Akademia Górniczo-Hutnicza
Wydział Elektrotechniki, Automatyki,
Informatyki i Inżynierii Biomedycznej

Adrian Horzyk

WYZWANIA SPOŁECZEŃSTWA INFORMACYJNEGO

SZYFROWANIE DANYCH

Czyli jak zabezpieczyć dane, ich bazy i transfery w sieci oraz nie dopuścić do wycieku danych?

Kryptologia: Kryptografia i Kryptoanaliza

Kryptologia jest nauką ścisłą o **szyfrowaniu**, czyli bezpiecznych sposobach przechowywania i przekazywania informacji.

Kryptologię dzielimy na:

- ✓ **Kryptografię** - naukę o tworzeniu **szyfrów**, zabezpieczaniu wiadomości przy pomocy kluczy szyfrujących.
- ✓ **Kryptoanalizę** - naukę o łamaniu **szyfrów**, tzn. o odczytywaniu zaszyfrowanej wiadomości bez znajomości klucza.

Szyfr i Szyfrogram

Szyfr – to algorytm służący do zaszyfrowania i odszyfrowania wiadomości.

Szyfry dzieli się na:

- ✓ **Symetryczne** – wykorzystują do szyfrowania i odszyfrowania ten sam klucz szyfrujący, który w związku z tym musi być chroniony
- ✓ **Asymetryczne** – wykorzystują parę kluczy szyfrujących, jeden do szyfrowania a drugi do odszyfrowania. Działają zwykle dużo wolniej niż szyfry symetryczne.

Szybkość szyfrowania i deszyfrowania ma istotne znaczenie, dlatego zwykle stosuje się klucze asymetryczne do zaszyfrowania i przesłania klucza do szyfru symetrycznego.

Szyfrogram (kryptogram) – to zaszyfrowana wiadomość.

Bezpieczeństwo szyfrogramu stosującego szyfr symetryczny zależy od utrzymania w tajemnicy klucza szyfrującego, dlatego do jego przesłania odbiorcy szyfrogramu stosujemy zwykle dużo bezpieczniejsze lecz wolniejsze szyfry asymetryczne.

Historia Kryptografii i Kryptoanalizy

Proste szyfry stosowane były od dawna:

- ✓ **Szyfry przestawieniowe** - polegające na przestawieniu znaków w tekście, np. Szyfr Atbasha lub Szyfr Cezara:

Alfabet jawny –	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z
	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓
Alfabet tajny –	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z	A	B	C

- ✓ **Szyfry podstawieniowe** – polegające na podstawieniu znaku lub sekwencji znaków w miejsce szyfrowanego znaku lub sekwencji znaków, np. szyfry stosowane w trakcie 1. i 2. wojny światowej przez wojska niemieckie, tj. szyfr ADFGX czy ADFGVX, polegające na zastąpieniu oryginalnych/szyfrowanych znaków przez dwuznak składający się z dwóch liter łatwych do przesłania kodem Morsa, kodujących litery oraz cyfry:

	A	D	F	G	V	X
A	c	o	8	x	f	4
D	m	k	3	a	z	9
F	n	w	1	0	j	d
G	5	s	i	y	h	u
V	p	1	v	b	6	r
X	e	q	7	t	2	g

Dzięki pracy francuskiego kryptologa Painvina udało się uratować Paryż przed zmasowanym atakiem wojsk niemieckich i doprowadzić szybciej do zakończenia 1. wojny światowej.

Steganografia i Historia Szyfrowania

Steganografia – to ogół metod ukrywania tajnych przekazów w wiadomościach, które nie są tajne:

- ✓ gdzie *steganos* oznacza ukryty, *graphein* oznacza pisać.
- ✓ Greg Dermatos w V w. p.n.e. ostrzegł Spartan przed ofensywą Persów wyrywając tekst w drewnie i pokrywając tabliczkę woskiem.
- ✓ W listach umieszczano zdjęcia na kliszy pomniejszonej do wymiaru ok. 1mm, zastępując nią kropkę w zdaniu.
- ✓ Nawet 64 pozycje Kamasutry były stosowane jako szyfr podstawieniowy.
- ✓ W II w. p.n.e. grecki historyk Polibiusz opracował system szyfrowania oparty na tablicy przyporządkowującej każdej literze parę cyfr:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Kolebka Kryptoanalizy

Kolebką kryptoanalizy były Państwa arabskie:

