Czym jest szyfrowanie?

Jakub Juszczakiewicz

2026-07-14

W celu zrozumienia czym jest szyfrowanie musimy cofnąć się do czasów Cesarstwa Rzymskiego. Pierszy znany szyfr został opracowany przez Juliusza Cezara na potrzeby przekazywania rozkazów między nim a jego dowódcami. Metoda była prosta i polegała na podmianie liter w słowach, jakby przesuwając je o 3, tzn. zamiast „A“ zapisywano „D”, zamiast „B“ - „E”, zamiast „C“ - F itd. jak w poniższej tabelce:

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

Łatwo zauważyć, że sam pomysł można uogólnić i przyjąć liczbę o którą przesuwamy alfabet za parametr. Np. ktoś może ustalić, że przesuwa litery o 10. Taki parametr nazywamy kluczem. Żeby odczytać tekst, który jest zaszyfrowany, potrzebujemy znać algorytm (w tym wypadku przestawianie liter) i klucz. W przeciwnym razie taki tekst będzie dla nas nieczytelny.

Ogólnie szyfrowanie polega na zapisanie wiadomości w taki sposób, żeby bez znajomości algorytmu i klucza do niego nie dało się odczytać przekazywanej treści.

W czasach współczesnych szyfr Cezara jest prosty do złamania - wystarczy znać język wiadomości. Wtedy można wziąć statystyczną częstotliwość występowania danych liter w tekstach danego języka i porównać z tym, co jest w zaszyfrowanym tekście. Dodatkowo współcześnie zakłada się, że algorytm szyfrowania jest zawsze znany i tylko jego złożoność jest problemem.

Współczesne algorytmy są zdecydowanie bardziej zaawansowane, jeśli chodzi o ich skuteczność (siłę), ale idea jest ta sama - bez znajomości algorytmu i klucza niewiele da się zrobić.