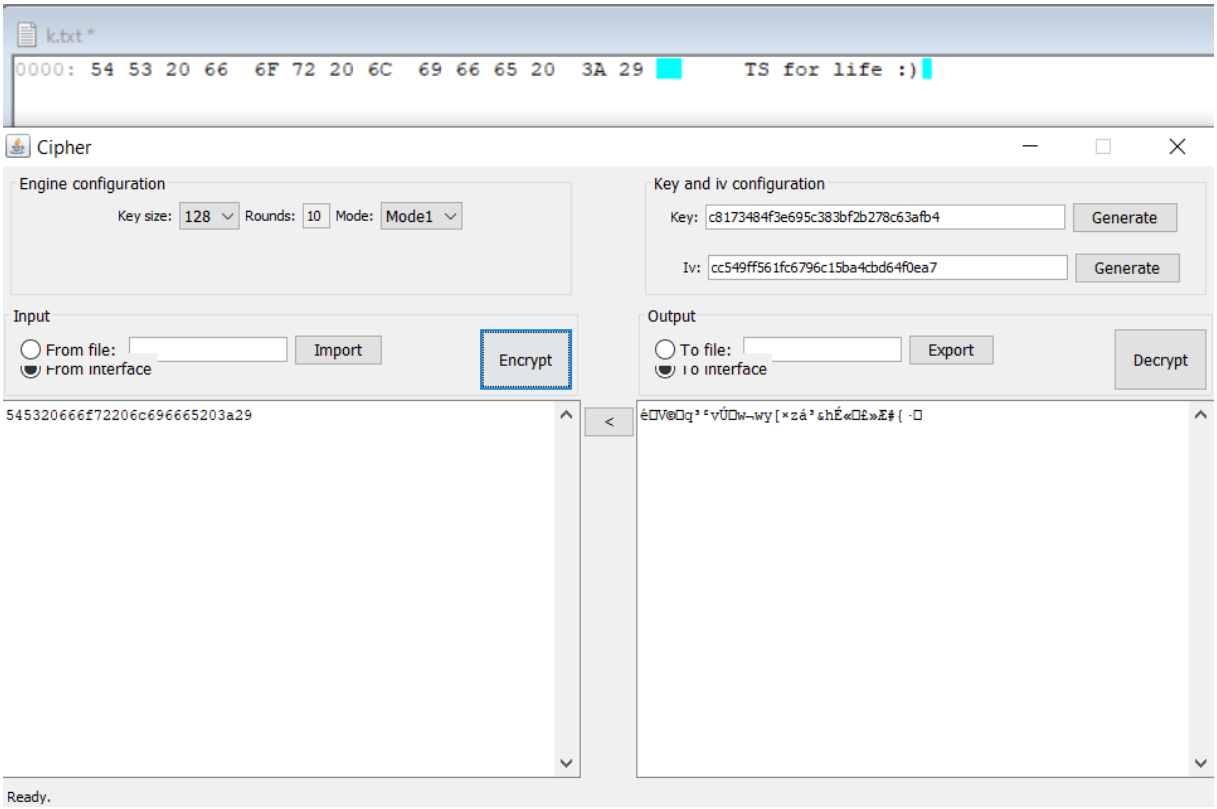
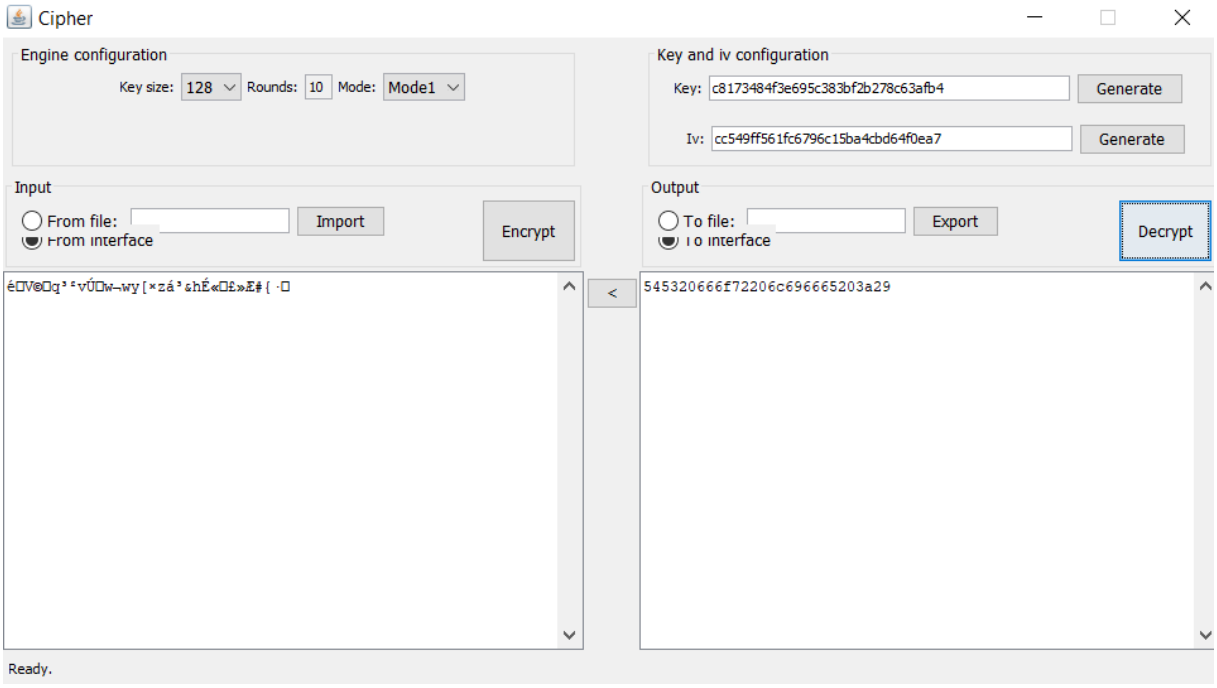
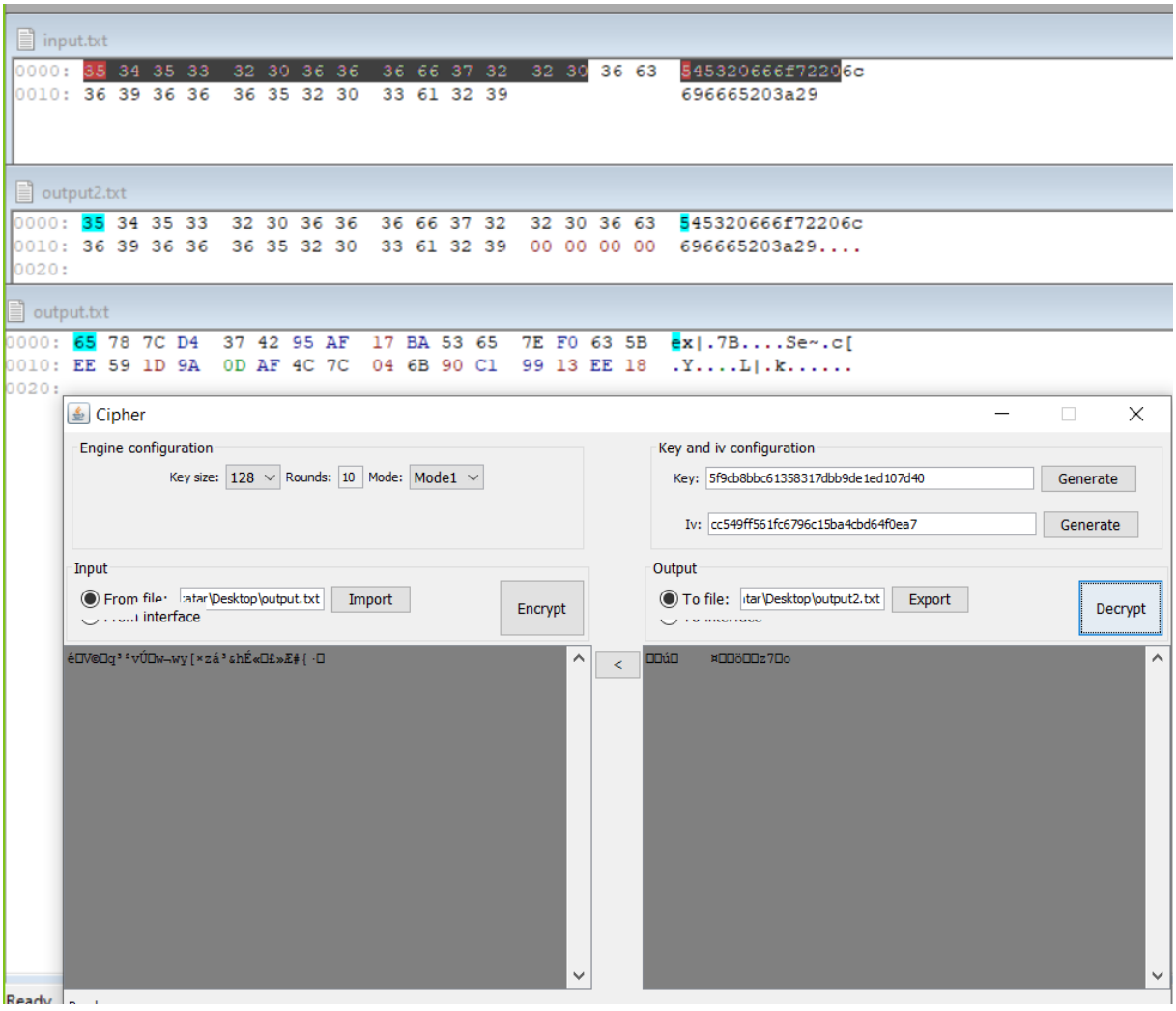
Bezpieczeństwo systemów i sieci teleinformatycznych – sprawozdanie z laboratorium 2

