Sprawozdanie z przedmiotu “Podstawy Kryptografii”

Szyfry blokowe

Ivan Kaliadzich 153936

1. Dla danych różnej welkości tryby ECB, CBC, OFB, CFB i CTR spędzają różne czasy. Jako przykład wybrałem rozmiary: 10^3 KB, 10^4 KB, 10^5 KB, wyszły u mnie takie dane:

```
Testowanie rozmiaru pliku: 1024000 bajtów
Tryb: ECB - Czas szyfrowania: 0.001995 s, Czas deszyfrowania: 0.000997 s
Tryb: CBC - Czas szyfrowania: 0.001992 s, Czas deszyfrowania: 0.001995 s
Tryb: OFB - Czas szyfrowania: 0.001996 s, Czas deszyfrowania: 0.002992 s
Tryb: CFB - Czas szyfrowania: 0.002992 s, Czas deszyfrowania: 0.002991 s
Tryb: CTR - Czas szyfrowania: 0.001995 s, Czas deszyfrowania: 0.001995 s
Testowanie rozmiaru pliku: 10240000 bajtów
Tryb: ECB - Czas szyfrowania: 0.015957 s, Czas deszyfrowania: 0.017952 s
Tryb: CBC - Czas szyfrowania: 0.024935 s, Czas deszyfrowania: 0.020942 s
Tryb: OFB - Czas szyfrowania: 0.052860 s, Czas deszyfrowania: 0.026927 s
Tryb: CFB - Czas szyfrowania: 0.028924 s, Czas deszyfrowania: 0.033908 s
Tryb: CTR - Czas szyfrowania: 0.019947 s, Czas deszyfrowania: 0.017952 s
Testowanie rozmiaru pliku: 102400000 bajtów
Tryb: ECB - Czas szyfrowania: 0.249334 s, Czas deszyfrowania: 0.248864 s
Tryb: CBC - Czas szyfrowania: 0.237397 s, Czas deszyfrowania: 0.185508 s
Tryb: OFB - Czas szyfrowania: 0.304187 s, Czas deszyfrowania: 0.360545 s
Tryb: CFB - Czas szyfrowania: 0.304910 s, Czas deszyfrowania: 0.304186 s
Tryb: CTR - Czas szyfrowania: 0.163562 s, Czas deszyfrowania: 0.139628 s
```

2. Analiza propagacji błędów w różnych trybach pracy:

```
Analiza propagacji błędów
Tryb: ECB
Wiadomość wejsciowa: b'This is a test message for encryption'

Tekst zaszyfrowany (z błędem): b'\x03\xd1\x9f\x89\x11\xa25\xed\xfe\xa4\xda\x84;\xbó\xe8)8\xf5\x90@'...
Wiadomość wyjsciowa (z błędem): b'\x9damf\xaf\x9e\x81\x0b\xe1\x95Dy(\xe0\xce\xefessage for encryption'



Tryb: CBC
Wiadomość wejsciowa: b'This is a test message for encryption'

Tekst zaszyfrowany (z błędem): b'9<\xd0\xee\x96\x1b\xb3m)\xcbf1^\x1f\xd1\xd3\xf9\t\xcó\xbf'...
Wiadomość wyjsciowa (z błędem): b'\x08?$\xa5\xfó\xb0\xbb+,\xf1 Yk\xb7\xf1\xb0essage for!encryption'



Tryb: OFB
Wiadomość wejsciowa: b'This is a test message for encryption'

Tekst zaszyfrowany (z błędem): b'WH\xab\xef\x87\x1c\xda0\xefW\xc2W\xb5\x13\x92=\xcf \xdb\xe1'...
Wiadomość wyjsciowa (z błędem): b'This is a uest message for encryption'



Tryb: CFB
Wiadomość wejsciowa: b'This is a test message for encryption'

Tekst zaszyfrowany (z błędem): b'WH\xab\xef\x87\x1c\xda0\xefW\xc2W\xb5\x13\x92=\xe2\xb5]\xaó'...
Wiadomość wyjsciowa (z błędem): b'This is a uest mT\x96\x88\xa4\x9b\x05\xdac\xb1V\x0cF\xfó`\xeó[ption'



Tryb: CTR
Wiadomość wejsciowa: b'This is a test message for encryption'

Tekst zaszyfrowany (z błędem): b'WH\xab\xef\x87\x1c\xda0\xefW\xc2W\xb5\x13\x92=\x03\xe1-\xb4'...
Wiadomość wyjsciowa (z błędem): b'This is a uest message for encryption'
```

3. Zrealizowany tryb CBC w pliku main.py