Exercise (1)

It is known that shift encryption has been used to encrypt the plaintext. Hence the encryption function has the form $y \equiv x + b \bmod N$, where N is the size of the alphabet. Also we know that the alphabet used consists of 26 symbols, that is $N = 26$. Thus, to find the encryption function we should define only the shift encryption key b. Applying frequency analysis we determine that the letter X is the most frequently occurring in the ciphertext. Hence we can suppose that E encrypts to X. The numerical equivalents of E and X are 4 and 23 respectively. Substituting 23 for y and 4 for x into $y \equiv x + b \bmod 26$ we obtain the equation $23 \equiv 4 + b \bmod 26$. Hence $b = 19$, and the encryption function is $y \equiv x + 19 \bmod 26$. The decryption function is $x \equiv y - 19 \bmod 26$. Now we can proceed to recovering of the plaintext.

First, write down the numerical equivalent of the encrypted text.

15 23 15 23 10 23 4 13 21 3 17 20 23 21 19 13 11 23 7 24 12 23 6 12 0 23 24 10 23 9 13 23 6 21 17 5 23 12 0 7 22 6 23 23 22 11 4 7 6 25 23 10 21 1 8 0 23 10 12 23 16 12.

Next, subtract 19 (mod 26) from each number of the above string. We obtain 22 4 22 4 17 4 11 20 2 10 24 1 4 2 0 20 18 4 14 5 19 4 13 19 7 4 5 17 4 16 20 4 13 2 24 12 4 19 7 14 3 13 4 4 3 18 11 14 13 6 4 17 2 8 15 7 4 17 19 4 23 19.

Now substitute into the last string letters from the alphabet corresponding to the numbers. We obtain the following text.

WEWERELUCKYBECAUSEOFTENTHEFREQUENCYMETHOD
NEEDSLONGERCIPHERTEXT

`Answer.` The plaintext is as follows: *We were lucky because often the frequency method needs longer ciphertext.*

Exercise (2). See the solution in tutorials.

Exercise (3).

First, let us find the encryption key (a, b) of the affine encryption function $y \equiv ax + b \bmod 41$. The frequency analysis shows that the most frequently occurring symbols in the ciphertext are I and 7, therefore we can suppose that E encrypts to I and T encrypts to 7. Hence $4 \to 8$, $19 \to 33$. Substituting corresponding values for x and y into $y \equiv ax + b \bmod 41$ we obtain the following system of congruences.

$8 \equiv 4a + b \bmod 41$

$33 \equiv 19a + b \bmod 41$.

Subtract the first congruence from the second to eliminate b . We obtain that $25 \equiv 15a \bmod 41$, i.e. $5 \equiv 3a \bmod 41$. Applying the Extended Euclidean Algorithm (see Problem Sheet 1) we calculate that the multiplicative inverse of 3 mod 41 equals 14. Hence $a \equiv 5 \cdot 3^{-1} \equiv 5 \cdot 14 \equiv 29 \bmod 41$. Substituting $a = 29$ into the first congruence of the above system, we obtain that $b = 15$. Hence the encryption function is $y \equiv 29x + 15 \bmod 41$.

To recover the plaintext we should find the function inverse to the encryption function $y \equiv 29x + 15 \bmod 41$, that is to solve the last congruence for x in terms of y. By Extended Euclidean Algorithm the multiplicative inverse of 29 mod 41

equals 17. Hence $x \equiv 17y - 17 \cdot 15 \bmod 41$. Thus the decryption function is as follows: $x \equiv 17y + 32 \bmod 41$.

Knowing the decryption function we can proceed to the final step of the process of recovering the plaintext. The numerical equivalents of symbols of the ciphertext are

33 13 8 23 35 14 15 4 1 37 6 16 20 11 21 .

Substituting these values for variable y into $x \equiv 17y + 32 \bmod 41$, we obtain the numerical equivalents of symbols of the plaintext:

19 7 4 13 12 24 0 18 8 5 11 17 3 14 20,

which yields the decryption

T H E N M Y A S I F L R D O U.

`Answer.` The plaintext is as follows: *The enemy has infiltrated our system.*

Exercise (4). See the solution in the tutorials.