**Wrocław, 01.10.2024**

**cyberbezpieczeństwo**

**Laboratorium nr3**

**Blokowe algorytmy szyfrowania**

**Plan zajęć**

[I. Wstęp.](#_Toc142225863)

[II. Zapoznanie się ze środowiskiem pracy - program CrypTool.](#_Toc142225864)

[III. Zadania](#_Toc142225865)

[1. Przykładowe algorytmy blokowe.](#_Toc142225866)

[2. Tryby pracy algorytmów blokowych.](#_Toc142225867)

[IV. Raport z przeprowadzonych eksperymentów.](#_Toc142225868)

# Wstęp.

Laboratorium obejmuje zagadnienia związane z szyfrowaniem symetrycznym - szyfry strumieniowe i blokowe. Ponadto algorytmy będą przedmiotem analizy pod kątem sposobu szyfrowania danych.

Kryptografia klucza symetrycznego jest znana pod różnymi terminami, takimi jak kryptografia klucza tajnego lub kryptografia klucza prywatnego. Algorytmy klucza symetrycznego mają tylko jeden klucz, który jest używany zarówno do szyfrowania, jak i deszyfrowania wiadomości. Dlatego podczas odbierania wiadomości nie jest możliwe jej odszyfrowanie, chyba że odbiorca zna klucz.

Istnieje jednak kilka problemów z algorytmami klucza symetrycznego, pierwszy to problem z dystrybucją kluczy. Chodzi o to, jak odebrać klucz od nadawcy. Odbiorca musi osobiście spotkać się z nadawcą, aby odebrać klucz albo klucz musi zostać wysłany do odbiorcy, a tym samym dostęp do niego mają osoby nieuprawnione. Jest to główny problem kryptografii klucza symetrycznego i nazywany jest problemem dystrybucji lub wymiany kluczy i jest nieodłącznym elementem kryptografii klucza symetrycznego.

Drugi problem jest również bardzo poważny. Załóżmy, że Alicja chce komunikować się zarówno z Bobem, jak i z Johnem. Powinien istnieć jeden klucz do całej komunikacji między Alicją a Bobem i inny klucz do całej komunikacji między Alicją a Janem. Ten sam klucz, który jest używany między Alicją i Bobem, nie może być używany do komunikacji między Alicją i Janem, ponieważ w takiej sytuacji istnieje szansa, że ​​John może zinterpretować wiadomości przekazywane między Alicją i Bobem. W przypadku dużej ilości wymiany danych staje się to niepraktyczne, ponieważ każda para nadawców i odbiorców wymagałaby oddzielnego klucza.

W kryptografii z kluczem symetrycznym ten sam algorytm jest używany przez nadawcę i odbiorcę. Jednak klucz od czasu do czasu powinien być zmieniany. Ten sam zwykły tekst zaszyfrowany różnymi kluczami prowadzi do innego tekstu zaszyfrowanego. Ponieważ algorytm szyfrowania jest publicznie dostępny, powinien być wystarczająco silny, aby uniemożliwić atakującemu odszyfrowanie zaszyfrowanego tekstu.

**Szyfr strumieniowy** - szyfr strumieniowy to taki, który szyfruje cyfrowy strumień danych po jednym bicie lub jednym bajcie. Odszyfrowywanie również odbywa się pojedynczo. Przykładem szyfru strumieniowego jest szyfr RC4.

**Szyfr blokowy** - w szyfrze blokowym blok zwykłego tekstu jest traktowany jako całość i używany do tworzenia bloku tekstu zaszyfrowanego o równej długości. Zwykle używany jest rozmiar bloku 64, 128 lub 256 bitów. Deszyfrator pobiera jednocześnie jeden cały blok zaszyfrowanych danych. Problem z szyframi blokowymi występuje, gdy występują powtarzające się wzorce tekstowe. Ponieważ ten sam szyfr jest generowany dla tych samych zwykłych tekstów, daje to kryptoanalitykowi wskazówkę dotyczącą oryginalnego zwykłego tekstu. Kryptoanalityk może szukać powtarzających się ciągów i próbować je złamać, a zatem istnieje szansa, że ​​duża część oryginalnej wiadomości może zostać odczytana. Aby uniknąć tego problemu, szyfry blokowe są używane w różnych trybach pracy, np. trybie łańcuchowym. W tym trybie poprzedni szyfr blokowy jest mieszany z bieżącym blokiem, aby zaciemnić zaszyfrowany tekst. Pozwala to uniknąć powtarzających się wzorów bloków z tymi samymi prostymi tekstami.

# Zapoznanie się ze środowiskiem pracy - program CrypTool.

* Podczas zajęć laboratoryjnych będą wykorzystywane głównie narzędzia dostępne z zakładki z programu CrypTool:
  + *Szyfrowanie/Symetryczne*
* *Cryptool zawiera tylko dwa tryby działania (CBC i ECB). OFB i CFB są dostępne w narzędziu do szyfrowania online. Szczegółowy opis poniżej:*
  + AES (CBC)
  + DES (CBC, ECB),
  + 3DES (CBC,ECB),
* *Online Encryption Tool –*

*https://encode-decode.com/:*

* + *AES (CBC,ECB, OFB, CFB),*
  + *DES (CBC,ECB, OFB, CFB),*
* *Przydać się może również edytor hexadecymalny*(np. HxD*)*

# Zadania

## Przykładowe algorytmy blokowe.

Proszę zapoznać się z demonstracją ilustrującą zasadę działania algorytmu DES. Zakładka: *Algorytmy/Wizualizacja algorytmów/DES*

Przygotuj trzy teksty o różnej entropii, każdy o długości co najmniej 1000 znaków:

* tekst jednorodny (np. tylko jeden znak - "hhhhhhhhhhhhhhhhhhhh...")
* tekst średnio zróżnicowany (np. powtarzające się ciągi znaków/słowa - "agree all use city with model agree all use city with model agree all use city with model ...."),
* tekst wysoce zróżnicowany (np. tekst normalny - ""Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis ..."),

Proszę dla kilku wybranych algorytmów blokowych[[1]](#footnote-1) (np. IDEA, DES, TripleDES, AES, Twofish, MARS, SERPENT,...) wykonać następujące operacje:

**Zadania:**

### Dla kilku ustalonych tekstów jawnych (TJ) o różnych entropiach (np. tekst jednorodny, tekst średnio zróżnicowany, tekst bardzo zróżnicowany) porównać entropię TJ z entropią po zaszyfrowaniu (entropią tekstu tajnego TT). Proszę przyjrzeć się również histogramom TT i TJ.

### Zaszyfruj dany tekst jawny korzystając z różnych dostępnych długości i wartości klucza, sprawdź, które algorytmy oferują zmianę długości klucza. Porównaj otrzymane wyniki jak zmiana parametrów wpływa na entropie TT..

**Pytania/Wnioski:**

### Gdzie obecnie stosowane są algorytmy blokowe? Które algorytmy są najbardziej popularne? Jakie wartości parametrów (długość bloku, długość klucza) uznaje się współcześnie za standardowe (bezpieczne)?

### Co możemy powiedzieć o obserwowanych zmianach w histogramach i wartościach entropii podczas realizacji powyższych zadań?

### Co możemy powiedzieć o tych wartościach w kontekście podobnych ćwiczeń realizowanych dla algorytmów historycznych (klasycznych)?

### Czy długość klucza wpływa na entropię TT?

### Czy obserwowana entropia TT zależy od entropii TJ?

### Czy obserwowana entropia TT zależy od wartość klucza?

### Czy obserwowana entropia TT zależy od użytego algorytmu?

## Tryby pracy algorytmów blokowych.

**Zadania:**

### Proszę wygenerować plik tekstowy z cyklicznie powtarzającą się zawartością (np. może to być plik zawierający jedynie litery – „A”, ciągi – „abcd”, itp.)[[2]](#footnote-2).

### Proszę wybrać jeden z dostępnych algorytmów szyfrowania oraz tekst zróżnicowany. Zaszyfruj TJ korzystając z różnych trybów pracy szyfratora, tzn. utworzyć kryptogram dla trybów: ECB, CBC,OFB,CFB

### Proszę obejrzeć histogramy i obliczyć entropię dla tak utworzonych TT.

### Proszę obejrzeć zawartość kryptogramu i ocenić przydatność każdego trybu pracy szyfratora do szyfrowania plików składających się z powtarzających się bloków bajtów.

