



**Ministry of Education, Culture and Research of the Republic of
Moldova**

Technical University of Moldova

Department of Software and Automation Engineering

REPORT

Laboratory Work Nr.1

Cryptographic methods of information protection

Realised by:

st.gr. FAF-213
Iatco Sorin

Checked by :

asist. univ.
Mîtu Cătălin,

Chişinău 2022

Subject: Caesar cipher.

Tasks.

1. Implement the Caesar algorithm for the English alphabet in one of the programming languages. Use only letter encoding as shown in Table 1 (encodings specified in the programming language, e.g., ASCII or Unicode, are not allowed). Key values will range from 1 to 25 inclusive, and no other values are allowed. Text character values range from 'A' to 'Z', 'a' and 'z' and no other values are allowed. If the user enters other values - the correct tuning fork will be suggested. Before encryption, text will be capitalized and spaces will be removed. The user will be able to choose the operation - encryption or decryption, enter the key, message or cryptogram and obtain respectively the cryptogram or the decrypted message.
2. Implement the algorithm Caesar with 2 keys, keeping the conditions expressed in Task 1. In addition, key 2 must contain only letters of the Latin alphabet, and be not less than 7 in length.

Caesar cipher:

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

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

$$m = d_k(y) = y - k \pmod{n},$$

where x and y are the numerical representation of the respective character of the clear text. The function called Modulo ($a \bmod b$) returns the remainder of dividing the integer a by the integer b . For example, for $k = 3$ we have (fig 1):

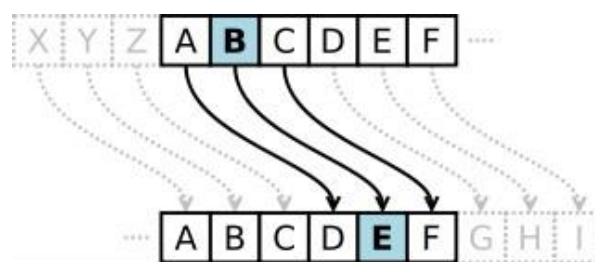


Figure 1. Example of alphabetical displacement

To increase the crypt strength of the cipher Caesar a permutation of the alphabet can be applied by applying a keyword (not to be confused with the basic key of the cipher). This key can be any sequence of letters of the alphabet - either a word in the vocabulary or a meaningless one.

Either the second key is k2=cryptography. We apply 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 we get:

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

We obtained this new order by placing the letters of k2 at the beginning, then follow the other letters of the alphabet in their natural order. We will take into account that the letters will not repeat, that is, if the letter meets several times, it is placed only once.

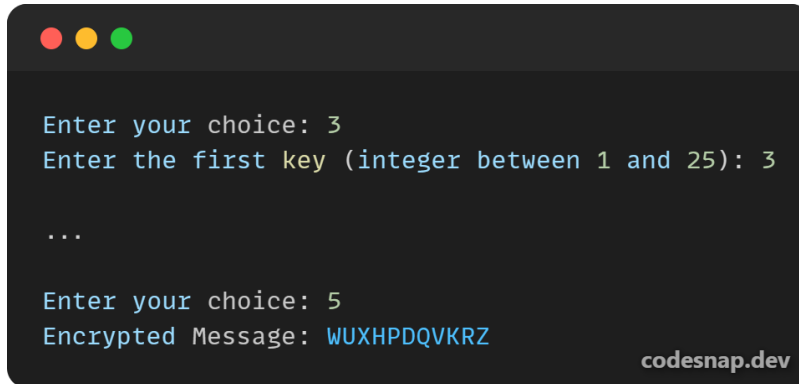
Results.

First of all the user is prompted by a menu of commands from which he can choose.



Figure 1. Brief overview of the menu.

To encrypt a message the user needs to first enter a message, the first key, optionally the second key and then select the encryption command from the menu list, the operation of encryption with a single key is in *figure 2* and using 2 keys is represented in the *figure 3*.

A terminal window with a dark background and three colored window control buttons (red, yellow, green) at the top left. The text inside the terminal is as follows:

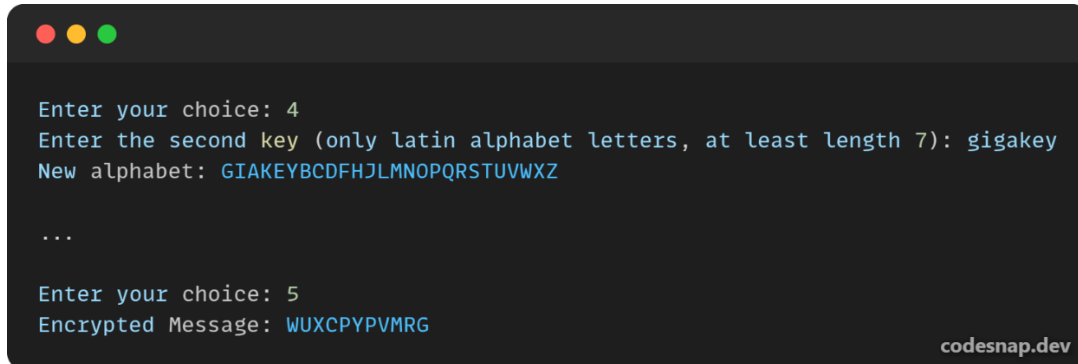
```
Enter your choice: 3
Enter the first key (integer between 1 and 25): 3

...

Enter your choice: 5
Encrypted Message: WUXHPDQVKRZ
```

The text "codesnap.dev" is visible in the bottom right corner of the terminal window.

