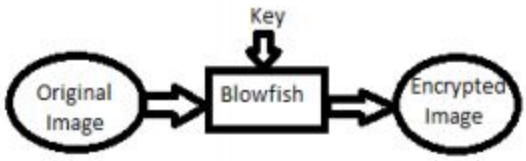
BlowFish Algo

Blowfish is a 64-bit symmetric block cipher that uses a variable-length key from 32 to 448-bits (14 bytes). The algorithm was developed to encrypt 64-bits of plaintext into 64-bits of cipher text efficiently and securely. The operations selected for the algorithm were table lookup, modulus, addition and bitwise exclusive-or to minimize the time required to encrypt and decrypt data on 32-bit processors. A conscious attempt was made in designing the algorithm to keep the operations simple and easy to code while not compromising security. As with DES, Blowfish incorporates a 16 round Feistel network for encryption and decryption. But during each round of Blowfish, the left and right 32-bits of data are modified unlike DES which only modifies the right 32-bits to become the next round's left 32-bits. Blowfish incorporated a bitwise exclusive-or operation to be performed on the left 32-bits before being modified by the F function or propagated to the right 32-bits for the next round. Blowfish also incorporated two exclusive-or operations to be performed after the 16 rounds and a swap operation. This operation is different from the permutation function performed in DES.

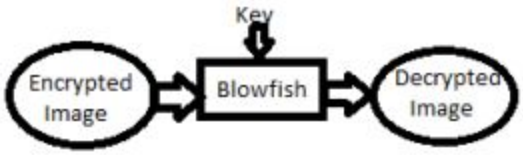
Encryption Process: Data image as a plaintext and the encryption key are two inputs of encryption process. In this case, original image data bit stream is divided into the blocks length of Blowfish algorithm




.

Image header is excluded to encrypt and the start of the bitmap pixel or array begins right after the header of the file. The byte elements of the array are stored in row order from left to right with each row representing one scan line of the image and the rows of the image are encrypted from top to bottom.

Decryption Process: The encrypted image is divided into the same block length of Blowfish algorithm from top to bottom.



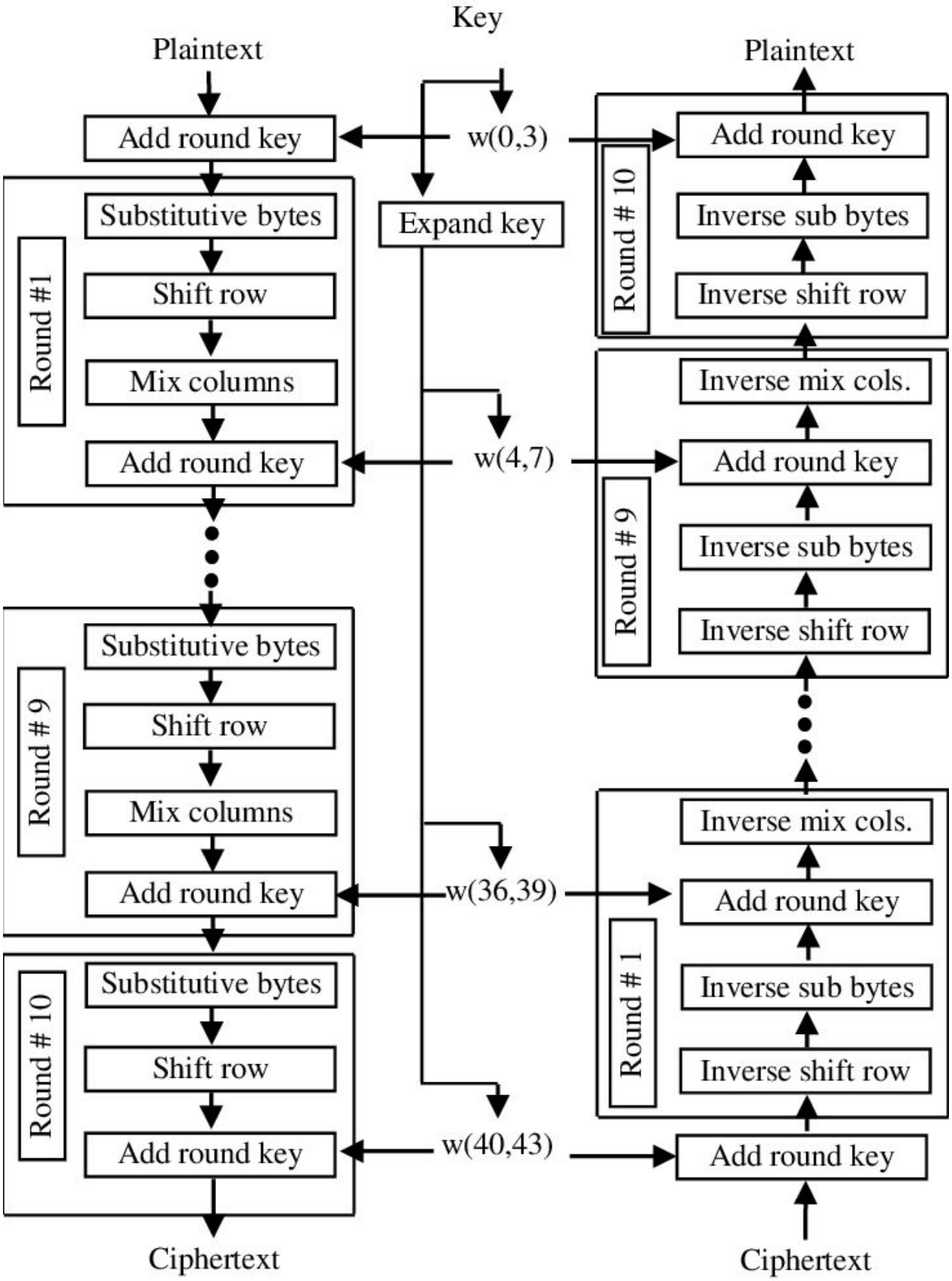
The first block is entered to the decryption function and the same encryption key is used to decrypt the image but the application of sub keys is reversed. The process of decryption is continued with other blocks of the image from top to bottom.

