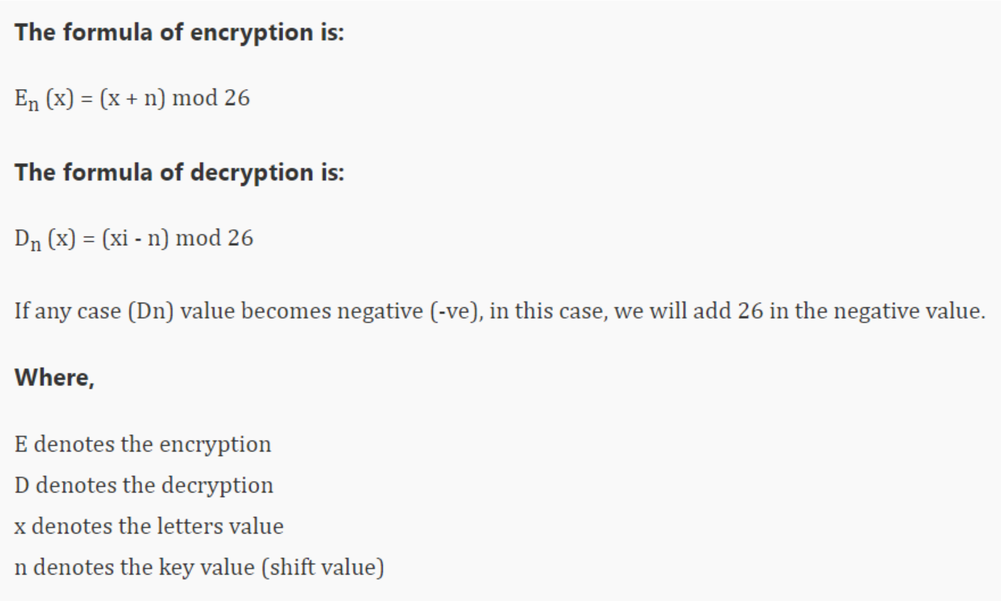
Substitution cipher



The formula of encryption is:

$E_n\,(x) = (x + n) \bmod 26$

The formula of decryption is:

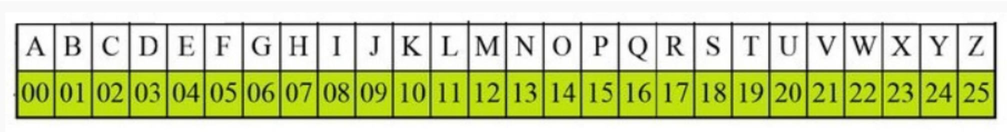
$D_n\,(x) = (xi - n) \bmod 26$

If any case (Dn) value becomes negative (-ve), in this case, we will add 26 in the negative value.

Where,

E denotes the encryption
D denotes the decryption
x denotes the letters value
n denotes the key value (shift value)

