|  |
| --- |
| Politechnika Wrocławska, Informatyka Stosowana |
| BLOKOWE ALGORYTMY SZYFROWANIA |
| Cyberbezpieczeństwo, Laboratorium nr.3 - raport |

|  |
| --- |
| Autor: Aleksander Stepaniuk  Nr. Indeksu: 272644 |

**Zad 1. Przykładowe algorytmy blokowe.**

Teksty których użyłem do analizy kolejnych algorytmów:

**Tekst 1:**

Litera „n” powtórzona 2000 razy.

**Tekst 2:**

Tekst „i potem jeszcze do biedronki na lody” powtórzony 1000 razy.

**Tekst 3:**

5000 pierwszych znaków pana Tadeusza („litwo ojczyzno moja ty jestes jak zdrowie ile cie trzeba cenic ten tylko sie dowie kto cie stracil…”)

Analizie poddałem następujące algorytmy: IDEA, AES, DES

IDEA:

Obraz zawierający zrzut ekranu, tekst, linia

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, Prostokąt, numer

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, numer, dokument

Opis wygenerowany automatycznie

DES (z ECB):

Obraz zawierający tekst, zrzut ekranu, numer, Czcionka

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, numer, linia

Opis wygenerowany automatycznie

AES (z CBC): (128 bitów klucz)

Obraz zawierający tekst, zrzut ekranu, numer, Czcionka

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, numer, linia

Opis wygenerowany automatycznie

**Zadanie 1.1;**

W tabeli poniżej znormalizowano entropię wszystkich tekstów w taki sposób, aby maksymalna możliwa wartość wynosiła 4,70.

|  |  |  |
| --- | --- | --- |
| Entropia tekstów zależnie od algorytmu | | |
| Algorytm | Tekst jawny | Tekst zaszyfrowany |
| IDEA | 0,00 | 1,78 |
| 3,92 | 4,19 |
| 4,25 | 4,67 |
| DES (ECB) | 0,00 | 1,00 |
| 3,92 | 4,24 |
| 4,25 | 4,68 |
| AES (CBC 128 bit klucz) | 0,00 | 4,64 |
| 3,92 | 4,69 |
| 4,25 | 4,67 |

Histogramy dla tekstów jawnych:

Obraz zawierający tekst, zrzut ekranu, wyświetlacz, numer

Opis wygenerowany automatycznieObraz zawierający tekst, zrzut ekranu, wyświetlacz, numer

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, Wykres, linia

Opis wygenerowany automatycznie

Histogramy dla tekstów tajnych z tekstu 1: (kolejno IDEA, DES (ECB), AES (CBC)): Obraz zawierający tekst, zrzut ekranu, numer, linia

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, numer, oprogramowanie

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, linia, Wykres

Opis wygenerowany automatycznie

Histogramy dla tekstów tajnych z tekstu 2: (kolejno IDEA, DES (ECB), AES (CBC)):

Obraz zawierający tekst, zrzut ekranu, linia, Czcionka

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, linia, Czcionka

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, linia, Wykres

Opis wygenerowany automatycznie

Histogramy dla tekstów tajnych z tekstu 3: (kolejno IDEA, DES (ECB), AES (CBC)):

Obraz zawierający tekst, zrzut ekranu, linia, Czcionka

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, linia, Wykres

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, linia, Wykres

Opis wygenerowany automatycznie

**Zadanie 1.2;**

Długości kluczy dla kolejnych algorytmów: (ACC949083C099087DF49807BF0320329)

**IDEA:**

K1 – 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

K2 – 12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78

K3 – AC C9 49 08 3C 09 90 87 DF 49 80 7B F0 32 03 29

**DES (ECB):**

K4 – 00 00 00 00 00 00 00 00

K5 – 12 34 12 34 12 34 12 34

K6 – AC C9 49 08 3C 09 90 87

**AES (CBC):**

K7 – 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

K8 –

11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11

K9 –

AC C9 49 08 3C 09 90 87 DF 39 A9 BC 10 02 05 8B CC 21 99 12 87 B9 F0 71 7A 4B C0 45 3B 89 6B A8

W tabeli poniżej znormalizowano entropię wszystkich tekstów w taki sposób, aby maksymalna możliwa wartość wynosiła 4,70.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Entropia TT oraz TJ zależnie od szyfru, długości i wartości klucza | | | | | | | | | | |
| Szyfr | | **IDEA** | | | **DES (ECB)** | | | **AES (CBC)** | | |
| Klucz | | K1 | K2 | K3 | K4 | K5 | K6 | K7 | K8 | K9 |
| tekst nr. | **TJ** | **TT** | | | | | | | | |
| Tekst1 | 0,00 | 1.19 | 1,78 | 1,78 | 1.76 | 0,00 | 1.76 | 4,64 | 4,64 | 4,64 |
| Tekst2 | 3,92 | 4.16 | 4,27 | 4,29 | 4.23 | 4.31 | 4.26 | 4,69 | 4,69 | 4,69 |
| Tekst3 | 4,25 | 4,51 | 4,67 | 4,68 | 4.68 | 4.68 | 4.67 | 4,68 | 4,68 | 4,68 |

