|  |
| --- |
| 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 ja jechalem na rowerze 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 |
| 4,01 | 4,19 |
| 4,25 | 4,67 |
| DES (ECB) | 0,00 | 1,00 |
| 4,01 | 4,24 |
| 4,25 | 4,68 |
| AES (CBC 128 bit klucz) | 0,00 | 4,64 |
| 4,01 | 4,69 |
| 4,25 | 4,67 |

Histogramy: