vidimo da je svaki od karaktera korišćenih za ključ u okviru granica koje smo prethodno definisali izborom alfabeta.

1. Izvršiti enkripiju poruke*: h o w t o e n c r y p t* ako je dat ključ *K = (10, 4, 24)*

Enkripciju pomoću ovog algoritma vršimo tako što ključ koji smo definisali koristimo iznova, sve dok ne dođemo do kraja poruke koju želimo da kriptujemo. U našem slučaju to izgleda ovako.

Poruka	**h**	**o**	**w**	**t**	**o**	**e**	**n**	**c**	**r**	**y**	**p**	**t**
Ključ	10	4	24	10	4	24	10	4	24	10	4	24
Enkripcija	R	S	U	D	S	C	X	G	P	I	T	R

Ključ primenjujemo tako što izbrojimo broj mesta od datog karaktera u poruci. U prvom slučaju, za karakter **h** je deset mesta udesno, čime dobijamo karakter **R**. Za drugo slovo iz naše poruke **o** je pomeraj po datom ključu **4**, te tako dobijamo **S**. Za treće slovo **w** imamo pomeraj za **24** mesta udesno, te tako dobijamo karakter **U**. Tako redom za sve karaktere iz poruke.

Engleski alfabet																									
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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Dekripcija sa poznatim ključem

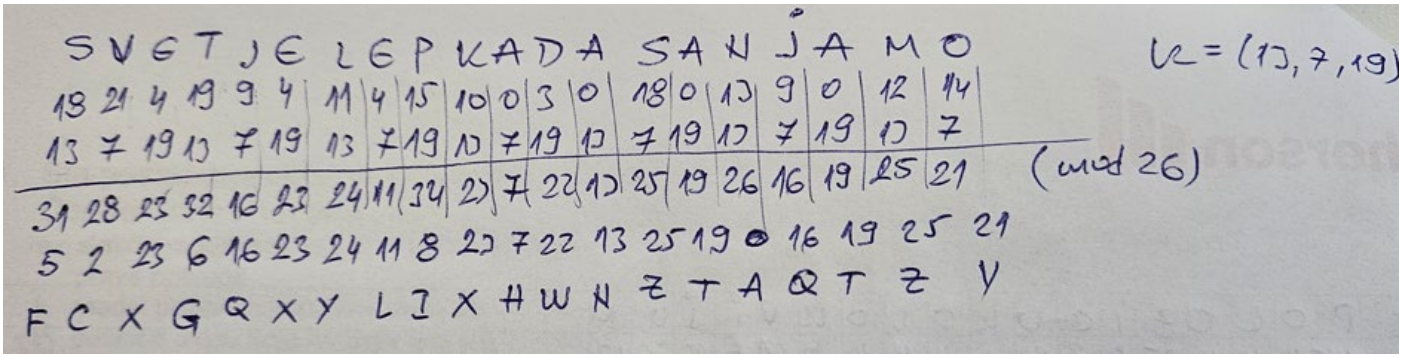
Poruka: **R S U D S C X G P I T R**

Ključ: **K = (10, 4, 24)**

Dekripciju vršimo pomoću poznatog ključa obrnuto od načina enkriptovanja poruke, što znači da se vrši operacija oduzimanja odnosno pomeraj ide u levom smeru. U tom slučaju postupak izgleda ovako.

Poruka	**R**	**S**	**U**	**D**	**S**	**C**	**X**	**G**	**P**	**I**	**T**	**R**
Ključ	-10	-4	-24	-10	-4	-24	-10	-4	-24	-10	-4	-24
Dekripcija	h	o	w	t	o	e	n	c	r	y	p	t

2. Izvršiti enkripciju teksta pomoću Vižnerovog algoritma SVET JE LEP KADA SANJAMO upotrebnom ključa K = (13, 7, 19)



Zadaci za samostalni rad studenta

Svaki od student je dužan da za poruke koje šifruje i dešifruje uzme **ime i prezime** svih članova porodice (min 4, ukoliko ima manje uzeti **ime i prezime** najboljeg prijatelja kao četvrti primer). Tako za svaki algoritam.