- ✓ Najwcześniejsze prace Al-Kindiego, „filozof Arabów", pochodzą już z IX wieku, który napisał traktat „O odczytywaniu zaszyfrowanych listów".
- ✓ Napisał: *„Jeden sposób na odczytanie zaszyfrowanej wiadomości, gdy wiemy, w jakim języku została napisana, polega na znalezieniu innego tekstu w tym języku, na tyle długiego, by zajął mniej więcej jedną stronę, i obliczeniu, ile razy występuje w nim każda litera.*
  Literę, która występuje najczęściej, nazywamy »pierwszą«, następną pod względem częstości występowania »drugą« i tak dalej, aż wyczerpiemy listę wszystkich liter w próbce jawnego tekstu.
  Następnie bierzemy tekst zaszyfrowany i również klasyfikujemy użyte w nim symbole.
  Znajdujemy najczęściej występujący symbol i zastępujemy go wszędzie »pierwszą« literą z próbki jawnego tekstu.
  Drugi najczęściej występujący symbol zastępujemy »drugą« literą, następny »trzecią« i tak dalej, aż wreszcie zastąpimy wszystkie symbole w zaszyfrowanej wiadomości, którą chcemy odczytać".
- ✓ Analiza częstości po dziś dzień stanowi podstawową technikę kryptoanalityczną!
- ✓ W każdym języku pewne znaki lub słowa pojawiają się z różną częstotliwością. Na tej podstawie można zidentyfikować te litery w kryptogramie, co pozwala odgadnąć niektóre ze znajdujących się w tajnym piśmie wyrazów, a dzięki temu rozszyfrowuje się kolejne litery, opierając się na prawdopodobieństwie, pozwalając znacznie zredukować liczbę możliwych podstawień i osiągnąć rozwiązanie metodą prób i błędów.

Szyfry monoalfabetyczne

Szyfry monoalfabetyczne to szyfry, w których jednej literze alfabetu tajnego odpowiada dokładnie jedna litera alfabetu jawnego, co praktycznie nie zapewnia bezpieczeństwa, ponieważ łatwo jest je złamać w bardzo krótkim czasie,
nawet nie stosując komputera czy innego urządzenia.

Należy policzyć rozkład statystyczny znaków w zaszyfrowanym tekście i porównać z rozkładem w dowolnym tekście jawnym z tego samego języka. Wystarczy więc przeprowadzić analizę częstości i metodą chybił trafił dobrać litery,
odszyfrowując szyfrogram,
a w przypadku szyfrów
przedstawieniowych jest jeszcze łatwiej:

$$f(a) = (a + k) \bmod n$$

a – szyfrowana litera

k – klucz

n – liczba liter w alfabecie

Szyfry Homofoniczne

Szyfry homofoniczne:

- ✓ Miały zabezpieczyć szyfr przed atakiem z użyciem analizy częstości występowania np. słów lub znaków.
- ✓ W celu ukrycia częstości, literom częściej występującym przypisywano kilka symboli szyfrujących.
- ✓ Jednak te szyfry też można dosyć łatwo złamać, gdyż w języku istnieją również charakterystyczne dwuznaki lub trójznaki z określoną częstotliwością, a więc można szybko dopasować do siebie symbole szyfrujące jedną literę, np.: ciągi zaszyfrowanych znaków: 45 62 21 32 oraz 65 23 21 32 sugerują, iż symbole 45 i 65 oraz 62 i 23 szyfrują te same litery.

Dla utrudnienia wprowadzono też symbole puste – czyli znaki alfabetu tajnego nie posiadające odpowiedników w alfabecie jawnym, co utrudnia dekryptaż oraz umożliwia wprowadzanie w błąd kryptoanalityka odnośnie analizy częstości.

Szyfry Polialfabetyczne

Szyfry polialfabetyczne to połączenie wielu szyfrów monoalfabetycznych:

- ✓ Stosujących wiele tajnych alfabetów do szyfrowania kolejnych znaków w tekście.
- ✓ Alfabety są cyklicznie zmieniane, a więc po wyczerpaniu się wszystkich alfabetów szyfrujących, powraca się do pierwszego.
- ✓ Tarcza Albartiego składa się z dwóch tarcz, umożliwiając szybką zmianę alfabetu szyfrowego, czyli sposobu kodowania znaków oraz dektryptaż, umożliwiający odszyfrowanie wiadomości. Oczywiście tarcze wewnętrzne mogą być różne lub wymienne.

Tabula Recta

Tabula Recta to tabela Trithemiusa określająca szyfr podstawieniowy polialfabetyczny :

- ✓ Zawierająca u góry alfabet tekstu tajnego.
- ✓ Kolejne wiersze zawierają tajne alfabety utworzone przez przesunięcie alfabetu.
- ✓ Szyfrowanie polega na stosowaniu:
- ✓ 1. wiersza do zaszyfrowania 1. litery,
- ✓ 2. wiersza do zaszyfrowania 2. litery,
- ✓ ...
- ✓ 26. wiersza do zaszyfrowania 26. litery,
- ✓ 1. wiersza do zaszyfrowania 27. litery,
- ✓ 2. wiersza do zaszyfrowania 28. litery,
- ✓ ...

