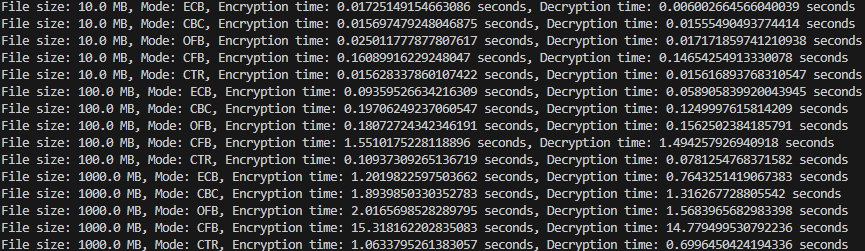
5.04.2024r.

Piotr Suchodolski

Sprawozdanie – Szyfry Blokowe

Zadanie 1

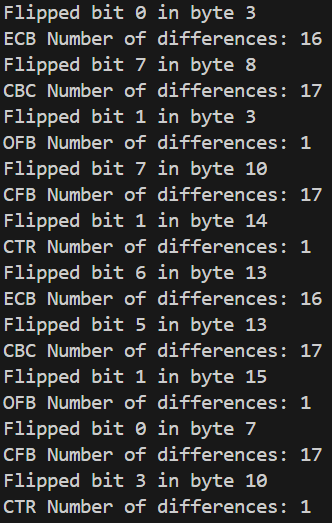
Analiza szybkości działania 5 podstawowych trybów szyfrowania dla 3 różnych wielkości plików wejściowych:



Z wyników można wyciągnąć wniosek, że algorytm CFB zajmuje najwięcej czasu zarówno pod względem szyfrowania jak i deszyfrowania oraz znacznie odstaje od innych algorytmów pod tym względem. W porównaniu do prostszych trybów szyfrowania takich jak np. ECB, szyfr ten używa mechanizmu ciągłej synchronizacji wyjścia do wejścia, ponieważ szyfr jest generowany w formie strumienia, który jest cięgle aktualizowany podczas generowania kodu. Dlatego, szyfr ten realizuje wiele operacji zapisu, bitowych oraz niemożliwe jest jego zrównoleglenie. Mogą to być przyczyny najdłuższego czasu wykonania.

Zadanie 2

Analiza propagacji błędów w konkretnych trybach szyfrowania. Dla każdego szyfrogramu został zmieniony jeden losowy bit w jednym losowym bajcie z pierwszego bloku. Dalej po odszyfrowaniu wiadomość została porównana z oryginałem oraz obliczona ilość różniących się bajtów.



W wynikach można zauważyć, że nie nastąpiła propagacja błędu tylko w algorytmach OFB oraz CTR. Reszta algorytmów zmieniła cały blok danych przez 1 błąd. Po wizualnej analizie wiadomości widać, że fragment, który został zmieniony jest kompletnie nieczytelny i tracona jest zawarta w nim informacja.

Przykłady:

Fragment odszyfrowanej wiadomości z algorytmu CTR gdzie wystąpił błąd



Fragment odszyfrowanej wiadomości z algorytmu CBC gdzie wystąpił błąd



Zadanie 3

Implementacja szyfrowania CBC używając EBC.

