

Sprawozdanie

Bezpieczeństwo Sieci Komputerowych

Pracownia Specjalistyczna 2-3



**Temat: Implementacja podstawowych
modułów kryptograficznych**

Wykonanie:

Busłowski Tomasz

Suchwałko Tomasz

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

BSK, semestr VI, 08-03-2017, Wydział Informatyki, Politechnika Białostocka

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 $\text{key} = 3-4-1-5-2$ (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.

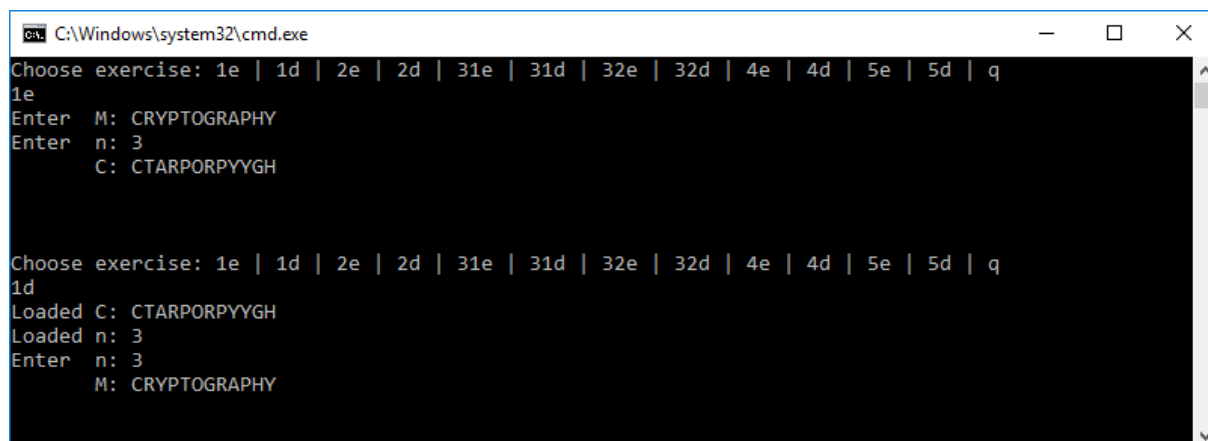
Wykonanie zadań:

Wszystkie zadania zostały wykonane.

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

Screeny wykonanych zadań:

1. Algorytm “rail fence”:

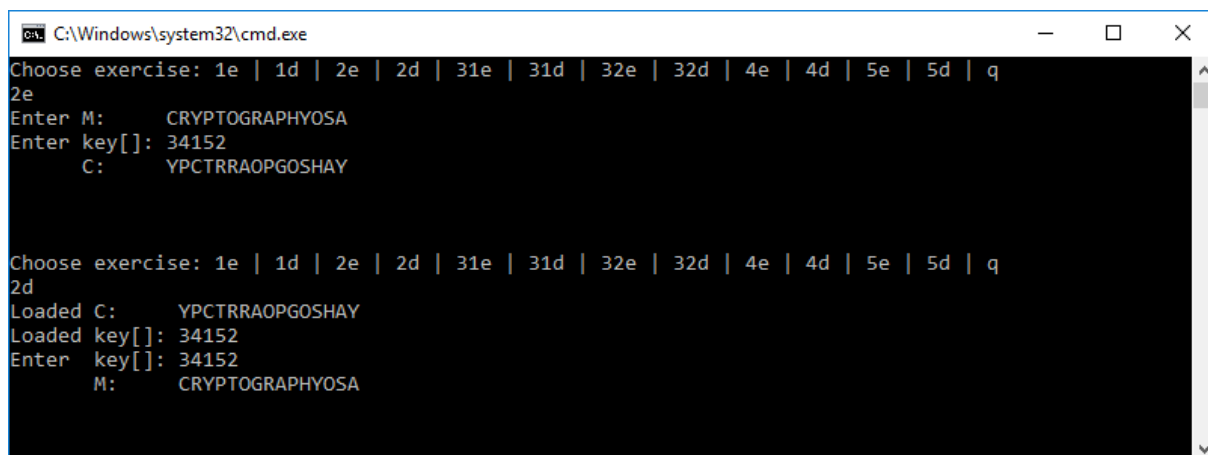


```
C:\Windows\system32\cmd.exe
Choose exercise: 1e | 1d | 2e | 2d | 31e | 31d | 32e | 32d | 4e | 4d | 5e | 5d | q
1e
Enter M: CRYPTOGRAPHY
Enter n: 3
C: CTARPORPYYGH

Choose exercise: 1e | 1d | 2e | 2d | 31e | 31d | 32e | 32d | 4e | 4d | 5e | 5d | q
1d
Loaded C: CTARPORPYYGH
Loaded n: 3
Enter n: 3
M: CRYPTOGRAPHY
```

