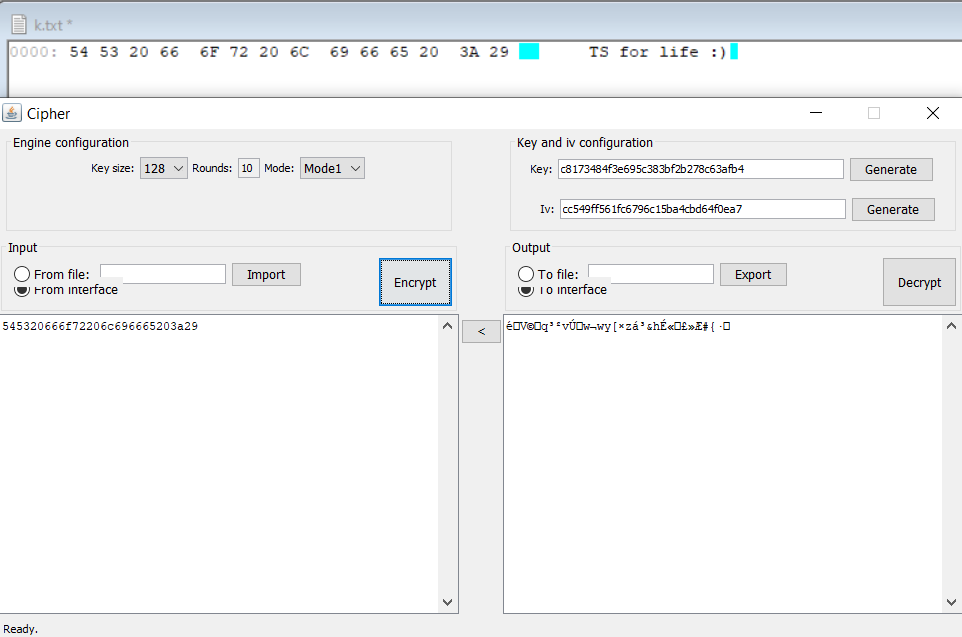
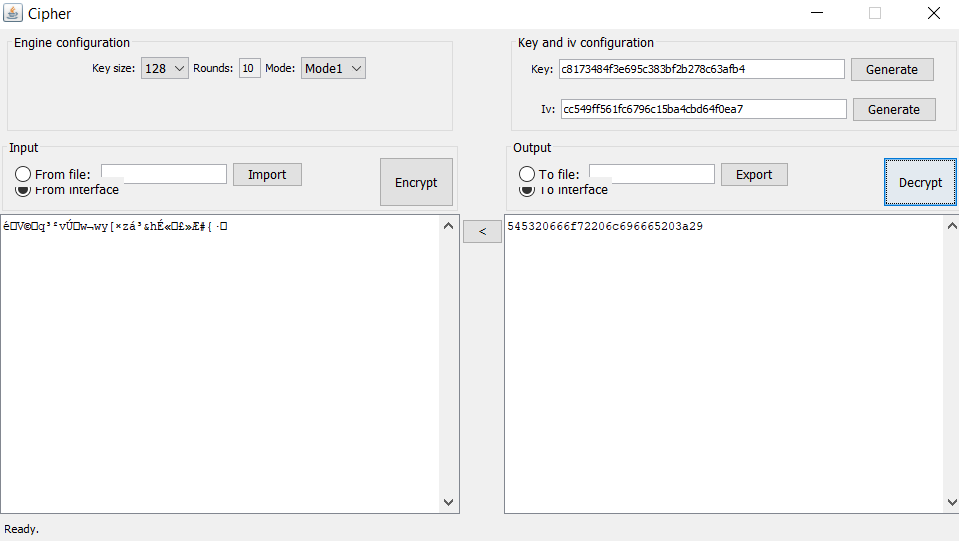
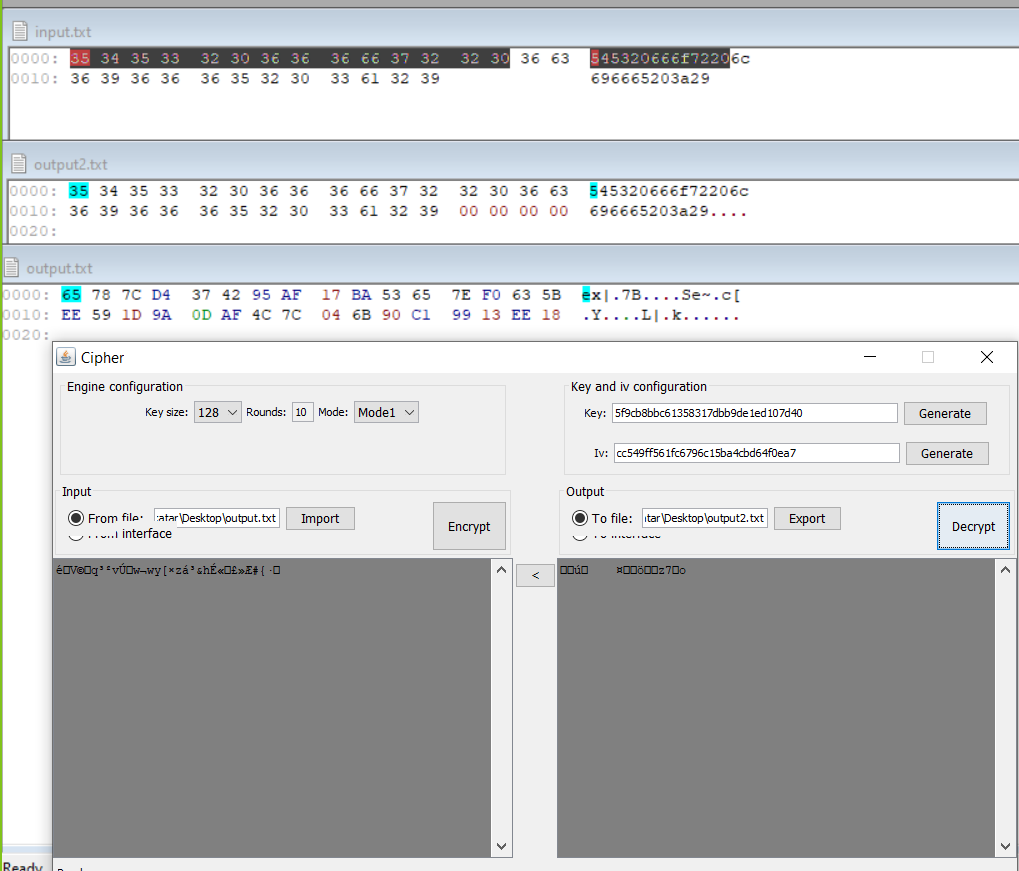
**Bezpieczeństwo systemów i sieci teleinformatycznych – sprawozdanie z laboratorium 2**

