Ministry of Education, Research and Culture
Technical University of Moldova
Software Engineering and Automation Departments

REPORT

Laboratory work No. 1

Course: Cryptography and Security

Theme: Caesar Cipher

Author: Corneliu Catlabuga
FAF-213

Checked by: univ. assist.
Cătălin Mîțu

Chisinau 2023

Objective:

Understand the Caesar Cipher and implement it in a programming language with encryption and decryption support.

Task:

1. Implement a program in which the user can choose to encrypt or decrypt a message (a-zA-Z) using a key (1-25).

2. Implement a program in which the user can choose to encrypt or decrypt a message (a-zA-Z) using a key (1-25) and a passkey (a-zA-Z) which modifies the alphabet.

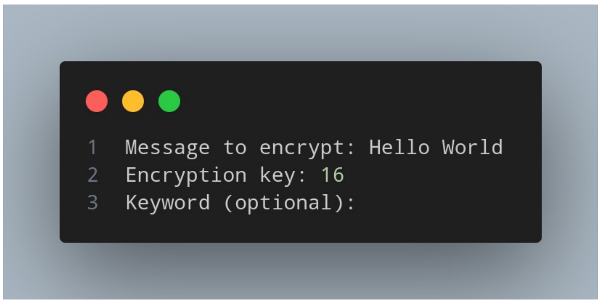
3. Compare the encryption and decription results with an other student's program.

Theoretical considerations:

In cryptography, a Caesar cipher, also known as Caesar's cipher, the shift cipher, Caesar's code, or Caesar shift, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet.

Implementation, practical results:

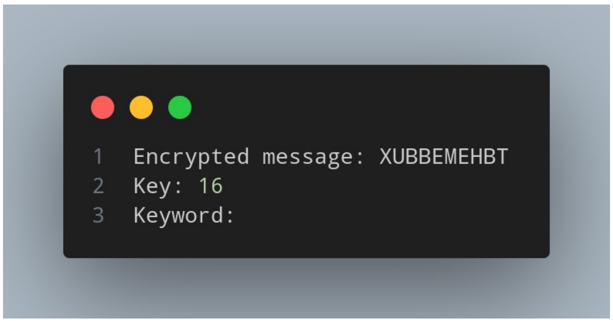
Encryption and deryption without keyword



```
Message to encrypt: Hello World
Encryption key: 16
Keyword (optional):
```

Figure 1: Input for encryption without keyword

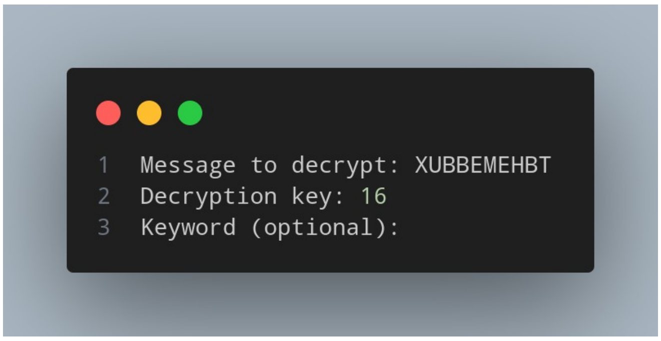
In this case the message to be encrypted is "Hello World" with the key: 16. The message has it's spaces removed, is checked for illegal characters and transforms the letters into uppercase then it gets encrypted with the specified key which gets checked it it's within the legal boundaries.



```
Encrypted message: XUBBEMEHBT
Key: 16
Keyword:
```

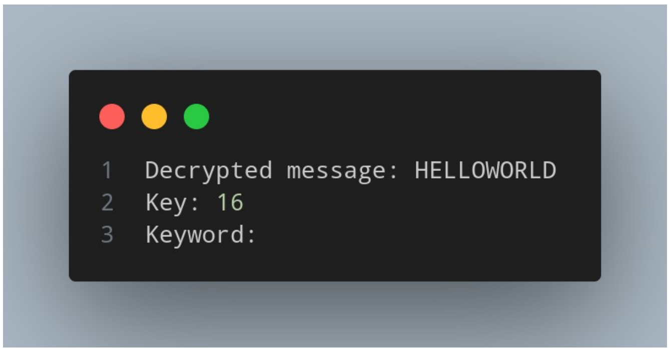
Figure 2: Output for encryption without keyword

The encrypted message for “Hello World” with key 16 is “XUBBEMEHBT”.



```
Message to decrypt: XUBBEMEHBT
Decryption key: 16
Keyword (optional):
```

