Ministerul Educației, Culturii și Cercetării al Republicii Moldova
Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică și Microelectronică
Departamentul Ingineria Software și Automatică

Raport

pentru lucrare de laborator Nr. 1
la cursul "*Metode criptografice de protectie a informației*"

A efectuat: Arteom KALAMAGHIN, FAF-211
A verificat: Aureliu ZGUREANU

Chișinău - 2023

Subject: Caesar Cipher

Tasks:

1. *De implementat algoritmul Cezar pentru alfabetul limbii engleze în unul din limbajele de programare ...*
2. *De implementat algoritmul Cezar cu 2 chei, cu păstrarea condițiilor exprimate ...*
3. *Pentru această sarcină studenții se vor diviza în perechi. Fiecare dintre ei va cripta câte un mesaj alcătuit din 7-10 simboluri (fără spații și scris doar cu majuscule) cu versiunea cifrului Caesar permutare, alegând fiecare cheile sale. Criptogramele astfel obținute vor fi transmise colegului, împreună cu cheile respective.Fiecare dintre cei doi va realiza criptarea și se va face compararea cu versiunea originală a colegului.*

Results:

Case 1 (T1) - One-key encryption:

```
What operation do you want to perform? 1. Enc / 2. Dec - 1
What is the key1 value? - 2
What is the key2 value? -
What is the message/cryptogram? ('A' -> 'Z', 'a' -> 'z') : ab cd e f
---------------------------------
CDEFGH
```

Case 2 (T1) - One-key decryption:

```
What operation do you want to perform? 1. Enc / 2. Dec - 2
What is the key1 value? - 2
What is the key2 value? -
What is the message/cryptogram? ('A' -> 'Z', 'a' -> 'z') : cdefgh
---------------------------------
ABCDEF
```

Case 3 (T2) - Two-key encryption:

```
What operation do you want to perform? 1. Enc / 2. Dec - 1
What is the key1 value? - 7
What is the key2 value? - michael
What is the message/cryptogram? ('A' -> 'Z', 'a' -> 'z') : i am in your
walls
---------------------------------
DJBDUEVIYHJNNZ
```

Case 4 (T2) - Two-key decryption:

```
What operation do you want to perform? 1. Enc / 2. Dec - 2
What is the key1 value? - 7
What is the key2 value? - michael
What is the message/cryptogram? ('A' -> 'Z', 'a' -> 'z') :
djbdueviyhjnnz
---------------------------------
IAMINYOURWALLS
```

Case 5 (T1) - Unknown character:

```
What operation do you want to perform? 1. Enc / 2. Dec - 1
What is the key1 value? - 1
What is the key2 value? -
What is the message/cryptogram? ('A' -> 'Z', 'a' -> 'z') : ma$ter
=================================
ERROR: Unknown character detected!
=================================
```

Task 3 (encryption by Mike ECHIM | FAF-211):

```
Cryptogram | MNSMBEYDXFNRRZ
Key 1      | 4
key 2      | aftonguy
```

Extended alphabet																									
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
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5

Decryption													
M	N	S	M	B	E	Y	D	X	F	N	R	R	Z
17	4	21	17	8	11	7	10	24	1	4	20	20	25
I	**A**	**M**	**I**	**N**	**Y**	**O**	**U**	**R**	**W**	**A**	**L**	**L**	**S**
13	0	17	13	4	7	3	6	21	23	0	16	16	21

Conclusion:

In conclusion, the implementation of both the one-key and two-key Caesar ciphers in this lab work has provided us with valuable insights into the world of cryptography and encryption techniques. Through this hands-on experience, we have gained a deeper understanding of the principles behind these classic encryption methods and their strengths and weaknesses. The one-key Caesar cipher, while simple to implement, serves as a basic introduction to the concept of encryption, while the two-key variant offers a more robust level of security by adding an additional layer of complexity. This lab work has underscored the importance of encryption in safeguarding sensitive information and has encouraged us to explore more advanced encryption techniques in our ongoing study of cybersecurity and information protection.

* You may see the code developed in the course of this laboratory work by accessing:
https://github.com/Starlight-Crusader/CS-Lab