Kryptografia, czyli szyfrowanie danych

Maciej Borowiecki

Konferencja metodyczna „Czy matematyka jest potrzebna informatykom?”
Warszawa, 2 marca 2016 roku

Ośrodek Edukacji Informatycznej i Zastosowań Komputerów w Warszawie

Kryptoanaliza,
czyli łamanie szyfrów

Kryptologia

Dziedzina wiedzy z pogranicza matematyki i informatyki oraz historii

Steganografia,
czyli ukrywanie wiadomości jawnej

Warszawa, 2 marca 2016 roku

OEiiZK

Podstawa programowa

IV etap edukacyjny, informatyka, zakres rozszerzony

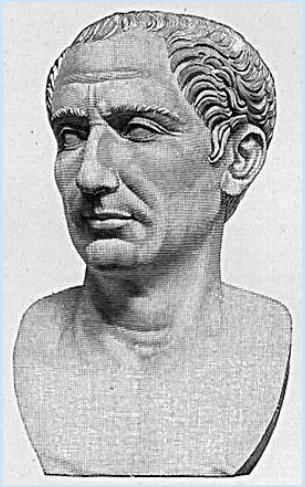
e) algorytmy kompresji i szyfrowania, np.:

- kody znaków o zmiennej długości, np. alfabet Morse'a, kod Huffmana,
- szyfr Cezara,
- szyfr przestawieniowy,
- szyfr z kluczem jawnym (RSA),
- wykorzystanie algorytmów szyfrowania, np. w podpisie elektronicznym,

Rodzaje szyfrów (historycznie)

- przestawieniowe

- podstawieniowe



Rodzaje szyfrów (współcześnie)

- szyfry z kluczem symetrycznym
- szyfry z kluczem asymetrycznym

Rivest

Shamir

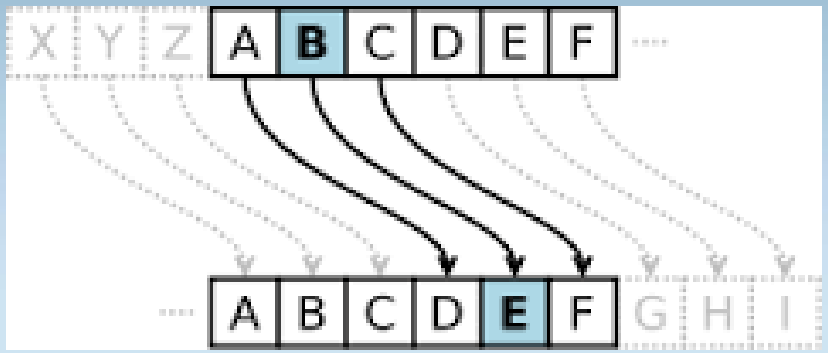
Adleman

Podstawy matematyczne

- arytmetyka modulo
- liczby pierwsze
- NWD, algorytm Euklidesa
- pojęcie funkcji, funkcja odwrotna

Szyfry podstawieniowe bliżej

- Szyfr Cezara



S(x)=x+przesunięcie (modulo długość alfabetu)

x – pozycja znaku w alfabecie (zaczynając od 0)

D(x)=x-przesunięcie (modulo długość alfabetu)

Jak złamać?

- mała liczba kluczy (przesunięć), można próbować wszystkie
- analiza częstości

Szyfry podstawieniowe bliżej (cd.)

- kluczem dowolna permutacja alfabetu

ZEBRANIEMETODYCZNE

ABCDEFGHIJKLMNOPQRSTUVWXYZ
ZEBRANIMTODYCFGHJKLPQSUVWX

Jak złamać?

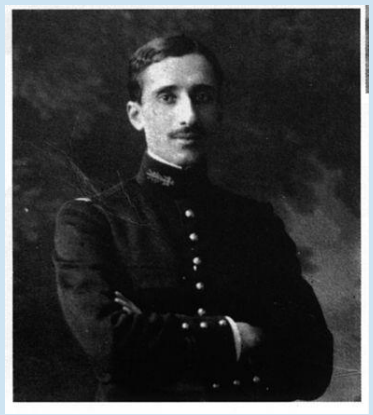
- testowanie kluczy odpada, 26! = 403291461126605635584000000
- analiza częstości

Rodzaje szyfrów (cd.)

