Ministerul Educaţiei și Cercetării al Republicii Moldova
Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică şi Microelectronică

Laboratory work 1

CRYPTOGRAPHY AND SECURITY

Elaborated:

st. gr. FAF-213
Bardier Andrei

Verified:

Zgureanu A.

Chisinau 2023

Subject: Caesar Cipher

Tasks:

- Implement the Caesar algorithm for the English alphabet in one of the programming languages. Use only letter encoding as shown in Table 1 (do not use encodings specified in the programming language, e.g., ASCII or Unicode). Key values will range from 1 to 25, inclusive, and no other values are allowed. Text character values are between 'A' and 'Z', 'a' and 'z', and no other values are allowed. If the user enters other values, they will be prompted with the correct range. Before encryption, the text will be converted to uppercase, and spaces will be removed. The user will be able to choose the operation - encryption or decryption, input the key, message, or ciphertext, and obtain the respective ciphertext or decrypted message.
- Implement the Caesar algorithm with 2 keys, while preserving the conditions expressed in Task 1. In addition, key 2 must consist of only Latin alphabet letters and have a length of no less than 7.

Caesar Cipher

In this cipher, each letter of the plaintext is replaced with a new letter obtained by an alphabetic shift. The secret key k, which is the same for both encryption and decryption, represents the number indicating the alphabetic shift, i.e., $k \in \{1, 2, 3,\ldots, n–1\}$, where n is the length of the alphabet. The encryption and decryption of the message with the Caesar cipher can be defined by the formulas

$$c = e_k(x) = x + k \pmod n,$$

$$m = d_k(y) = y – k \pmod n,$$

where x and y are the numeric representations of the respective characters of the plaintext. The Modulo function (a mod b) returns the remainder of the integer division of a by b. For example, for k = 3, we have (Figure 1):

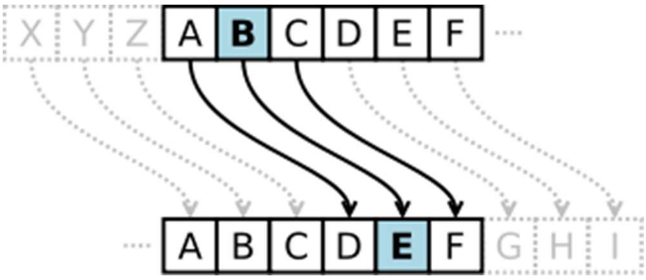


Figure 1. Example of alphabetic shift

To enhance the cryptographic strength of the Caesar cipher, a permutation of the alphabet can be applied by using a keyword (not to be confused with the base cipher key). This keyword can be any sequence of alphabet letters - either a word from the vocabulary or one without meaning.

Let the second key be k_2 = cryptography. Applying this key to the alphabet:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

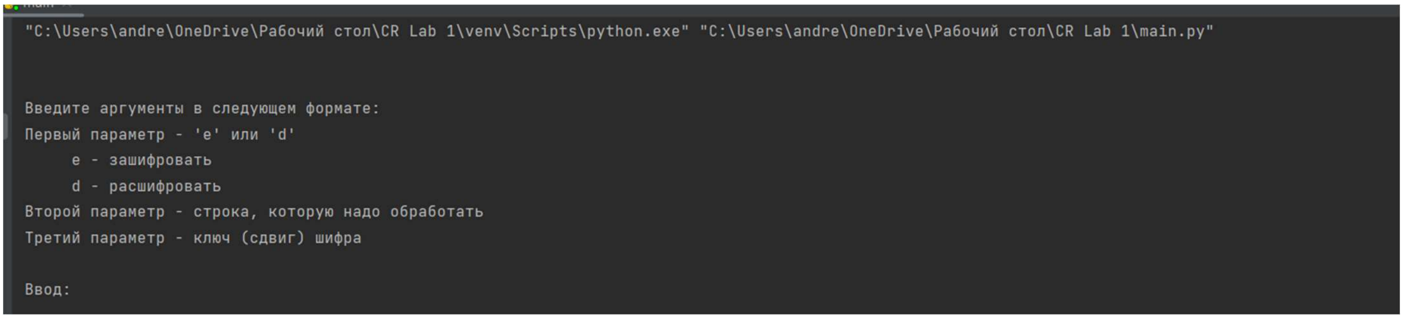
and obtaining:

C R Y P T O G A H B D E F I J K M L N Q S U V W X Z

This new order is obtained by placing the letters of k_2 at the beginning, followed by the other letters of the alphabet in their natural order. It should be noted that letters will not repeat, meaning that if a letter appears multiple times, it is placed only once.

