code decoded

one-time pad

A **pad** is a large nonrepeating set of letters.

Each letter in the pad encrypts one character of the plaintext by addition modulo 26.

- The pad characters must be generated randomly.
- The pad sequence can never be reused. If the same key is used, someone can slide the ciphertexts and count the matches to reversely construct the key.
- The pad cannot be smaller than the plaintext.
- The Sender & Recipient both have access to the pad.

Example

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
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

plaintext H E L L O W O R L D

pad A B C D Z Y X W V U

ciphertext I G O P O V M O H Y

H + A mod 26 = I
E + B mod 26 = G
L + C mod 26 = O
L + D mod 26 = P
O + Z mod 26 = O

W + Y mod 26 = V
O + X mod 26 = M
R + W mod 26 = O
L + V mod 26 = H
D + U mod 26 = Y