Blow Fish Cipher

An unbroken cipher

Introduction

- Blowfish is an encryption technique designed by Bruce Schneier in 1993 as an alternative to DES
- It is a block cipher with a block size of 64
- It uses keys of variable size ranging from 32 to 448 bits
- The number of subkeys used is 18
- The number of substitution boxes used is 4
- And it has 16 rounds
- The encryption process can be divided into two stages: the key expansion stage and the encryption stage.

Key expansion

- Step 1: 18 subkeys(stored in the P-array : P[0]…P[17]) are needed for encryption and the same subkeys are used in decryption. The hex values of pi(∏) (less the initial 3) and stored in an array (S-array) with each element being a 32 bit entry . Each of the entries is XORed with a part of the input key and stored in the P-array as shown below with K being the number of 32 bit divisions in the key:

  $P[0] = S[0] \oplus 1^{st}$ 32-bits of input key

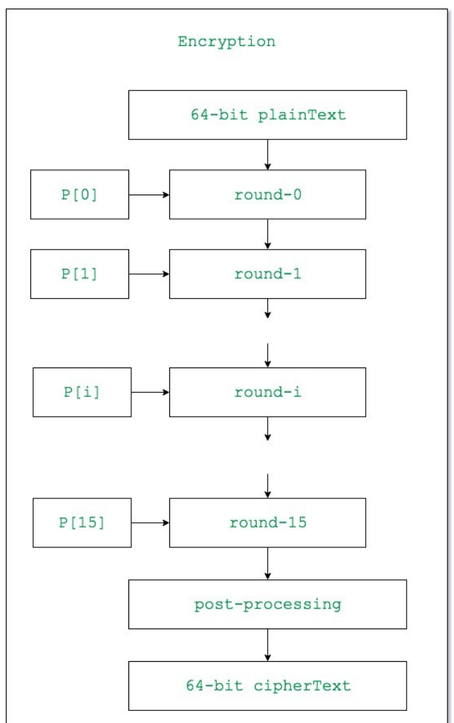
  $P[1] = S[1] \oplus 2^{nd}$ 32-bits of input key

  $P[i] = S[i] \oplus$ ((i+1)%k)th 32-bits of input key

  where k is the input key divided by 32

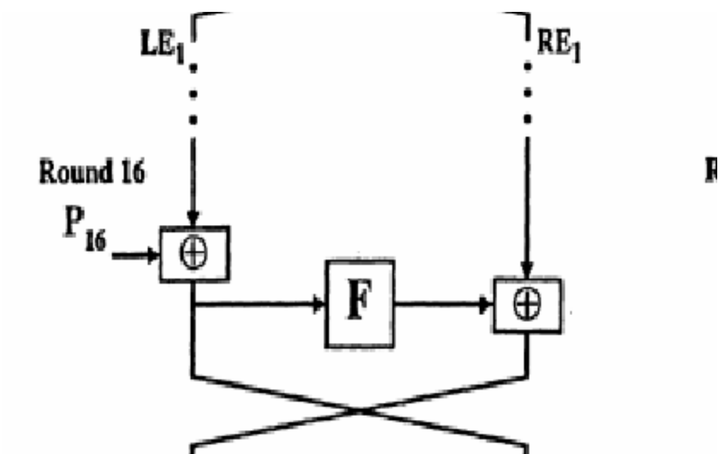
- Step 2: the S-boxes are also initialized with the rest of the hexadecimal values of pi(∏)

Encryption


Encryption
64-bit plainText
P[0]
round-0
P[1]
round-1
P[i]
round-i
P[15]
round-15
post-processing
64-bit cipherText