JAWNY:		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
B	2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
C	3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
D	4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
E	5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
F	6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
G	7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
H	8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
I	9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
J	10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
K	11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
L	12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
M	13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
N	14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
O	15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Q	17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
R	18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
S	19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
T	20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
U	21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
V	22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
W	23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
X	24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Y	25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
Z	26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Szyfr Vigenere'a

Szyfr podstawieniowy polialfabetyczny Vigenere'a:

- ✓ Polega na szyfrowaniu kolejnych liter wiadomości za pomocą różnych, a nie kolejnych wierszy tablicy Trithemiusa.
- ✓ Litera określa wiersz wykorzystany do jej zaszyfrowania, np. wiersz 14 szyfruje literę 1., wiersz 23 literę 2. itd.
- ✓ Należało oczywiście określić tą kolejność wierszy, więc stosowano np. jakieś słowo, którego kolejność liter w słowniku wskazywała numery wierszy dla kolejnych szyfrowanych liter, np. słowo **tajemnica**, zawiera 9 liter, które występują w alfabecie na następujących pozycjach **20, 1, 10, 5, 13, 14, 9, 3, 1**.

JAWNY:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
B	2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
C	3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
D	4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
E	5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
F	6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
G	7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
H	8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
I	9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
J	10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
K	11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
L	12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
M	13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
N	14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
O	15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Q	17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
R	18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
S	19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
T	20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
U	21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
V	22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
W	23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
X	24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Y	25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
Z	26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Autoklucz Vigenere'a

Vigenere stworzył dwa systemy szyfrowania oparte na koncepcji autoklucza, czyli odkodowany tekst jawny:

- ✓ Potrzebna była tylko 1. litera, czyli tzw. klucz pierwotny, który odszyfrowywał pierwszą literę tekstu jawnego, następnie jej kolejność w alfabecie wskazywała numer wiersza do odszyfrowania drugiej litery, ta zaś trzeciej itd.
- ✓ Taki sposób szyfrowania oczywiście mógł sprawić trudności, jeśli część szyfrogramu uległa zniszczeniu lub zamazaniu!

JAWNY:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
B	2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
C	3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
D	4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
E	5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
F	6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
G	7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
H	8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
I	9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
J	10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
K	11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
L	12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
M	13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
N	14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
O	15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Q	17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
R	18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
S	19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
T	20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
U	21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
V	22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
W	23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
X	24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Y	25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
Z	26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Autoklucz Vigenere'a

Drugi system z autokluczem Vigenere wykorzystywał klucz pierwotny, lecz po zaszyfrowaniu pierwszej litery tekstu jawnego jej odpowiednik w kryptogramie stawał się kolejną literą klucza.

Te szyfry z autokluczem były znacznie ciekawsze i trudniejsze do odkodowania niż podstawowy szyfr oparty o tabelę Trithemiusa.

JAWNY:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
B	2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
C	3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
D	4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
E	5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
F	6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
G	7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
H	8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
I	9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
J	10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
K	11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
L	12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
M	13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
N	14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
O	15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Q	17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
R	18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
S	19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
T	20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
U	21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
V	22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
W	23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
X	24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Y	25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
Z	26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Jak złamać szyfr Vigenere'a?

Przy łamaniu szyfrów warto wziąć pod uwagę ich własności:

- ✓ Szyfr Vigenere'a wykorzystuje cyklicznie słowo o określonej długości N.
- ✓ Z tego wynika, iż co N-ta litera w tekście jest szyfrowana przy pomocy identycznego alfabetu.
- ✓ Wystarczy więc podzielić tekst na grupy liter szyfrowane tą samą literą klucza i dokonać kryptoanalizy opartej na częstości, gdyż to są proste szyfry podstawieniowe.
- ✓ Kryptoanalityk nie zna jednak długości klucza N, ale może zdobyć tą informację w trakcie badania kryptogramu, gdyż przy dłuższych tekstach zdarzają się powtórzenia wyrazów lub ich fragmentów szyfrowane tym samym fragmentem klucza, co spowoduje wystąpienie powtarzających się kombinacji liter.
- ✓ Powtarzające się kombinacje możemy wykrywać metodami eksploracji danych.
- ✓ Analiza odległości w tekście powtarzających się kombinacji liter wskazuje na pewną wielokrotność długości klucza: k * N. Znajdując więc różne powtórzenia, wystarczy policzyć największy wspólny dzielnik, który wskaże N.