Histogramy:

IDEA, tekst 1:

Obraz zawierający tekst, zrzut ekranu, wyświetlacz, oprogramowanie

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, linia, Wykres

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, linia, Wykres

Opis wygenerowany automatycznie

IDEA, tekst 2:

Obraz zawierający tekst, zrzut ekranu, linia, Wykres

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, linia, Czcionka

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, linia, Wykres

Opis wygenerowany automatycznie

IDEA, tekst 3:

Obraz zawierający tekst, zrzut ekranu, linia, Wykres

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, linia, Wykres

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, linia, Wykres

Opis wygenerowany automatycznie

DES (ECB), tekst 1:

Obraz zawierający tekst, zrzut ekranu, wyświetlacz, numer

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, wyświetlacz, numer

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, wyświetlacz, numer

Opis wygenerowany automatycznie

DES (ECB), tekst 2: Obraz zawierający tekst, zrzut ekranu, linia, Wykres

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, Czcionka, linia

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, linia, Wykres

Opis wygenerowany automatycznie

DES (ECB), tekst 3: Obraz zawierający tekst, zrzut ekranu, Wykres, linia

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, Wykres, Czcionka

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, linia, Wykres

Opis wygenerowany automatycznie

AES (CBC), tekst 1: Obraz zawierający tekst, zrzut ekranu, linia, Czcionka

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, linia, Wykres

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, linia, Wykres

Opis wygenerowany automatycznie

AES (CBC), tekst 2: Obraz zawierający tekst, zrzut ekranu, linia, Wykres

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, linia, Wykres

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, linia, Wykres

Opis wygenerowany automatycznie

AES (CBC), tekst 3: Obraz zawierający tekst, zrzut ekranu, linia, Wykres

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, linia, Równolegle

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, linia

Opis wygenerowany automatycznie

**Pytanie 1.3;**

Algorytmy blokowe są stosowane głównie w kryptografii do szyfrowania danych. Wykorzystuje się je w generatorach liczb pseudolosowych, adresach MAC jak i mechanizmach do sprawdzania integralności danych. Ich podstawowe zastosowania obejmują:

* **Szyfrowanie danych** (np. plików lub wiadomości)
* **Bezpieczeństwo transmisji** w sieciach (np. VPN, HTTPS)
* **Szyfrowanie dysków** (np. BitLocker)
* **Systemy bankowe** i **płatności online** (szyfrowanie danych kart płatniczych)
* **Bezpieczne przechowywanie danych** (w bazie danych w chmurze)

Popularne algorytmy blokowe:

1. **AES (Advanced Encryption Standard)** - najczęściej stosowany algorytm blokowy, uznawany za standard
2. **DES (Data Encryption Standard)** - obecnie uznawany za przestarzały, zastąpiony przez AES
3. **3DES (Triple DES)** - wzmocniona wersja DES, ale powoli wychodzi z użycia
4. **Blowfish** - stosowany w starszych systemach
5. **Twofish** - następca Blowfish, również bezpieczny, ale mniej popularny niż AES

Standardowe i bezpieczne parametry:

* **Długość bloku**: **128 bitów** (AES), choć niektóre algorytmy (np. Blowfish) używają 64-bitowych bloków, co jest uznawane za raczej mniej bezpieczne
* **Długość klucza**: AES obsługuje klucze o długości 128, 192 lub 256 bitów. Długość klucza **128 bitów** jest uznawana za wystarczającą dla większości zastosowań, ale 256-bitowe klucze są stosowane w szczególnie wrażliwych aplikacjach.

**Pytanie 1.4;**

Dla wszystkich algorytmów blokowych entropia wzrosła po zaszyfrowaniu tekstów jawnych. W przypadku tekstu nr. 1 algorytmy DES i IDEA spowodowały najmniejszy wzrost entropii, a zaszyfrowany tekst wciąż posiadał znaki powtarzających się znaków, co widać dokładnie na histogramach dla tego tekstu. Z kolei na AES entropia wzrosła znacząco, zbliżając się za każdym razem do maksymalnej (4,64/4,7 – po przeskalowaniu), a słupki histogramów zdawały się być bardziej wyrównane w swoim rozkładzie, a znaki nie były tak powtarzalne jak dla dwóch poprzednich algorytmów.