### Zaszyfruj za pomocą algorytmu AES lub DES zaszyfruj tekst jawny (tekst zróżnicowany).

##### zmień po jednym lub kilka bitów w różnych bajtach (blisko lub daleko od siebie),

##### dodanie jednego bajtu,

##### usunięcie jednego bajtu,

##### dodaj/ usuń fragmentu tekstu równego długości bloku algorytmu,

Odszyfruj szyfrogramy i sprawdzić ich zawartość.

### Proszę spróbować dla poniższych kryptogramów zidentyfikować i umotywować swoją decyzję odnośnie użytego:

##### trybu pracy algorytmu (ECB,CBC,OFB,CFB),

##### długości bloku algorytmu,

685c281585d8c0eeb59022def8488a78

685c281585d8c0eeb59022def8488a78

685c281585d8c0eeb59022def8488a78

685c281585d8c0eeb59022def8488a78

685c281585d8c0eeb59022def8488a78

685c281585d8c0eeb59022def8488a78

685c281585d8c0eeb59022def8488a78

43d9f1d44ebea3e411ad70dd41b2c24e

af20e9491c13f9d419862d7f1bceca14

43d9f1d44ebea3e411ad70dd41b2c24e

af20e9491c13f9d419862d7f1bceca14

43d9f1d44ebea3e411ad70dd41b2c24e

af20e9491c13f9d419862d7f1bceca14

43d9f1d44ebea3e411ad70dd41b2c24e

af20e9491c13f9d419862d7f1bceca14

43d9f1d44ebea3e411ad70dd41b2c24e

af20e9491c13f9d419862d7f1bceca14

6a239123a19647032e3e637ab0b02d56

26b593edf8445c07e9e79e408ec89e56

16d9e89bef28c92d61ab6d82d39921ac

8109e9d03dafd2fd6416a0ba97513ede

0615a2688a785319d75d95a4a9aed55e

e6c221cfa51d7e89f93a5dfbc4a2bc22

368ecba0bd42c8f56c2710723b883e5

**Pytania/Wnioski:**

### Jak wyglądają kryptogramy i ich entropie dla tekstu jawnego o jednorodnej strukturze w zależności od wybranego trybu szyfrowania?

### Jak propagują się błędy z kryptogramu do tekstu jawnego przy deszyfracji TT z przekłamanym bitem/wieloma bitami (odpowiedź zilustruj odpowiednimi przykładami).

### Jak poszczególne tryby pracy algorytmów blokowych radzą sobie z utratą części wiadomości. Tzn. jaka jest możliwość odtworzenia TJ na podstawie TT z którego usunięto część zawartości (odpowiedź zilustruj odpowiednimi przykładami).

### Dla jakich zastosowań możemy wykorzystać tryby pracy: ECB, CBC?

### W przypadku których trybów proces szyfrowania/deszyfrowania można prowadzić równolegle? W przypadku którego trybu pracy można podzielić TT/TJ na kilka niezależnych części które będą deszyfrowane/szyfrowane równolegle na kilku komputerach, a następnie połączone dadzą ten sam rezultat co w przypadku realizowania całego procesu na jednym stanowisku.

# Raport z przeprowadzonych eksperymentów.

Raport powinien mieć postać dokumentu elektronicznego, w którym zostanie zapisany przebieg realizowanych w trakcie zajęć eksperymentów (np. fragment treści tekstu jawnego, parametry algorytmu szyfrowania, fragment kryptogramu) oraz wnioski, spostrzeżenia, odpowiedzi na pytania umieszczone w instrukcji laboratoryjnej, itp.

1. Minimalnie 2 różne algorytmy. Proszę się zastanowić, korzystając z opisu wybranych algorytmów, na ile wybrane algorytmy są „podobne”. [↑](#footnote-ref-1)
2. Przy szyfrowaniu proszę zaznaczyć opcję „Plaintext”, zaś przy deszyfrowaniu „Hex” [↑](#footnote-ref-2)