Szyfry Digraficzne

Szyfry digraficzne opierają się na szyfrowaniu par znaków:

- ✓ Tekst jawny dzielony jest na pary znaków, a następnie przekształcany w szyfrogram według ustalonego wzoru.
- ✓ Szyfr Playfaira (stworzony przez Charlsa Wheatstone'a) opierał się na tablicy 5x5, w którą wpisywano słowo klucz, a następnie kolejne litery alfabetu w porządku alfabetycznym, oczywiście pomijając już wpisane oraz traktując I i J jako jedną literę, np. stosując słowo szyfrujące PLAYFAIR otrzymamy tablicę:
- ✓ Szyfry digraficzne są trudniejsze do złamania za pomocą analizy częstości, gdyż liczba digrafów jest znacznie większa, np. dla 26 liter otrzymujemy 676 digrafów!
  Z tego też powodu był uważany za bezpieczny i wykorzystywany w trakcie 1. i 2. wojny światowej.

P	L	A	Y	F
IJ	R	B	C	D
E	G	H	K	M
N	O	Q	S	T
U	V	W	X	Z

Szyfr Playfair

Szyfrowanie szyfrem Playfaira:

- ✓ rozpoczynało się od podzielenia tekstu na pary znaków, zaś gdy dwie takie same litery wystąpiły obok siebie należało je oddzielić znakiem X.
- ✓ Następnie przekształcano wiadomość w szyfrogram w oparciu o następujące reguły:
  - Jeśli obie litery znajdowały się w tym samym rzędzie, były zastępowane literami znajdującymi się bezpośrednio po ich prawej stronie. Obowiązywała tutaj zasada cykliczności, tzn. ostatnia litera w rzędzie była zastępowana pierwszą po lewej.
  - Jeśli obie litery znajdowały się w tej samej kolumnie, zastępowano je literami znajdującymi się pod spodem. Tutaj również obowiązywała zasada cykliczności.
  - Litery znajdujące się w innych kolumnach i wierszach były zastępowane literami z tego samego wiersza, ale znajdującymi się w kolumnie drugiej litery tekstu jawnego.
- ✓ Przykład: ZA SZ YF RU JX
  ZA leżą w różnych wierszach i kolumnach, więc ZA → WF.
  YF leżą w tym samym wierszu, więc YF → CD.

P	L	A	Y	F
IJ	R	B	C	D
E	G	H	K	M
N	O	Q	S	T
U	V	W	X	Z

Szyfr „nie do złamania”

Czy istnieje szyfr nie do złamania (*one-time pad*)?

- ✓ Jeśli klucz szyfrujący będzie tak samo długi jak szyfrowana wiadomość.
- ✓ Jeśli wykorzystamy ten klucz tylko jednorazowo.
- ✓ Jeśli zakładamy dowolne podstawienia znaków.

Wtedy nie mamy na czym oprzeć kryptoanalizy, gdyż np.:

„DZISIAJ JEST SŁONECZNA POGODA” może oznaczać w zależności od zastosowanego klucza cokolwiek o tej samej ilości liter, np.: „ATAK W POŁUDNIE O GODZ. 10:00.”

gdyż każdy znak może być zastąpiony przez indywidualne podstawienie:

D → A, Z → T, Z → A, S → K itd., co można zapisać liczbowo przy pomocy przesunięć.

Trudność polega na tym, iż klucz jest równie długi, jak szyfrowana wiadomość, więc pojawia się problem z przesłaniem takiego klucza, który też może być przechwycony, gdyż jego zapamiętanie byłoby raczej trudne!

Szyfr jest nie do złamania, jeśli znajdziemy równie dobrą metodę zaszyfrowania klucz szyfrującego! Kółko się więc zamyka. Szyfr jest więc niepraktyczny.

Rozwój Kryptografii

Duży wpływ na rozwój kryptografii miały kolejno wynalezienie telegrafu, radia, Internetu, gdyż przyspieszył się transfer wiadomości oraz stał się możliwy do przechwycenia, wręcz publiczny! Stąd trzeba było wymyślić bardziej skuteczne metody zabezpieczenia i szyfrowania.

- ✓ Telegraf
- ✓ Radio
- ✓ Internet

ENIGMA

Enigma to niemiecka wirnikowa maszyna szyfrująca:

- ✓ Wirniki miały zdefiniowany układ połączeń, ale można było je wkładać w różnej kolejności, a każdy z nich można było ustawić w jednej z 26 możliwych pozycji.
- ✓ Podczas szyfrowania pierwszy z wirników obracał się o jedną pozycję z każdą szyfrowaną literą, a po pełnym obrocie powodował przesunięcie o jedną pozycję drugiego wirnika, gdy ten wykonał pełny obrót, trzeciego itd.
- ✓ Na działanie maszyny wpływały:
  - ✓ Wybór wirników szyfrujących (4 lub 5 z 8 możliwych)
  - ✓ Kolejność wirników w maszynie (ilość permutacji)
  - ✓ Początkowe pozycje wirników (1 z 26 pozycji)
- ✓ Ponadto szyfrowanie było oparte na systemie kluczy dziennych, które determinowały ustawienie wirników.
- ✓ Klucz dzienny był zawsze szyfrowany dwukrotnie na początku wiadomości, co ułatwiło jego odczytanie. Ponadto leniwi niemieccy szyfranci, często go nie zmieniali!