Dla tekstu nr. 2 entropia także była wyższa w przypadku użycia AES w porównaniu do DES czy IDEA, ale różnica ta była o wiele mniejsza niż w przypadku tekstu nr. 1. Histogramy dla AES wydają się być bardziej wyrównane, gdzie w przypadku DES i IDEA niektóre znaki występowały znacznie częściej co było bardzo zauważalne na histogramach.

Dla tekstu nr. 3 entropia wzrosła w podobny sposób dla wszystkich algorytmów. Wszystkie histogramy wydają się być zbliżone, niezależnie od użytego algorytmu. IDEA najgorzej zmienia entropię dla klucza składającego się z samych zer (tworzyła widoczne wzniesienie na środku rozkładu). Dla AES zmiana entropii była znacząca, niezależnie od rodzaju klucza czy natury tekstu, a histogramy były wypłaszczone w każdym jego szyfrowaniu.

**Pytanie 1.5;**

Dla niektórych algorytmów klasycznych entropia albo nie ulegała zmianie wcale, albo dla takiego adfgvx nawet malała. Wzrost entropii zależał od długości i poziomu skomplikowania klucza. Histogramy często zachowywały swój kształt, ale były przesunięte, co mogło ujawnić użyty algorytm (np. Cezar).

Dla algorytmów blokowych z kolei entropie rośnie znacząco, co utrudnia łamanie szyfrów prostymi metodami, jak analiza histogramów, które są w tym przypadku dużo bardziej wyrównane w poziomie.

**Pytanie 1.6;**

Dla algorytmu z możliwością zmiany długości klucza AES wydłużenie klucza nie dało żadnej zauważalnej zmiany w entropi. Różnica ta jest prawdopodobnie minimalna i niezauważalna zarówno przy badaniu samego tekstu jak i jego histogramu.

**Pytanie 1.7;**

Dla zaszyfrowanego tekstu entropia w dużej mierze zależy od entropii tekstu jawnego. Jednak dla lepszych algorytmów takich jak AES nie ma to większego znaczenia – entropia pozostaje wysoka, niezależnie od tego czy tekst jawny jest jednorodny czy bardziej złożony.

**Pytanie 1.8;**

Dla szyfrowania IDEA wartość klucza zdecydowanie wpływa na entropię tekstu zaszyfrowanego. Szczególnie jest to widoczne dla klucza K1, gdzie entropia jest nieco niższa od pozostałych kluczy dla tego algorytmu. Natomiast w pozostałych kluczach zmiana klucza nie miała znacznego wpływu na entropię tekstu.

**Pytanie 1.9;**

Dla wszystkich algorytmów szyfrujących entropia tekstu zaszyfrowanego była zależna od użytego algorytmu. AES powodował zwiększenie entropii do wartości zbliżonej do tej maksymalnej (4,70 po przeskalowaniu) niezależnie długości klucza czy rodzaju szyfrowanego tekstu. Dla DES oraz IDEA widać było bardzo silną zależność między entropią tekstu jawnego a tajnego. Algorytmy te radziły sobie o wiele gorzej z szyfrowaniem tekstów nr. 1 i nr. 2 niż tekstu nr. 3 ze względu na ich większą jednorodność.

**Zad 2. Tryby pracy algorytmów blokowych.**

**Zadanie 2.1-2.4;**

Użyłem poniższych tekstów do kolejnych zadań:

**Tekst 1:**

Litera „n” powtórzona 2000 razy.

Do analizy wybrałem algorytm AES, w wariancie 128-bitowym.

Klucz: B3 A4 09 34 3B C2 72 7B 34 C9 FF 87 96 05 3A F2

Wektor: 2B 17 A8 3B 91 C9 4F 37 E1 29 4D 79 12 A4 79 A1

ECB:  
Entropia: 4,05/8 (niska), widoczne powtórzenia tekstu, histogram zdecydowanie nierównomierny.

