

## KRYPTOLOGIA

# Szyfrowanie symetryczne

Coraz więcej ludzi uczy się i pracuje dziś zdalnie.

Gdy pracujemy przez Internet, należy zadbać o bezpieczeństwo danych.

**Wymień rodzaj danych, o których bezpieczeństwo w Internecie chcesz dbać.**

Ale jak to zrobić?

**Zacznijmy od wiadomości:**

KFTUFN HJSM 4 UFDI

**Czy potrafisz ją odczytać? Dlaczego nie?**

Jeżeli odpowiedziałś: dlatego, że jest **zakodowana** lub **zaszyfrowana**, to masz rację!

Specjaliści, którzy wykorzystują matematykę do tworzenia takich kodów, są nazywani **kryptologami**.

Mastercard korzysta z **kluczy**, aby szyfrować informacje przesyłane w swojej sieci.

Wyobraź sobie kłódkę.  Aby ją zamknąć i otworzyć potrzebujesz konkretnego klucza .

Jeżeli ten sam **klucz** służy do blokowania i odblokowania wiadomości, nazywa się go **algorytmem symetrycznym**.

Szyfrowanie  
zamiana  
informacji w kod,  
szczególnie po to,  
by uniemożliwić  
dostęp osobom  
niepożądanym

Symetryczny  
złożony z dwóch  
części będących  
swoim odbiciem



## KRYPTOLOGIA

# Szyfrowanie symetryczne

Jednym z przykładów algorytmu symetrycznego jest **kod ROT1**.

Polega on na przesunięciu liter o jedną.

A zamienia się w B, B zamienia się w C.

Kod ROT1 jest **kluczem** stosowanym do zakodowania wiadomości.

KFTUFN HJSM 4 UFDI

Czy teraz możesz to odczytać? Co tam jest napisane?

Spróbuj zaszyfrować własną wiadomość, korzystając z kodu ROT1.

Zobacz, czy inni będą potrafili ją odgadnąć.

Możliwe, że będziesz musiała zdradzić klucz!

A co jeżeli ktoś znajdzie, odgadnie lub ukradnie klucz?

Ponieważ ten sam klucz służy do szyfrowania i odszyfrowania informacji, dość łatwo jest odkodować wiadomość.

## ROT 1 CODE

LETTER	WRITTEN AS...
A	B
B	C
C	D
D	E
E	F
F	G
G	H
H	I
I	J
J	K
K	L
L	M
M	N
N	O
O	P
P	Q
Q	R
R	S
S	T
T	U
U	V
V	W
W	X
X	Y
Y	Z
Z	A

## KRYPTOLOGIA

# Tokenizacja

A co jeżeli związek między danymi a szyfrowaniem będzie losowy?

Co jeżeli nie można zaobserwować prawidłowości?

**Spójrzmy na inną wiadomość. Czy możesz ją odczytać?**



To     T     O     K     E     N     I     Z     A     C     J     A

To kolejna forma szyfrowania, która pozwala na ochronę danych.

W powyższych przykładach każda litera jest zastąpiona tokenem, np. emotikonem.

Jakie inne losowe tokeny przychodzą Ci na myśl?

Zaszyfruj swoją wiadomość, tworząc własne tokeny.

Użyj wyobraźni, by stworzyć **tokeny** w poniższej tabeli.

Mogą to być symbole, obrazy lub nawet kolory!

**Tokenizacja to proces zastępowania danych wymagających szczególnej ochrony tzw. tokenem, który nie jest szczególnie chroniony.**

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

Zaszyfruj tu swoją wiadomość.

Spytaj innych, czy potrafią odkodować twoją tajną wiadomość.

Zastanów się teraz, które z rozwiązań – **algorytm symetryczny tokenizacja** – wydaje się bezpieczniejsze?

Pomyśl o drzwiach z zamkiem. Jeden klucz, żeby wejść i wyjść? CZY może wiele kluczy i wiele zamków?

Jeżeli uważasz, że **tokenizacja** to bezpieczniejsze rozwiązanie, to masz rację.

**Jesteś specjalistką ds. kryptologii Girls4Tech!**

CERTYFIKAT

Gratulacje!

JESTEŚ CERTYFIKOWANĄ  
**SPECJALISTKĄ DS. KRYPTOLOGII**



A handwritten signature in black ink, appearing to read "Michael Miebach".

**Michael Miebach**  
CEO, Mastercard

A handwritten signature in black ink, appearing to read "Susan Warner".

**Susan Warner**  
Founder, Girls4Tech