

Stefan Sokołowski

# KRYPTOGRAFIA

wykład 1

Inst. Informatyki Stosowanej, ANS  
Elbląg, 2026/2027

Wykład 1, str. 1

## Cele kryptografii (kryptografia = szyfrowanie)



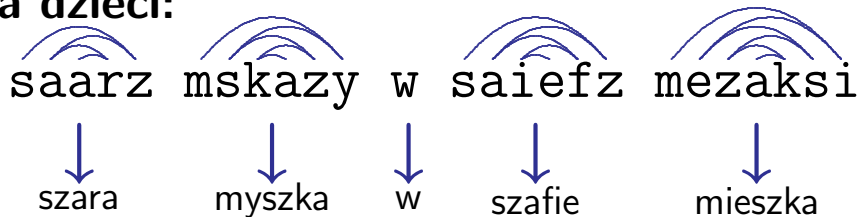
**Poufność:** żeby osoby nieuprawnione nie miały dostępu do treści



**Uwierzytelnienie:** żeby nie było wątpliwości, kto jest autorem

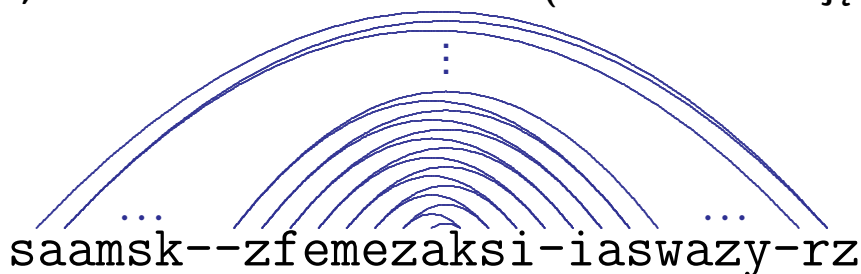
## Klasyka: proste przestawienia

### Szyfr dla dzieci:



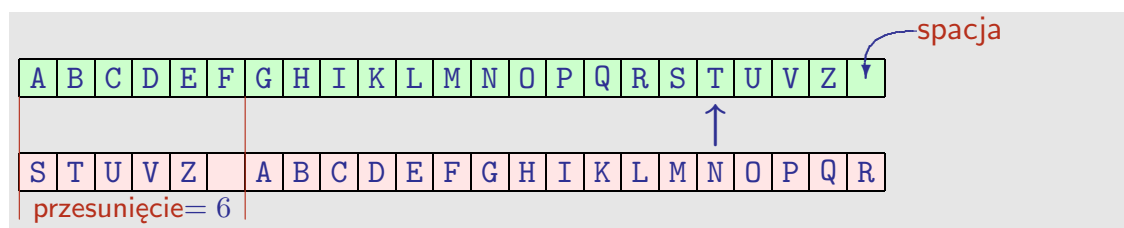
- szyfrowane jest każde słowo z osobna, a interpunkcja (w tym spacje) jest zachowana;
- ciąg liter w słowie jest przestawiany w taki sposób, że najpierw wypisywane są litery z pozycji parzystych (0-wa, 2-ga, ...), a potem dopisywane są litery z pozycji nieparzystych w odwrotnej kolejności.

### To samo, ale całe zdanie na raz (kreseczki oznaczają spacje):



## Klasyka: szyfr Cezara

To jest szyfr z kluczem, który trzeba znać, żeby szyfrować i odszyfrowywać. Kluczem w szyfrze Cezara jest liczba określająca **przesunięcie** w alfabecie:



SEZSRCSUNSRZMN

↓

ALEA IACTA EST = kości zostały rzucone

## Proste przestawienia

„Szyfr dla dzieci” jest przykładem prościutkiego szyfru **przestawieniowego** (przestawiamy litery w słowie lub zdaniu).

