

Ministry of Education, Culture and Research of the Republic of Moldova Technical University of Moldova

Faculty of Computers, Informatics and Microelectronics Department of Software Engineering and Automation

# Report

# for laboratory work no. 3

# in the course "Cryptanalysis of polyalphabetic

# ciphers"

A efectuat:Ceban Andrei, gr. FAF-211

A verificat: Cǎtǎlin MÎŢU

Chișinău – 2023

**Subject:** Polyalphabetic ciphers

## Tasks:

1. To implement the Vigenere algorithm in one of the programming languages for messages in Romanian (31 letters), these being coded with the numbers 0, 1, ... 30. The values of the text characters are between 'A' and 'Z', ' a' and 'z' and no other values are assumed. If the user enters other values - the correct range of characters will be suggested. The length of the key must not be less than 7. Encryption and decryption will be done according to the formulas in the mathematical model presented above. In the message, spaces must first be removed, then all letters will turn into uppercase. The user will be able to choose the operation - encryption or decryption, will be able to enter the key, message or cryptogram and get the decrypted cryptogram or message

## Cryptanalysis of The Vigenère Cipher

Polyalphabetic substitution ciphers (polyalphabetic ciphers). Weakness of numbers monoalphabetic is defined by the fact that their frequency distribution reflects the distribution of the alphabet used. A cipher is cryptographically more secure if it exhibits an even distribution regular, which does not provide information to the cryptanalyst. One way to flatten the distribution is to combine high and low distributions. If the letter T is sometimes encrypted as a and sometimes as b, and if the letter X is also sometimes encrypted as a and another time as b, the high frequency of T combines with the low frequency of X producing a more moderate distribution for a and for b. Two distributions can be combined by using two separate encryption alphabets, the first for characters in even positions clear text, second for characters in odd positions, resulting in the need to use alternatively two translation tables, for example permutations p(a)=(3·a) mod 26 and p2(a)=(7·a +13) mod 26. The difference between polyalphabetic and monoalphabetic ciphers is that the substitution of a character varies in the text, depending on various parameters (position, context, etc.). It leads of course to a much larger number of possible keys. It is considered the first encryption system polyalphabetic was created by Leon Battista in 1568. Some current applications still use for certain sections such encryption systems. The encryption method known as the "Vigenère cipher" has been wrongly attributed to him Blaise de Vigenère in the 19th century and was actually first described by Giovan Battista Bellaso in his 1553 book La cifra del. Sig. Vigenère created a similar cipher, but yet different and stronger in 1586. On the other hand, the Vigenere cipher uses the same operations as the Caesar cipher. cipher Vigenere and the like move the letters, but unlike Caesar, it cannot be easily broken into 26 combinations. The Vigenere cipher uses a multiple shift. The key is not constituted by one displacement, but several, being generated by several integers ki, where 0 ≤ ki ≤ 25, if we take as a benchmark the Latin alphabet with 26 letters. Encryption is done as follows: ci = (mi + ki) mod 26. The key could be, for example, k = (5, 20, 17, 10, 20, 13) and would cause the first letter to be moved with 5, c1=m1 + 5 (mod 26), of the second one with 20, c2 = m2 + 20 (mod 26), etc. until the end keys and then from the beginning, again. The key is usually a word, to make it easier to remember – the key above corresponds to the word “storm”. The multiple displacement method provides protection additional for two reasons: • the first reason is that others do not know the length of the key; • the second reason is that the number of possible solutions increases with the size of the key; for example, for key length equal to 5, the number of combinations that would be required for the exhaustive search would be 265 = 11,881,376.

## The result of performing the tasks:

The Vigenere algorithm:

