Podstawy Kryptografii	
Szyfry blokowe	
Imię i Nazwisko	Oliwia Przybyła
Grupa i Nr indeksu	(L3) 149429
Data	27.04.2023

```
Tryb: ECB
Rozmiar: small
Czas szyfrowania: 0.0016349999999999976 sek
Czas deszyfrowania: 5.379999999999274e-05 sek

Rozmiar: medium
Czas szyfrowania: 3.3399999999988994e-05 sek
Czas deszyfrowania: 1.7900000000015126e-05 sek

Rozmiar: large
Czas szyfrowania: 0.0001588000000001449 sek
Czas deszyfrowania: 3.78000000000045e-05 sek

Tryb: CBC
Rozmiar: small
Czas szyfrowania: 0.0003171000000000146 sek
Czas deszyfrowania: 0.00032999999999999696 sek

Rozmiar: medium
Czas szyfrowania: 0.002943000000000001 sek
Czas deszyfrowania: 0.003095300000000023 sek

Rozmiar: large
Czas szyfrowania: 0.040951600000000005 sek
Czas deszyfrowania: 0.045181900000000025 sek
```

```
Tryb: OFB
Rozmiar: small
Czas szyfrowania: 0.0003842000000000012 sek
Czas deszyfrowania: 0.0001270999999999911 sek

Rozmiar: medium
Czas szyfrowania: 7.40000000000185e-05 sek
Czas deszyfrowania: 7.569999999995636e-05 sek

Rozmiar: large
Czas szyfrowania: 0.00032409999999999384 sek
Czas deszyfrowania: 0.0002846000000000237 sek

Tryb: CFB
Rozmiar: small
Czas szyfrowania: 0.0002569999999999517 sek
Czas deszyfrowania: 0.00011280000000002399 sek

Rozmiar: medium
Czas szyfrowania: 9.059999999999624e-05 sek
Czas deszyfrowania: 5.39999999999898494e-05 sek

Rozmiar: large
Czas szyfrowania: 0.0004539999999999995444 sek
Czas deszyfrowania: 0.00023330000000004736 sek
```

```
Tryb: CTR
Rozmiar: small
Czas szyfrowania: 0.00022319999999997897 sek
Czas deszyfrowania: 9.10999999999551e-05 sek

Rozmiar: medium
Czas szyfrowania: 6.02000000000010245e-05 sek
Czas deszyfrowania: 2.889999999999837e-05 sek

Rozmiar: large
Czas szyfrowania: 0.00018899999999999473 sek
Czas deszyfrowania: 6.350000000004963e-05 sek
```

1. Wyniki wskazują, że czasy szyfrowania i deszyfrowania różnią się znacznie między różnymi trybami szyfrowania oraz między różnymi rozmiarami plików. Tryb ECB, który jest jednym z najprostszych trybów, jest najszybszy, ale jest również najsłabszy pod względem bezpieczeństwa, ponieważ ten sam blok wejściowy będzie zawsze mapowany na ten sam blok wyjściowy, co może prowadzić do łatwego ataku przez kryptoanalizę. Z drugiej strony, tryb CBC, który jest jednym z najbezpieczniejszych trybów, ale wymaga dodatkowego wektora inicjalizacyjnego, jest znacznie wolniejszy niż tryb ECB. Tryby OFB, CFB i CTR oferują lepsze bezpieczeństwo niż ECB, a jednocześnie są znacznie szybsze niż CBC.
Co do rozmiaru pliku, to można zauważyć, że czas szyfrowania i deszyfrowania rośnie wraz z rozmiarem pliku, co jest zgodne z intuicją, ponieważ im większy plik, tym więcej danych trzeba przetworzyć. Jednak wzrost czasu jest zwykle mniejszy niż proporcjonalny do rozmiaru pliku, co sugeruje, że szyfrowanie blokowe jest dość efektywne, szczególnie w przypadku mniejszych plików.
Warto zwrócić uwagę, że czas szyfrowania i deszyfrowania różni się dla różnych trybów szyfrowania, ale nie ma jasnego zwycięzcy. W zależności od konkretnego zastosowania, należy wybrać tryb szyfrowania, który spełnia wymagania bezpieczeństwa i wydajności.

2. W zależności od trybu szyfrowania, błędy w szyfrogramie będą miały różne konsekwencje. Tryb ECB umożliwia niezależne szyfrowanie każdego bloku, więc błąd w jednym bloku nie wpłynie na pozostałe bloki, jednakże może prowadzić do utraty informacji w bloku deszyfrowanego tekstu. Tryb CBC jest zależny od poprzedniego bloku szyfru, co oznacza, że błąd w jednym bloku szyfru wpłynie na kolejne bloki tekstu jawnego. Tryby OFB i CFB są również zależne od poprzedniego bloku szyfru lub strumienia klucza, co oznacza, że błąd w jednym bloku szyfru wpłynie na wszystkie kolejne bloki. W trybie CTR błąd w jednym bloku szyfru wpłynie tylko na ten konkretny blok tekstu jawnego.