Permutation - What it is in cryptography and how it differs from substitution

Gridinsoft Help Center

What it is

A permutation is a cryptography trick that rearranges characters or bits without changing them. Think of it as shuffling the deck - the same cards, new order. By itself it only hides the order, but combined with other steps it helps build strong ciphers.

Why it matters

Permutation is a core building block in both old-school ciphers and modern algorithms. Paired with substitution (changing symbols), it creates the mix-and-mash that makes patterns hard to spot and messages hard to crack.

How it works - quick tour

- Start with a message and a secret rule (the key) that tells where each character moves.

- Example: using the rule 3-1-5-2-4, HELLO becomes LHOEL (take letters in that order).

- Modern encryption applies many rounds of substitution + permutation to scramble data thoroughly.

Good to know

- Permutation vs substitution: permutation only reorders, substitution changes symbols.

- Because permutation keeps letter counts the same, it’s usually paired with substitution to defeat frequency analysis.