**Przykład:** (inny przykład szyfru przestawieniowego)

Tekst jawny wpisujemy do kwadratowej tablicy wierszami.  
Szyfrogram otrzymamy, odczytując go kolumnami.

tekst jawny (48 znaków):

KTO, MOGĄC WYBRAĆ, WYBRAŁ ZAMIAST DOMU...

tablica  $7 \times 7$  miejsc:

|   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|
| K | T | O | , |   | M | O |
| G | A | C |   | W | Y | B |
| R | A | Ć | , |   | W | Y |
| B | R | A | Ł |   | Z | A |
| M | I | A | S | T |   | D |
| O | M | U | . | . | . |   |

szyfrogram:

KGRBMOTĄARIMOCĆAAU, ,ŁS. W T.MYWZ .OBYAD

## Proste przestawienia

**Szyfry przestawieniowe są słabe (= na ogół łatwe do złamania).**

Można je trochę komplikować przez ustalanie bardziej skomplikowanych schematów przestawiania liter. Na ogół

- rysuje się jakąś figurę geometryczną,
- wypełnia się ją literami tekstu jawnego wg jakiejś zasady,
- poddaje się ją jakiemuś przekształceniu (np. obrotowi, lub odbiciu),
- odczytuje się szyfrogram wg tej samej zasady z przekształconej figury.

Współcześnie metody przestawieniowe stosuje się jako uzupełnienie innych metod szyfrowania.



## Podstawienia z kluczem

— za każdą literę podstawiać inną, ale nie zawsze tą samą, tylko wg *klucza*, którym może być dowolny dłuższy tekst.

**Przykład:** (klucz: „Kwiaty polskie” Tuwima)

| ALFABET |    |      |
|---------|----|------|
|         | 0  | N 14 |
| A       | 1  | O 15 |
| B       | 2  | P 16 |
| C       | 3  | Q 17 |
| D       | 4  | R 18 |
| E       | 5  | S 19 |
| F       | 6  | T 20 |
| G       | 7  | U 21 |
| H       | 8  | V 22 |
| I       | 9  | W 23 |
| J       | 10 | X 24 |
| K       | 11 | Y 25 |
| L       | 12 | Z 26 |
| M       | 13 |      |

|              |    |    |    |    |   |    |    |   |    |    |   |    |    |    |    |   |   |    |     |    |     |
|--------------|----|----|----|----|---|----|----|---|----|----|---|----|----|----|----|---|---|----|-----|----|-----|
| tekst jawny: | K  | O  | C  | H  | A | M  | C  | I | E  | S  | K | R  | Y  | C  | I  | E |   |    |     |    |     |
| nry liter:   | 11 | 15 | 3  | 8  | 1 | 13 | 0  | 3 | 9  | 5  | 0 | 19 | 11 | 18 | 25 | 3 | 9 | 5  |     |    |     |
| klucz:       | B  | U  | K  | I  | E | T  | Y  | W | I  | E  | J | S  | K  | I  | E  | J | A | K  | ... |    |     |
| nry liter:   | 2  | 22 | 11 | 9  | 5 | 20 | 25 | 0 | 23 | 9  | 5 | 10 | 19 | 11 | 9  | 5 | 0 | 10 | 1   | 11 | ... |
| sumy mod 27: | 13 | 10 | 14 | 17 | 6 | 6  | 25 | 3 | 5  | 14 | 5 | 2  | 3  | 2  | 7  | 8 | 9 | 15 |     |    |     |
| szyfrogram:  | M  | J  | N  | Q  | F | F  | Y  | C | E  | N  | E | B  | C  | B  | G  | H | I | O  |     |    |     |

Te same litery są kodowane różnie zależnie od klucza; np.

C → N

C → C

C → H

To jest lekko zmieniony  
szyfr Vigenère'a z 1553  
„le chiffre indéchiffrable”

Nikt oprócz nadawcy i odbiorcy nie powinien znać klucza.

## Szyfrowanie systemem arcyksięcia Albrechta

Jaroslav Hašek „Przygody dobrego wojaka Szwejka” t. III, rozdz. I

— Mówiłem już o nowym sposobie szyfrowania depesz w polu, a jeśli panowie nie wiedzieli, dlaczego polecono wam właśnie jedną z nowel Ludwika Ganghofer'a, *Die Sünden der Väter*, stronica 161, to dodam, że to jest klucz do tej nowej metody, obowiązującej na podstawie nowego rozporządzenia sztabu korpusu, do którego zostaliśmy przydzieleni.

