**Sprawozdanie**

*Bezpieczeństwo Sieci Komputerowych*

Pracownia Specjalistyczna 2-3



Temat: **Implementacja podstawowych modułów kryptograficznych**

Wykonanie:

**Busłowski Tomasz**

**Suchwałko Tomasz**

Prowadzący zajęcia: **dr inż. Maciej Brzozowski**

**Zadania do wykonania:**

1. Zaimplementuj algorytm kodujący i dekodujący z wykorzystaniem szyfru prostego przestawiania „rail fence” dla k = n. Skorzystaj z przykładu 1 (1 punkt).
2. Zaimplementuj kryptosystem przedstawieniowy bazujący na przykładzie 2a dla d = 5 oraz klucza key = 3-4-1-5-2 (1 punkt).
3. Zaimplementuj kryptosystem przedstawieniowy bazujący na przykładzie 2b (1 punkt) oraz 2c (2 punkty) dla dowolnego klucza.
4. Zaimplementuj szyfr cezara bazujący na przykładzie 3b (1 punkt).
5. Zaimplementuj kryptosystem bazujący na tablicy Vigenere’a (1 punkt).

**Środowisko, framework i język implementacji zadań:**

* Microsoft Visual Studio Enterprise 2015 (Version 14.0.25431.01 Update 3).
* Microsoft .NET Framework (Version 4.6.01586).
* C# 6.0.

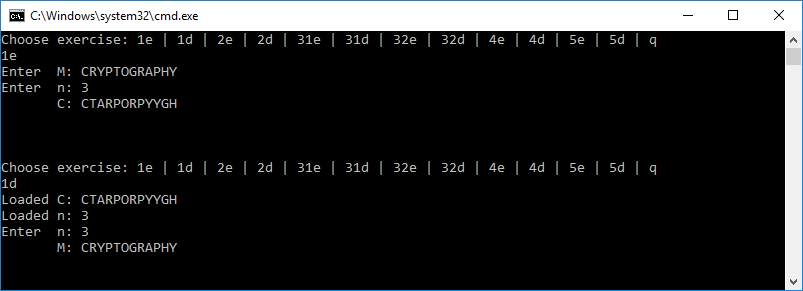
**Wykonanie zadań:**

Wszystkie zadania zostały wykonane.

* Tomasz Busłowski - zadanie 1, 2.
* Tomasz Suchwałko – zadanie 3, 4, 5.

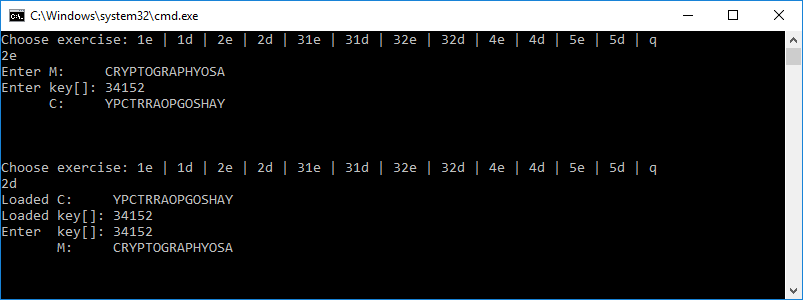
**Screeny wykonanych zadań:**

1. Algorytm “rail fence”:



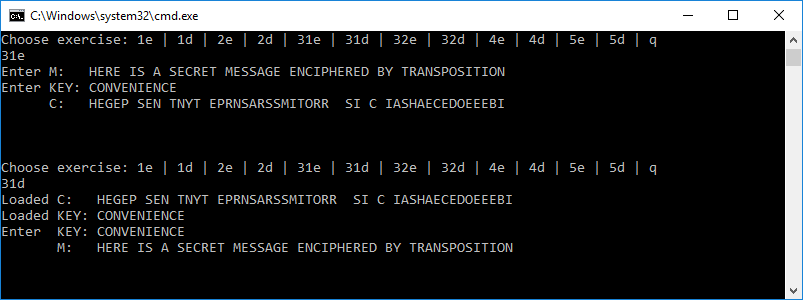
Rysunek 1 – kodowanie i dekodowanie MESSAGE = CRYPTOGRAPHY, KEY = 3

