

Caesar's Cipher

Enkripsi menggunakan algoritma tertentu yang mengubah data asli menjadi data terenkripsi. Algoritma tersebut biasa disebut Cipher. Salah satu cipher yang sederhana adalah Caesar's Cipher yang melakukan penggeseran alfabet. Algoritma ini menggunakan nama Caesar karena terinspirasi oleh Julio Caesar seorang Kaisar Romawi yang menggunakan algoritma ini saat berkorespondensi.

Contoh penggeseran alfabet dengan Caesar's Cipher sebanyak sekali ke kanan:

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

Sehingga teks:

"selamat ulang tahun" akan menjadi "rdkzlzs tkzmf szgtm"

"ini adalah teks biasa" akan menjadi "hnh zczkzg sdjr ahzrz"

Bisakah kalian menebak teks asli: "zjt zczkzg zmzj fdlazkz"? "hmenqlzshjz rlo"?

Mengubah kembali teks yang telah terenkripsi menjadi teks asli disebut melakukan dekripsi. Dekripsi adalah proses yang membalik enkripsi, mengambil pesan rahasia dan mereproduksi teks asli.

Enkripsi dengan penggeseran alfabet dengan Caesar's Cipher ialah cara yang sederhana. Ada cara yang lebih sulit untuk enkripsi alfabet daripada hanya menggeser, misalnya dengan mengubah suatu huruf dengan huruf yang lain. Contoh pengubahan:

Original:	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
Intape to:	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

Sehingga teks:

"selamat ulang tahun" akan menjadi "zmucwcr fucdq rcsfd"

"ini adalah teks biasa" akan menjadi "jdj cecucs rmxz kjczc"

Bisakah kalian menebak teks asli: "zmucwcr ecrdq"? "wcxd gcqj zfecszjcg"?

Enkripsi dengan cara ini akan menjadikan teks hasil menjadi lebih sulit untuk dikembalikan ke teks aslinya daripada dengan Caesar's Cipher.