Autor: Katarzyna Pencak

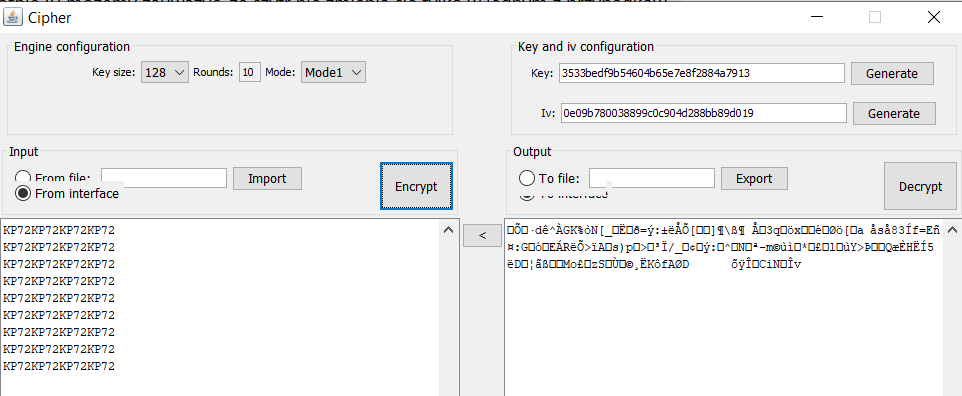
2. Na pierwszych dwóch screenach działanie szyfrowania i deszyfrowania tekstu przez interfejs. Na trzecim to samo, tylko za pomocą pliku. Treść plików zamieniona na heksadecymalne przy użyciu HexEditor.

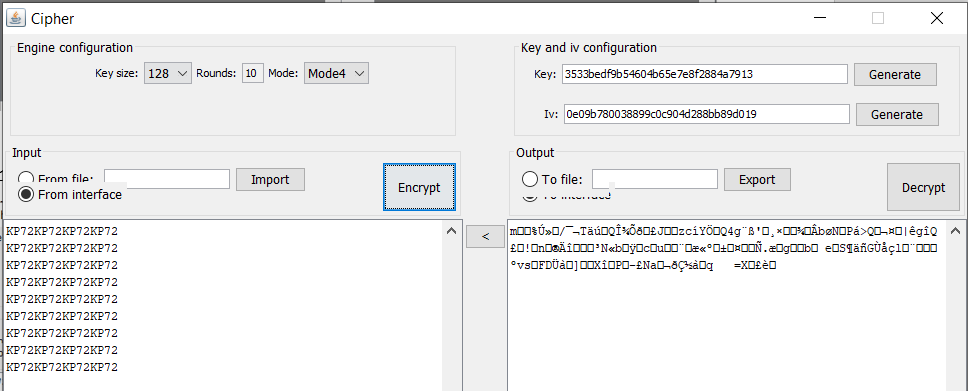


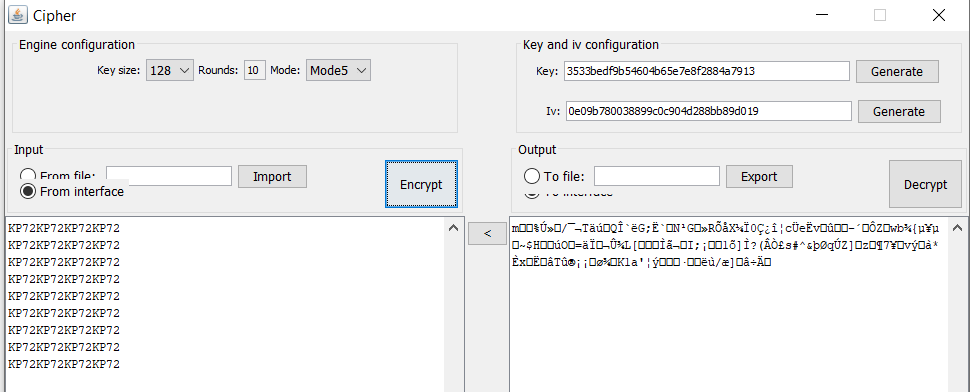


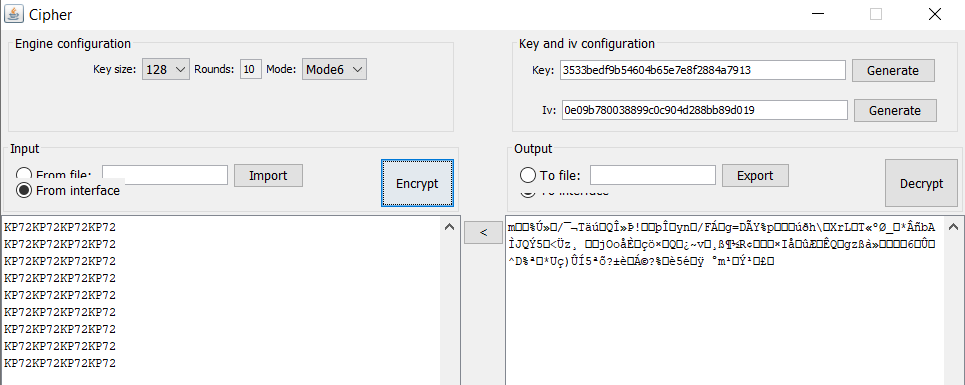
3. Kolejność odgadywania trybów (3, 2, 1, 5, 4, 6)