Figure 2. Encryption with single key.

A terminal window with a dark background and three colored window control buttons (red, yellow, green) at the top left. The text inside the terminal is as follows:

```
Enter your choice: 4
Enter the second key (only latin alphabet letters, at least length 7): gigakey
New alphabet: GIAKEYBCDFHJLMNOPQRSTUVWXYZ

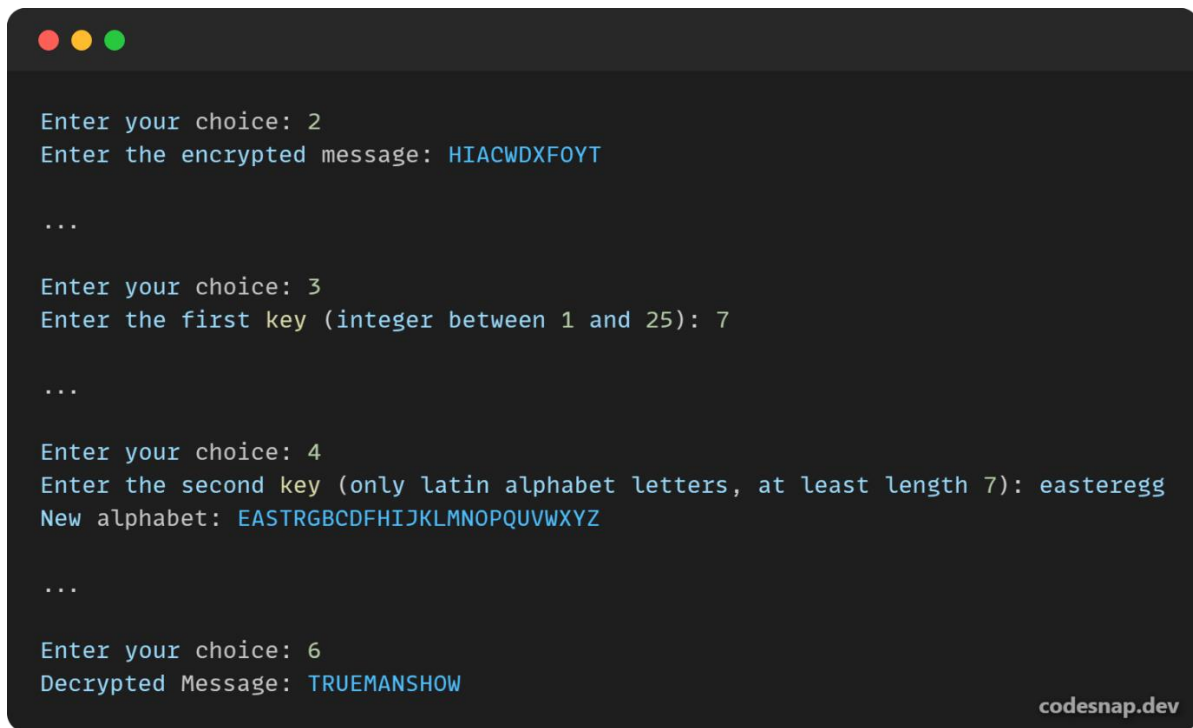
...

Enter your choice: 5
Encrypted Message: WUXCPYPVMRG
```

The text "codesnap.dev" is visible in the bottom right corner of the terminal window.

Figure 3. Encryption using 2 keys.

The user can also decrypt the message if he selects the 6'th option in the menu and the encrypted text will be transformed to the initial semnification. The user can prompt the encrypted text and the keys and selet decrypt message, this example is shown in *figure 4*. The user can also prompt a encrypted message with just one key and it will be able to decrypt it.

A terminal window with a dark background and three colored window control buttons (red, yellow, green) in the top-left corner. The terminal displays a series of prompts and user inputs for a Caesar cipher decryption process. The prompts are in a light blue color, and the user inputs are in a light green color. The process involves entering a choice, an encrypted message, a first key, a second key, and finally a choice to decrypt a message, which results in a decrypted message.

```
Enter your choice: 2
Enter the encrypted message: HIACWDXFOYT

...

Enter your choice: 3
Enter the first key (integer between 1 and 25): 7

...

Enter your choice: 4
Enter the second key (only latin alphabet letters, at least length 7): easteregg
New alphabet: EASTRGBCDFHIJKLMNOPQVWXYZ

...

Enter your choice: 6
Decrypted Message: TRUEMANSHOW
```

codesnap.dev

Figure 4. Decryption with 2 keys.

Conclusion.

In conclusion, our laboratory work involved the implementation of the Caesar Cipher encryption and decryption algorithm. The primary goal was to create a user-friendly program that allows users to interact with the cipher through a menu-driven interface.

The menu presented the user with several options, including entering a text message, entering an encrypted message, specifying the first and second keys, encrypting a message, decrypting a message, displaying the entered data, and exiting the program. This menu-driven approach added convenience and flexibility to the cipher's usage.

Throughout the implementation of the Caesar Cipher, I understood the basics of ciphers and the fundamentals of cryptography.

Finally, this laboratory work not only provided me with a practical understanding of the Caesar Cipher but also improved my ability to create user-friendly interfaces for various applications. It highlighted the importance of balancing security and user experience in cryptography implementations.