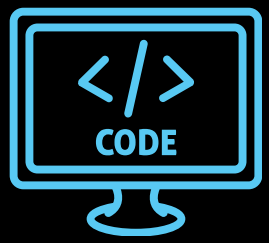

DeepDive™

Projekty matematyczne



Projekty programistyczne

Aplikacje webowe

Artykuły popularnonaukowe

Wydarzenia

Integracje

DeepDive™

Co to kryptologia i kryptografia?

DeepDive™

Kryptologia

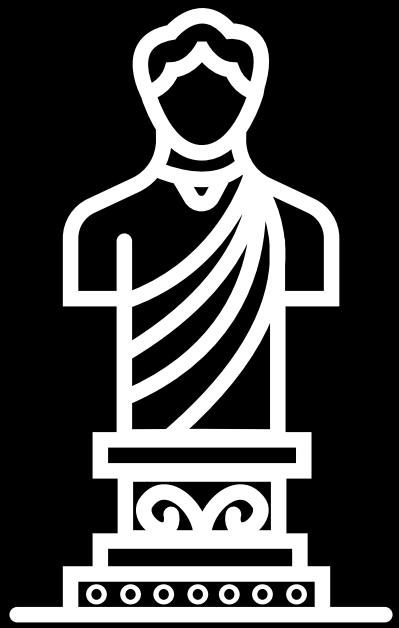
nauką o szyfrowaniu danych w sposób bezpieczny tak, aby tylko osoby posiadające odpowiednie narzędzia i klucze mogły odczytać zaszyfrowaną treść lub pliki

Kryptografia

stosowanie kryptologii, czyli tworzenie algorytmów i ich zastosowanie w celu zabezpieczania i szyfrowania informacji

Kryptologia

jedna z najstarszych nauk,
używana już w czasach starożytnych



DeepDive™

Znaczenie kryptografii

DeepDive™

Znaczenie kryptografii

W dzisiejszej erze informacji bezpieczny przekaz danych jest wymogiem. Bez szyfrowania danych hasła do naszych portali społecznościowych czy inne dane takie jak numery kart kredytowych, adresy i inne krążyłyby po Internecie w formie czytelnej dla każdego.

Nikt nie chce aby ktoś inny mógł dostać się do naszego konta bankowego i wziął kredyt, albo przeglądał lub tworzył kontrowersyjne posty na FB, IG i Snapie.

Szyfrowanie vs Hashowanie

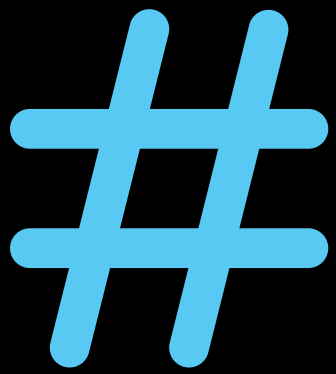
Szyfrowanie i hashowanie to dwie różne, ale powiązane ze sobą techniki bezpieczeństwa danych.

Szyfrowanie to proces przekształcania danych w **nieczytelny format, zwany szyfrogramem, za pomocą klucza.**
Klucz ten jest niezbędny do **odszyfrowania danych** z powrotem do oryginalnej postaci.

DeepDive™

Szyfrowanie vs Hashowanie

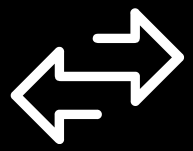
Hashowanie to **jednokierunkowa funkcja matematyczna**, która przekształca dowolny ciąg danych w ciąg o stałej długości, zwany hashem. Hashowanie nie służy do odwracania procesu, czyli odzyskania oryginalnych danych z hasha.



DeepDive™

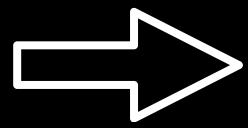
Szyfrowanie vs Hashowanie

odwracalne



służy do ochrony poufności danych

nieodwracalne



służy do weryfikacji integralności danych

DeepDive™

Najprostsze szyfry

Kryptologia jest jedną z najstarszych nauk używanych już w czasach starożytnych.

Jednym z przykładów prostych algorytmów używanych jeszcze przed naszą erą jest szyfr Cezara, należący do rodziny szyfrów substytucyjnych, tzn. każdy symbol ma swój odpowiednik w danym kluczu.

Jakie są najprostsze szyfry?

DeepDive™

Najprostsze szyfry

Jednym z przykładów prostych algorytmów używanych jeszcze przed naszą erą jest szyfr Cezara, należący do rodziny **szyfrów substytucyjnych**, tzn. każdy symbol ma swój odpowiednik w danym kluczu.

DeepDive™

Szyfr Cezara

Opiera się na przesunięciu znaków alfabetu o daną ilość.

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

Sam algorytm jest też bardzo prosty w szyfrowaniu i odszyfrowywaniu.
Szyfr = (Np litery + przesunięcie) mod Ilość znaków w alfabecie

DeepDive™

W dzisiejszych czasach...

Kryptografia odgrywa kluczową rolę w dzisiejszym świecie, zapewniając bezpieczeństwo danych i komunikacji w różnych dziedzinach.

Jest niezbędna w dzisiejszym cyfrowym świecie, a jej zastosowania i algorytmy ciągle się rozwijają, aby sprostać rosnącym wymaganiom bezpieczeństwa.

Zastosowania kryptografii

- Bezpieczna komunikacja
  - Używana w protokołach takich jak HTTPS, który zabezpiecza połączenia internetowe, chroniąc dane przesyłane między przeglądarką a serwerem.

- Zabezpieczanie transakcji finansowych
  - W sektorze bankowym: ochrony danych finansowych oraz zabezpieczanie transakcji online.

Zastosowania kryptografii

- Ochrona danych osobowych
  - W e-commerce i usługach online chroni dane użytkowników (tj. hasła i informacje osobiste).
- Podpisy cyfrowe
  - Używane do weryfikacji tożsamości nadawcy oraz integralności wiadomości
- Szyfrowanie end-to-end
  - Stosowane w komunikatorach, jak WhatsApp, aby zapewnić, że tylko nadawca i odbiorca mogą odczytać wiadomości.

Współczesne algorytmy

AES (Advanced Encryption Standard)

- Uznawany za jeden z najbezpieczniejszych algorytmów szyfrowania, używa kluczy o długości 128, 192 lub 256 bitów.

RSA (Rivest-Shamir-Adleman)

- Popularny algorytm asymetryczny, używany do szyfrowania danych oraz do podpisów cyfrowych.

SHA (Secure Hash Algorithm)

- Rodzina funkcji skrótu, w tym SHA-256, używana do weryfikacji integralności danych.

ECDSA (Elliptic Curve Digital Signature Algorithm)

- Algorytm podpisu cyfrowego oparty na krzywych eliptycznych, oferujący wysoki poziom bezpieczeństwa przy krótszych kluczach.


DeepDive™