ENIGMA

Enigma to niemiecka wirnikowa maszyna szyfrująca:

- ✓ Posiadała walec odwracający, co umożliwiało wykorzystanie jej zarówno do szyfrowania, jak i do deszyfrowania wiadomości.
- ✓ Ta praktyczna zaleta Enigmy była zarazem jej piętą Achillesa z punktu widzenia kryptografii, gdyż wymuszało powstanie tzw. negatywnego wzorca, co ograniczało liczbę możliwych kryptogramów!
- ✓ Między innymi żadna litera nie mogła zostać zaszyfrowana jako ona sama, czyli niemożliwe było zaszyfrowanie np. N jako N.
- ✓ Wiedza o tym ułatwiła zadanie polskim kryptoanalitykom w złamaniu szyfrów Enigmy w trakcie II wojny światowej.

ENIGMA

Ze względu na to, iż szyfrogram Enigmy oparty był na negatywnych wzorcu badany (poszukiwany) wyraz nie mógł mieć żadnej litery zakodowanej przy pomocy tej samej litery, więc takie przesunięcia odpadały, np.:

Pozycja początkowa:

Kryptogram:	G	S	A	G	K	F	I	H	U	B	F	O	V	D
Badany wyraz:	A	N	G	R	I	F	F							

Pierwsze przesunięcie:

Kryptogram:	G	S	A	G	K	F	I	H	U	B	F	O	V	D
Badany wyraz:		A	N	G	R	I	F	F						

Drugie przesunięcie:

Kryptogram:	G	S	A	G	K	F	I	H	U	B	F	O	V	D
Badany wyraz:			A	N	G	R	I	F	F					

Trzecie przesunięcie:

Kryptogram:	G	S	A	G	K	F	I	H	U	B	F	O	V	D
Badany wyraz:				A	N	G	R	I	F	F				

Colossus i Eniac

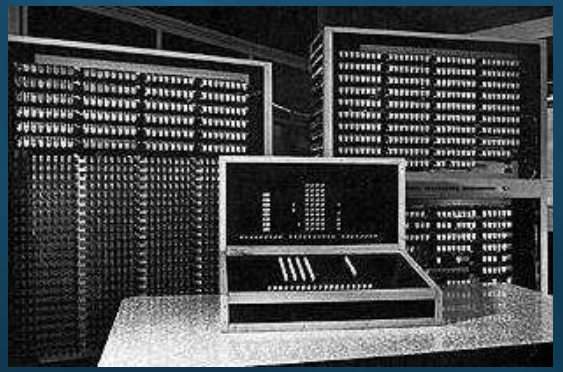
Wiadomości między najwyższymi rangą wojskowymi Trzeciej Rzeszy były szyfrowane przy pomocy przystawki szyfrującej, wykorzystującej specjalny kod, w którym każdy znak był reprezentowany w systemie dwójkowym z wykorzystaniem taśmy perforowanej: dziura – oznaczała 1, jej brak – 0:

- ✓ **Przystawka odczytywała jednocześnie dwie taśmy, jedna z tekstem jawnym, a druga z kluczem, wykonując operację dodawania bez przenoszenia reszt (czyli modulo 2), zapisując wynik na trzeciej taśmie. W efekcie część 0 zmieniała się na 1 i część 1 na 0 w zależności od zastosowanego klucza szyfrującego.**
- ✓ **Colossus opierał się na teoretycznym modelu opracowanym przez Alana Turinga i zawierał 1,5 tysiąca lamp (później 2,5 tyś.), potrafiąc zapamiętać dane do dalszego przetwarzania. Był więc pierwszym komputerem, o którego istnieniu dowiedział się świat dopiero po 1975 r., gdyż był objęty tajemnicą wojskową. Trzy lata później powstał ENIAC.**

Kryptoanaliza Doprowadziła do Powstania Komputerów

Historia Komputerów została zapoczątkowana przez potrzeby kryptoanalityków, którzy mieli coraz większe trudności ze sprawdzaniem różnych permutacji i dopasowywaniem wzorców:

- ✓ Colossus to pierwszy model urządzenia elektronicznego zawierającego półtora tysiąca lamp został stworzony i oddany do użytku w 1943 na postawie modelu teoretycznego opracowanego przez Alana Turinga.
- ✓ Trzy lata później powstał pierwszy słynny komputer ENIAC.