Task Results:

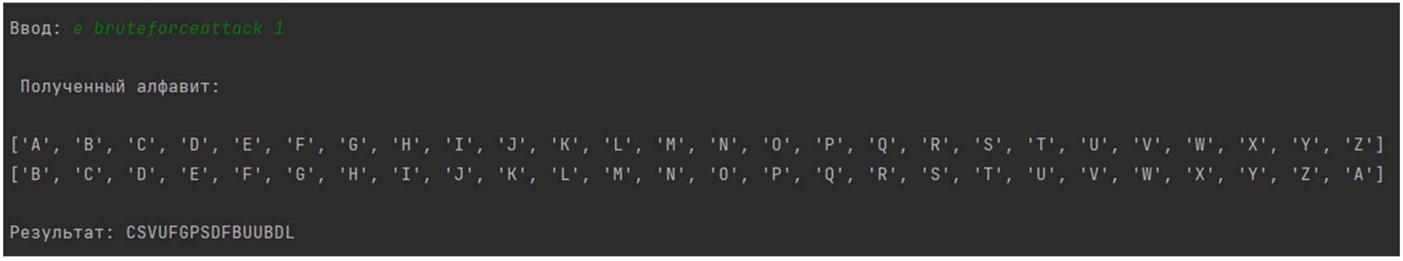
Initially, if the user does not input any arguments, an instructional message will be displayed (Figure 2).



```
"C:\Users\andre\OneDrive\Рабочий стол\CR Lab 1\venv\Scripts\python.exe" "C:\Users\andre\OneDrive\Рабочий стол\CR Lab 1\main.py"


Введите аргументы в следующем формате:
Первый параметр - 'e' или 'd'
     e - зашифровать
     d - расшифровать
Второй параметр - строка, которую надо обработать
Третий параметр - ключ (сдвиг) шифра

Ввод:
```

Figure 2. Informational Message

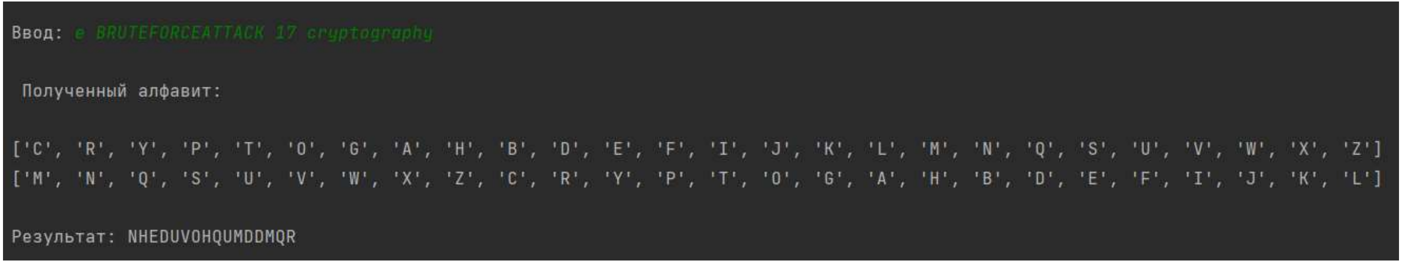
To encrypt a message, enter the action "e," the message, the shift key, and optionally the secondary key. An example of encryption with one key is shown in Figure 3.



```
Ввод: e bruteforceattack 1

 Полученный алфавит:

['A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z']
['B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z', 'A']

Результат: CSVUFGPSDFBUUBDL
```

Figure 3. Encryption with One Key

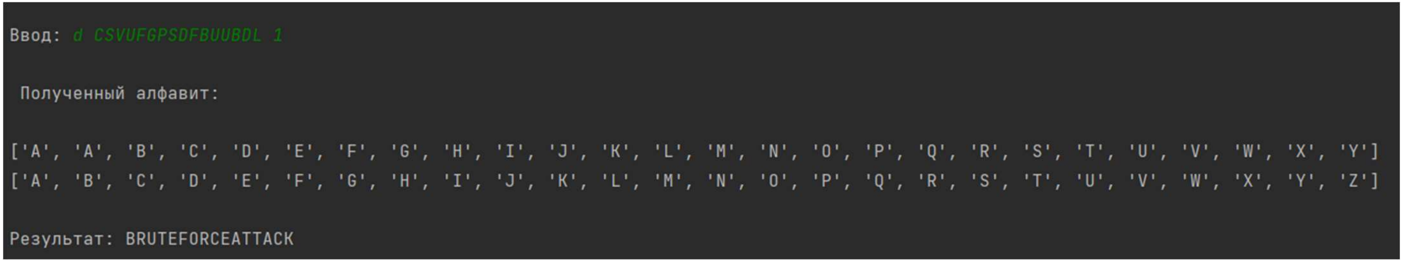
An example of encryption with two keys is shown in Figure 4.



```
Ввод: e BRUTEFORCEATTACK 17 cryptography

 Полученный алфавит:

['C', 'R', 'Y', 'P', 'T', 'O', 'G', 'A', 'H', 'B', 'D', 'E', 'F', 'I', 'J', 'K', 'L', 'M', 'N', 'Q', 'S', 'U', 'V', 'W', 'X', 'Z']
['M', 'N', 'Q', 'S', 'U', 'V', 'W', 'X', 'Z', 'C', 'R', 'Y', 'P', 'T', 'O', 'G', 'A', 'H', 'B', 'D', 'E', 'F', 'I', 'J', 'K', 'L']

Результат: NHEDUVOHQUMDDMQR
```

