Cryptography

15 January 2021
11:52

1. Shift cipher ✓
2. Vignere cipher ✓
3. Affine cipher ✓
4. Permutation cipher
5. Autokey cipher

Permutation cipher

given msg = We are studying cryptography

Key =

1	2	3	4
3	4	2	1

Encryption:

steps ① generate the plaintext by removing spaces & special symbols

x = weare studying cryptography , size[x] = 25

② As given key size is 4, so devide the plaintext into blocks of size 4.

K2

1	2	3	4
2	1	4	3

Plaintext Position

1 2 3 4
3 4 2 1

Position

ciphertext

Total No. of blocks = 7

B1	B2	B3	B4	B5	B6	B7
wear	esta	dyin	gcry	ptog	raph	yabc

③ Permute all Blocks according to given Key.

1 2 3 4
wear → rawe
esta → utes
dyin → nidy
gcry → yrgc
ptog → gopt
raph → hpra
yabc → cbya

④ Block after Permutation generate the cipher text.

Decryption:

⑤ convert the cipher text into Block according given key tablesize.

rawe utes nidy yrgc gopt hpra cbya

⑥ convert the given key table for decryption

key for decryption =

3	4	2	1
1	2	3	4

⑦ Apply the permutation on cipher blocks with new key table.

rawe utes nidy yrgc gopt hpra cbya
wear esta dyin gcry ptog raph yabc

⑧ convine the blocks and generate the plaintext and convert it into msg.

we are studying cryptography.