

# Sprawozdanie

*Bezpieczeństwo Sieci Komputerowych*

Pracownia Specjalistyczna 6-7



Temat:

## **KRYPTOSYSTEMY SYMETRYCZNE – ALGORYTM DES.**

Wykonanie:

**Busłowski Tomasz**

**Suchwałko Tomasz**

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

BSK, semestr VI, 04-04-2017, Wydział Informatyki, Politechnika Białostocka

## Zadanie do wykonania

Wykonaj program realizujący szyfrowanie oraz deszyfrowanie z wykorzystaniem algorytmu DES. Więcej informacji w dokumencie źródłowym fips46-3.

## 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.

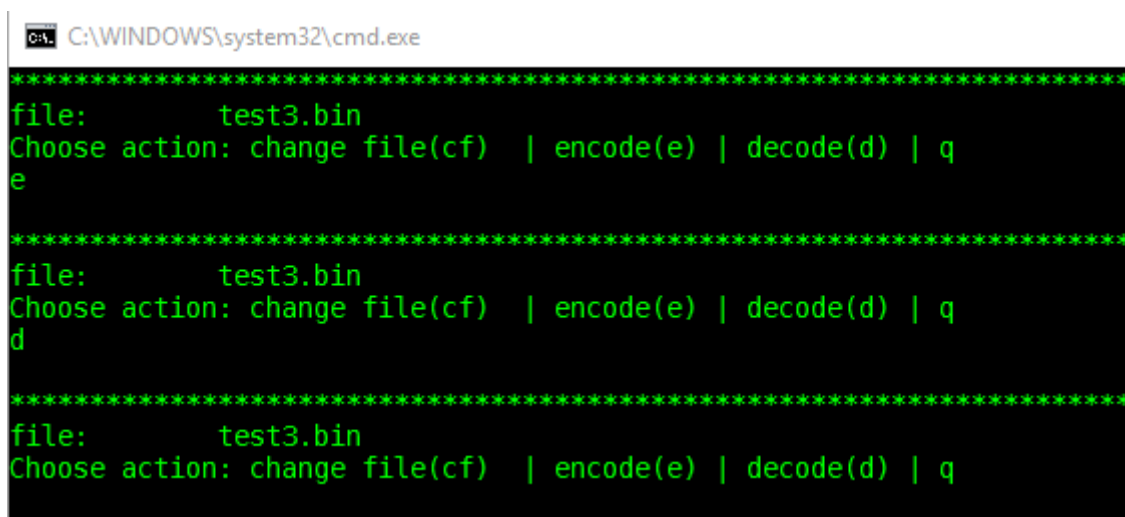
## Wykonanie zadań:

Wszystkie zadania zostały wykonane.

- Tomasz Busłowski – szyfrowanie & deszyfrowanie
- Tomasz Suchwałko – szyfrowanie & deszyfrowanie

## Screeny wykonanych zadań:

Przykład szyfrowanie i deszyfrowania wiadomości naszym programem przy wykorzystaniu algorytmu DES:



```
C:\WINDOWS\system32\cmd.exe
*****
file:      test3.bin
Choose action: change file(cf) | encode(e) | decode(d) | q
e
*****
file:      test3.bin
Choose action: change file(cf) | encode(e) | decode(d) | q
d
*****
file:      test3.bin
Choose action: change file(cf) | encode(e) | decode(d) | q
```

Rysunek 1(konsola, szyfrowanie i deszyfrowanie pliku test3.bin)

Rysunek 2(plik key.txt)

Data View	
test3.bin :Zone.Identifier:\$DATA	
Add...	Binary
000000	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000016	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000032	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000048	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000064	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000080	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000096	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000112	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000128	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000144	00000000 00000000 00000000 00000000 00000000 00000000 00111111 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

Rysunek 3(test3.bin, przed zaszyfrowaniem)

Data View	
test3OUT.bin :Zone.Identifier:\$DATA	
Add...	Binary
000000	10000011 10100001 11101000 00010100 10001000 10010010 01010011 11100000 10000011 10100001 11101000 00010100 10001000 10010010 01010011 11100000
000016	10000011 10100001 11101000 00010100 10001000 10010010 01010011 11100000 10000011 10100001 11101000 00010100 10001000 10010010 01010011 11100000
000032	10000011 10100001 11101000 00010100 10001000 10010010 01010011 11100000 10000011 10100001 11101000 00010100 10001000 10010010 01010011 11100000
000048	10000011 10100001 11101000 00010100 10001000 10010010 01010011 11100000 10000011 10100001 11101000 00010100 10001000 10010010 01010011 11100000
000064	10000011 10100001 11101000 00010100 10001000 10010010 01010011 11100000 10000011 10100001 11101000 00010100 10001000 10010010 01010011 11100000
000080	10000011 10100001 11101000 00010100 10001000 10010010 01010011 11100000 10000011 10100001 11101000 00010100 10001000 10010010 01010011 11100000
000096	10000011 10100001 11101000 00010100 10001000 10010010 01010011 11100000 10000011 10100001 11101000 00010100 10001000 10010010 01010011 11100000
000112	10000011 10100001 11101000 00010100 10001000 10010010 01010011 11100000 10000011 10100001 11101000 00010100 10001000 10010010 01010011 11100000
000128	10000011 10100001 11101000 00010100 10001000 10010010 01010011 11100000 10000011 10100001 11101000 00010100 10001000 10010010 01010011 11100000
000144	11001000 11000001 11011101 11110100 01110101 11110101 00101011 00001000 10000011 10100001 11101000 00010100 10001000 10010010 01010011 11100000

Rysunek 4(test3OUT.bin, zaszyfrowany plik test3.bin)

Data View	
test3OUT.bin :Zone.Identifier:\$DATA	
Add...	Binary
000000	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000016	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000032	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000048	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000064	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000080	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000096	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000112	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000128	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000144	00000000 00000000 00000000 00000000 00000000 00000000 00111111 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

Rysunek 5 (test3OUT.bin, po rozszyfrowaniu)

Algorytm DES do poprawnego działania potrzebuje plików o wielokrotności 64 bitów(8bajtów). Pliki mają różne rozmiary, nie mamy gwarancji odpowiedniej wielkości pliku. Problem ten rozwiązaliśmy stosując padding pliku, który chcemy zaszyfrować. Działa on w taki sposób: jeżeli plik nie jest wielokrotnością 8 bajtów, to dopisujemy dodatkowe bajty o randomowych wartościach tak aby otrzymać wielokrotność 8 bajtów a w ostatnim bajcie zapisujemy informacje ile bajtów dodaliśmy(ile mamy zignorować przy deszyfracji). Jeśli natomiast plik jest wielokrotnością 8 bajtów, to dodajemy 7 randomowych bajtów i w 8 zapisujemy wartość 8.