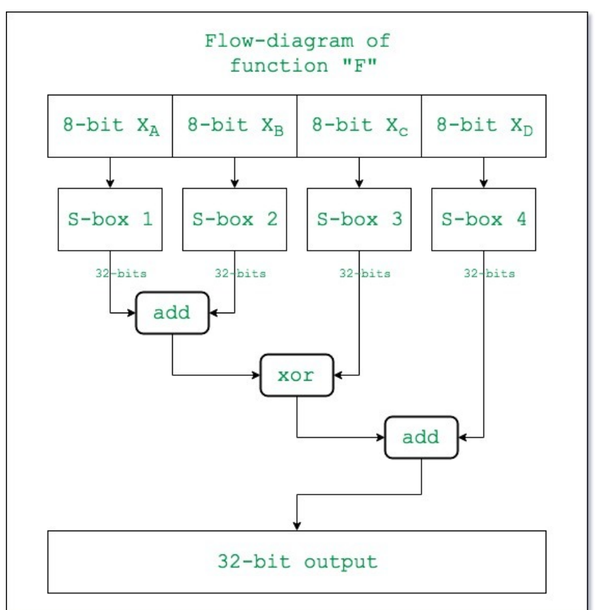
Encryption

- Step 3: The encryption consists of 16 rounds taking inputs from the previous round and corresponding subkey (P[i]).



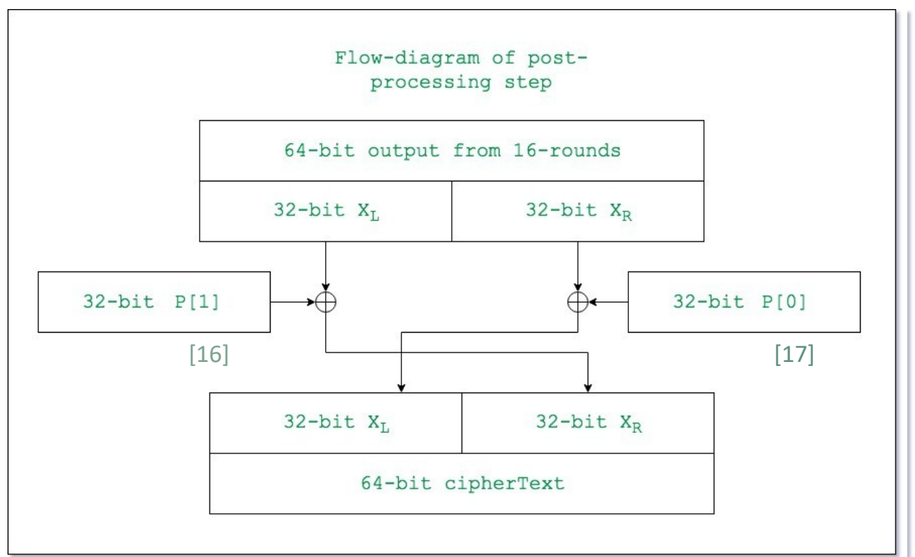
The “F” function

- The description of the “F” function is as follows:



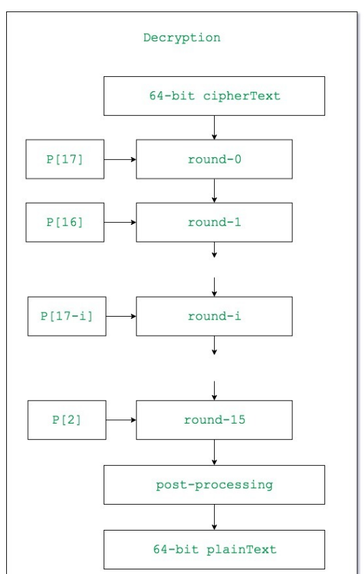
Post-processing

- The output after 15 rounds goes through the post-processing round as follows

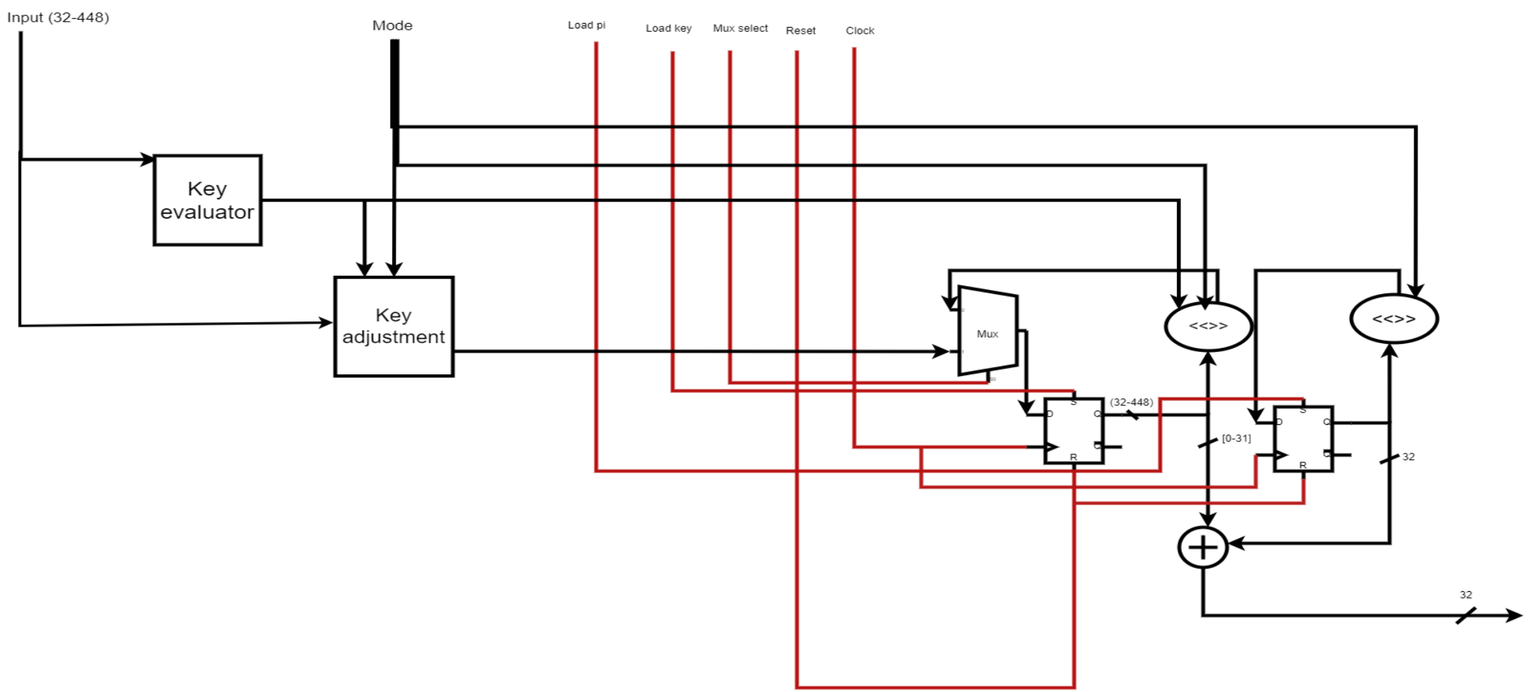


Decryption

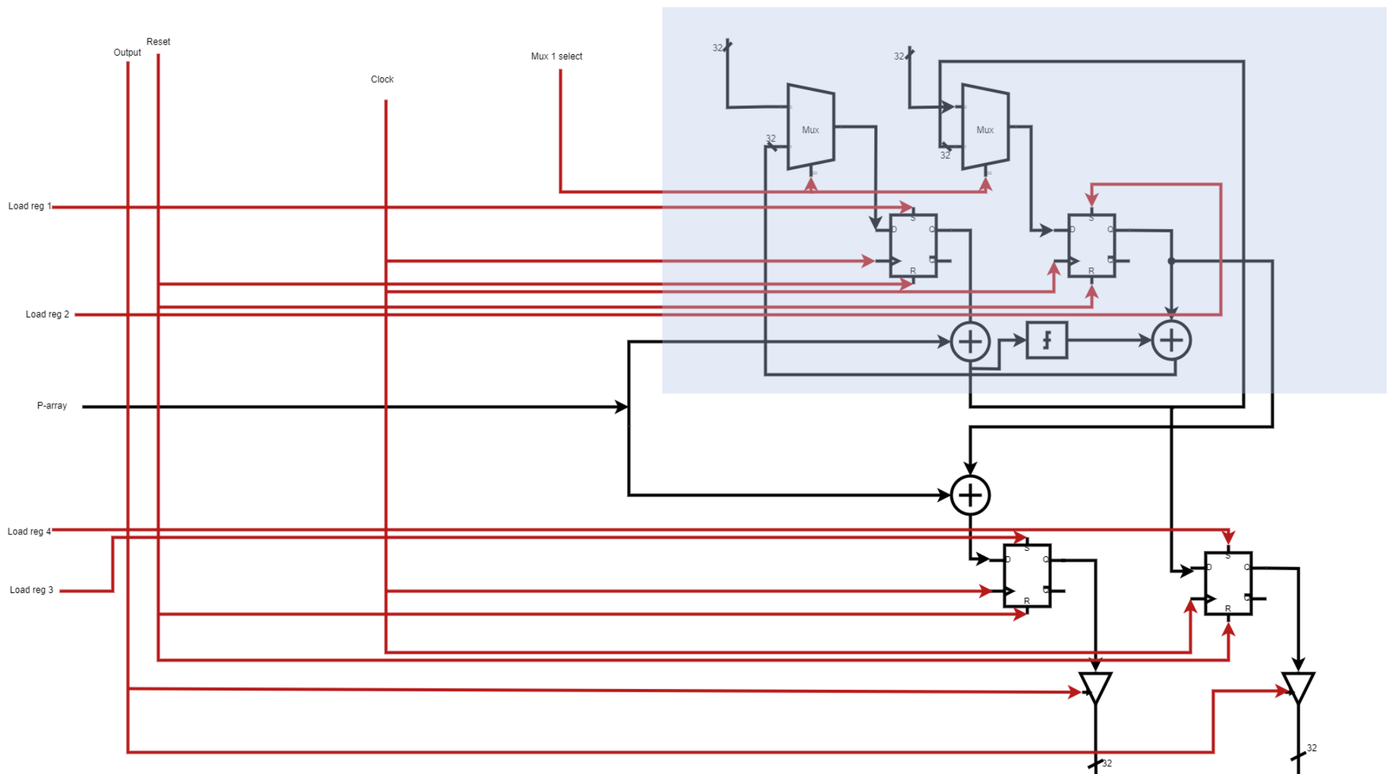
