AKADEMIIJA TEHNIČKO VASPITAČKIH NAUKA
KOMUNIKACIONE TEHNOLOGIJE
ZAŠTITA PODATAKA U KOMUNIKACIONIM MREŽAMA

RAČUNSKA VEŽBA BR. 3

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.

Poruka: **h o w t o e n c r y p t**

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

Hilov algoritam – Hill cipher

(Matrica 2x2)

Enkripcija

Enkripcija pomoću Hilovog algoritma se vrši nad matricama. Ključ za enkripciju je dat u vidu matrice čiji su elementi iz skupa karaktera engleskog alfabeta. Iz datog primera možemo uvideti da postoje par pravila koja moramo ispoštovati kako bi ovaj algoritam funkcionisao. Prvo, dužina poruke je **četiri** samim tim ne možemo da pomnožimo matrice. Ono što možemo da uradimo jeste da našu poruku razbijemo na dva dela, **he lp**. Za vrednosti karaktera uzimamo redni broj karaktera iz engleskog alfabeta.

Poruka: **h e l p**

he = $\begin{bmatrix}7\\4\end{bmatrix}$ **lp** = $\begin{bmatrix}11\\15\end{bmatrix}$

Ključ: **K** = $\begin{bmatrix}3 & 3\\2 & 5\end{bmatrix}$

Postupak enkripcije formulom: **C = K*P(mod26)**

$$\mathbf{C_1}=\begin{bmatrix}3 & 3\\2 & 5\end{bmatrix}*\begin{bmatrix}7\\4\end{bmatrix}=\begin{bmatrix}(3*7)+ & (3*4)\\(2*7)+ & (5*4)\end{bmatrix}=\begin{bmatrix}21+ & 12\\14+ & 20\end{bmatrix}=\begin{bmatrix}33\\34\end{bmatrix}\ (\mathbf{mod\ 26})=\begin{bmatrix}7\\8\end{bmatrix}=\mathbf{HI}$$

$$\mathbf{C_2}=\begin{bmatrix}3 & 3\\2 & 5\end{bmatrix}*\begin{bmatrix}11\\15\end{bmatrix}=\begin{bmatrix}(3*11)+ & (3*15)\\(2*11)+ & (5*15)\end{bmatrix}=\begin{bmatrix}33+ & 45\\22+ & 75\end{bmatrix}=\begin{bmatrix}78\\97\end{bmatrix}(\mathbf{mod\ 26})=\begin{bmatrix}0\\19\end{bmatrix}=\mathbf{AT}$$

Enkriptovana poruka: **H I A T**

Dekripcija

Dekripcija se vrši obrnutim putem, a formula je: $\mathbf{P = K^{-1}*C(mod26).}$
U ovom slučaju, ključ pretvaramo u inverznu matricu $\mathbf{K^{-1}}$.

Inverznu matricu nalazimo pomoću formule: $\mathbf{A^{-1}=(ad - bc)^{-1}}\begin{bmatrix}d & -b\\-c & a\end{bmatrix}$, u našem slučaju je poznata matrica $\mathbf{A}\begin{bmatrix}a & b\\c & d\end{bmatrix}$, **K** = $\begin{bmatrix}3 & 3\\2 & 5\end{bmatrix}$.
Dakle:

$$\mathbf{K^{-1}=(3*5-3*2)*}\begin{bmatrix}5 & -3\\-2 & 3\end{bmatrix}\mathbf{(mod\ 26)=(9)^{-1}*}\begin{bmatrix}5 & -3\\-2 & 3\end{bmatrix}\mathbf{(mod\ 26)}$$

Sledeći korak bi bio rešavanje $\mathbf{(9)^{-1}.}$ Inverzni broj broja **9** je **1/9**, u tom slučaju imamo da je: **9*(1/9)=1**. Ali u sličaju modula 26, moramo izračunati **9*x = 1(mod 26)**. Ovo se rešava pomoću Proširenog Euklidovog Algoritma. Ukoliko odaberemo da je **x = 3**, onda imamo: **9*3=1(mod 26)=>27(mod 26)=1**. **Dakle inverzni broj broja 9 po modulu 26 je 3.**

$$\mathbf{K^{-1}} = \mathbf{(9)^{-1}*}\begin{bmatrix}5 & -3\\-2 & 3\end{bmatrix}\mathbf{(mod\ 26)} = \mathbf{3*}\begin{bmatrix}5 & 23\\24 & 3\end{bmatrix} = \begin{bmatrix}15 & 69\\72 & 9\end{bmatrix}(\mathbf{mod\ 26}) = \begin{bmatrix}15 & 17\\20 & 9\end{bmatrix}$$