Figure 4. Encryption with Two Keys

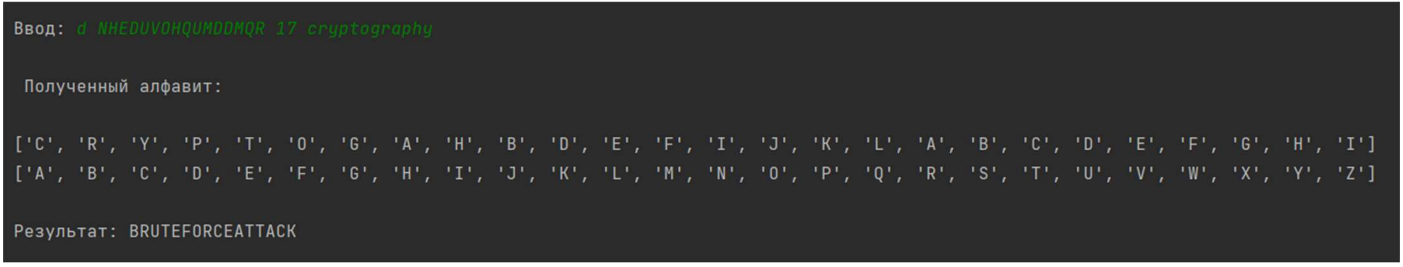
To decrypt a message, enter the action "d," the message, and the decryption key, and if necessary, the secondary key. An example of decryption with one key is shown in Figure 5.



```
Ввод: d CSVUFGPSDFBUUBDL 1

 Полученный алфавит:

['A', 'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y']
['A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z']

Результат: BRUTEFORCEATTACK
```

Figure 5. Decryption with One Key

An example of decryption with two keys is shown in Figure 6.



```
Ввод: d NHEDUVOHQUMDDMQR 17 cryptography

 Полученный алфавит:

['C', 'R', 'Y', 'P', 'T', 'O', 'G', 'A', 'H', 'B', 'D', 'E', 'F', 'I', 'J', 'K', 'L', 'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I']
['A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z']

Результат: BRUTEFORCEATTACK
```

Figure 6. Decryption with Two Keys

Conclusion:

During the course of this laboratory experiment, we delved into the fundamental workings of the Caesar cipher algorithm. Our primary achievement was the development of a software application that effectively applies the Caesar cipher with both single and dual keys for the encryption and decryption of messages. While on the surface, the two-key version of the cipher may not appear notably more intricate, it undeniably enhances the security of the encryption, substantially diminishing the likelihood of unauthorized decryption compared to the single-key variant.

The pivotal concept behind the Caesar cipher is the alphabetic shift, governed by a secret key denoted as 'k.' This key is identical for both encryption and decryption, and it signifies the magnitude of the alphabetic shift. The key 'k' falls within the range of {1, 2, 3,…, n–1}, where 'n' denotes the length of the alphabet. This mathematical manipulation of shifting characters makes it computationally challenging for unauthorized individuals to reverse the process.

To heighten the cryptographic robustness of the Caesar cipher, we introduced the concept of a secondary key. By applying a keyword to the alphabet, we rearranged the order of letters, ensuring that duplicates are omitted. This permutation technique adds an additional layer of security, further complicating any attempts to crack the cipher. In practical terms, using an exhaustive approach to decipher a message encoded with this two-key Caesar cipher would necessitate evaluating a staggering 26! * 25 combinations—an astronomical computational task. In conclusion, our exploration not only shed light on the Caesar cipher's mechanics but also demonstrated how enhancing its complexity can significantly bolster message security.

GitHub link:
https://github.com/Ricigeroi/CR-Lab-1/