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

Laboratory work 1:
Cryptography and Security

Elaborated:
st. gr. FAF-211 Echim Mihail

Verified:
asist. univ. Aureliu ZGUREANU

Chişinău - 2023

CRYPTOGRAPHY AND SECURITY

Subject:

Caesar’s Cipher

Tasks:

1. De implementat algoritmul Cezar pentru alfabetul limbii engleze în unul din
limbajele de programare. Utiliza i doar codificarea literelor cum este ar tat în tabelul 1 (nu se
ț ă permite de folosit codific rile specificate în limbajul de programare, de ex. ASCII sau ă
Unicode). Valorile cheii vor fi cuprinse între 1 i 25 inclusiv i nu se permit alte valori. ş ş
Valorile caracterelor textului sunt cuprinse între ‘A’ i ’Z’, ’a’ i ’z’ i nu sunt premise alte ş ş ş
valori. În cazul în care utilizatorul introduce alte valori - i se va sugera diapazonul corect.
Înainte de criptare textul va fi transformat în majuscule i vor fi eliminate spa iile. ş ț
Utilizatorul va putea alege opera ia - criptare sau decriptare, va putea introduce cheia, ț
mesajul sau criptograma i va ob ine respectiv criptograma sau mesajul decriptat. ş ț

2. De implementat algoritmul Cezar cu 2 chei, cu p strarea condi iilor exprimate în ă ț
Sarcina 1. În plus, cheia 2 trebuie s con in doar litere ale alfabetului latin, i s aib o ă ț ă ş ă ă
lungime nu mai mic de 7.

Caesar’s Cipher:

Caesar's Cipher, also known as the Caesar Shift or Caesar's Code, is one of the simplest and earliest encryption techniques used in cryptography. It's a substitution cipher that involves shifting the letters of the alphabet by a fixed number of positions. This fixed number is the "key" or "shift value." For example, if you use a Caesar Cipher with a shift value of 3, "A" would be replaced by "D," "B" would become "E," and so on.

A Caesar Cipher with alphabet permutation based on a keyword is a more advanced form of the classic Caesar Cipher that introduces additional security through the use of a keyword to determine the letter permutation. This variation is sometimes called a "Keyword Cipher" or "Caesar Cipher with Keyword."

1. Keyword Selection: You start by selecting a keyword. This keyword can be any word or phrase you choose. Let's use the example keyword "SECRET" for illustration.

2. Permutation Key: Next, you create a permutation key from the keyword. To do this, you first convert the keyword to lowercase (or uppercase, depending on your preference). Then, you remove any duplicate letters from the keyword. In this case, after removing duplicates, the keyword becomes "SECR." Finally, you arrange these unique letters in alphabetical order to create the permutation key, which becomes "CERS."

3. Encryption: Now, you're ready to encrypt your message. Suppose your plaintext message is "HELLO, WORLD!" Here's how you would encrypt it using the permutation key "CERS":

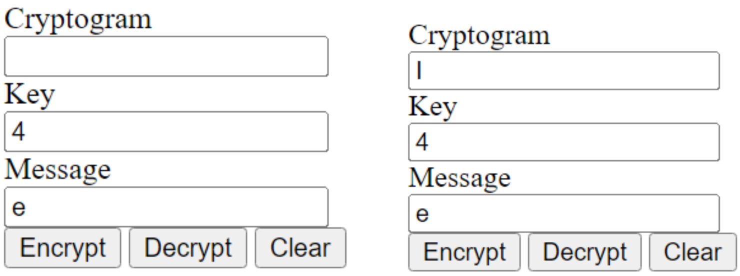
    - You iterate through each character in the plaintext.
    - For each letter in the plaintext, you find its corresponding position in the standard alphabet. For example, "H" corresponds to position 7 in the alphabet (counting from 0).
    - You then substitute the letter with the letter from the permutation key at the same position. So, in this case, "H" becomes "C" because "C" is at position 7 in the permutation key.
    - You repeat this process for each letter, always referencing the permutation key. Non-letter characters (like punctuation) remain unchanged.
4. Result: After encrypting the entire message, you get the ciphertext. In our example, "HELLO, WORLD!" would become "CERSR, VJNRY!" based on the keyword "SECRET" and the permutation key "CERS."