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

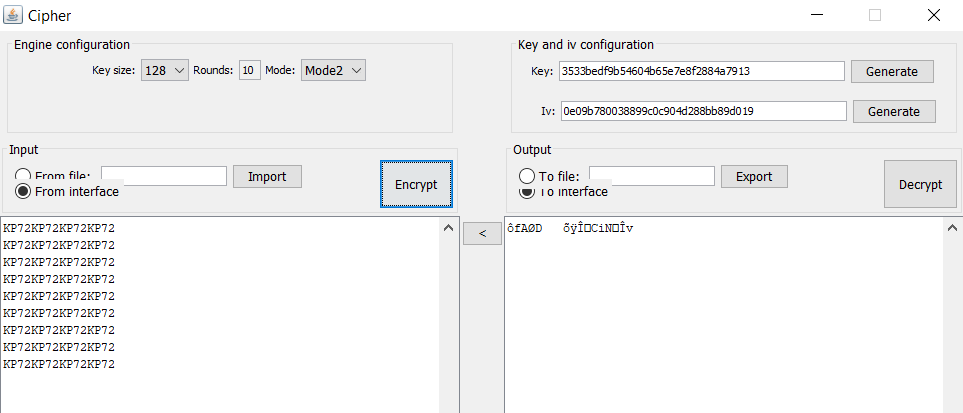




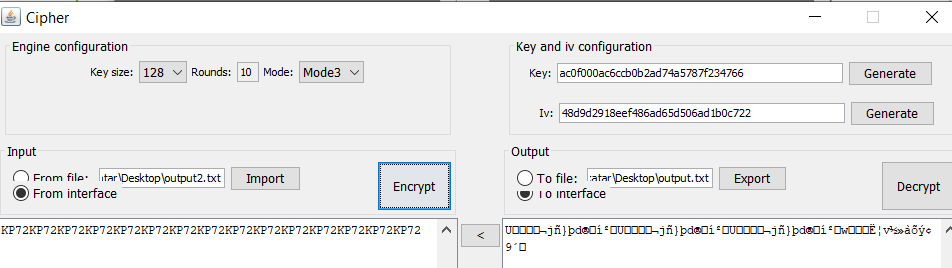


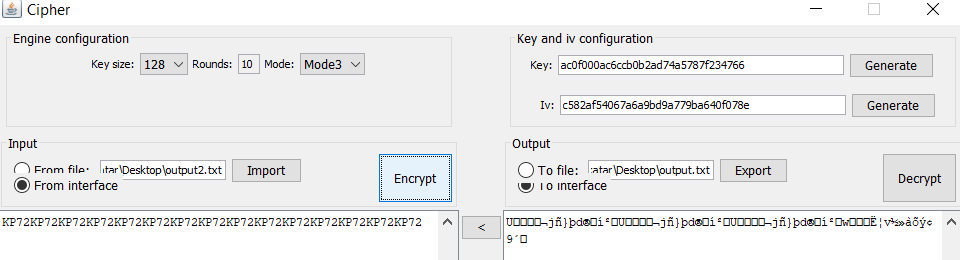


Tryb 2 – CBC – MAC, powstaje najkrótszy szyfr ze wszystkich opcji (hash)

