Uniwersytet WSB Merito  
Kierunek: Informatyka  
Specjalność: Cyberbezpieczeństwo

Rok akademicki: 2024/2025  
semestr letni

**Analiza szyfrów symetrycznych z wykorzystaniem narzędzia CrypTool**

Wykonał: Maciej Niemiec

Numer albumu: 107162



# **Wprowadzenie**

Bezpieczeństwo informacji jest jednym z fundamentalnych elementów współczesnych systemów teleinformatycznych, a szyfrowanie danych odgrywa kluczową rolę w zapewnianiu poufności, integralności i dostępności informacji. W ramach drugiego laboratorium z przedmiotu ***Cyberbezpieczeństwo*** analizowano działanie wybranych szyfrów symetrycznych, takich jak DES, AES czy IDEA, ze szczególnym uwzględnieniem ich właściwości kryptograficznych oraz wpływu struktury danych wejściowych na jakość szyfrowania.

Zajęcia miały na celu zrozumienie zasad funkcjonowania szyfrów blokowych oraz oceny ich efektywności z punktu widzenia entropii – czyli miary nieprzewidywalności danych. W tym celu przygotowano trzy różne teksty jawne o zróżnicowanej entropii (jednorodny, średnio zróżnicowany i wysoko zróżnicowany), które następnie szyfrowano przy użyciu różnych algorytmów i konfiguracji. Porównanie histogramów oraz wartości entropii przed i po szyfrowaniu pozwoliło na lepsze zrozumienie mechanizmów działania szyfrów symetrycznych i ich odporności na analizę statystyczną.

W dalszej części laboratorium analizowano wpływ trybu pracy szyfratora (ECB i CBC) na strukturę kryptogramu, a także przeprowadzono eksperymenty związane z modyfikacjami szyfrogramów – w tym zmianą pojedynczych bitów oraz manipulacją długością danych. Szczególną uwagę poświęcono także wpływowi długości klucza oraz rodzaju algorytmu na wynik szyfrowania.

Zajęcia wpisują się w szerszy kontekst zagadnień omawianych na wykładach, takich jak ochrona informacji, identyfikacja zagrożeń w cyberprzestrzeni oraz praktyczne aspekty stosowania kryptografii w systemach informatycznych. Laboratorium to miało również na celu rozwijanie umiejętności praktycznej oceny bezpieczeństwa różnych metod kryptograficznych, zgodnie z aktualnymi standardami i wymaganiami bezpieczeństwa teleinformatycznego

# **Część Laboratoryjna**

## **Zadanie 1.**

### **Załcznik – Tekst jednorodny**

### **Załacznik - Tekst średnio zróżnicowany**

### **Załacznik - Tekst wysoce zróżnicowany**

### **Dla kilku ustalonych tekstów jawnych o różnych entropiach (np. tekst jednorodny, tekst średnio zróżnicowany, tekst bardzo zróżnicowany) porównać entropię tekstu jawnegoz entropią po zaszyfrowaniu (entropią tekstu tajnego)**

**Szyfr IDEA**

1. Tekst jednorodny

Tekst zawierał wyłącznie powtarzający się znak „a”, co skutkuje całkowitym brakiem różnorodności danych.

**Entropia tekstu jawnego:** 0.00 (maksymalna możliwa: 4.70)

Obraz zawierający tekst, oprogramowanie, Strona internetowa, Oprogramowanie multimedialne

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 1 - Wynik programu CrypTool dla tekstu jawnego pliku jednorodny.txt

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, linia

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 2 - Histogram wartości tekstu jawnego w pliku jednorodny.txt

**Entropia po szyfrowaniu (IDEA):** 3.06 / 8.00

Obraz zawierający tekst, numer, Czcionka, oprogramowanie

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 3 - Wynik programu CrypTool dla szyfrowania IDEA pliku jednorodny.txt

Obraz zawierający tekst, zrzut ekranu, linia, numer

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 4 - Histogram wartości dla szyfrowania IDEA pliku jednorodny.txt

Pomimo skrajnie niskiej entropii danych wejściowych, algorytm IDEA skutecznie zwiększył różnorodność danych wyjściowych, co jest pożądane z punktu widzenia bezpieczeństwa – świadczy to o dobrej dyfuzji i zatarciu wzorców danych wejściowych.

1. Tekst średnio zróżnicowany

Tekst zawierał powtarzające się frazy („agree all use city with model…”).

**Entropia tekstu jawnego:** 3.80 / 4.70

Obraz zawierający tekst, oprogramowanie, Strona internetowa, Czcionka

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 5 - Wynik programu CrypTool dla tekstu jawnego pliku sredni.txt

Obraz zawierający tekst, zrzut ekranu, Wykres, linia

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 6 - Histogram wartości tekstu jawnego w pliku sredni.txt

**Entropia po szyfrowaniu (IDEA):** 4.25 / 8.00

Obraz zawierający tekst, zrzut ekranu, numer, Czcionka

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 7 - Wynik programu CrypTool dla szyfrowania IDEA pliku sredni.txt

Obraz zawierający tekst, zrzut ekranu, linia, Wykres

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 8 - Histogram wartości tekstu dla szyfrowania IDEA w pliku sredni.txt

Tekst o średnim poziomie entropii został zaszyfrowany w sposób zwiększający jego złożoność. Histogram po szyfrowaniu pokazuje większe rozproszenie bajtów, co oznacza skuteczne maskowanie powtarzalnych wzorców.