Autor: Katarzyna Pencak

2. Na pierwszych dwóch screenach działanie szyfrowania i deszyfrowania tekstu przez interfejs. Na trzecim to samo, tylko za pomocą pliku. Treść plików zamieniona na heksadecymalne przy użyciu HexEditor.

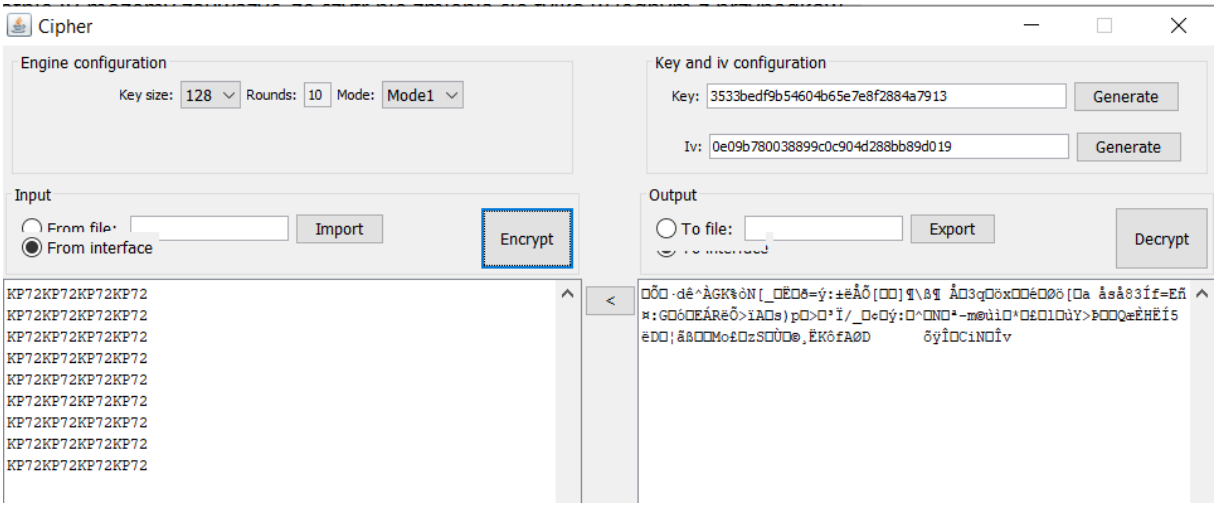


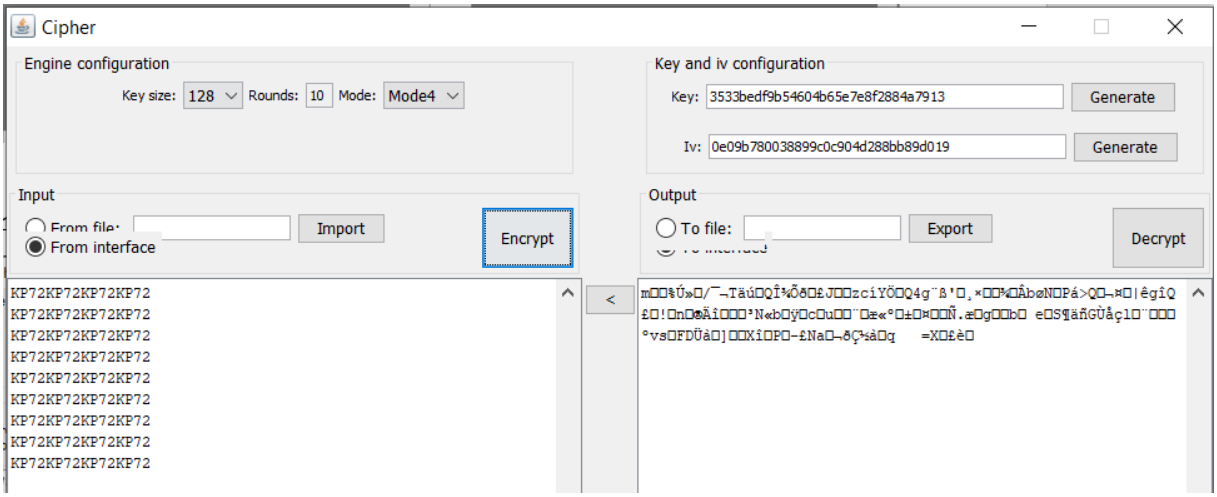

Cipher
Engine configuration
Key size: 128 Rounds: 10 Mode: Mode1
Key and iv configuration
Key: c8173484f3e695c383bf2b278c63afb4
Generate
Iv: cc549ff561fc6796c15ba4cbd64f0ea7
Generate
Input
From file:
Import
Encrypt
Output
To file:
Export
Decrypt
545320666f72206c696665203a29
Ready.

