# Podstawy kryptografii

Andrzej M. Borzyszkowski

Instytut Informatyki
Uniwersytet Gdański

sem. letni 2019/2020

`inf.ug.edu.pl/~amb`

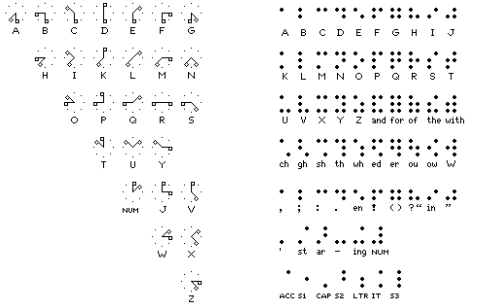
Podstawy kryptografii
Andrzej M. Borzyszkowski
Wykład 1
Złożoność
Założenia kryptografii
Kryptografia klasyczna vs. współczesna
Kryptografia klucza asymetrycznego
Kryptografia klasyczna

# Kryptografia klasyczna

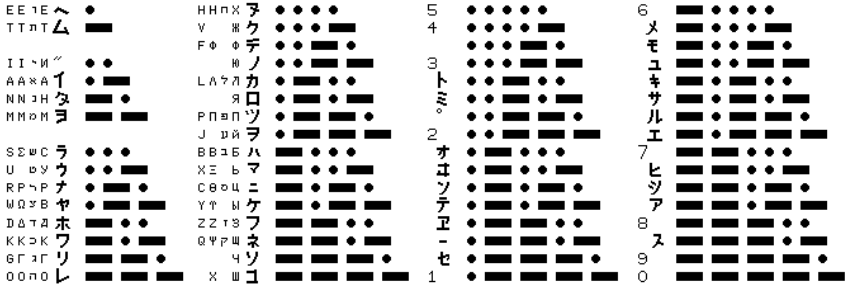
Podstawy kryptografii
Andrzej M. Borzyszkowski
Wykład 1
Złożoność
Założenia kryptografii
Kryptografia klasyczna vs. współczesna
Kryptografia klucza asymetrycznego
Kryptografia klasyczna

## Kodowanie vs. szyfrowanie

- kodowanie: zamiana alfabetu na inny
  - alfabet Braille'a
  - kod ASCII
  - alfabet Morse'a
- kodowanie to nie szyfrowanie



źródło: `is.gd/lxNX4A`



Podstawy kryptografii
Andrzej M. Borzyszkowski
Wykład 1
Złożoność
Założenia kryptografii
Kryptografia klasyczna vs. współczesna
Kryptografia klucza asymetrycznego
Kryptografia klasyczna

## Działy

- kryptografia: nauka/sztuka szyfrowania ( i odszyfrowywania)
- kryptoanaliza: nauka/sztuka łamania szyfrów
- kryptologia: suma powyższych plus całościowe spojrzenie (właściwa nazwa przedmiotu)
  jednak powszechne użycie: kryptografia

kodowanie też ma znaczenie
np. kody poprawiające błędy (*error correction codes*)
w dobrym szyfrze zmiana jednego bitu zaszyfrowanej wiadomości może uniemożliwić odszyfrowanie

## Cztery główne pojęcia

- informacja
  dane, możliwość kopiowania, kradzież??
  tekst jawny – wiadomość
  tekst zaszyfrowany – kryptogram
- uczestnik (entity)
  człowiek, komputer, urządzenie,...
  Alicja, Bolek, Celina, Tadeusz, Pelagia, Wiktor,...
  (*Alice, Bob, Cindy, Trent, Peggy, Victor*)
- przeciwnik, Ewa, Mariola,... (*Eve, Mallory*)
- klucz
  znany nie wszystkim, łatwo zaszyfrować/odszyfrować
  z kluczem, trudno bez klucza
  uwaga: inne znaczenie niż w teorii baz danych



## Złożoność

- *MMMCDLXXVII* $*$ *MDCCCXLIV*
  było trudne dla Rzymian
  ale nie dziś: $3477 * 1844 = 6411588$
- złożoność asymptotyczna, zależy od wielkości zadania, parametr $n \to \infty$
  - liniowa: $n$, żadna złożoność
  - wielomianowa, np.: $n^2, n^3, n^{100}$
  - wykładnicza, np.: $2^n, n!, n^n$
  - podwykładnicza, np.: $e^{\sqrt{n}}$, $e^{C \cdot \sqrt[3]{n \cdot \ln 2 \cdot \ln(n \cdot \ln 2)}}$
- stała też się liczy, np. $n = 1024$ bity i tylko ta wielkość nas interesuje



## np. $n^3$ vs. $e^{2 \cdot \sqrt{n}}$

| n | n**3 | 2*sqrt(n) | exp(2*sqrt(n)) |
|---|---|---|---|
| 2 | 8 | 3 | 17 |
| 4 | 64 | 4 | 55 |
| 8 | 512 | 6 | 286 |
| 16 | 4096 | 8 | 2981 |
| 32 | 32768 | 11 | 81937 |
| 64 | 262144 | 16 | 8886111 |
| 128 | 2097152 | 23 | 6713706353 |
| 256 | 16777216 | 32 | 78962960182681 |
| 512 | 134217728 | 45 | 4.507385299E+0019 |
| 1024 | 1073741824 | 64 | 6.235149081E+0027 |
| 2048 | 8589934592 | 91 | 2.031652223E+0039 |
| 4096 | 68719476736 | 128 | 3.887708406E+0055 |
| 8192 | 549755813888 | 181 | 4.127610756E+0078 |
| 16384 | 4398046511104 | 256 | 1.511427665E+0111 |
| 32768 | 35184372088832 | 362 | 1.703717056E+0157 |



