# BEZPIECZEŃSTWO SYSTEMÓW KOMPUTEROWYCH

Wykład 5

### 5.1. Wstęp

### Pvtania:

- Jaki zasób w systemach komputerowych jest najważniejszy (najcenniejszy)?
- Jaki jest najczęstszy powód ataków na systemy komputerowe?
- Jaki jest najskuteczniejszy sposób dzięki któremu możemy zapobiegać ujawnieniu lub modyfikacji informacji? Jak nazywa się dziedzina wiedzy dająca nam narzędzia ochrony?
- Co jest (powinno byé) standardowym elementem współczesnych aplikacji?
- Co jest (powinno byé) standardowym elementem współczesnych sieci teleinformatycznych?

5. Techniki ochrony kryptograficznej
(wybrane zagadnienia)

- 1. Wste
- 2. Klucze kryptograficzne
- 3. Algorytmy szyfrowania
  - 1. Szyfrowanie kluczem symetrycznym
  - 2. Szyfrowanie kluczem asymetrycznym

2

# 5.1.1. trochę faktów z historii

### Ważne daty

- Ok. 1900 p.n.e pierwsze odkryte w inskrypcjach grobowych przykłady przekształceń kryptograficznych
- Ok. 475 r p.n.e pierwsze zastosowanie szyfrowania w celach przekazania informacji (łączność w Sparcie)
- Ok. 60 p.n.e pierwsze wzmianki o zastosowaniu tzw. "szyfru Cezara"
- 1412 pierwszy znany traktat o kryptologii napisany przez egipskiego prawnika i uczonego Kalkashandi
- 1971 firma IBM stworzyła system szyfrowania Lucifer
- 1975 opracowanie przez IBM standardu DES na zlecenie Narodowego Biura Standardów USA (obecnie NIST)
- 1976 Diffie i Hellman koncepcja szyfrowania asymetrycznego
- 1978 Rivest, Shamir, Adelman algorytm RSA
- 1991 James L.Massey i Xuejia Lai algorytm IDEA
- 1997 Vincent Rijmen i Joan Daemen opracowali AES (Rijandael).

### 5.1.2 Podstawowe pojęcia

### kryptologia:

( z języka greckiego - *kryptos* - "ukryty" i logos - "słowo") - jest to dziedzina wiedzy traktująca o sposobach przekazywania informacji zabezpieczonej przed niepowołanym dostępem.

5

# 5.1.2 Podstawowe pojęcia kryptologia kryptografia kryptoanaliza

### 5.1.2 Podstawowe pojęcia

### kryptografia:

- sztuka zabezpieczania wiadomości
- wiedza o budowie i działaniu systemów kryptograficznych

7

### 5.1.2 Podstawowe pojęcia

### kryptoanaliza:

 dziedzina wiedzy zajmująca się łamaniem szyfrów (odczytywaniem zaszyfrowanych wiadomości bez znajomości kluczy rozszyfrowujących)

### 5.1.2 Podstawowe pojęcia

### kryptogram:

- jest to zaszyfrowana postać czytelnej wiadomości
- zwany jest także szyfrogramem

9

### 5.1.2 Podstawowe pojęcia

### klucz szyfrujący:

 ciąg znaków służących do zaszyfrowania wiadomości czytelnej w kryptogram za pomocą algorytmu szyfrowania

### klucz deszyfrujący:

 ciąg znaków służących do rozszyfrowania kryptogramu do wiadomości czytelnej, przy wykorzystaniu algorytmu deszyfrowania

11

### 5.1.2 Podstawowe pojęcia

### szyfrowanie:

 proces, podczas którego wiadomość jawna jest przekształcana w tekst zaszyfrowany (kryptogram) przy pomocy funkcji matematycznych oraz klucza

### klucz kryptograficzny:

• ciąg symboli (hasło) od którego zależy wynik przekształcenia kryptograficznego

10

### 5.1.2 Podstawowe pojęcia

### Przestrzeń kluczy kryptograficznych:

 Jest to zbiór wszystkich kluczy kryptograficznych o zadanej długości

Jaka jest zależność ilości możliwych kombinacji od długości klucza?

### 5.1.2 Podstawowe pojęcia

Jaka jest zależność ilości możliwych kombinacji od długości klucza?

Długość klucza w bitach	Ilość kombinacji
40	$2^{40} = 1,1 * 10^{12}$
56	$2^{56} = 7,2 * 10^{16}$
128	$2^{128} = 3.4 * 10^{38}$
512	$2^{512} = 1.3 * 10^{154}$
1024	$2^{1024} = 1.8 * 10^{308}$

13

### 5.2 Klucze kryptograficzne

**Historyczne metody kryptograficzne:** 

- tajny współdzielony algorytm przekształcania
- tajny współdzielony klucz

Współczesne metody kryptograficzne:

- jawność algorytmu przekształcania
- tajny klucz kryptograficzny (lepszy dłuższy)
- odporność na atak ze spreparowanym tekstem jawnym

15

### 5.1.3 Zastosowanie kryptografii

- ochrona informacji przechowywanych w systemach komputerowych
- ochrona informacji przesyłanych w i pomiędzy systemami komputerowymi
- potwierdzanie tożsamości użytkownika systemu
- potwierdzanie tożsamości aplikacji (procesu) żądającego obsługi
- ochrona przed nieautoryzowaną modyfikacją
- wiele innych...

14

### 5.2 Klucze kryptograficzne

Liczba N wszystkich sprawdzeń niezbędnych do odgadnięcia właściwego klucza, to liczba wszystkich możliwych kluczy o długości M:

$$N = B^M$$

\* (B - podstawa, dla dwójkowego B = 2, dla systemu dziesiętnego B = 10 itd.)

Wydłużenie klucza o jedną pozycję zwiększa pulę możliwych kluczy B-krotnie (liczba ta rośnie wykładniczo).

### 5.2 Klucze kryptograficzne

Zależność pomiędzy długością klucza M a liczbą wszystkich kluczy N w systemie binarnym:

Długość klucza (M)	Liczba kluczy (N)	Długość klucza (M)	Liczba kluczy (N)
1	2	16	65 536
2	4	32	4 294 967 296
3	8	64	1,84467 E+19
4	16	128	3,40282 E+38
8	256	256	1,15792 E+77

17

### 5.2 Klucze kryptograficzne

Teoretycznie tyle czasu potrzebujemy na złamanie klucza:

Długość klucza (M)	Oczekiwany czas odgadnięcia: jeden komputer z zegarem 4GHz	Oczekiwany czas odgadnięcia: milion komputerów z zegarem 4GHz
8	0,000064 s	0,000000000064 s
32	1,19 h	0,004 s
56	571 lat	5 h
64	146 235 lat	53 dni
96	2,5 E15 lat	2 512 308 552 lat
128	1,8 E25 lat	1,08 E19 lat
256	3,67 E63 lat	3,67 E57 lat

5.2 Klucze kryptograficzne

Szacowanie czasu potrzebnego do poznania klucza:

- Zakładamy, że atakujący trafi na właściwy klucz już po N/2 sprawdzeń
- czas sprawdzenia to suma:
  - czasu wykonania pełnego algorytmu dla sprawdzanego klucza
  - czasu na analizę uzyskanego wyniku
- sprawdzenie klucza i analiza wyników to od kilku do kilkunastu tysięcy taktów zegara (przyjmijmy tysiąc)

Ile czasu potrzebujemy na złamanie klucza?

18

### 5.2 Klucze kryptograficzne

Jeśli policzymy, że od początku istnienia wszechświata do dnia dzisiejszego upłynęło w przybliżeniu około 5 E17 sekund, to możemy mieć dość dokładne wyobrażenie o tym, jaki jest poziom bezpieczeństwa zapewnianego przez stosowane współcześnie algorytmy ochrony danych.

By lepiej to widzieć załóżmy, że od początku świata milion komputerów z procesorami 4 GHz próbuje odgadnąć klucz kryptograficzny - do chwili obecnej zadanie to zostałoby rozwiązane jedynie dla przypadku kluczy o długości nie większej niż 96 bitów.

### 5.2 Klucze kryptograficzne

Czy jest możliwe, że jedna osoba (instytucja) będzie dysponować milionem (lub więcej) komputerów?

Czy to zadanie jest zadaniem prostym?

21

### 5.2 Klucze kryptograficzne

Podstawowym celem ataku na szyfr jest odgadnięcie używanego do ochrony informacji klucza.