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

2. Kryptosystem przedstawieniowy bazujący na przykładzie 2a:

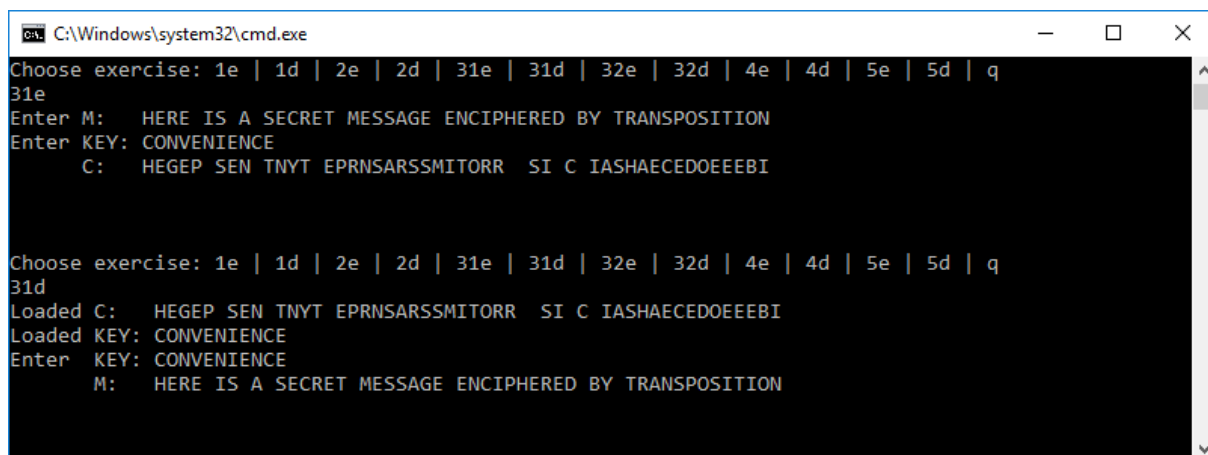


```
C:\Windows\system32\cmd.exe
Choose exercise: 1e | 1d | 2e | 2d | 31e | 31d | 32e | 32d | 4e | 4d | 5e | 5d | q
2e
Enter M:      CRYPTOGRAPHYOSA
Enter key[]:  34152
C:      YPCTRR AOPGOSHAY

Choose exercise: 1e | 1d | 2e | 2d | 31e | 31d | 32e | 32d | 4e | 4d | 5e | 5d | q
2d
Loaded C:      YPCTRR AOPGOSHAY
Loaded key[]:  34152
Enter key[]:  34152
M:      CRYPTOGRAPHYOSA
```

Rysunek 2 - kodowanie i dekodowanie kryptosystemem przestawieniowym, $M = \text{CRYPTOGRAPHYOSA}$, $K = 3\text{-}4\text{-}1\text{-}5\text{-}2$

