Sprawozdanie

Cel zadania

- **Zadanie 1:** Zmierzyć czasy szyfrowania/deszyfrowania dla 3 rozmiarów plików (ok. 100KB, 1MB, 10MB) w 5 trybach AES (ECB, CBC, OFB, CFB, CTR) i zinterpretować wyniki.

- **Zadanie 2:** Zanalizować propagację błędów w szyfrogramach – sprawdzić, czy pojedynczy błąd skutkuje utratą całej wiadomości czy jedynie fragmentu.

- **Zadanie 3:** Zaimplementować tryb CBC przy użyciu trybu ECB.

Implementacja i wyniki

1. Pomiar czasów

- **Generacja plików:** Dla zadanych rozmiarów generowane są pliki z losowymi danymi.

- **Funkcja pomiaru:** `zmierzCzasSzyfrowaniaIDeszyfrowania` odczytuje plik, szyfruje (z paddingiem tam, gdzie wymagane) i mierzy czas operacji.

- **Wyniki:**

    - **CTR i ECB** – najkrótsze czasy operacji (CTR jeszcze szybszy, dzięki możliwości równoległego przetwarzania).

    - **CBC, OFB, CFB** – dłuższe czasy, przy czym CFB najwolniejszy, ze względu na zależności między blokami.
      Interpretacja: Szybkość operacji rośnie wraz z rozmiarem pliku; wybór trybu zależy od kompromisu między wydajnością a bezpieczeństwem (ECB szybko, ale niebezpiecznie).

2. Propagacja błędów

- **Procedura:** Po szyfrowaniu wprowadzany jest błąd (zmiana jednego bajtu w środku szyfrogramu) i wykonywane jest deszyfrowanie.

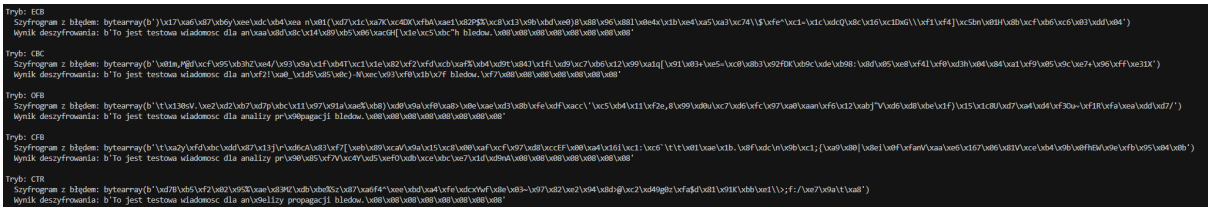
- **Obserwacje:**

- **ECB, CTR, OFB:** Błąd wpływa tylko na dany blok, reszta pozostaje poprawna.

- **CBC i CFB:** Błąd propaguje się na kolejny blok (a w CFB nawet na więcej), co może skutkować utratą części wiadomości.

Wnioski: Tryby lokalizujące błąd (np. CTR, OFB) są bardziej odporne na pojedyncze błędy transmisji.

- **Wyniki:**



3. Implementacja trybu CBC przy użyciu ECB

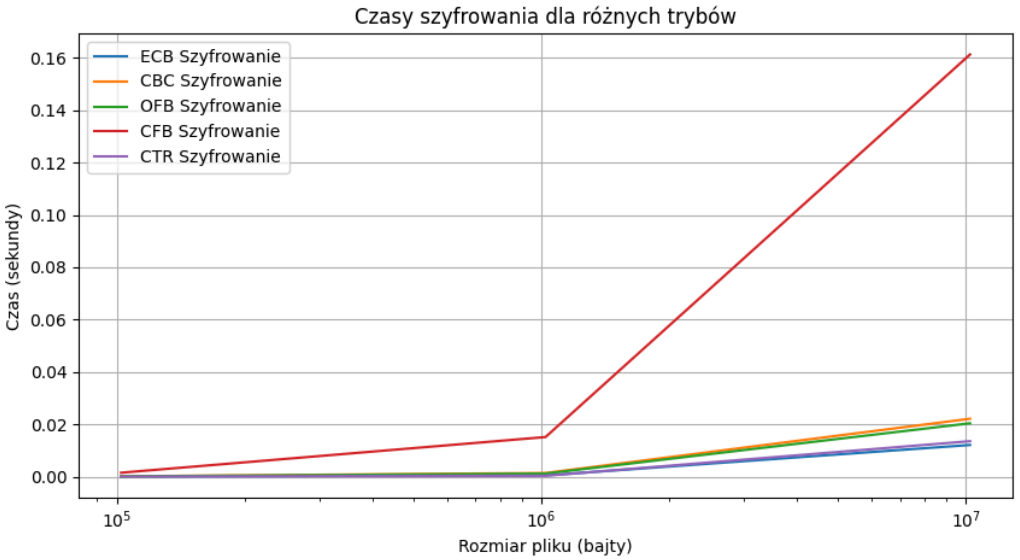
- **Metoda:**

  - **Szyfrowanie:** Pierwszy blok jest XOR-owany z IV, kolejne bloki z poprzednim szyfrogramem, a następnie szyfrowane trybem ECB.

  - **Deszyfrowanie:** Odszyfrowane bloki są XOR-owane z IV lub poprzednim blokiem szyfrogramu.

- **Weryfikacja:** Implementacja została sprawdzona asercją, która potwierdza, że odszyfrowany tekst odpowiada tekstowi oryginalnemu.

4. Wykres


Czasy szyfrowania dla różnych trybów
ECB Szyfrowanie
CBC Szyfrowanie
OFB Szyfrowanie
CFB Szyfrowanie
CTR Szyfrowanie
Czas (sekundy)
0.16
0.14
0.12
0.10
0.08
0.06
0.04
0.02
0.00
10^5
10^6
10^7
Rozmiar pliku (bajty)