Pierwsze komputery zostały zainspirowane potrzebą przetwarzania symbolicznego stosowanego właśnie w łamaniu szyfrów na potrzeby militarne w trakcie drugiej wojny światowej. Można więc powiedzieć, iż rozwój kryptografii i kryptoanalizy zapoczątkował rozwój komputerów oraz informatyki!

Klasyczne Szyfry Symetryczne

Szyfry symetryczne dzielimy na:

- ✓ **Blokowe – dzielące tekst na bloki o określonej długości, z których każdy szyfrowany jest oddzielnie.**
- ✓ **Strumieniowe – generujące ciąg szyfrujący o długości równiej szyfrowanej wiadomości.**

Klasyczne Szyfry Symetryczne

Szyfry symetryczne to np.:

- ✓ Szyfr Cezara – zastępujący poszczególne litery alfabetu innymi wg określonego przesunięcia.
- ✓ Szyfr AtBasha – zastępujący poszczególne litery alfabetu innymi tak samo odległymi od końca alfabetu, co szyfrowana litera od jego początku.
- ✓ Szyfr Playfaire'a – stosuje 2D tabelę, do której wpisuje się litery klucza i uzupełnia pozostałymi.
- ✓ Szyfr Nihilistów – działa podobnie jak szyfr Playfaire'a, lecz szyfrowany jest dodatkowo klucz szyfrujący.
- ✓ Szyfr Vigenere'a – swoje działanie opiera na tablicy Trithemiusa.
- ✓ Szyfr DES (*Data Encryption Standard*) – szyfruje bloki 64-bitowe przy użyciu 56 bitowego klucza symetrycznego.
- ✓ Szyfr AES (*advanced encryption standard*) – to współczesny szyfr symetryczny blokowy wykorzystujący klucze o długości 128, 192 i 256 bitów.

Szyfr Cezara

Szyfr Cezara polega na przesunięciu cyklicznym liter alfabetu o określoną ilość liter i podstawienie w miejsce szyfrowanych liter tych po przesunięciu. Deszyfrowanie polega na przesunięciu liter alfabetu o określoną ilość wstecz.

Łamanie Szyfru Cezara jest bardzo proste. Można sprawdzić 26 wszystkich przesunięć i ew. wyznaczyć częstość liter w szyfrogramie oraz wyznaczyć prawdopodobne przesunięcie z wykorzystaniem wiedzy na temat częstości występowania poszczególnych liter w danym języku.

Szyfrowanie:	W	D	I		T	O		C	I	E	K	A	W	Y		P	R	Z	E	D	M	I	O	T
Szyfrogram:	O	V	B		L	G		U	A	W	C	S	O	R		H	I	Q	W	V	E	A	G	L

Alfabet:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	Q	S	T	U	V	W	X	Y	Z
Szyfrowanie:	→ Przesunięcie o 8																						↓			
Szyfr:	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	Q
Deszyfrowanie:	← Przesunięcie o 8 wstecz																									

Szyfrogram:	O	V	B		L	G		U	A	W	C	S	O	R		H	I	Q	W	V	E	A	G	L
Deszyfrowanie:	W	D	I		T	O		C	I	E	K	A	W	Y		P	R	Z	E	D	M	I	O	T

Szyfr Atbasha

Szyfr AtBasha polega na odwróceniu kolejności liter alfabetu tak, że podstawiamy za literę alfabetu taką, która jest od końca alfabetu w takiej samej kolejności, co szyfrowana od jego początku.

Deszyfrowanie polega na odwróceniu kolejności liter alfabetu i sprawdzeniu przyporządkowania. **Łamanie Szyfru AtBasha** jest więc również prymitywnie proste.

Szyfrowanie:	W	D	I		T	O		C	I	E	K	A	W	Y		P	R	Z	E	D	M	I	O	T
Szyfrogram:	D	W	Q		G	L		X	Q	V	P	Z	D	B		K	J	A	V	W	N	Q	L	G

Alfabet:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	Q	S	T	U	V	W	X	Y	Z
Szyfrowanie:	←	←	←	←	←	←	←	←	←	Odległość od początku							↓	←	←	←	←	←	←	←	←	←
Szyfr:	Z	Y	X	W	V	U	T	S	Q	R	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A
Deszyfrowanie:	→	→	→	→	→	→	→	→	→	Odległość od końca																

Szyfrogram:	D	W	Q		G	L		X	Q	V	P	Z	D	B		K	J	A	V	W	N	Q	L	G
Deszyfrowanie:	W	D	I		T	O		C	I	E	K	A	W	Y		P	R	Z	E	D	M	I	O	T