- szyfry monoalfabetyczne
- szyfry polialfabetyczne
- szyfry digraficzne
- …

I wojna światowa

Georges Painvin – złamanie szyfru ADFGVX



	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

Tablica Polibiusza

	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

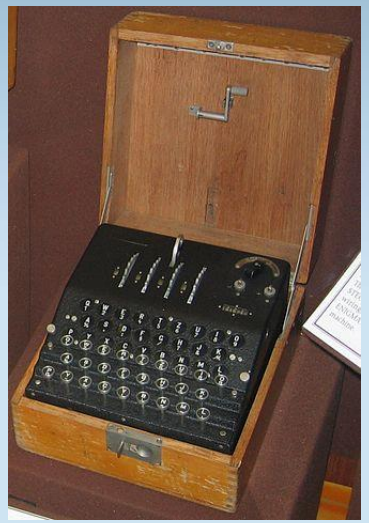
II wojna światowa

Złamanie szyfru Enigmy

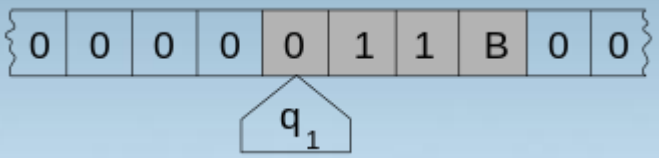
Marian Rejewski

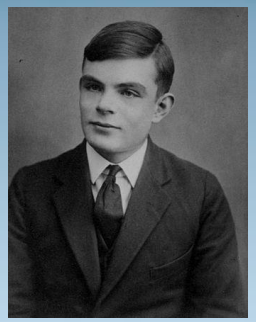
Henryk Zygalski

Jerzy Różycki

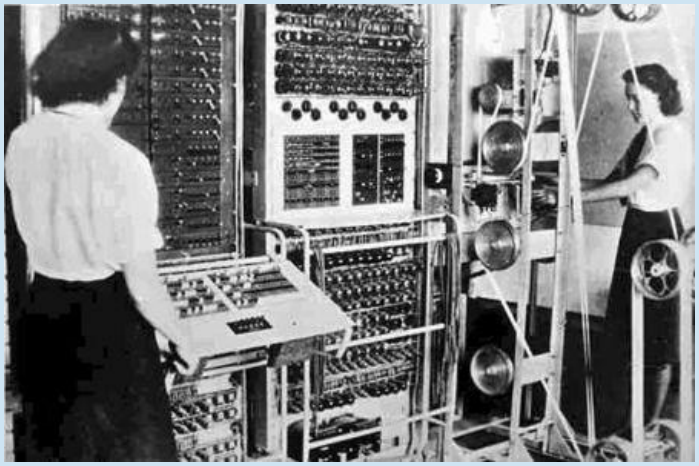


Alan Turing

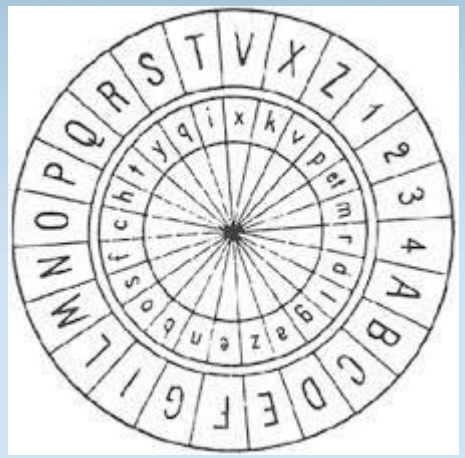


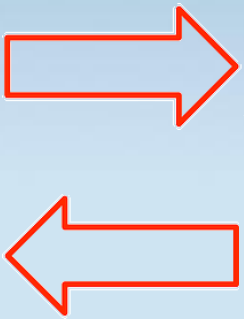


- kontynuacja prac nad złamaniem szyfru Enigmy
- abstrakcyjny model komputera – maszyna Turinga
- Colossus - pierwsza maszyna elektroniczna zdolna pamiętać dane



Związki kryptologii z komputerami



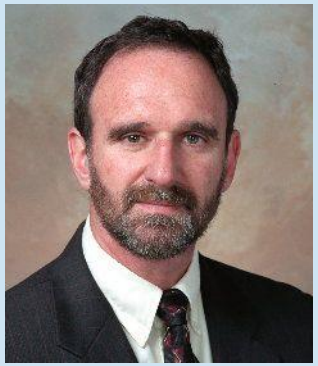


- wykorzystanie w kryptoanalizie
- szyfrowanie połączeń internetowych
- podpis elektroniczny

Szyfr z kluczem asymetrycznym

- klucz publiczny,
  funkcja szyfrująca oparta na kluczu publicznym
- klucz prywatny potrzebny do odszyfrowania
- nie można szybko wyznaczyć klucza prywatnego na podstawie klucza publicznego
  (funkcji odwrotnej do funkcji szyfrującej)

Whitfield Diffie



Martin Hellman

Szyfr RSA

- klucz publiczny – para liczb (n,d)
  n=p*q (dwie wielkie liczby pierwsze)
  NWD(d,(p-1)*(q-1))=1
- funkcja szyfrująca $S(x)=x^d$ (modulo n)
- klucz prywatny – para liczb (n,e)
  e*d (modulo (p-1)*(q-1))=1
- funkcja deszyfrująca $D(x)=x^e$ (modulo n)

Podstawa programowa (cd.)

III etap edukacyjny, informatyka
IV etap edukacyjny, informatyka, zakres podstawowy

Projekt gimnazjalny

Dziękuję za uwagę