1. Kryptosystem przedstawieniowy bazujący na przykładzie 2a:



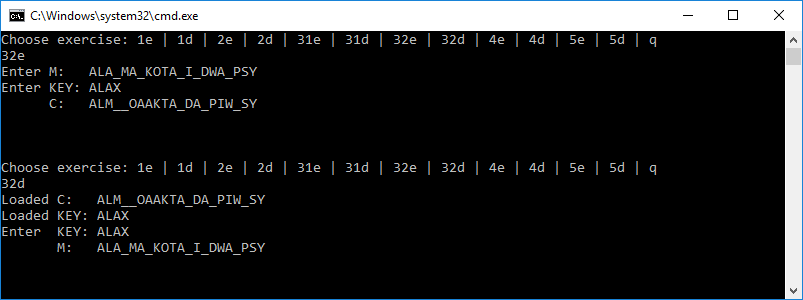
Rysunek 2 - kodowwanie i dekodowanie kryptosystemem przestawieniowym, M = CRYPTOGRAPHYOSA, K = 3-4-1-5-2

1. Kryptosystem przedstawieniowy bazujący na przykładzie 2b:



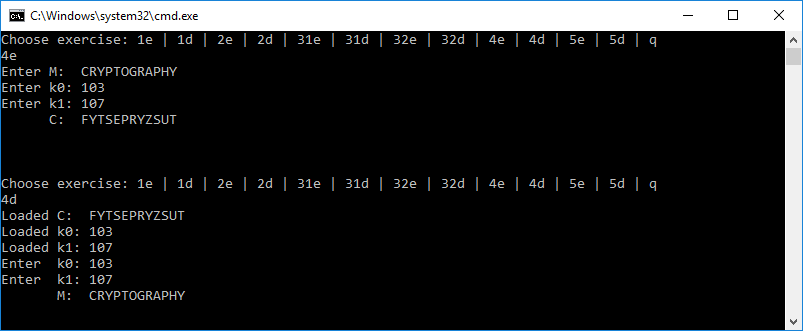
Rysunek 3 - kodowwanie i dekodowanie kryptosystemem przestawieniowym  
M = HERE IS A SECRET MESSAGE ENCIPHERED BY TRANSPOSITION, K = CONVENIENCE

Kryptosystem przestawieniowy dla dowolnego klucza:



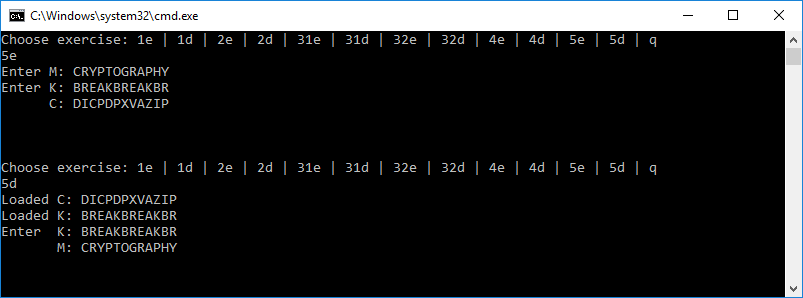
Rysunek 4 - kryptosystem przestawieniowy dla M = ALA\_MA\_KOTA\_I\_DWA\_PSY, KEY = ALAX

1. Szyfr cezara:



Rysunek 5 - kodowanie i dekodowanie szyfrem cezara dla M = CRYPTOGRAPHY, k0 = 103, k1 = 107

1. Kryptosystem bazujący na tablicy Vigenere’a:



Rysunek 6 - kodowanie i dekodowanie kryptosystemem Vigenere'a dla M = CRYPTOGRAPHY, K = BREAKBREAKBR