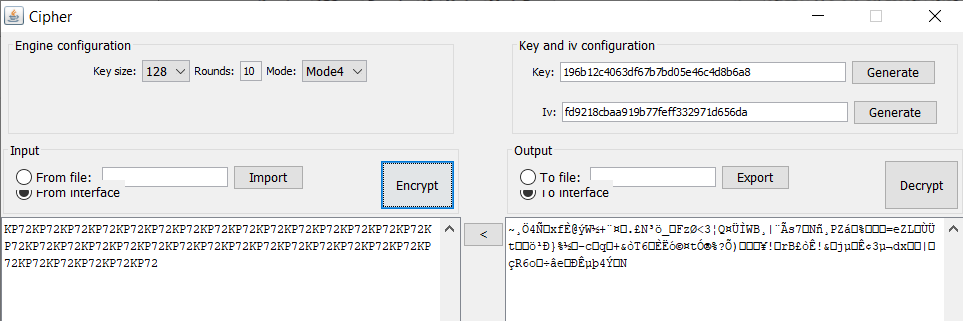


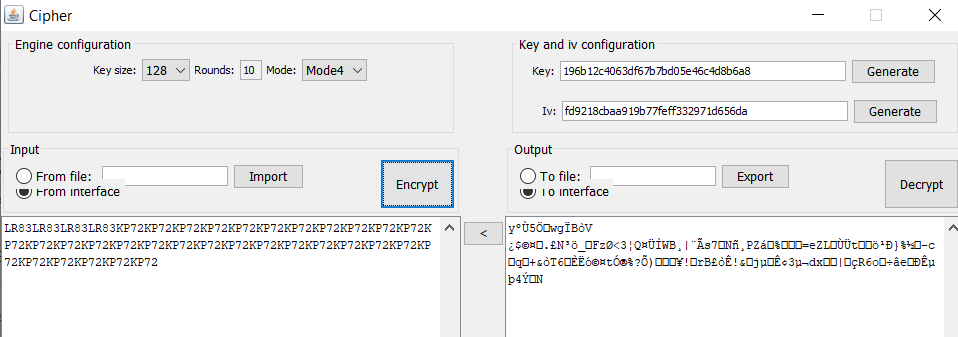
Tryb 3 – ECB, gdyż nie zmienia się wynik w zależności generowanego IV



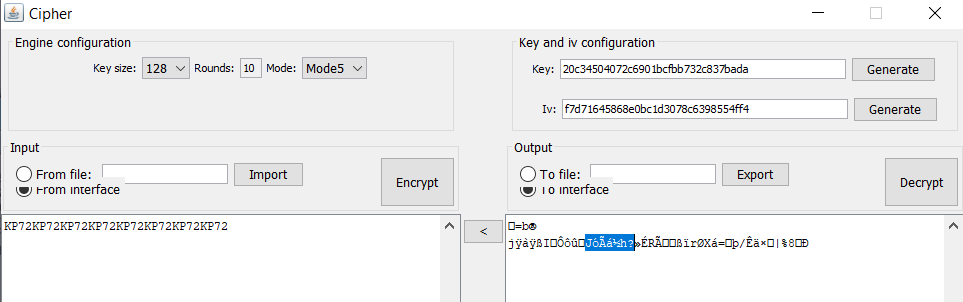


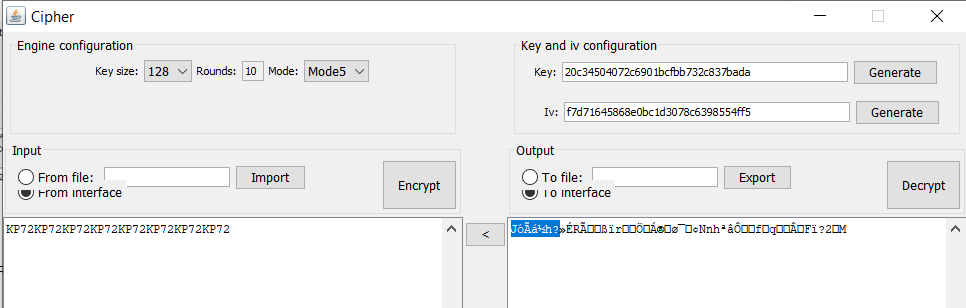
Tryb 4 – OFB – przy zmianie pierwszego bloku danych nie zmienia się reszta.



