# Problem 4. «Matrix and reduction»

Alice used an alphabet with 30 characters from A to Z and 0, 1, «,», «!». Each of the letters is encoded as follows:

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| P | Q | R | S | T | U | V | W | X | Y | Z | 0 | 1 | , | ! |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |

**Encryption.** The plaintext is divided into consequent subwords of length 4 that are encrypted independently via the same encryption $(2\times2)$-matrix $F$ with elements from $\mathbb{Z}_{30}$. For example, let the $j$-th subword be WORD and the encryption matrix $F$ be equal to

$$F = \begin{pmatrix} 11 & 9 \\ 11 & 10 \end{pmatrix}.$$

The matrix that corresponds to WORD is denoted by $P_j$ and the matrix that corresponds to the result of the encryption of WORD is $C_j$ and calculated as follows:

$$C_j = F \cdot P_j = \begin{pmatrix} 11 & 9 \\ 11 & 10 \end{pmatrix} \cdot \begin{pmatrix} 22 & 17 \\ 14 & 3 \end{pmatrix} = \begin{pmatrix} 8 & 4 \\ 22 & 7 \end{pmatrix} \pmod{30},$$

that is the $j$-th subword of the ciphertext is IWEH.

Eve has intercepted a ciphertext that was transmitted from Alice to Bob:

CYPHXWQE!WNKHZ0Z

Also, she knows that the third subword of the plaintext is FORW. Will Eve be able to restore the original message?