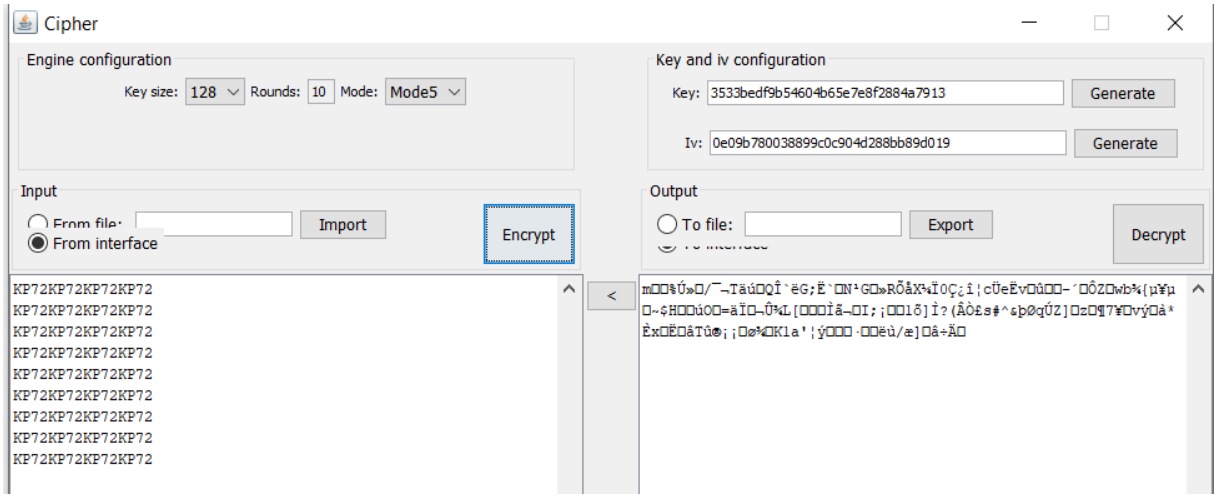

input.txt
0000: 35 34 35 33 32 30 36 36 36 66 37 32 32 30 36 63 545320666f72206c
0010: 36 39 36 36 36 35 32 30 33 61 32 39 696665203a29
output2.txt
0000: 35 34 35 33 32 30 36 36 36 66 37 32 32 30 36 63 545320666f72206c
0010: 36 39 36 36 36 35 32 30 33 61 32 39 00 00 00 00 696665203a29....
0020:
output.txt
0000: 65 78 7C D4 37 42 95 AF 17 BA 53 65 7E F0 63 5B ex|.7B....Se~.c[
0010: EE 59 1D 9A 0D AF 4C 7C 04 6B 90 C1 99 13 EE 18 .Y....L|.k......
0020:
Cipher
Engine configuration
Key size: 128 Rounds: 10 Mode: Mode1
Key and iv configuration
Key: 5f9cb8bbc61358317dbb9de1ed107d40
Generate
Iv: cc549ff561fc6796c15ba4cbd64f0ea7
Generate
Input
Import
Encrypt
Output
To file:
Export
Decrypt

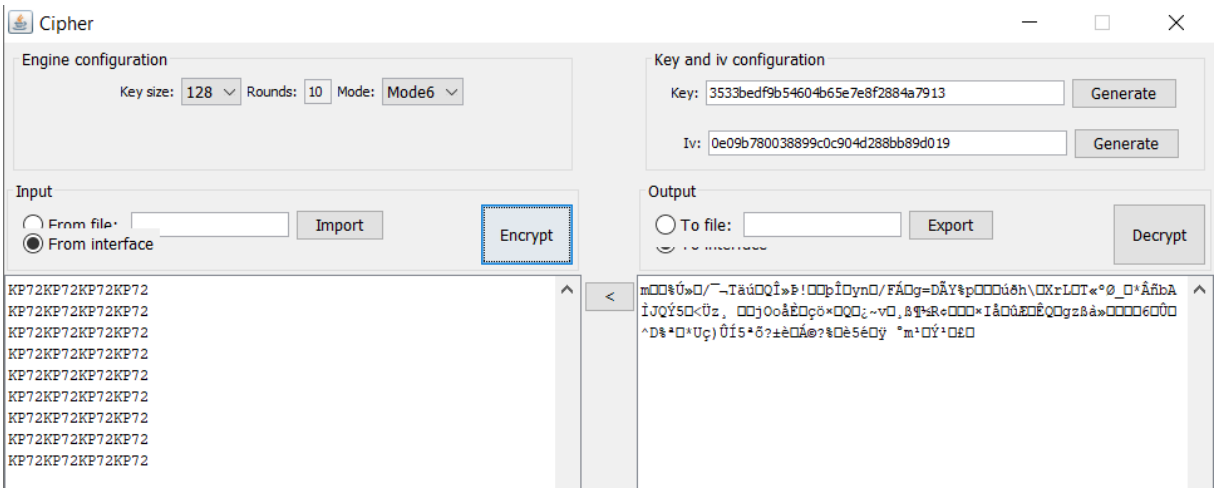
3. Kolejność odgadywania trybów (3, 2, 1, 5, 4, 6)

