Ceaser cypher

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plaintext = RED

Key = 13

➔ Encryption (direct substitution)

R → E, E → R, D → Q

➔ Encryption (algebraic representation)

$c_i = (p_i + K) \bmod 26$

$p_1 = R = 17, k = 13$

$c_1 = (17 + 13) \bmod 26$

$c_1 = 30 \bmod 26$

$c_1 = 4 = E$

$p_2 = E = 4, k = 13$

$c_2 = (4 + 13) \bmod 26$

$c_2 = 17$ mode 26

$c_2 = 17 = R$

$p_3 = D = 3, k = 13$

$c_3 = (3 + 13) \bmod 26$

$c_3 = 16 \bmod 26$

$c_3 = 16 = Q$

Cyphertext = ERQ

➔ Decryption (direct substitution, counting backwards)

E → R, R → E, Q → D

➔ Decryption (algebraic representation)

$p_i = (c_i - k) \bmod 26$

$c_1 = E = 4, k = 13$

$p_1 = (4 - 13) \bmod 26$

$p_1 = -9 \bmod 26$

$p_1 = 26 - (9 \bmod 26)$

$p_1 = 26 – 9$

$p_1 = 17 = R$

$c_2 = R = 17, k = 13$

$p_2 = (17 - 13) \bmod 26$

$p_2 = 4 \bmod 26$

$p_2 = 4 = E$

$c_3 = Q = 16, k = 13$

$p_3 = (16 - 13) \bmod 26$

$p_3 = 3 \bmod 26$

$p_3 = 3 = D$

Plaintext = RED

➔ **Breaking the cypher:** If a 3rd party gains access to at least two pairs of the plaintext and the cyphertext, and the complete cyphertext, the remaining letters of the plaintext can be derived using pattern recognition.

Two pairs of plaintext and cyphertext; R → E, D → Q

It can be seen that there are 13 alphabets mapping to each other and the rest of the plaintext can be obtained.

Multiplicative cypher

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plaintext = RED

Key = 3

gcd(k, 26) = 1

To ascertain that gcd(3, 26) = 1 and find the multiplicative inverse of k (k^{-1}), we use the extended Euclidian algorithm.

➔ Encryption

$c_i = (p_i * K) \bmod 26$

p_1 = R = 17, k = 3

$c_1 = (17 * 3) \bmod 26$

$c_1 = 51 \bmod 26$

$c_1 = 25 = Z$

p_2 = E = 4, k = 3

$c_2 = (4 * 3) \bmod 26$

$c_2 = 12 \bmod 26$

$c_2 = 12 = M$

p_3 = D = 4, k = 3

$c_3 = (3 * 3) \bmod 26$

$c_3 = 9 \bmod 26$

$c_3 = 9 = J$

Cyphertext = ZMJ

➔ Decryption

$p_i = (c_i * k^{-1}) \bmod 26$

To obtain k^{-1}, we first ensure that gcd(3, 26) = 1

26 = 3 * 8 + 2

3 = 2 * 1 + 1 ← remainder is 1, so gcd is 1

1 = 3 - 2 * 1

2 = 26 - 3 * 8

1 = 3 - (26 - 3 * 8) * 1

1 = 9 (3) + (-1) 26

$k^{-1} = 9$

$c_1 = Z = 25, k = 3$

$p_1 = (25 * 9) \bmod 26$

$p_1 = 225 \bmod 26$

$p_1 = 17 = R$

$c_2 = M = 12, k = 3$

$p_2 = (12 * 9) \bmod 26$

$p_2 = 108 \bmod 26$

$p_2 = 4 = E$

$c_3 = J = 9, k = 3$

$p_3 = (9 * 9) \bmod 26$

$p_3 = 81 \bmod 26$

$p_3 = 3 = D$

Plaintext = RED