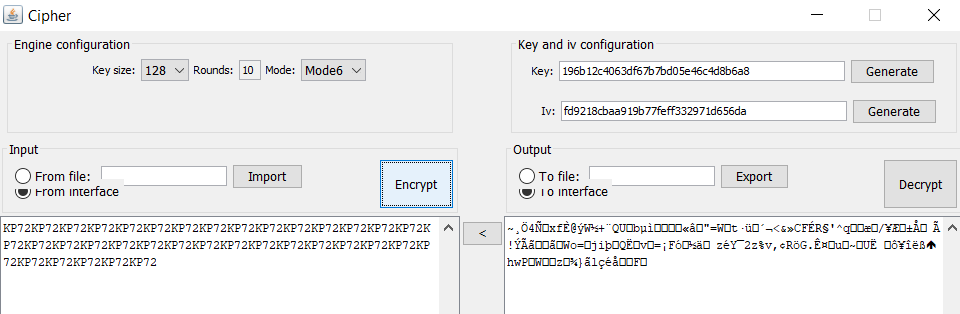


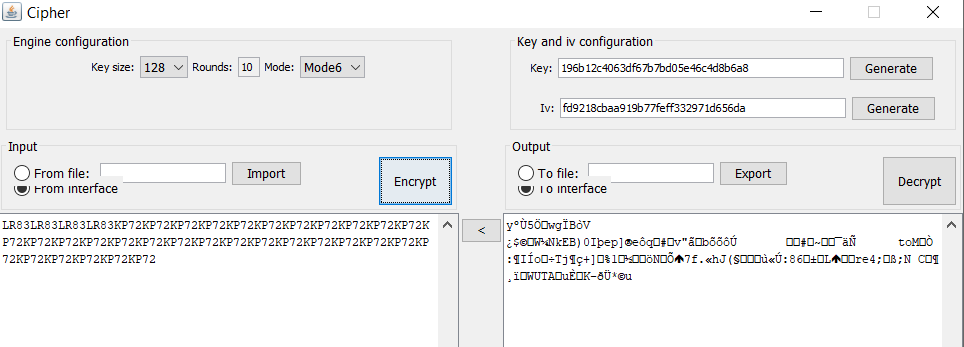
Tryb 5 – CTR – ten sposób szyfrowania opiera się w głównej mierze na IV. Jeśli zmienimy IV na IV+1, to nasz szyfrogram też przesunie się o 1, tj. drugi blok w pierwszym szyfrogramie, stanie się pierwszym blokiem w drugim.



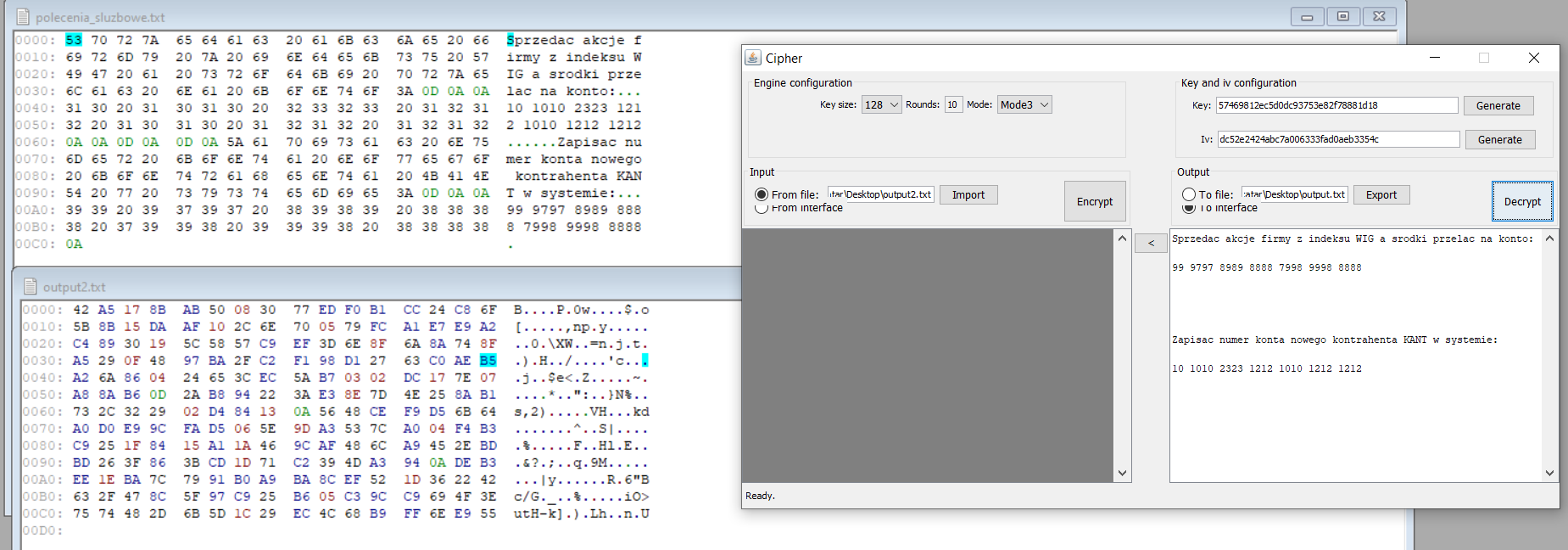


Tryb 6 – CFB – przy zmianie pierwszego bloku zmienia się też reszta szyfrogramu





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)