Tryb 1 – CBC, dla pierwszego bloku danych jest inny szyfr niż dla pozostałych opcji (tj. 4, 5 i 6)

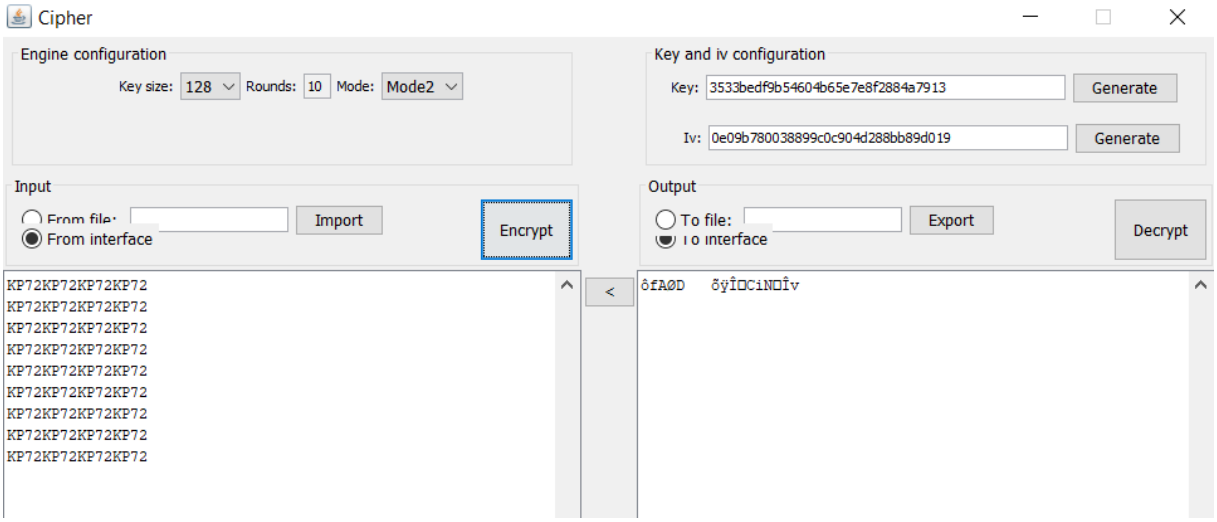




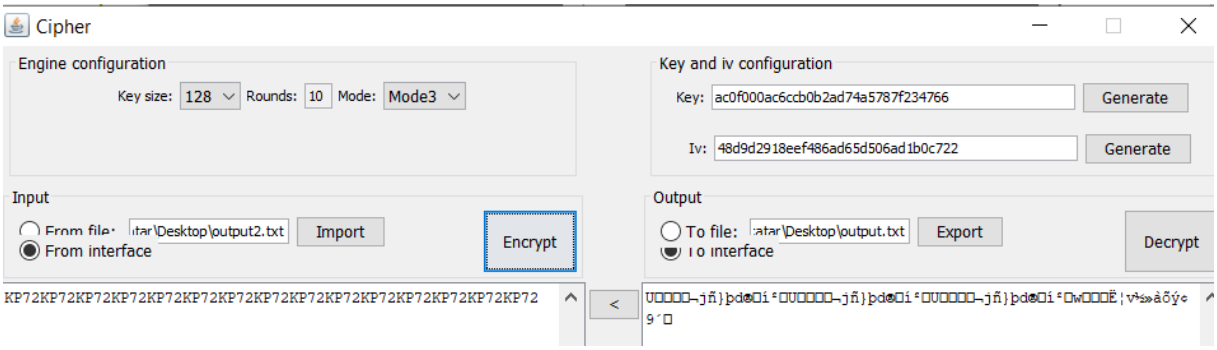


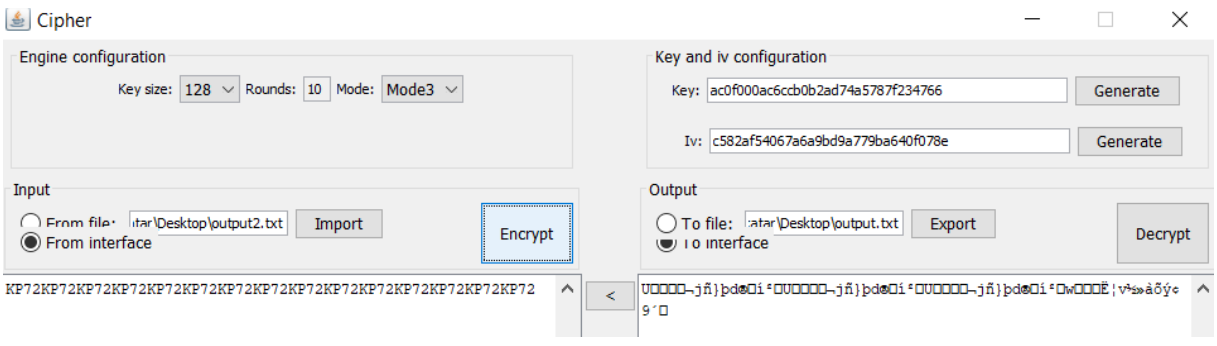


Tryb 2 – CBC – MAC, powstaje najkrótszy szyfr ze wszystkich opcji (hash)