Po formuli za dekripciju imamo:

$$\mathbf{P_1}=\begin{bmatrix}15 & 17\\20 & 9\end{bmatrix}*\begin{bmatrix}7\\8\end{bmatrix}=\begin{bmatrix}(15*7)+ & (17*8)\\(20*7)+ & (9*8)\end{bmatrix}=\begin{bmatrix}105+ & 136\\140+ & 72\end{bmatrix}=\begin{bmatrix}241\\212\end{bmatrix}(\mathbf{mod\ 26})=\begin{bmatrix}7\\4\end{bmatrix}=\mathbf{H\ E}$$

$$\mathbf{P_2}=\begin{bmatrix}15 & 17\\20 & 9\end{bmatrix}*\begin{bmatrix}0\\19\end{bmatrix}=\begin{bmatrix}(15*0)+ & (17*19)\\(20*0)+ & (9*19)\end{bmatrix}=\begin{bmatrix}0+ & 323\\0+ & 171\end{bmatrix}=\begin{bmatrix}323\\171\end{bmatrix}(\mathbf{mod\ 26})=\begin{bmatrix}11\\15\end{bmatrix}=\mathbf{L\ P}$$

Dobijena reč pomoću dekripcije se poklapa: **H E L P**.

Hilov algoritam – Hill cipher

(Matrica 3x3)

Enkripcija

Poruka: **A T T A C K I S T O N I G H T**

$$\begin{bmatrix} A & T & T \\ A & C & K \\ I & S & T \\ O & N & I \\ G & H & T \end{bmatrix} = \begin{bmatrix} 0 & 19 & 19 \\ 0 & 2 & 10 \\ 8 & 18 & 19 \\ 14 & 13 & 8 \\ 6 & 7 & 19 \end{bmatrix}$$

Ključ: **K** = $\begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix}$

Po formuli za enkripciju **C = K*P(mod26)** dobijamo:

$$\mathbf{C}=\begin{bmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \\ C_{41} & C_{42} & C_{43} \\ C_{51} & C_{52} & C_{53} \end{bmatrix}$$

$$\mathbf{C_{11}}=\begin{bmatrix} 0 & 19 & 19 \\ 0 & 2 & 10 \\ 8 & 18 & 19 \\ 14 & 13 & 8 \\ 6 & 7 & 19 \end{bmatrix} * \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix} = (0*3+19*20+19*9) = 551$$

$$\mathbf{C_{12}}=\begin{bmatrix} 0 & 19 & 19 \\ 0 & 2 & 10 \\ 8 & 18 & 19 \\ 14 & 13 & 8 \\ 6 & 7 & 19 \end{bmatrix} * \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix} = (0*10+19*9+19*4) = 247$$

$$\mathbf{C_{13}}=\begin{bmatrix} 0 & 19 & 19 \\ 0 & 2 & 10 \\ 8 & 18 & 19 \\ 14 & 13 & 8 \\ 6 & 7 & 19 \end{bmatrix} * \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix} = (0*20+19*17+19*17) = 646$$

Ovim postupkom za ostale članove matrice dobijamo rešenje:

$$\mathbf{C}=\begin{bmatrix} 551 & 247 & 646 \\ 130 & 58 & 204 \\ 555 & 318 & 789 \\ 374 & 289 & 637 \\ 329 & 199 & 562 \end{bmatrix} \mathbf{mod26} = \begin{bmatrix} 5 & 13 & 22 \\ 0 & 6 & 22 \\ 9 & 6 & 9 \\ 10 & 3 & 13 \\ 17 & 17 & 16 \end{bmatrix} = \begin{bmatrix} F & N & T \\ A & C & K \\ I & S & T \\ O & N & I \\ G & H & T \end{bmatrix}$$

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.