Cryptography 1

https://www2.karlin.mff.cuni.cz/~kuncova/en/index.php

kuncova@karlin.mff.cuni.cz

Matrices can be used for encryption.

The first step is the substitution of letters by numbers. Instead of A we have 0, instead of B we have 1, . . . , instead of Z we have 25.

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

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

For example POLAR BEAR can be written as
15 14 11 0 17 1 4 0 17

However, this cipher (so called substitution cipher) can be easily decrypted, especially with a computer. So let us complicate the situation. The second step is to write the numbers into a matrix.

$$\mathbf{B} = \begin{pmatrix} 15 & 14 & 11 \\ 0 & 17 & 1 \\ 4 & 0 & 17 \end{pmatrix}.$$

Now the really encryption part is coming. We choose a nice matrix $\mathbf{A}$, for example

$$\mathbf{A} = \begin{pmatrix} 6 & 2 & 3 \\ 3 & 1 & 1 \\ 10 & 3 & 4 \end{pmatrix}.$$

(There are some conditions on the matrix $\mathbf{A}$, which we will discuss later.)

Then we apply the matrix multiplication:

$$\mathbf{C} = \mathbf{AB} = \begin{pmatrix} 242 & 77 & 103 \\ 61 & 20 & 21 \\ 194 & 59 & 80 \end{pmatrix}.$$

The resulting product $\mathbf{C}$ is really hard to decrypt without the knowledge of the ciphering principle and without the matrix $\mathbf{A}$.

However, if you know the matrix $\mathbf{A}$, you can decrypt the message with the following steps.

1. Find the inverse matrix $\mathbf{A}^{-1}$.
2. Make the product $\mathbf{A}^{-1}\mathbf{C} = \mathbf{A}^{-1}\mathbf{A}\mathbf{B} = \mathbf{B}$.
   (Be careful, you have to make the product $\mathbf{A}^{-1}\mathbf{C}$, not $\mathbf{C}\mathbf{A}^{-1}$!)
3. Change numbers back to letters.

You can check the steps on the polar bear.

Now it is Your turn. You have captured part of an encrypted message - every group has different part. You know, that the matrix $\mathbf{A}$ was used. **Find the original message and write it on the whiteboard.**

Message for the group V:

$$\mathbf{AB} = \begin{pmatrix} 160 & 36 & 138 \\ 78 & 18 & 68 \\ 260 & 54 & 223 \end{pmatrix}$$

Message for the group W:

$$\mathbf{AB} = \begin{pmatrix} 74 & 74 & 132 \\ 30 & 31 & 62 \\ 108 & 110 & 211 \end{pmatrix}$$

Message for the group X:

$$\mathbf{AB} = \begin{pmatrix} 159 & 222 & 98 \\ 71 & 99 & 45 \\ 248 & 339 & 154 \end{pmatrix}$$

Message for the group Y:

$$\mathbf{AB} = \begin{pmatrix} 76 & 90 & 134 \\ 37 & 43 & 63 \\ 119 & 146 & 211 \end{pmatrix}$$

Message for the group Z:

$$\mathbf{AB} = \begin{pmatrix} 160 & 173 & 161 \\ 77 & 77 & 77 \\ 255 & 268 & 257 \end{pmatrix}$$