Podstawy Ochrony Danych – laboratorium AGC
Tryby pracy szyfrów blokowych

Najprostszym trybem szyfrowania jest ECB (elektroniczna książka kodowa), który przetwarza każdy blok tekstu jawnego niezależnie, co jest bezpieczne jedynie wtedy, jeśli wiadomość jest niedłuższa niż rozmiar jednego bloku. Zaprojektowano dlatego wiele innych trybów pracy szyfrów blokowych, łączących, czy sprzęgających bloki szyfrogramu lub dodających wartości inicjujące, które zapewniają bezpieczeństwo dowolnej szyfrowanej wiadomości.

**Cel ćwiczenia laboratoryjnego:** zapoznanie się z tematyką trybów pracy szyfrów blokowych ECB, CBC, OFB, CFB, CTR.

**Materiały do laboratorium:** materiały z wykładu oraz materiały dodatkowe podane przez prowadzącego.

**Zadanie:**

1. Przeanalizuj dostępne tryby pracy szyfrów blokowych w wybranym środowisku programowania i zmierz czasy szyfrowania i deszyfrowania dla 3 różnej wielkości plików we wszystkich 5 podstawowych trybach ECB, CBC, OFB, CFB, i CTR. Zinterpretuj otrzymane wyniki.
2. Przeanalizuj propagację błędów w wyżej wymienionych trybach pracy. Czy błąd w szyfrogramie będzie skutkował niemożnością odczytania po deszyfrowaniu całej wiadomości, fragmentu, ..? Zinterpretuj wyniki obserwacji.
3. Zaimplementuj tryb CBC (korzystając z dostępnego w wybranym środowisku programowania trybu ECB).

**Przydatne linki**:

Dokumentacja szyfru AES:
https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf

tryby pracy:
https://www.tutorialspoint.com/cryptography/block_cipher_modes_of_operation.htm