Cryptography 1

https://www2.karlin.mff.cuni.cz/~kuncova/en/teaching.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 GALAPAGOS PENGUIN can be written as
6 0 11 0 15 0 6 14 18 15 4 13 6 20 8 13.

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

$$\mathbf{B} = \begin{pmatrix} 6 & 0 & 11 & 0 \\ 15 & 0 & 6 & 14 \\ 18 & 15 & 4 & 13 \\ 6 & 20 & 8 & 13 \end{pmatrix}.$$

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

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & -1 & 3 \\ 2 & -2 & 0 & 0 \\ -1 & 4 & 2 & 1 \\ -1 & 2 & 0 & 1 \end{pmatrix}.$$

(There are some conditions on the matrix $\mathbf{A}$ - please, wait until next week.)

Then we apply the matrix multiplication:

$$\mathbf{C} = \mathbf{AB} = \begin{pmatrix} 6 & 45 & 31 & 26 \\ -18 & 0 & 10 & -28 \\ 96 & 50 & 29 & 95 \\ 30 & 20 & 9 & 41 \end{pmatrix}.$$

The resulting product $\mathbf{C}$ can be easily decrypted with knowledge of the original matrix $\mathbf{A}$.

We find the inverse matrix $\mathbf{A}^{-1}$ and then we make the product $\mathbf{A}^{-1}\mathbf{C} = \mathbf{A}^{-1}\mathbf{AB} = \mathbf{B}$. (You can check it with the galapagos penguin.)

Now it is Your turn. You have captured part of an encrypted message. You know, that the matrix $\mathbf{A}$ was used. Find the original message and write it into the shared document.

Message for the group X: $\mathbf{AB} = \begin{pmatrix} 32 & 8 & 21 & 33 \\ 8 & -30 & 26 & 16 \\ 58 & 72 & 12 & 40 \\ 18 & 34 & -6 & 6 \end{pmatrix}$

Message for the group Y: $\mathbf{AB} = \begin{pmatrix} 34 & 26 & 61 & 12 \\ 2 & 16 & -6 & 28 \\ 79 & 54 & 99 & 10 \\ 23 & 6 & 41 & -10 \end{pmatrix}$

Message for the group Z: $\mathbf{AB} = \begin{pmatrix} 30 & -11 & -2 & -11 \\ -10 & -32 & -30 & -18 \\ 74 & 96 & 84 & 98 \\ 30 & 34 & 34 & 26 \end{pmatrix}$