Obraz zawierający tekst, zrzut ekranu, wzór, Prostokąt

Opis wygenerowany automatycznieObraz zawierający tekst, zrzut ekranu, numer, Czcionka

Opis wygenerowany automatycznieObraz zawierający tekst, zrzut ekranu, Wykres, linia

Opis wygenerowany automatycznie

CBC:  
Entropia: 7,9/8 (wysoka), brak widocznych powtórzeń tekstu, histogram wyrównany

Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, numer, Czcionka

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, Wykres, linia

Opis wygenerowany automatycznie

OFB:  
Entropia: 7,89/8 (wysoka), brak widocznych powtórzeń tekstu, histogram wyrównany

Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, numer, Czcionka

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, Wykres, linia

Opis wygenerowany automatycznie

CFB:  
Entropia: 7,91/8 (wysoka), brak widocznych powtórzeń tekstu, histogram wyrównany (początek tekstu taki sam jak OFB)

Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, numer, Czcionka

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, linia, Wykres

Opis wygenerowany automatycznie

Wnioski:

Najgorzej z zaszyfrowaniem tekstu nr. 1 poradził sobie ECB, wyraźnie widać powtarzające się 128bitowe bloki tekstu. CBC, OFB i CFB są jednak dużo lepsze i nie da się zauważyć natury tekstu jednorodnego (wysoka entropia, wyrównane histogramy)

**Zadanie 2.5;**

Użyłem poniższego tekstu:

**Tekst 4:**

„litwo ojczyzno moja ty jestes jak zdrowie ile cie trzeba cenic ten tylko sie dowie kto cie stracil dzis pieknosc twa w calej ozdobie widze i opisuje bo tesknie po tobie panno swieta co jasnej bronisz czestochowy i w ostrej swiecisz bramie ty co grod zamkowy nowogrodzki ochraniasz z jego wiernym ludem jak mnie dziecko do zdrowia powrocilas cudem gdy od placzacej matki pod twoje opieke ofiarowany martwa podnioslem powieke i zaraz moglem pieszo do twych swiatyn progu isc za wrocone zycie podziekowac bogu”

Do analizy wybrałem algorytm AES, w wariancie 128-bitowym.

Klucz: B3 A4 09 34 3B C2 72 7B 34 C9 FF 87 96 05 3A F2

Wektor: 2B 17 A8 3B 91 C9 4F 37 E1 29 4D 79 12 A4 79 A1

**ECB:**

Obraz zawierający tekst, zrzut ekranu, Czcionka, linia

Opis wygenerowany automatycznie Obraz zawierający tekst, Czcionka, linia, zrzut ekranu

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, Czcionka, linia

Opis wygenerowany automatycznie

Dla zmienionego jednego bitu, po odszyfrowaniu zmieniony jest 16-znakowy fragment tekstu, pozostała część jest nienaruszona. Dla zmienionych kilku bitów w różnych bajtach, to gdy są one w jednej 128-bitowej grupie, to zmienia się tylko jeden 16-znakowy fragment, zaś gdy zmieniane bity są w odległości większej niż 128 bitów, to zmienianych jest klika grup 16-znakowych (do których należą zmienione bity), pozostała część tekstu nie ulega zmianie.

**CBC:**

**Obraz zawierający tekst, Czcionka, linia, zrzut ekranu

Opis wygenerowany automatycznieObraz zawierający tekst, Czcionka, linia, zrzut ekranu

Opis wygenerowany automatycznie**

(zmiany są identyczne jak dla ECB)

**OFB:**

**Obraz zawierający tekst, zrzut ekranu, Czcionka, linia

Opis wygenerowany automatycznie** **Obraz zawierający tekst, zrzut ekranu, Czcionka, linia

Opis wygenerowany automatycznie**Obraz zawierający tekst, zrzut ekranu, Czcionka, linia

Opis wygenerowany automatycznie

Zmianie ulegają tylko te specyficzne znaki, w których były zmienione bity. Pozostałe znaki pozostają bez zmian.

**CFB:**

**Obraz zawierający tekst, zrzut ekranu, Czcionka, linia

Opis wygenerowany automatycznie** **Obraz zawierający tekst, zrzut ekranu, Czcionka, linia

Opis wygenerowany automatycznie**

Przy każdej zmianie pojedynczego bitu, po odszyfrowaniu zmienia się blok tekstu, znajdujący się w okolicy zmienionego bitu. Jeśli zmienionych zostanie kilka bitów w różnych bajtach, to zmienia się kilka bloków tekstu. Natomiast gdy zmiany dotyczą bitów leżących bliżej siebie, zmienia się tylko jeden blok tekstu, a reszta pozostaje bez zmian. Bloki nie zmieniają się równomiernie, bo np. po zmianie pierwszego bitu:  
Obraz zawierający tekst, zrzut ekranu, Czcionka, linia

Opis wygenerowany automatycznieZmianie uległ fragment „litwo” oraz „moja ty jesteś jak”, ale zmianie nie uległa „ojczyzno”.

**Zadanie 2.6;**