W kryptografii mówi się o trzech rodzajach takich ataków:

- atak bez tekstu jawnego
- atak z tekstem jawnym
- atak ze spreparowanym tekstem jawnym

23

### 5.2 Klucze kryptograficzne

### Pomysł (już wykorzystany):

- napiszmy program, który pełni powszechnie pożądane i pożyteczne funkcje
- umieśćmy w tym programie działającą w tle, ukryta funkcję sprawdzania kluczy
- rozpowszechnijmy za darmo ww. program w internecie

22

### 5.2 Klucze kryptograficzne

Jednym z najważniejszych założeń współczesnych technik kryptograficznych była konieczność zapewnienia odporności na atak ze spreparowanym tekstem jawnym.

### 5.3 Algorytmy szyfrowania

Przyjęty został podział na dwie podstawowe grupy algorytmów szyfrowania:

- z kluczem symetrycznym
- z kluczem asymetrycznym

25

# 5.3.1 Szyfr z kluczem symetrycznym

 $E_K[M]=S \rightarrow D_K[S]=M$ 

obydwie strony są w posiadaniu tej samej tajnej informacji – klucza K

M – wiadomość jawna

E – szyfrowanie (encrypt)

S - szyfrogram

D – rozszyfrowanie (decrypt)

27

### 5.3.1 Szyfr z kluczem symetrycznym

klucz używany do zaszyfrowania danych jest identyczny jak klucz wymagany do ich odszyfrowania

obydwie strony są w posiadaniu tej samej tajnej informacji

26

# 5.3.1 Szyfr z kluczem symetrycznym

zamiana tekstu jawnego w tekst tajny (kryptogram) następuje w wyniku stosowania:

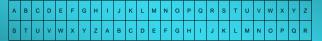
**podstawień -** zamiany znaków tekstu jawnego na inne znaki według określonej zasady

**przestawień -** zamiany kolejności znaków tekstu jawnego według określonego schematu

obecnie używane szyfry symetryczne wykorzystują najczęściej kombinację obydwu ww. technik

### 5.3.1 Szyfr z kluczem symetrycznym

zamiana tekstu jawnego w tekst tajny w wyniku stosowania podstawień według określonej zasady:



Jest to tzw. "szyfr Cezara" z przesunięciem o .... pozycji.

Tajną i współdzielonym informacją pomiędzy stroną szyfrującą a odbiorcą wiadomości jest w szyfrze Cezara wartość przesunięcia ciągu znaków.

CJOHLGYJSXAS TWVRA FS WYRSEAFAW

\* obydwie strony są w posiadaniu tej samej tajnej informacji

### 5.3.1 Szyfr z kluczem symetrycznym

Omówione na dwóch poprzednich slajdach metody da się złamać wykorzystując charakterystyczna cechę każdego języka

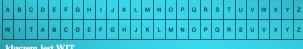
Częstość z jaką w danym alfabecie występują kolejne znaki. Np. w języku polskim:

- litera A występuje średnio w 7,3% tekstu
- litera I występuje średnio w 6,9% tekstu
- litera E występuje średnio w 6,4% tekstu

31

# 5.3.1 Szyfr z kluczem symetrycznym

zamiana tekstu jawnego w tekst tajny w wyniku stosowania podstawień przy pomocy tabliczek kodowania:





kluczem jest WYKLADBSK

\* obydwie strony są w posiadaniu tej samej tajnej informacji

### 5.3.1 Szyfr z kluczem symetrycznym

Omówione na dwóch poprzednich slajdach metody opierały się o fakt, że każdemu znakowi tekstu jawnego była przyporządkowana wyłącznie jedna litera kryptogramu:

to szyfr podstawieniowy monoalfabetyczny

By zapobiec łamaniu szyfru na podstawie analizy częstości, wymyślono szyfry, gdzie jednemu znakowi wiadomości można było przypisać wiele różnych wartości:

• to szyfry podstawieniowe polialfabetyczne

### 5.3.1 Szyfr z kluczem symetrycznym

W szyfrach polialfabetycznych klucz jest zbiorem informacji o sposobie kodowania kolejnych liter szyfrowanego tekstu – kolejne litery szyfrowanego tekstu są zastępowane w sposób zależny od kolejnych liter klucza:

- jeżeli pierwszą literą klucza jest A (pierwsza litera alfabetu), odpowiadający jej znak kodowanego tekstu będzie zastępowany literą położoną o jedną pozycję dalej (jeżeli w tekście było S, zostanie ono zastąpione przez T)
- jeżeli drugą literą klucza jest C, to drugi znak szyfrowanego tekstu jest zastępowany literą o trzy pozycje dalszą (zamiast I bedzie L) itd.

