WZK - Zadanie 3

Dariusz Max Adamski
Nr indeksu 136674

Eksperyment 1

- Cel: porównanie wydajności trybów pracy szyfrów blokowych
  - ECB, CBC, OFB, CTR i CFB
- Wykorzystałem bibliotekę PyCryptodome
- Czasy szyfrowania i deszyfrowania mierzyłem dla trzech plików:
  - Mały plik pdf z tekstem i obrazkami - “paper.pdf” (485KB)
  - Archiwum z programem Weka - “weka.zip” (130MB)
  - Film Full HD - “movie.mp4” (1.5GB)
- Losowy klucz o długości 16 bajtów
- Dane plików uzupełniałem zerami do osiągnięcia bufora o długości wielokrotności wielkości bloku

Wynki: czas szyfrowania i deszyfrowania

	ECB - encrypt	ECB - decrypt	CBC - encrypt	CBC - decrypt	OFB - encrypt	OFB - decrypt	CTR - encrypt	CTR - decrypt	CFB - encrypt	CFB - decrypt
paper.pdf	0.00145912	0.00027895	0.00180173	0.00122571	0.00107026	0.000911713	0.000677586	0.000554085	0.0124083	0.0119822
weka.zip	0.12773	0.131356	0.367219	0.351085	0.347466	0.351746	0.245869	0.246997	3.42448	3.28912
movie.mp4	1.38244	1.41528	4.01625	3.87674	3.92575	3.88002	2.70915	2.71288	39.2416	37.8456

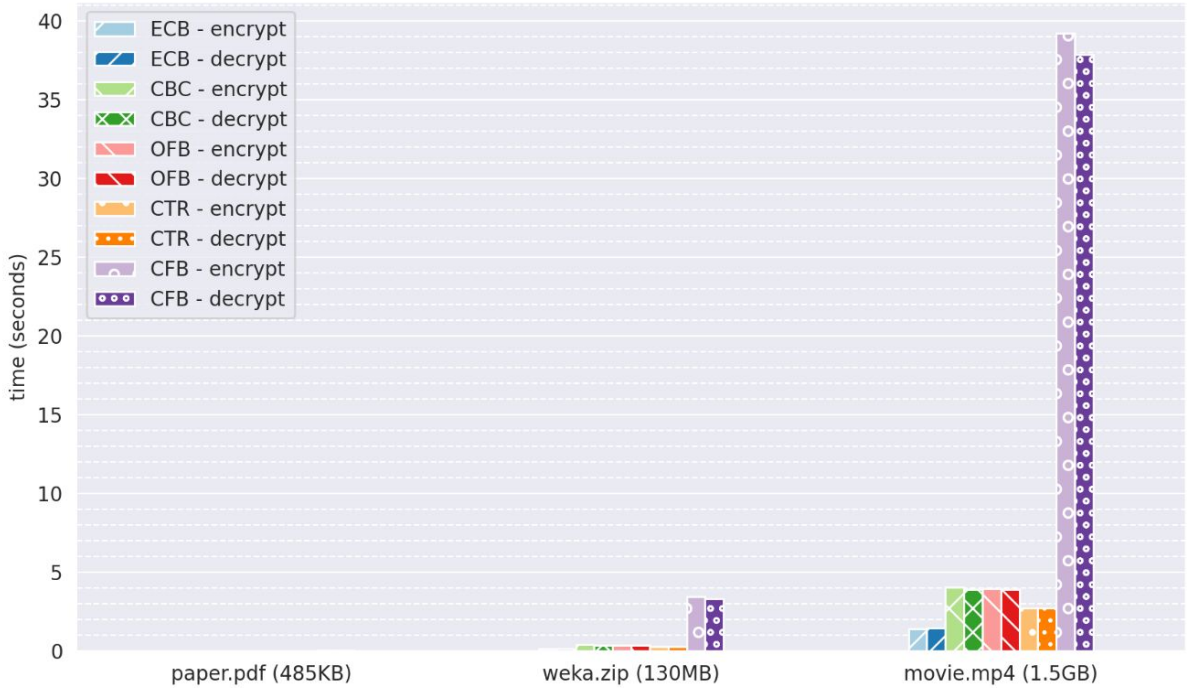
Czasy w sekundach

Czas szyfrowania i deszyfrowania

Tryb CFB jest wyraźnie najwolniejszy.

Duży wzrost czasu przetwarzania ze wzrostem wielkości pliku utrudnia analizę danych.

Rozwiązanie: analiza szybkości zamiast czasu, lub alternatywnie wprowadzenie skali logarytmicznej.



