

# 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 (Electronic Codebook)

Błąd wpływa tylko na jeden blok danych. Nie występuje propagacja błędów – inne bloki pozostają nienaruszone.

## CBC (Cipher Block Chaining)

Błąd wpływa na dwa bloki: ten, w którym wystąpił (zostaje kompletnie zniekształcony), oraz kolejny. Dalsze bloki są poprawne. Występuje propagacja błędu do dwóch bloków.

## OFB (Output Feedback)

Błąd wpływa tylko na jeden bajt danych. Nie występuje propagacja błędu. Tryb działa jak szyfr strumieniowy – odporny na błędy transmisji.

### CFB (Cipher Feedback)

Błąd wpływa na kilka bajtów. Występuje częściowa propagacja błędu.

### CTR (Counter)

Błąd wpływa tylko na jeden bajt. Nie występuje propagacja błędów. Tryb działa jak szyfr strumieniowy – odporny na błędy transmisji.

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

- **Wyniki:**

[illegible]

### 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