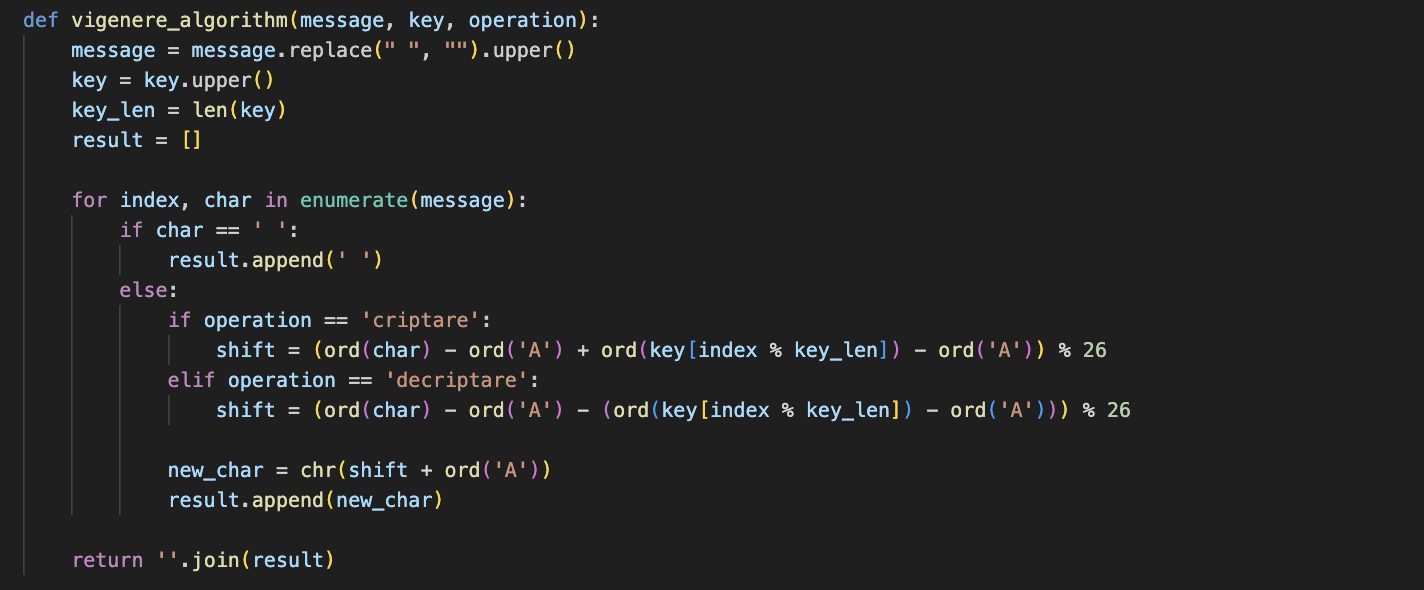


Fig 1 – Vigenere algorithm

**Execution :**

First step is to give the algotirhm a message, a key, and an operation (either encryption or decryption) as input. The algorithm removes spaces, converts the text and key to uppercase, and then processes each character in the text. For encryption ('criptare'), it shifts each character in the text by a value determined by the corresponding character in the key, wrapping around the English alphabet (26 letters). For decryption ('decriptare'), it reverses the shift. The result is a transformed ciphertext or plaintext, depending on the chosen operation.

The encryption of a message with key ‘SUPER’ :

The encrypted message is ‘HYGEJHYGERVUHXIS’ .

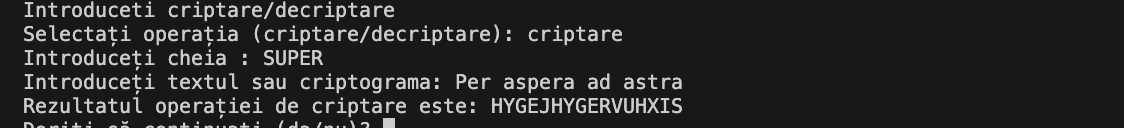


Fig 2 – Encrypted message

The description of a message with key ‘SUPER’

The decrypted message is ‘PERASPERAADASTRA’ .

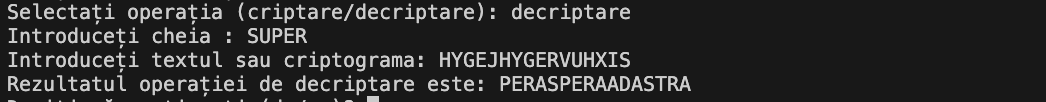


Fig 3 – Decrypted message

**Conclusion:** Vigenere cipher is a polyalphabetic substitution cipher that offers increased security compared to monoalphabetic ciphers. It achieves this by using a keyword to create a shifting mechanism, which varies the encryption of each letter in the message. While it provides better security, it is not immune to cryptanalysis, especially with shorter keys. Frequency analysis and other techniques can still be used to break the Vigenere cipher. Nonetheless, it remains a historically significant and interesting encryption method that illustrates the evolution of cryptographic techniques.