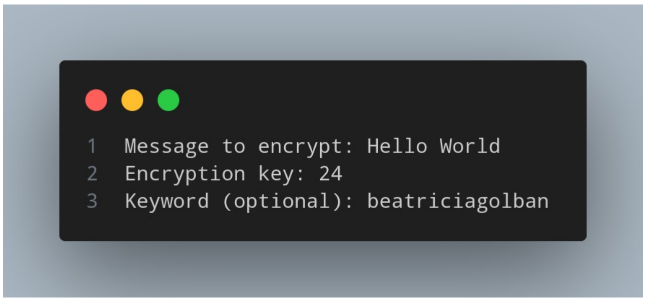
Figure 3: Input for deryption without keyword



```
Decrypted message: HELLOWORLD
Key: 16
Keyword:
```

Figure 4: Output for decryption without keyword

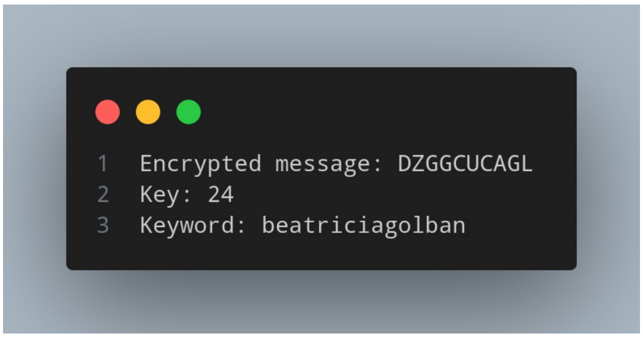
Encryption and decryption with keyword



```
Message to encrypt: Hello World
Encryption key: 24
Keyword (optional): beatriciagolban
```

Figure 5: Input for encryption with keyword

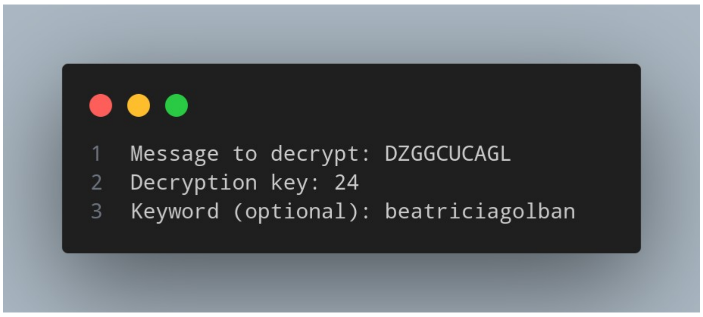
In this case the message to be encrypted is “Hello World” with the key: 24 and keyword “beatriciagolban”. The message has it’s spaces removed, is checked for illegal characters and transforms the letters into uppercase. They key is checked to be within the limits. The keyword is checked for illegal characters, gets transferred to uppercase then the new alphanbet get created with the respected keyword. After the new alphabet gets created the formated message gets encrypted with respect to the new alphabet.



```
Encrypted message: DZGGCUCAGL
Key: 24
Keyword: beatriciagolban
```

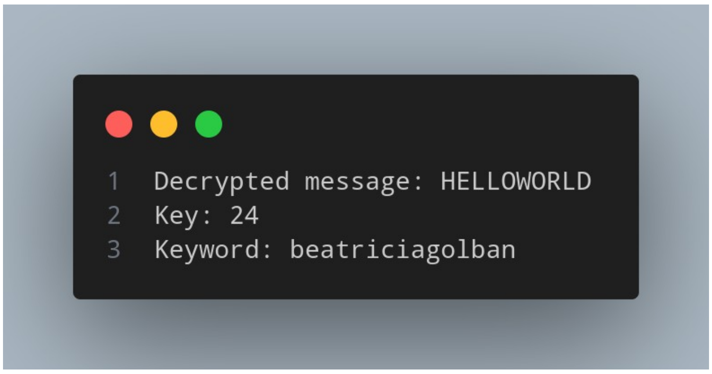
Figure 6: Output for encryption with keyword

The encrypted message for “Hello World” with the key 24 and keyword “beatricia golban” is “DZGGCUCAGL”. The respective alphabet is “BEATRICGOLNDFHJKMPQSUVWXYZ”.



```
Message to decrypt: DZGGCUCAGL
Decryption key: 24
Keyword (optional): beatriciagolban
```

Figure 7: Input for decryption with keyword



```
Decrypted message: HELLOWORLD
Key: 24
Keyword: beatriciagolban
```

Figure 8: Output for decryption with keyword

Conclusions:

Caesar cipher is a simple and historically significant encryption technique that involves shifting each letter in a message by a fixed number of positions in the alphabet. While it is easy to implement and understand, it is also highly vulnerable to modern cryptographic attacks due to its limited key space and lack of security features. As a result, the Caesar cipher is not suitable for secure communications in today's digital age but remains a valuable tool for educational purposes and historical context.

References:

1. Github repository: https://github.com/muffindud/CS_Lab/tree/lab1