## Założenia kryptografii

- przestrzeń tekstów jawnych $M$, kluczy $K$, kryptogramów $C$
  - algorytm generowania klucza $G : \to K$
  - algorytm szyfrowania $E : K \times M \to C$ ( czy deterministyczny ? )
  - algorytm odszyfrowywania $D : K \times C \to M$
- zasada Kerckhoffsa (1883):
  przeciwnik zna szyfr (tzn. protokół/algorytmy)
  przeciwnik ma duże zasoby obliczeniowe i duże umiejętności
  przeciwnik NIE ZNA klucza
- dlaczego?
  łatwiej utrzymać w tajemnicy klucz niż algorytm
  nie da się opracować wielu (tajnych) algorytmów
- JEDYNY BEZPIECZNY szyfr: jednorazowy
  w zasadzie nie ma dowodów, że inne szyfry są bezpieczne

## Scenariusze ataków

- przeciwnik ma tylko tekst zaszyfrowany
- przeciwnik ma przykłady tekstów jawnych plus ich zaszyfrowane wersje
- przeciwnik może zaszyfrować żądaną wiadomość lub odszyfrować żądany tekst

- ataki pasywne vs. aktywne
- ilość: duża liczba tekstów lub par tekstów vs. pojedynczy tekst zaszyfrowany
- atak brutalny: przeszukiwanie całej przestrzeni kluczy $K$
  - aby zadziałał musi być metoda rozpoznania znalezienia klucza
  - przestrzeń kluczy musi być duża, np. $> 2^{60}$ elementów

Podstawy kryptografii
Andrzej M. Borzyszkowski
Wykład 1
Złożoność
Założenia kryptografii
Kryptografia klasyczna vs. współczesna
Kryptografia klucza asymetrycznego
Kryptografia klasyczna

## Cele kryptografii

- poufność (tajność)
  – tylko uprawnieni uczestnicy mają dostęp do informacji, szyfrowanie, klucz
- integralność danych
  – dane są niezmienione (wykrycie zmiany, również/głównie celowej)
- uwierzytelnianie
  – w czasie rzeczywistym: identyfikacja uczestnika
  – odłożone w czasie: identyfikacja źródła dokumentu
- niezaprzeczalność
  – podpis: nie można się wyprzeć
  – niemożliwa w kryptografii klucza symetrycznego

Podstawy kryptografii
Andrzej M. Borzyszkowski
Wykład 1
Złożoność
Założenia kryptografii
Kryptografia klasyczna vs. współczesna
Kryptografia klucza asymetrycznego
Kryptografia klasyczna

## Kryptografia klasyczna vs. współczesna

- tekst jawny $\rightarrow$ tekst zaszyfrowany $\rightarrow$ tekst jawny
  $M \rightarrow E_K M \rightarrow D_K E_K M$ (zawsze przekształcenie z kluczem)
- klasyczna kryptografia (do lat '70): ten sam klucz
  – obie strony muszą wymienić klucz wspólny klucz
  – jak to zrobić?
- współczesna kryptografia: para kluczy (kryptografia asymetryczna, PKC),
  – idea: Diffie, Hellman (1976)
  – implementacja: RSA (Rivest, Shamir, Adleman) (1977)
  – wada: słaba wydajność
  – zaleta: nie trzeba przedtem przekazywać klucza

Podstawy kryptografii
Andrzej M. Borzyszkowski
Wykład 1
Złożoność
Założenia kryptografii
Kryptografia klasyczna vs. współczesna
Kryptografia klucza asymetrycznego
Kryptografia klasyczna

## Kryptografia klucza asymetrycznego

- przykład zastosowania
  1. Alicja prosi Bolka o przekazanie klucza publicznego, albo odczytuje z ogłoszenia, albo od wspólnego znajomego
  2. szyfruje wiadomość kluczem publicznym Bolka
  3. przekazuje wiadomość $E_B M$
  4. Bolek odszyfrowuje wiadomość swoim kluczem prywatnym $D_B E_B M = M$
- NIKT nie przesyła tajnego klucza
- problem: czy to naprawdę Bolek przekazał klucz publiczny?!

## Kryptografia klasyczna

- szyfr Cezara
  – przesunięcie liter np. o 3 t.j. $y = x + 3 \mod 26$, $x = 0, 1, \ldots, 25$
  – kryptoanaliza: wypróbowanie 25 przesunięć
  – jedna litera pary tekst jawny+zaszyfrowany wystarczy!
- szyfr afiniczny: $y = ax + b \mod 26$
  – odszyfrowywanie: $x = (y - b)/a \mod 26$
  – musi być określone dzielenie $1/a = a'$ t.ż. $a \cdot a' = 1$ mod 26 istnieje w.t.w. gdy $NWD(a, 26) = 1$
  – dla klucza $(13, 4)$ „input" i „alter" szyfrują się do „ERRER"
  – kryptoanaliza: przestrzeń kluczy ma 312 elementów
  – dwie litery tekstu jawnego+zaszyfrowanego często wystarczą, kilka par prawie na pewno