Zasady Łamania Szyfrów

Kryptoanaliza zajmuje się łamaniem szyfrów, czyli odnajdywaniem algorytmu pozwalającego na **zdeszyfrowanie** szyfrogramu, odgadnięcie szyfru, sposobu szyfrowania, hasła itp. Co można statystycznie badać w szyfrogramie:

- ✓ **Częstość występowania poszczególnych liter/liczb w szyfrogramie** oraz ich porównywanie z częstością występowania liter w słowach danego języka, co można zrobić na podstawie analiz frekwencji ich występowania w tekstach.
- ✓ **Długość zaszyfrowanych słów** w szyfrogramie, co ogranicza ilość słów możliwych do podstawienia/odgadnięcia w danym języku.
  Można się ponadto posłużyć słownikami frekwencyjnymi, podającymi częstość występowania słów w danym języku.

Dobry szyfr więc nie powinien ujawniać częstości występowania poszczególnych znaków ani długości słów.

Ponadto znając jakiś stary klucz, szyfrogram i tekst jawny, można spróbować odgadnąć szyfr, czyli sposób i hasło/a, które doprowadziły tekst jawny poprzez ten znany klucz do określonego szyfrogramu.

Rodzaje Ataków Kryptograficznych

Istnieją teoretyczne modele atakowania szyfrów:

- ✓ **Atak ze znanym tekstem jawnym (*known-plaintext*) polegający na próbie odgadnięcia sekretnego klucza na podstawie wcześniejszych wiadomości wraz z ich szyfrogramami albo wymyśleniu algorytmu, dzięki któremu stanie się możliwe odszyfrowanie kolejnych wiadomości.**
- ✓ **Atak z wybranym tekstem jawnym (*chosen-plaintext*) polegający na możliwości wielokrotnego szyfrowania dowolnej wiadomości i porównywaniu szyfrogramów z tekstami jawnymi w celu odgadnięcia klucza lub algorytmu szyfrującego.**
- ✓ **Atak z szyfrogramami (*ciphertext-only*) polegający na analizie wielu szyfrogramów i próbie odgadnięcia klucza na ich podstawie.**
- ✓ **Atak z wybranym szyfrogramem (*chosen-ciphertext*) polegający na możliwości eksperymentowania w różnymi szyfrogramami dla tego samego tekstu jawnego**
- ✓ **Atak z wybranym kluczem (*chosen-key*) polegający na możliwości wykorzystania informacji o sposobie powiązania kluczy w celu złamania zabezpieczeń danego szyfru.**

Typy Ataków Kryptograficznych

W obrębie powyższych grup, można wyodrębnić kilka typów ataków:

- ✓ **Atak siłowy (*brute force*) – polegający na próbie odszyfrowania wiadomości stosując możliwie wszystkie klucze szyfrujące (wspomagając się np. słownikami) z nadzieją, iż któryś okaże się prawdziwy. Współczesne komputery są w stanie sprawdzić i złamać tą metodą w przeciągu jednego dnia ok. 260 bitowe klucze.**
- ✓ **Atak na *two-time pad* – polegający na wykorzystaniu dwóch szyfrogramów zakodowanych tym samym kluczem.**
- ✓ **Atak statystyczny (*frequency analysis*) – polegający na analizie częstotliwości występowania znaków w szyfrogramie.**
- ✓ **Atak *man-in-the-middle* – polegający na włączenie się komunikację pomiędzy dwoma stronami i pośredniczenie w niej poprzez utworzenie dla każdej strony po jednym kluczu i rozpoczęciu komunikacji ze stronami, mogąc podszywać się pod nie.**

Typy Ataków Kryptograficznych

W obrębie powyższych grup, można wyodrębnić kilka typów ataków:

- ✓ **Atak *meet-in-the-middle* – polegający na łamaniu szyfru używających wielu różnych kluczy do zakodowania tej samej wiadomości stosując ten sam algorytm.**
- ✓ **Atak metodą powtórzenia – polegający na ponownym wysłaniu tego samego szyfrogramu do odbiorcy z nadzieją, iż zareaguje tak samo/podobnie ze względu na poprawność wiadomości po jej odszyfrowaniu przez odbiorcę.**
- ✓ **Atak homograficzny (*homograph attack*) – polegający na zbudowaniu domeny i strony internetowej łudząco podobnych do oryginalnych i podszycie się pod oryginalną instytucję, celem wyłudzenia od użytkowników (np. banku) loginów, haseł i kodów.**

Współczesne Szyfry Asymetryczne

Szyfry asymetryczne wykorzystują dwa klucze:

- ✓ **publiczny**, który służy do zaszyfrowania wiadomości,
- ✓ **prywatny**, który jest tajny i służy do jej odszyfrowania.