Give numbers alphabetically

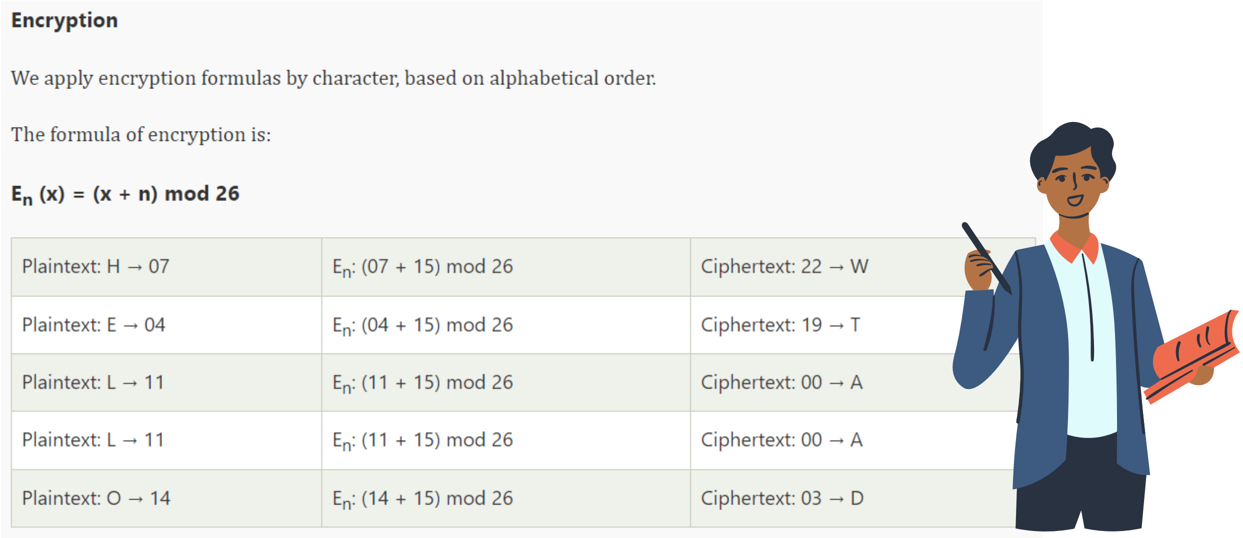


A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- The Caesar cipher is the simplest and oldest method of cryptography. The Caesar cipher method is based on a mono-alphabetic cipher and is also called a shift cipher or additive cipher. Julius Caesar used the shift cipher (additive cipher) technique to communicate with his officers. For this reason, the shift cipher technique is called the Caesar cipher. The Caesar cipher is a kind of replacement (substitution) cipher, where all letter of plain text is replaced by another letter.
- Let's take an example to understand the Caesar cipher, suppose we are shifting with 1, then A will be replaced by B, B will be replaced by C, C will be replaced by D, D will be replaced by C, and this process continues until the entire plain text is finished.
- Caesar ciphers is a weak method of cryptography. It can be easily hacked. It means the message encrypted by this method can be easily decrypted.

Lets see one example

The message "HELLO," and the key (shift) value of this message is 15.



Encryption

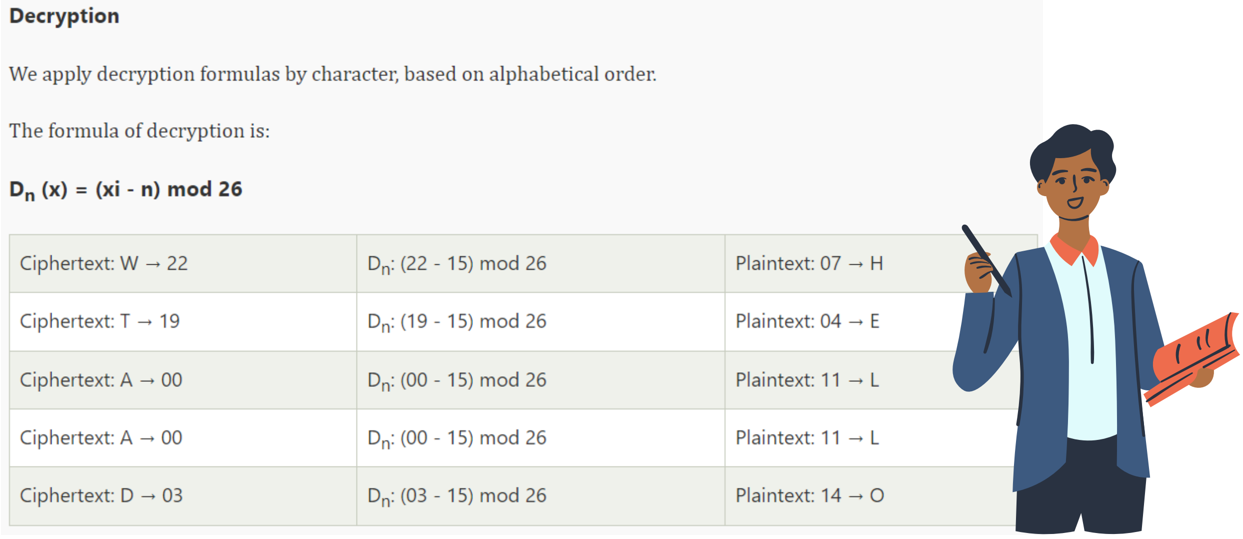
We apply encryption formulas by character, based on alphabetical order.

The formula of encryption is:

E_n (x) = (x + n) mod 26

Plaintext: H → 07	E_n: (07 + 15) mod 26	Ciphertext: 22 → W
Plaintext: E → 04	E_n: (04 + 15) mod 26	Ciphertext: 19 → T
Plaintext: L → 11	E_n: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: L → 11	E_n: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: O → 14	E_n: (14 + 15) mod 26	Ciphertext: 03 → D

The encrypted message of this plain text is "WTAAD".



Decryption

We apply decryption formulas by character, based on alphabetical order.

The formula of decryption is:

D_n (x) = (xi - n) mod 26

Ciphertext: W → 22	D_n: (22 - 15) mod 26	Plaintext: 07 → H
Ciphertext: T → 19	D_n: (19 - 15) mod 26	Plaintext: 04 → E
Ciphertext: A → 00	D_n: (00 - 15) mod 26	Plaintext: 11 → L
Ciphertext: A → 00	D_n: (00 - 15) mod 26	Plaintext: 11 → L
Ciphertext: D → 03	D_n: (03 - 15) mod 26	Plaintext: 14 → O

The decrypted message is "HELLO".