# Modified Playfair Cipher

The modified Playfair cipher is based on additional XOR operation that adds an extra layer of security. XOR operations are crucial to cryptographic implementations as they can be used as a simple cipher for encrypting and decrypting messages with a single key. This is known as symmetric encryption. It acts like a one-time pad.

# Methodology:

## Encryption process:

1) The key value is obtained from the user.
2) The plain-text is also obtained similarly for Playfair cipher.
3) Construct the 5*5 matrix with the key and fill in the alphabets.
4) Find corresponding Playfair encrypted message for the given plaintext.
5) After obtaining the play-fair encrypted message, apply alphabet-wise XOR operation with its corresponding position in English alphabet set.
6) The message is the output from individual XOR operations in given sequence.
7) The final key consist of keyword selected by user and alphabet set used for XOR.

## Decryption Process:

**1)** The cipher text is obtained from user.
**2)** Given symbols' ascii code are XORed with numerical key extracted from the provided keyset.
**3)** After finding the alphabet back, decryption of playfair is applied to get back the original text.

**Example:**

Plaintext: good

Key: love

5*5 matrix creation and key filling:

l o v e a

b c d f g

h i k m n

p q r s t

u w x y z

After matrix preparation, We encrypt using playfair cipher

**Encrypted text**: cavc

Now, we apply character wise XOR operation to double encrypt them.

1st alphabet is c, so c's position in alphabet set is 3 from start.Therefore 3 should be XORed with c to give final output.

C(01100011) (xor) 00000011(3) = 01100000 (ascii representation: ` )

a(01100001) ( xor) 00000001(1) = 01100000 (ascii representation: ` )

v(01110110) (xor) 00010110(22)= 01100000 (ascii representation: ` )

c(01100011) (xor) 00000011(3) = 01100000(ascii representation: `)

final encrypted message: ````

Decryption:

Modified key: cavc + {3,1,22,3};

Numerical part is used for decryption by XORing.

⇨ ` (01100000) (xor) 00000011(3) = 01100011(ascii of 'c')

- ⇨ `(01100000) (xor) 00000001(1)= 01100001( ascii of ‘a’)
- ⇨ `(01100000) (xor) 00010110(22) = 01110110 (ascii of ‘v’ )
- ⇨ `(01100000) (xor) 00000011(3) = 01100011(ascii of ‘c’)

After obtaining the text, we feed that to playfair for decryption and get “love”as original text back.

This eliminates frequency distribution attack as it adds double strong layer of encryption  process rather than conventional one.