The basic algorithm for Blowfish is illustrated as follows:
Divide X into two 32-bit halves XL and XR
For i=1 to 16:
XL = XL Pi
XR = F (XL) XR
Swap XL and XR
End for Swap XL and XR
XR = XR P17
XL = XL P18
Recombine XL and XR
Output X (64-bit data block: cipher text)

For decryption, the same process is applied, except that the sub-keys Pi must be supplied in reverse order. The nature of the Feistel network ensures that every half is swapped for the next round.

## AES Algorithm

AES is a modern block symmetric cipher, one of the most popular ciphers in the world. It was developed in 1997 by Vincent Rijmen and Joan Daemen, and later approved as a federal encryption standard in the United States in 2002.
A secret key in AES, for both data encryption and decryption, may contain 128 or 192 or 256 bits. Based on the length of the key, a different number of encrypting cycles is performed.
AES is considered as a strong and secure cipher.


Key
Plaintext
Plaintext
Add round key
w(0,3)
Add round key
Round # 10
Inverse sub bytes
Inverse shift row
Substitutive bytes
Expand key
Round #1
Shift row
Mix columns
Inverse mix cols.
Add round key
w(4,7)
Add round key
Round # 9
Inverse sub bytes
Inverse shift row
Substitutive bytes
Round # 9
Shift row
Mix columns
Inverse mix cols.
Add round key
w(36,39)
Add round key
Round # 1
Inverse sub bytes
Inverse shift row
Substitutive bytes
Round # 10
Shift row
Add round key
w(40,43)
Add round key
Ciphertext
Ciphertext

## AES Encryption

1. Preparing Subkeys: one starting subkey is created first, and later one more subkey for every subsequent cycle of encryption (see below).
2. Initial Round: all bytes of data block are added to corresponding bytes of the starting subkey using XOR operation.
3. A number of encrypting cycles takes place. The number of repetitions depends on the length of a secret key:

- 9 cycles of repetition for a 128-bit key,

- 11 cycles of repetition for a 192-bit key,

- 13 cycles of repetition for a 256-bit key.

## AES Description:

During decryption, the encrypted text is used as input data to the algorithm. The corresponding, inverse operations should be performed, as during encryption:

4. Inverse bytes substitution (ISB).
5. Bytes shifting to the right (ISR).
6. Adding XOR to a subkey (IAR).
7. Inverse multiplication of columns (IMC).