

A is substituted as Z, B is substituted as Y, and so on.

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	26
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
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A
26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Plaintext = RED

→ **Encryption**

R → I, E → V, D → W

Ciphertext = IVW

→ **Decryption**

I → R, V → E, W → D

Plaintext = RED

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

Two pairs of plaintext and ciphertext; R → I, D → W

It can be seen that in the first pair, the 18th alphabet maps to the 9th alphabet in the reverse order.

$$18 + 9 = 27, \rightarrow 27 - 9 = 18$$

And in the second pair, 4th alphabet maps to the 23rd alphabet in the reverse order.

$$4 + 23 = 27, \rightarrow 27 - 23 = 4$$

Therefore, subtracting the ciphertext numerical value from 27 would result in the plaintext numerical value.