3. Kryptosystem przedstawieniowy bazujący na przykładzie 2b:

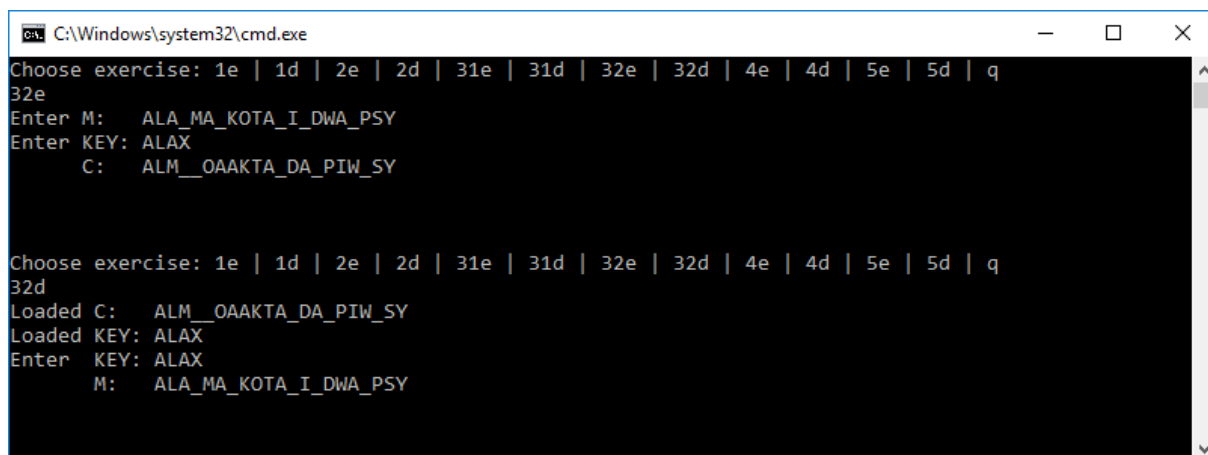


```
C:\Windows\system32\cmd.exe
Choose exercise: 1e | 1d | 2e | 2d | 31e | 31d | 32e | 32d | 4e | 4d | 5e | 5d | q
31e
Enter M:      HERE IS A SECRET MESSAGE ENCIPHERED BY TRANSPOSITION
Enter KEY:    CONVENIENCE
C:      HEGEP SEN TNYT EPRNSARSSMITORR SI C IASHAECEDOE EEBI

Choose exercise: 1e | 1d | 2e | 2d | 31e | 31d | 32e | 32d | 4e | 4d | 5e | 5d | q
31d
Loaded C:      HEGEP SEN TNYT EPRNSARSSMITORR SI C IASHAECEDOE EEBI
Loaded KEY:    CONVENIENCE
Enter KEY:    CONVENIENCE
M:      HERE IS A SECRET MESSAGE ENCIPHERED BY TRANSPOSITION
```

Rysunek 3 - kodowanie i dekodowanie kryptosystemem przestawieniowym
 $M = \text{HERE IS A SECRET MESSAGE ENCIPHERED BY TRANSPOSITION}$, $K = \text{CONVENIENCE}$

Kryptosystem przestawieniowy dla dowolnego klucza:

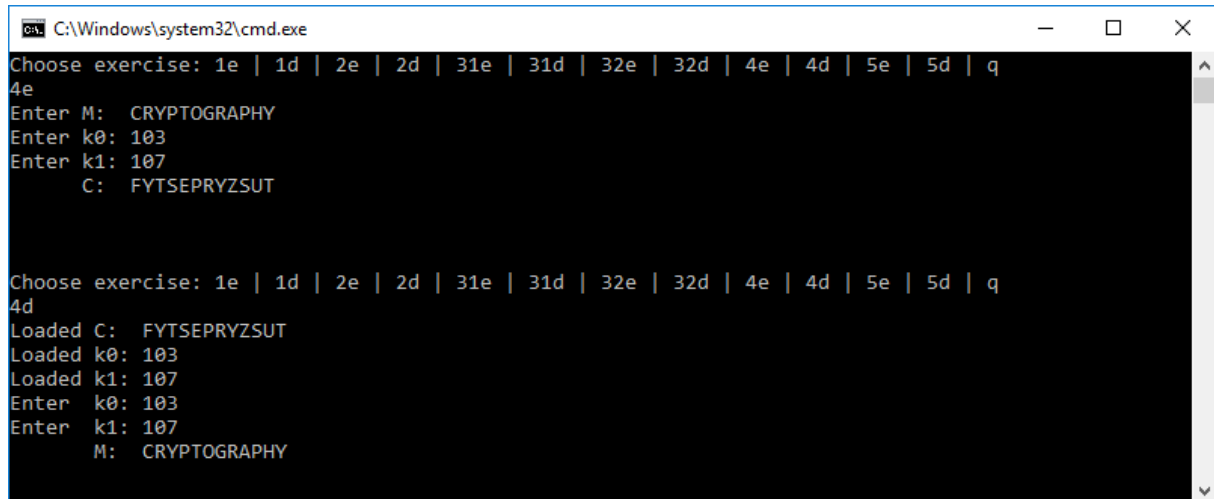


```
C:\Windows\system32\cmd.exe
Choose exercise: 1e | 1d | 2e | 2d | 31e | 31d | 32e | 32d | 4e | 4d | 5e | 5d | q
32e
Enter M:      ALA_MA_KOTA_I_DWA_PSY
Enter KEY:    ALAX
C:      ALM__OAAKTA_DA_PIW_SY

Choose exercise: 1e | 1d | 2e | 2d | 31e | 31d | 32e | 32d | 4e | 4d | 5e | 5d | q
32d
Loaded C:      ALM__OAAKTA_DA_PIW_SY
Loaded KEY:    ALAX
Enter KEY:    ALAX
M:      ALA_MA_KOTA_I_DWA_PSY
```