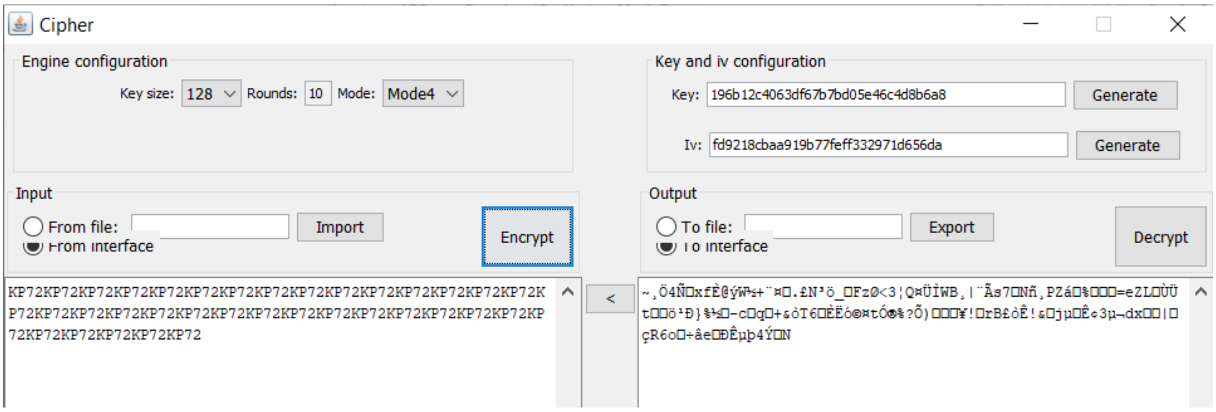


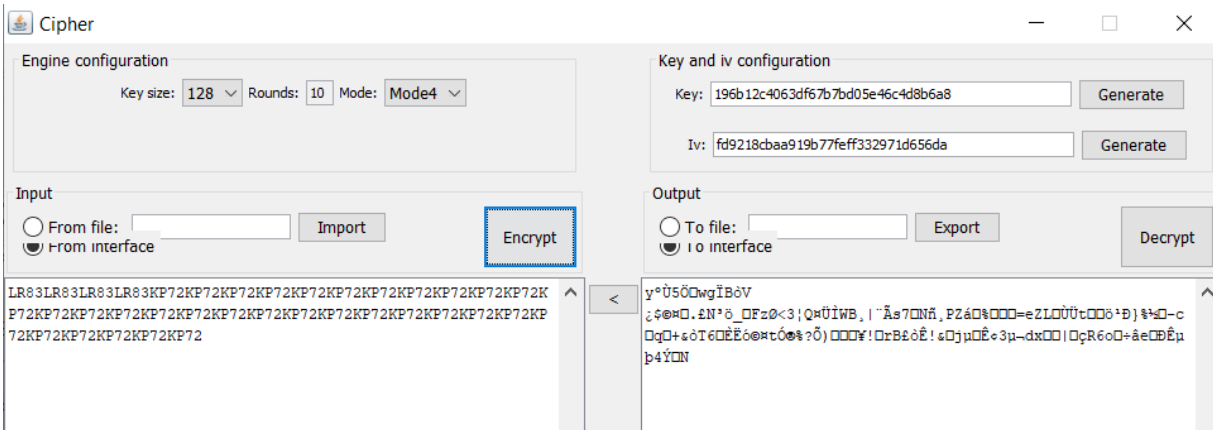
Tryb 3 – ECB, gdyż nie zmienia się wynik w zależności generowanego IV