Działanie algorytmów wykorzystujących dwa klucze asymetryczne:

1. Obydwa klucze (prywatny i publiczny) generowane są przez algorytm szyfrujący odbiorcy szyfrogramu.
2. Odbiorca przesyła klucz publiczny nadawcy(om).
3. Nadawca szyfruje wiadomość z wykorzystaniem otrzymanego klucza publicznego i przesyła zaszyfrowaną wiadomość (szyfrogram) odbiorcy.
4. Odbiorca z wykorzystaniem bezpiecznie przechowywanego i nigdzie nie wysyłanego klucza prywatnego odszyfrowuje wiadomość.

.

Elektroniczne Podpisy Cyfrowe

Szyfry asymetryczne wykorzystywane są również
do **elektronicznych podpisów cyfrowych**,
gdyż można podpisywać dokumenty kluczem prywatnym,
ponieważ zna go tylko nadawca
(szyfrant, np. twórca zeznania lub oprogramowania),
a odczytać może go każdy
(np. urząd lub kupujący oprogramowanie klient),
mając pewność, iż został zaszyfrowany przez znanego nadawcę,
co można potwierdzić za pośrednictwem **urzędu certyfikacji**,
w którym rejestruje się nadawca.

RSA

RSA – to współczesny szyfr asymetryczny umożliwiający bezpieczne przesyłanie informacji przez sieć Internet:

- ✓ Koncepcja RSA opiera się na problemie rozkładu dużych liczb na czynniki pierwsze, który charakteryzuje się bardzo dużą złożonością obliczeniową.
- ✓ Klucz publiczny generowany jest przez pomnożenie przez siebie dwóch dużych, losowo wybranych liczb pierwszych. Następnie wybierana jest kolejna duża liczba o określonych właściwościach — stanowi ona klucz szyfrujący. Klucz publiczny tworzony jest na podstawie klucza szyfrowania oraz wspomnianego iloczynu liczb pierwszych.
- ✓ Klucz prywatny można łatwo obliczyć, jeśli zna się liczby pierwsze tworzące iloczyn zastosowany przy tworzeniu klucza publicznego. Są one znane właścicielowi pary kluczy, natomiast kryptoanalityk może je uzyskać jedynie dzięki rozwiązaniu problemu faktoryzacji dużych liczb.
- ✓ Do złamania szyfru RSA potrzebne jest rozbicie klucza publicznego na dwie bardzo duże liczby pierwsze, będące jego dzielnikami.
- ✓ Na razie nie opracowano metody pozwalającej szybko znaleźć takie dzielniki.
- ✓ Dla 128-bitowego klucza sprawdzenie podzielności zajmie współczesnemu komputerowi kilkadziesiąt lat.

http://eduinf.waw.pl/inf/alg/001_search/0067.php

Zwiększanie Bezpieczeństwa

W celu zwiększenia bezpieczeństwa stosuje się:

- ✓ Identyfikację (*identification*) – podmiot deklaruje swoją tożsamość (identity), która musi zostać potwierdzona, np. na podstawie loginu i hasła.
- ✓ Uwierzytelnianie (*authentication*) – strona ufająca stosuje odpowiednią technikę uwierzytelniania (*authentication mechanism*) w celu weryfikacji zadeklarowanej wcześniej tożsamości, np. na podstawie trudno dostępnych danych personalnych, loginu i hasła albo danych biometrycznych, które muszą być zgodne z wcześniej stworzonym profilem.
- ✓ Autoryzację (*authorisation*) – to proces potwierdzenia, czy dany podmiot jest uprawniony do uzyskania dostępu do żądanego zasobu po etapie jego uwierzytelnienia.

Bibliografia, Odnośniki i Literatura

1. Dominic Chell, Tyrone Erasmus, Shaun Colley, Ollie Whitehouse, „Bezpieczeństwo aplikacji mobilnych. Podręcznik hakera”, Helion, 2018.
2. Marcin Karbowski, Podstawy Kryptografii, Wydanie III, Helion, 2015.
3. Michael, Welschenbach, Kryptografia w C i C++, MIKOM, Warszawa, 2002
4. Kryptografia: http://www.cryptography.ovh.org
5. Kryptoanaliza: http://www.crypto-it.net/pl/ataki/index.html
6. Szyfr Cezara: http://eduinf.waw.pl/inf/alg/001_search/0063.php
7. Algorytm RSA: http://eduinf.waw.pl/inf/alg/001_search/0067.php
8. Szyfr Enigmy: http://eduinf.waw.pl/inf/alg/001_search/0066.php
9. Algorytmy struktury danych: http://eduinf.waw.pl/inf/alg/001_search/index.php

Google: Horzyk