\* obydwie strony są w posiadaniu tej samej tajnej informacji

### 5.3.1 Szyfr z kluczem symetrycznym

### Przykład:

Jeżeli do zaszyfrowania tekstu ALA użyjemy klucza BAT, uzyskamy w wyniku tekst CMU, powstały z:

- przesunięcia litery A o dwa znaki
- litery L o jeden znak
- litery A o dwadzieścia znaków

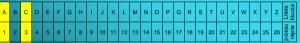
Jak widać ta sama litera wiadomości (czyli A) jest w otrzymanym kryptogramie kodowana różnymi znakami.

\* obydwie strony są w posiadaniu tej samej tajnej informacji

3.

### 5.3.1 Szyfr z kluczem symetrycznym

- jeżeli pierwszą literą klucza jest A (pierwsza litera alfabetu), odpowiadający jej znak kodowanego tekstu będzie zastępowany literą położoną o jedną pozycję dalej (jeżeli w tekście było S, zostanie ono zastapione przez T)
- jeżeli drugą literą klucza jest C, to drugi znak szyfrowanego tekstu jest zastępowany literą o trzy pozycje dalszą (zamiast I będzie L) itd.



\* obydwie strony są w posiadaniu tej samej tajnej informacji

34

# 5.3.1 Szyfr z kluczem symetrycznym

Teoretycznie do uzyskania szyfru niemożliwego do złamania, muszą być spełnione dwa warunki:

- 1) klucz musi być dłuższy od szyfrowanej wiadomości (każda z liter wiadomości jest wtedy zakodowana według innej zasady)
- 2) klucz powinien być ciągiem zupełnie przypadkowych znaków

\* obydwie strony są w posiadaniu tej samej tajnej informacji

### 5.3.1 Szyfr z kluczem symetrycznym

Wszystkie stosowane obecnie szyfry symetryczne to kombinacja szyfrów przestawieniowych i podstawieniowych. Pierwszym przyjętym powszechnie standardem był szyfr DES. Tekst podlegający szyfrowaniu przy użyciu algorytmu DES jest dzielony na ośmiobajtowe bloki danych, które są argumentem operacji przestawień i podstawień, zależnych od wykorzystywanego klucza szyfrowania. Klucze szyfrowania w algorytmie DES mają długość 56 bitów, co przy mocach obliczeniowych ówczesnych komputerów teoretycznie zapewniało bezpieczeństwo i odporność szyfru na ataki.

\* obydwie strony są w posiadaniu tej samej tajnej informacji

### 5.3.1 Szyfr z kluczem symetrycznym

Obecnie jako standard szyfrowania symetrycznego przyjęty jest szyfr o nazwie **AES** (nazywany roboczo Rijndael) opracowany przez Vincent Rijmen i Joan Daemen. Możliwe jest w nim użycie kluczy o długościach 128, 192 i 256 bitów i operuje on na blokach danych o długości 128 bitów (oryginalna specyfikacja *Rijndael* dopuszczała również bloki 192- i 256-bitowe). W związku z licznie pojawiającymi się (lecz mało prawdopodobnymi) atakami na AES, Vincent Rijmen opublikował w 2010 roku ironiczny artykuł opisujący "atak nazwany praktycznym".

- http://eprint.iacr.org/2010/337.pdf

### 5.3.1 Szyfr z kluczem symetrycznym

Następcą algorytmu DES stał się algorytm 3DES. Stanowi on odmianę algorytmu DES używającą trzech kluczy 56 bitowych - różnica polega na trzykrotnym użyciu algorytmu DES w stosunku do każdego bloku. Wydłużenie długości klucza sprawiło, że 3DES może być nadal bezpiecznie stosowany.

Szacunkowy czas potrzebny na złamanie klucza 3DES wynosi dzisiaj około tysiąca lat.

38

\* obydwie strony są w posiadaniu tej samej tajnej informac

### 5.3.1 Szyfr z kluczem symetrycznym

Problemy związane ze stosowaniem kluczy symetrycznych:

- problem tajności klucza wiadomość jest bezpieczna do czasu gdy ktoś niepowołany nie pozna tajnego klucza K
- problem dystrybucji klucza np. jak bez pośrednictwa strony trzeciej uzgodnić wspólny klucz (np. jeśli jesteśmy daleko od siebie)
- skalowalność 2 osoby 1 klucz, 3 3 klucze, 10 45 ...
- autentyczność skąd pewność, że tajność klucza zapewnia autentyczność?

# 5.3.2 Szyfr z kluczem asymetrycznym ... to już na następnym wykładzie ☺