Jeśli na przykład dostaniemy rozkaz: „Auf der Kote 228, Maschinengewehrfeuer linksrichten” — to otrzymujemy, moi panowie, taką depeszę: „Sache... mit... uns... das... wir... aufsehen... in... die... wirklich... denke... Idee... ganz... herrscht... Stimme... letzten”.

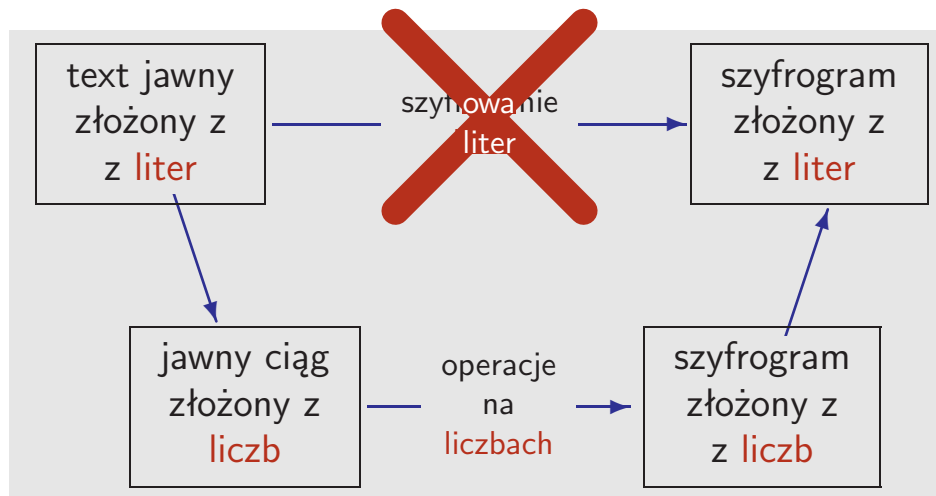
„Grzechy ojców”

„Na wzgórzu 228  
ogień karabinów  
maszynowych  
kierować w lewo”

Bierze *Die Sünden der Väter*, otwiera książkę na stronicy 161 i szuka na górze na przeciwległej stronicy, 160, słowa „Sache”. Proszę panów, po raz pierwszy słowo „Sache” znajdujemy na stronicy 160, jako kolejne słowo 52, więc na przeciwległej stronicy 161 odszukujemy 52 literę na górze, Zauważmy, że jest to litera „a”. Dalszym słowem depeszy jest

To jest szyfr **podstawieniowy** — słowa za litery  
wg klucza, którym jest fragment powieści

## Matematyka i informatyka w szyfrowaniu



Zasady przekształcania liczb są łatwiejsze do zaprogramowania niż zasady przekształcania tekstów.

O przekształcaniu liczb łatwiej jest rozumować niż o przekształcaniu tekstów.

## Matematyka i informatyka w szyfrowaniu

char — 8 bitów } — jak *umieścić* 4 litery w liczbie całkowitej?  
 int — 32 bity } — jak *wydobyć* 4 litery z liczby całkowitej?

```

liczba = 0;
for(i=0; i<4; i++) {
    liczba = liczba*256; // przesunięcie w lewo o 8 bitów
    liczba = liczba+(char)litera[i];
    // wstawienie kolejnej litery
    // w wolne 8 bitów na prawym końcu liczby
}
  
```

Zapisujemy litery **ROK3** :

|                    |                    |                    |                    |
|--------------------|--------------------|--------------------|--------------------|
| kod ascii <b>R</b> | kod ascii <b>O</b> | kod ascii <b>K</b> | kod ascii <b>3</b> |
| 82                 | 79                 | 75                 | 33                 |

Wynik:

$$((82 \cdot 256 + 79) \cdot 256 + 75) \cdot 256 + 33 = 1\,380\,928\,289$$