

We use an alphabet composed of a blank space and the 26 letters of the English alphabet.

$$n = 27, m = 2$$

We will use as key the assignment number and current date: 1, 23, 10, 13

$$K = \begin{pmatrix} 1 & 23 \\ 10 & 13 \end{pmatrix}$$

The plaintext is SZABO, which is numerically: 19, 26, 1, 2, 15. Because it has an length that is not a multiple of m , we pad it with a space character.

$$P = (19, 26), (1, 2), (15, 0)$$

To encrypt we multiply modulo 27 K with each group of two letters from the plaintext:

$$\left[\begin{pmatrix} 19 & 26 \end{pmatrix} \begin{pmatrix} 1 & 23 \\ 10 & 13 \end{pmatrix} = \begin{pmatrix} 9 \\ 19 \end{pmatrix}, \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 23 \\ 10 & 13 \end{pmatrix} = \begin{pmatrix} 21 \\ 22 \end{pmatrix}, \begin{pmatrix} 15 & 0 \end{pmatrix} \begin{pmatrix} 1 & 23 \\ 10 & 13 \end{pmatrix} = \begin{pmatrix} 15 \\ 21 \end{pmatrix} \right]$$

Converting 9, 19, 21, 22, 15, 21 to our alphabet, we get that the ciphertext is ISUVOU.

For decryption we need the decryption key, which is the inverse of our encryption key. Using Cramer's rule:

$$K^{-1} = (1 \cdot 13 - 23 \cdot 10)^{-1} \begin{pmatrix} 13 & -23 \\ -10 & 1 \end{pmatrix} = 26 \begin{pmatrix} 13 & -23 \\ -10 & 1 \end{pmatrix} = \begin{pmatrix} 14 & 23 \\ 10 & 26 \end{pmatrix}$$

To decrypt the cyphertext, we multiply the decryption key with each group of two letters from the cypertext:

$$\left[\begin{pmatrix} 9 & 19 \end{pmatrix} \begin{pmatrix} 14 & 23 \\ 10 & 26 \end{pmatrix} = \begin{pmatrix} 19 \\ 26 \end{pmatrix}, \begin{pmatrix} 21 & 22 \end{pmatrix} \begin{pmatrix} 14 & 23 \\ 10 & 26 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 15 & 21 \end{pmatrix} \begin{pmatrix} 14 & 23 \\ 10 & 26 \end{pmatrix} = \begin{pmatrix} 15 \\ 0 \end{pmatrix} \right]$$

The result is SZABO_, which is what we encrypted in the first place, with the trailing space.