Results of the implementation:

I wrote the logic in javascript and made html forms to make the process simple

1.1

In order to encrypt the message, the user needs to input the message and the key and leave the cryptogram field empty, otherwise, an alert will pop up asking to leave the cryptogram field empty. Then just press the Encrypt button.

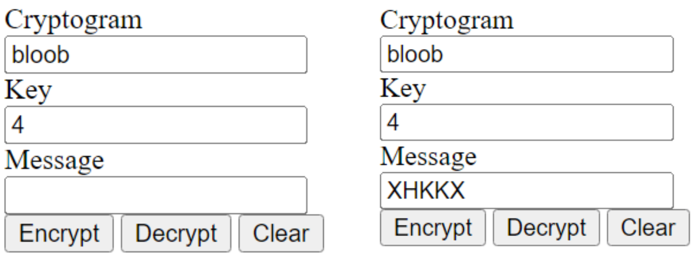

Cryptogram

Key
4
Message
e

Cryptogram
I
Key
4
Message
e

fig.1

To decrypt a message you need to do the same but the other way around and press the Decrypt button.

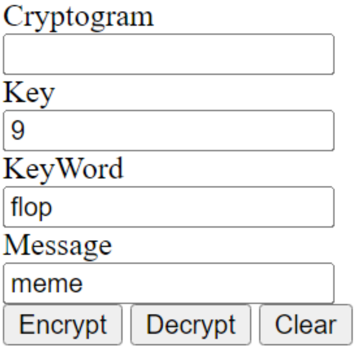

Cryptogram
bloob
Key
4
Message

Cryptogram
bloob
Key
4
Message
XHKKX

fig.2

1.2

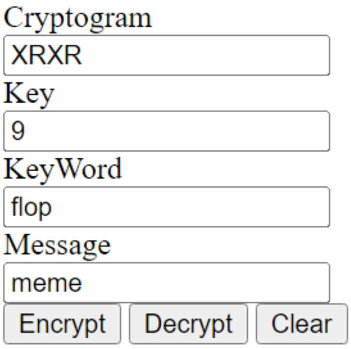
In order to encrypt with two keys, the user needs to correctly fill the message, the key and the keyword without any repeating letters. Then press the Encrypt button.


Cryptogram

Key: 9

KeyWord: flop

Message: meme


Cryptogram: XRXR

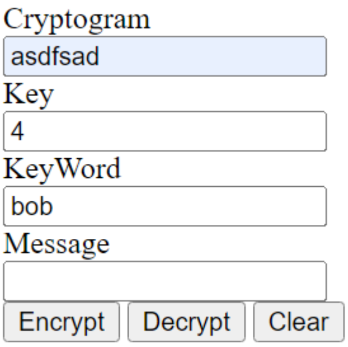
Key: 9

KeyWord: flop

Message: meme

fig.3

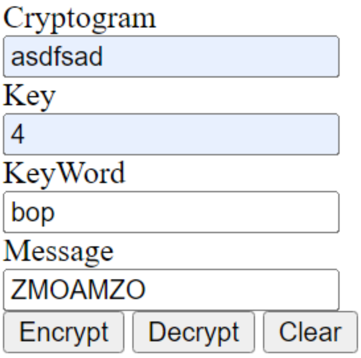
In order to decrypt, the user needs to do the same thing but the other way around.


Cryptogram: asdfsad

Key: 4

KeyWord: bob

Message


Cryptogram: asdfsad

Key: 4

KeyWord: bop

Message: ZMOAMZO

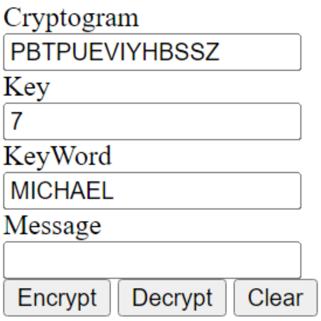
fig.4

1.3

I and a groupmate switched encrypted messages and keys and to our surprise, we gave each other the same message encrypted in different ways :)

He gave me this cryptogram:

