"FUNDAMENTALS of CRYPTOGRAPHY" course.

Laboratory work No. 3. (Decoding)

Task:

Perform decoding of the cryptotext obtained during laboratory work No.1 and No.2.

Specification of the task:

1. Assuming that the encryption algorithms are known (items 1a, 1b of laboratory work No.1 and 1. of laboratory 2) develop algorithms for deciphering the ciphertext created during the performance of laboratory work No.1 and 2.
2. In a high-level language, write a program (programs) for decoding informational messages.
3. Use software to calculate the processor's operating time for each program.
4. Create a report on the performance of laboratory work, in which to provide the developed algorithms, program listings and the results of their work - decoded information messages and processor operating time.

Additional information for completing the task.

The programs written during laboratory work No.1 and No.2 must generate the incoming open message used in laboratory work No.3 by decoding the ciphertext that was obtained as a result of laboratory work No.1 and No.2.

The algorithm of the program assumes that the following information is known: coding is performed by one of the used methods (in laboratory work No.1 - it is either 1a, 1b; in laboratory work No.2 – it is Caesar cipher).

This, limited set of encoding methods, determines the decoding algorithm, which consists in a sequential (option: parallel) search of all three possible options for deciphering the ciphertext.

If the program works correctly, one of the decoding methods (which corresponds to the selected encoding algorithm) will lead to receiving the original message. At the same time, the two second methods of decoding will not lead to receiving the original message.

Optional.

Propose an algorithm and write a program to complete the task: How to use the XOP operation for encryption?

If you cannot find a solution to this problem, then in the next lesson I will show one of the solutions.