1. Tekst wysoce zróżnicowany

Naturalny tekst o dużej różnorodności słów, znaków i struktury językowej.

**Entropia tekstu jawnego:** 4.27 / 4.70

Obraz zawierający tekst, oprogramowanie, Strona internetowa, Czcionka

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 9 - Wynik programu CrypTool dla tekstu jawnego pliku bardzo.txt

Obraz zawierający tekst, zrzut ekranu, Wykres, linia

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 10 - Histogram wartości tekstu jawnego w pliku bardzo.txt

**Entropia po szyfrowaniu (IDEA):** 4.95 / 8.00

Obraz zawierający tekst, numer, Czcionka, linia

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 11 - Wynik programu CrypTool dla szyfrowania IDEA pliku bardzo.txt

Obraz zawierający tekst, zrzut ekranu, linia, Wykres

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 12 - Histogram wartości tekstu po szyfrowaniu IDEA w pliku bardzo.txt

Dla danych wejściowych o wysokiej entropii algorytm IDEA nieznacznie zwiększył entropię danych wyjściowych, co oznacza, że tekst jawny był już bardzo trudny do przewidzenia, ale szyfrowanie dodatkowo zwiększyło jego losowość.

Szyfr DES

Dla porównania skuteczności algorytmu DES (Data Encryption Standard) w trybie CBC, zaszyfrowano te same trzy teksty jawne co w przypadku algorytmu IDEA – o różnym poziomie entropii: tekst jednorodny, średnio zróżnicowany i wysoce zróżnicowany. Dla każdego z nich obliczono entropię tekstu zaszyfrowanego i przeanalizowano histogram rozkładu bajtów.

1. Tekst jednorodny

**Entropia tekstu jawnego:** 0.00 / 4.70

**Entropia po szyfrowaniu (DES CBC):** 7.81 / 8.00

Obraz zawierający tekst, zrzut ekranu, numer, Czcionka

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 13 - Wynik programu CrypTool dla szyfrowania DES pliku jednorodny.txt

Obraz zawierający tekst, zrzut ekranu, linia, Wykres

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 14 - Rozkład bajtów jest równomierny, nie wykazuje powtarzalnych wzorców.

DES skutecznie zaciera strukturę danych nawet w przypadku skrajnie jednorodnych danych wejściowych. Entropia wzrosła niemal do maksimum, co wskazuje na wysoki poziom nieprzewidywalności danych wyjściowych.

1. Tekst średnio zróżnicowany

**Entropia tekstu jawnego:** 3.80 / 4.70

**Entropia po szyfrowaniu (DES CBC):** 7.83 / 8.00

Obraz zawierający tekst, numer, Czcionka, oprogramowanie

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 15 - Wynik programu CrypTool dla szyfrowania DES pliku sredni.txt

Obraz zawierający tekst, zrzut ekranu, linia, Wykres

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 16 - Podobnie jak w przypadku tekstu jednorodnego, histogram prezentuje równomierny rozkład bajtów.

Również w przypadku danych o umiarkowanej różnorodności DES w trybie CBC osiąga wysoki poziom losowości kryptogramu.

1. Tekst wysoce zróżnicowany

**Entropia tekstu jawnego:** 4.27 / 4.70

**Entropia po szyfrowaniu (DES CBC):** 7.87 / 8.00

Obraz zawierający tekst, numer, Czcionka, linia

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 17 - Wynik programu CrypTool dla szyfrowania DES pliku bardzo.txt

Obraz zawierający tekst, zrzut ekranu, linia, Wykres

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 18 - Rozkład jest równomierny i losowy, charakterystyczny dla skutecznie zaszyfrowanego strumienia bajtów.

Dla tekstów o już wysokiej entropii, szyfrowanie DES w trybie CBC nadal potrafi zwiększyć nieprzewidywalność danych, zbliżając entropię do teoretycznego maksimum.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| |  | | --- | | **Typ tekstu** | | |  | | --- | | **Entropia jawna** |  |  | | --- | |  | | Entropia po szyfrowaniu (DES CBC) |
| |  | | --- | | Jednorodny | | |  | | --- | | 0.00 |  |  | | --- | |  | | 7.81 |
| |  | | --- | | Średnio zróżnicowany | | |  | | --- | | 3.80 | | |  | | --- | | 7.83 | |
| |  | | --- | | Wysoce zróżnicowany | | |  | | --- | | 4.27 | | |  | | --- | | 7.87 | |

### **Porównać parametry szyfrowania (długość klucza) i zbadać ich wpływ na tekst tajny (np. na jego entropię). Należy w tym punkcie zaszyfrować dany tekst korzystając z różnych dostępnych długości i wartości klucza.**

## **Pytania / Wnioski**

# **Podsumowanie**

1. Tekst jednorodny
2. Tekst średnio zróżnicowany
3. Tekst wysoce zróżnicowany