Wynki: czas szyfrowania i deszyfrowania

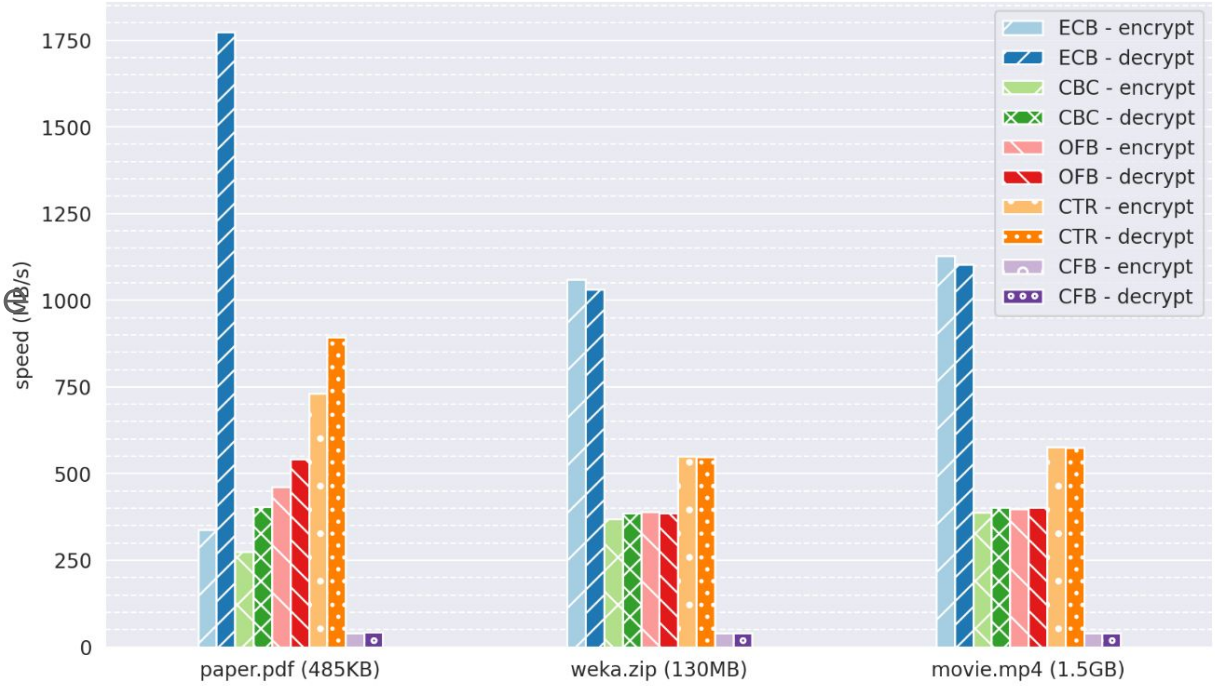
	ECB - encrypt	ECB - decrypt	CBC - encrypt	CBC - decrypt	OFB - encrypt	OFB - decrypt	CTR - encrypt	CTR - decrypt	CFB - encrypt	CFB - decrypt
paper.pdf	339.245	1774.51	274.736	403.848	462.504	542.934	730.535	893.365	39.8928	41.3113
weka.zip	1061.07	1031.78	369.071	386.032	390.053	385.307	551.229	548.712	39.5768	41.2055
movie.mp4	1128.74	1102.55	388.524	402.506	397.48	402.165	575.978	575.185	39.7642	41.231

Szybkość w megabajtach na sekundę

Szybkość szyfrowania i deszyfrowania

Dla małego pliku w trybie ECB odszyfrowywanie jest kilka razy szybsze. Dla pozostałych trybów odszyfrowywanie jest szybsze o kilka-kilkadziesiąt procent.

Uważam, że różnice dla małego pdf'a są zawyżone, przez dużą niepewność pomiaru.



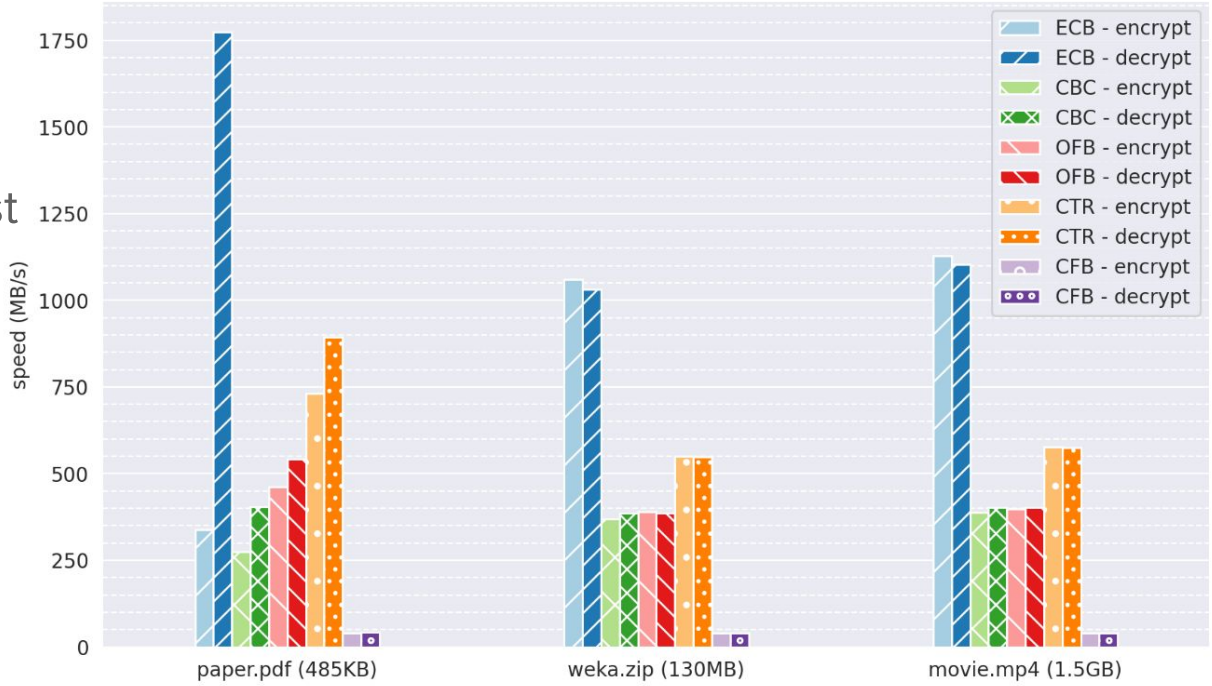
Szybkość szyfrowania i deszyfrowania

Dla średniego i dużego pliku pomiary są bardzo zbliżone.

Szyfrowanie w trybie ECB jest o 50MB/s szybsze od odwrotności.

Pozostałe tryby są marginalnie szybsze w odszyfrowywaniu.

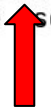
Tryb CFB jest prawie 29 razy wolniejszy od ECB



Eksperyment 2

- Cel: porównanie propagacji błędów dla wybranych trybów pracy szyfrów blokowych
- Dane wejściowe: pierwsze zdanie z “Alicji w krainie czarów”
- Wprowadzone uszkodzenie: zamiana 120. bajtu bufora danych na wartość ‘0’

```
--- ORIGINAL ---
b'Alice was beginning to get very tired of sitting by her sister on the bank, and of having nothing to do: once or
twice she had peeped into the book her sister was reading, but it had no pictures or conversations in it, "and what
is the use of a book," thought Alice "without pictures or conversations?"\n'
```



0x00

Tryb ECB, CBC i CFB

- Zamiana jednego bajta powoduje uszkodzenie całego bloku
- W trybie ECB uszkodzone są bajty od pozycji 120-8 do 120+8
- W trybie CBC uszkodzone są bajty od pozycji 120-8 do 120+8 oraz w następnym bloku na pozycji 120+16
- W trybie CFB uszkodzone są bajty od pozycji 120 do 120+16

```
--- ECB ---
b'Alice was beginning to get very tired of sitting by her sister on the bank, and of having nothing to do: once or\
xf3D\xe9\x95\x9a\x0c4U\x18\xb5C\x18\x1a\xedrUeeped into the book her sister was reading, but it had no pictures or
conversations in it, "and what is the use of a book," thought Alice "without pictures or conversations?"\n'

--- CBC ---
b'Alice was beginning to get very tired of sitting by her sister on the bank, and of having nothing to do: once orR
*\xa0 \xf5:8\x84\x13s\x9c\xbaQ\xbd\x1c,eeped in@o the book her sister was reading, but it had no pictures or conver
sations in it, "and what is the use of a book," thought Alice "without pictures or conversations?"\n'

--- CFB ---
b'Alice was beginning to get very tired of sitting by her sister on the bank, and of having nothing to do: once or
twice s\xfcev$\xe5\xd3.8\xd8-\xb97@\x93\xb6G\\o the book her sister was reading, but it had no pictures or conversa
tions in it, "and what is the use of a book," thought Alice "without pictures or conversations?"\n'
```

Tryb OFB i CTR

- Zamiana jednego bajta powoduje uszkodzenie tylko tego bajta
- Wynika to ze strumieniowej natury tych trybów

```
--- OFB ---
b'Alice was beginning to get very tired of sitting by her sister on the bank, and of having nothing to do: once or
twice s\xdce had peeped into the book her sister was reading, but it had no pictures or conversations in it, "and w
hat is the use of a book," thought Alice "without pictures or conversations?"\n'

--- CTR ---
b'Alice was beginning to get very tired of sitting by her sister on the bank, and of having nothing to do: once or
twice s\xe3e had peeped into the book her sister was reading, but it had no pictures or conversations in it, "and w
hat is the use of a book," thought Alice "without pictures or conversations?"\n'
```

Dziękuję za uwagę