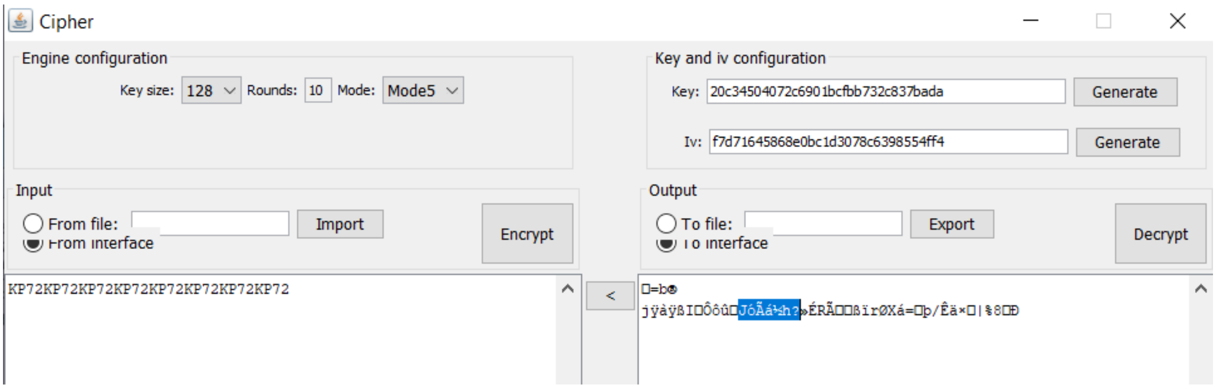


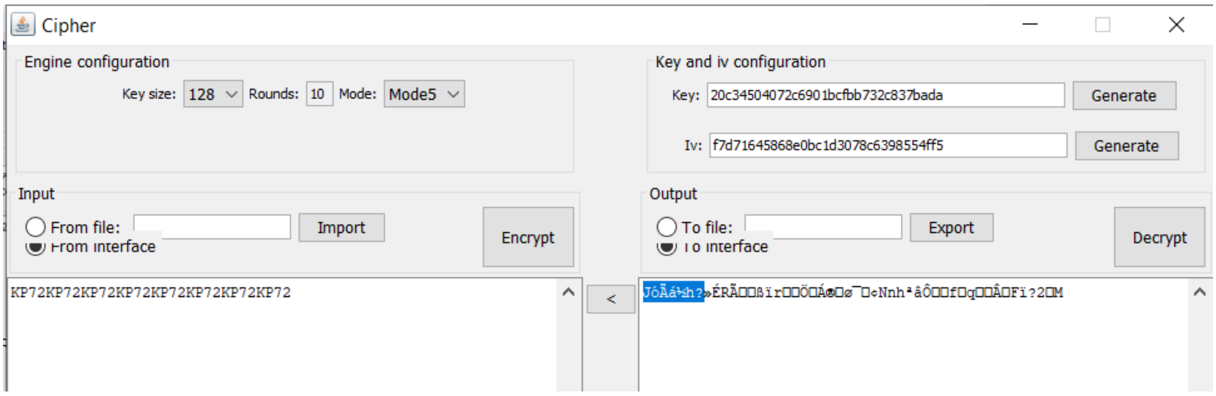
Tryb 4 – OFB – przy zmianie pierwszego bloku danych nie zmienia się reszta.