Rysunek 4 - kryptosystem przestawieniowy dla $M = \text{ALA_MA_KOTA_I_DWA_PSY}$, $\text{KEY} = \text{ALAX}$

4. Szyfr cezara:

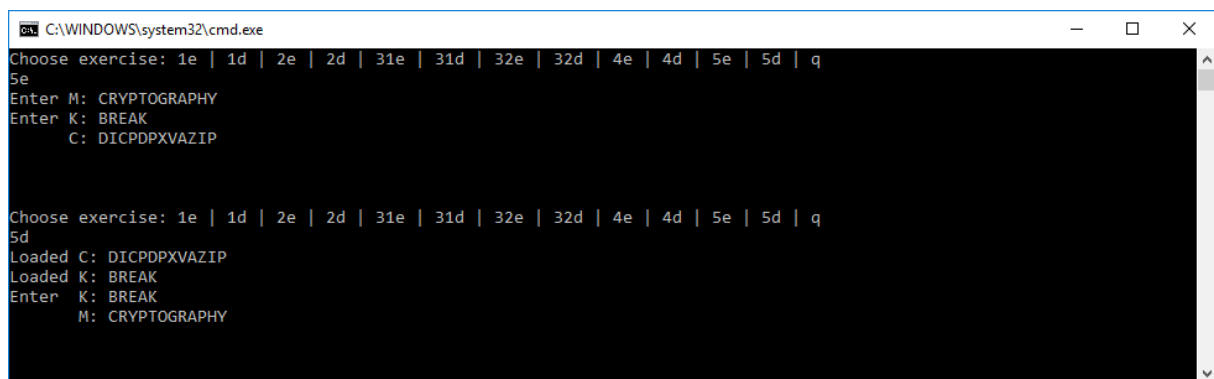


```
C:\Windows\system32\cmd.exe
Choose exercise: 1e | 1d | 2e | 2d | 31e | 31d | 32e | 32d | 4e | 4d | 5e | 5d | q
4e
Enter M: CRYPTOGRAPHY
Enter k0: 103
Enter k1: 107
C: FYTSEPRYSUT

Choose exercise: 1e | 1d | 2e | 2d | 31e | 31d | 32e | 32d | 4e | 4d | 5e | 5d | q
4d
Loaded C: FYTSEPRYSUT
Loaded k0: 103
Loaded k1: 107
Enter k0: 103
Enter k1: 107
M: CRYPTOGRAPHY
```

Rysunek 5 - kodowanie i dekodowanie szyfrem cezara dla $M = \text{CRYPTOGRAPHY}$, $k_0 = 103$, $k_1 = 107$

5. Kryptosystem bazujący na tablicy Vigenere'a:



```
C:\WINDOWS\system32\cmd.exe
Choose exercise: 1e | 1d | 2e | 2d | 31e | 31d | 32e | 32d | 4e | 4d | 5e | 5d | q
5e
Enter M: CRYPTOGRAPHY
Enter K: BREAK
C: DICDPXVAZIP

Choose exercise: 1e | 1d | 2e | 2d | 31e | 31d | 32e | 32d | 4e | 4d | 5e | 5d | q
5d
Loaded C: DICDPXVAZIP
Loaded K: BREAK
Enter K: BREAK
M: CRYPTOGRAPHY
```

Rysunek 6 - kodowanie i dekodowanie kryptosystemem Vigenere'a dla $M = \text{CRYPTOGRAPHY}$, $K = \text{BREAK}$