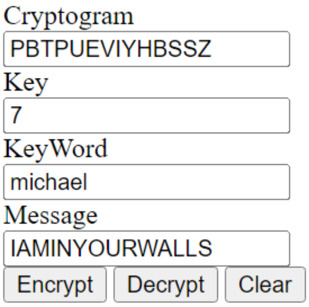
cryptogram: PBTPUEVIYHBSSZ
shift: 7
keyword: MICHAEL


Cryptogram: PBTPUEVIYHBSSZ

Key: 7

KeyWord: MICHAEL

Message


Cryptogram: PBTPUEVIYHBSSZ

Key: 7

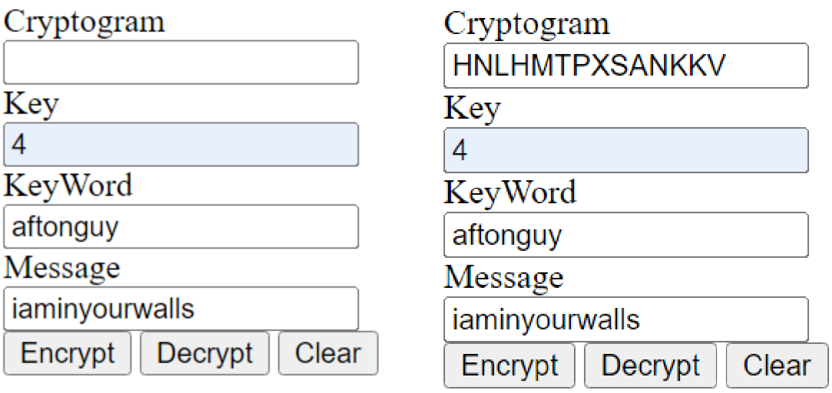
KeyWord: michael

Message: IAMINYOURWALLS

fig.5

Here is my cryptogram:

cryptogram: HNLHMTPXSANKKV
shift: 4
keyword: aftonguy



Cryptogram

Key
4

KeyWord
aftonguy

Message
iaminyourwalls

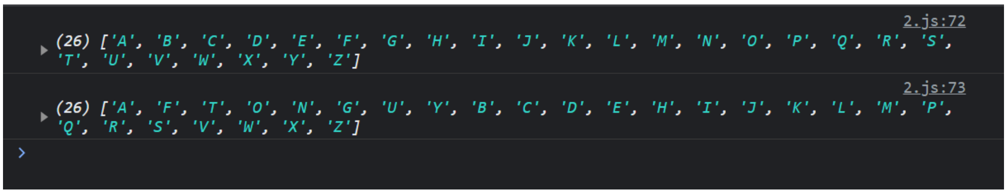
Cryptogram
HNLHMTPXSANKKV

Key
4

KeyWord
aftonguy

Message
iaminyourwalls

fig.6



```
                                                                                    2.js:72
▸ (26) ['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']
                                                                                    2.js:73
▸ (26) ['A', 'F', 'T', 'O', 'N', 'G', 'U', 'Y', 'B', 'C', 'D', 'E', 'H', 'I', 'J', 'K', 'L', 'M', 'P',
  'Q', 'R', 'S', 'V', 'W', 'X', 'Z']
>
```

fig.7

Conclusion:

In conclusion, this lab work provided valuable insights into classical encryption techniques, specifically the Caesar Cipher and the Caesar Cipher with Keywords.

I began by implementing the traditional Caesar Cipher, which involved shifting characters by a fixed value. This simple encryption method helped me understand the fundamentals of substitution ciphers and their limitations in terms of security.

Subsequently, I explored an enhanced version of the Caesar Cipher with Keywords. By introducing a keyword-based permutation key, I added an additional layer of complexity to the encryption process. This improved the security of the cipher, making it more resistant to decryption without knowledge of the keyword.

Through these exercises, I gained hands-on experience in both encryption techniques and appreciated the importance of selecting strong keywords to enhance the security of classical ciphers. While these methods are educational and historically significant, it's crucial to acknowledge their vulnerability to modern cryptographic attacks, and they should not be relied upon for securing sensitive information in practical applications.