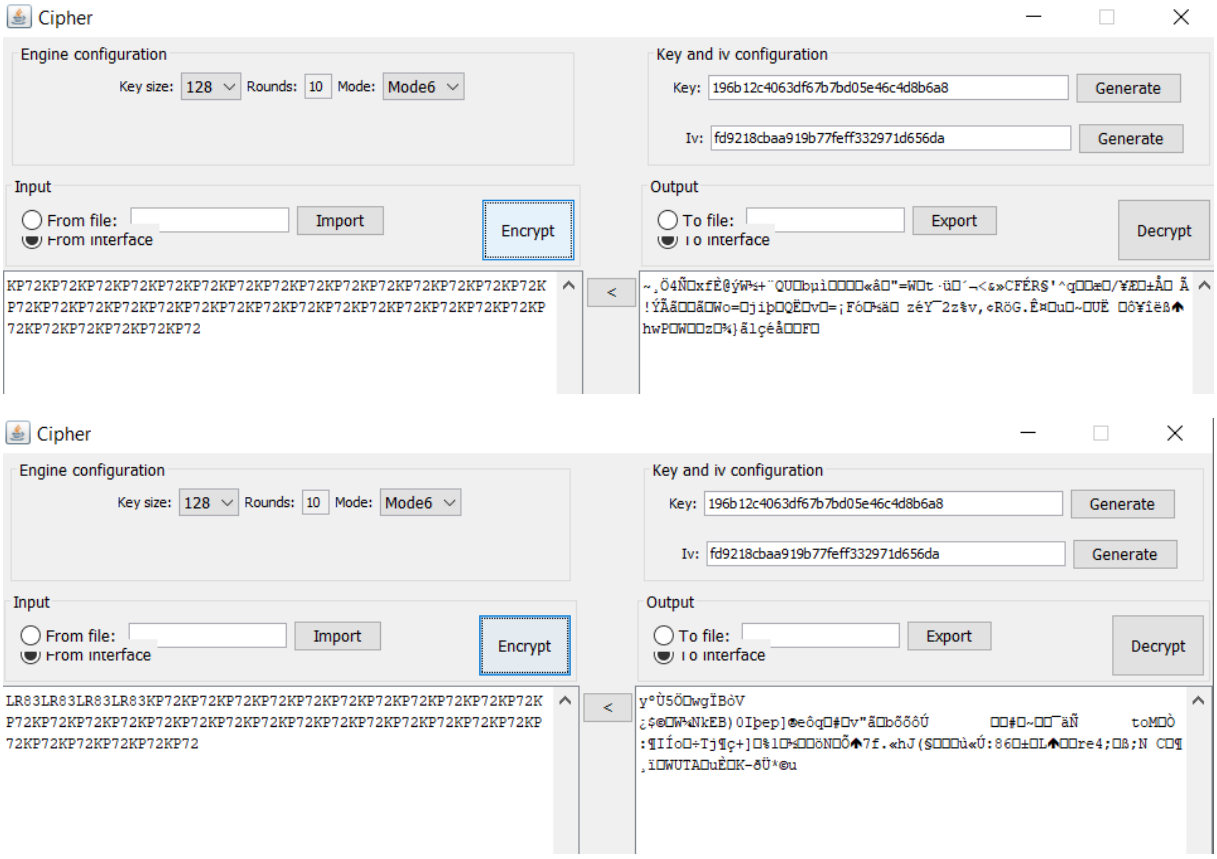


Tryb 5 – CTR – ten sposób szyfrowania opiera się w głównej mierze na IV. Jeśli zmienimy IV na IV+1, to nasz szyfrogram też przesunie się o 1, tj. drugi blok w pierwszym szyfrogramie, stanie się pierwszym blokiem w drugim.



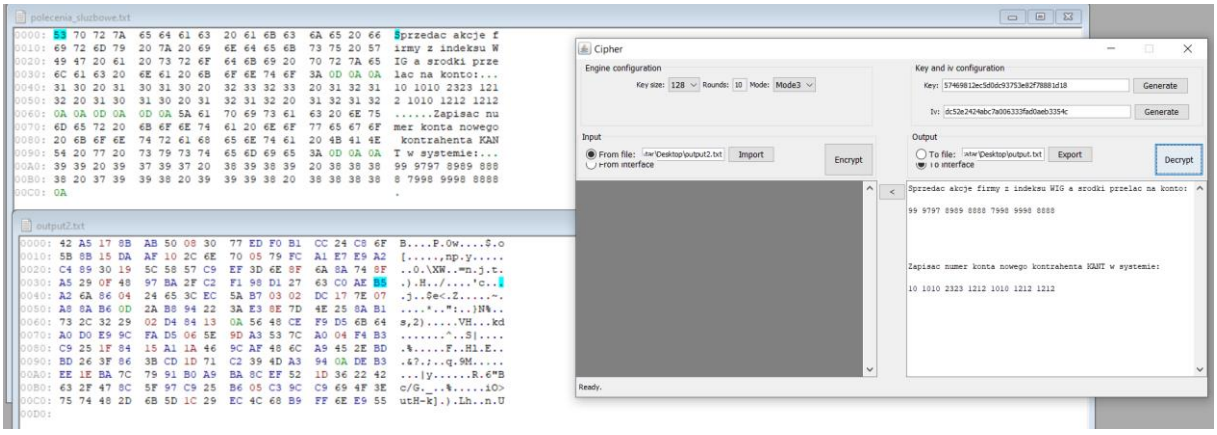


Tryb 6 – CFB – przy zmianie pierwszego bloku zmienia się też reszta szyfrogramu



Używając tego samego algorytmu szyfrującego i tego samego klucza kryptograficznego, ale różnych trybów szyfrowania, otrzymamy różne szyfrogramy. Spowodowane to jest tym, że każdy z tych trybów ma nieco zmieniony sposób liczenia w algorytmie szyfrującym (np. CFB wykorzystuje sprzężenie zwrotne szyfrogramu).

4. Należy zamienić ze sobą bloki odpowiadające obu numerom bankowym



Szyfru ECB można używać do szyfrowania krótkich wiadomości. Wiąże się to z tym, że szyfr ten wykorzystuje ten sam klucz dla kolejnych bloków, więc w szyfrogramie występują powtórzenia. DO zaszyfrowania notatki służbowej użyłabym albo trybu CFB ze względu na zmianę szyfrogramu przy każdej zmianie pierwszego bloku lub trybu CBC – MAC, gdyż skraca on tekst i opiera się na funkcji haszującej.

Wnioski:

W szyfrowaniu symetrycznym wykorzystuje się ten sam klucz zarówno do szyfrowania, jak i do deszyfrowania wiadomości, zatem nadawca jak i odbiorca wiadomości muszą wiedzieć jaki jest klucz, co zdecydowanie ułatwia np. wykradzenie takiego klucza.

W przypadku szyfrów strumieniowych wykorzystuje się fakt, że tekst jawny, przedstawiony jest jako ciąg znaków, zatem szyfrowanie odbywa się bit po bicie lub bajt po bajcie. Trochę inna sytuacja pojawia się w przypadku szyfrów blokowych, gdzie bierzemy określony blok tekstu jawnego (najczęściej długości 64 lub 128 bitów) i traktujemy go jako całość, produkując szyfrogram o tej samej długości. Mają one znacznie szersze zastosowanie niż szyfry strumieniowe. (Źródło: W.Stallings, Cryphography and Network Security. Principles and Practice, 2017)