- The decryption process is exactly the same as the encryption process only that the subkeys are used in reverse order as follows



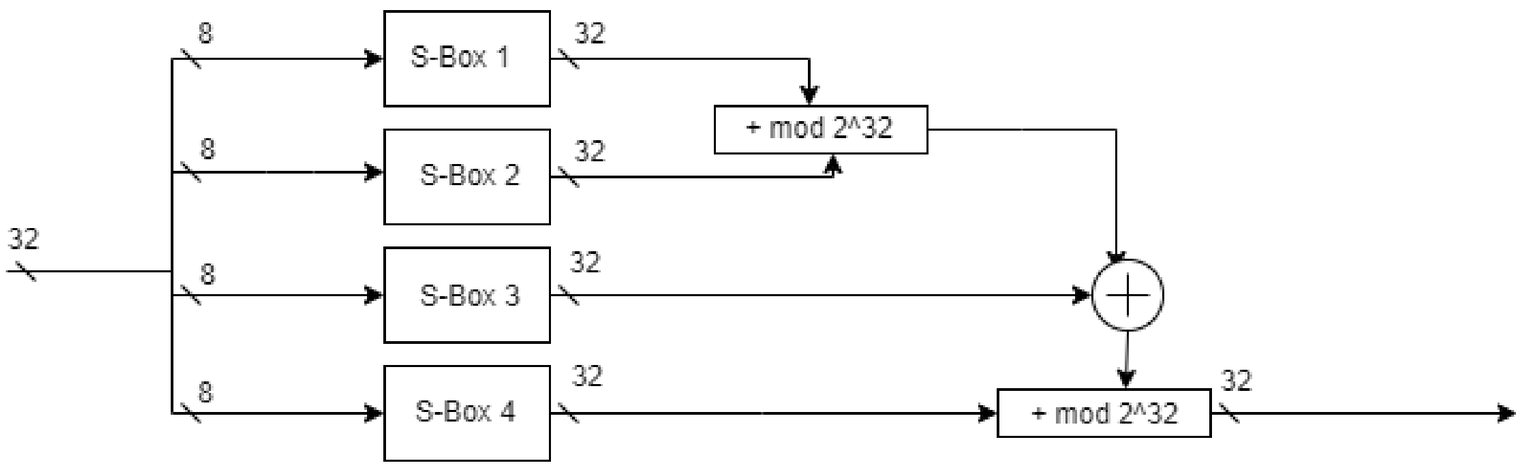
Key expansion datapath



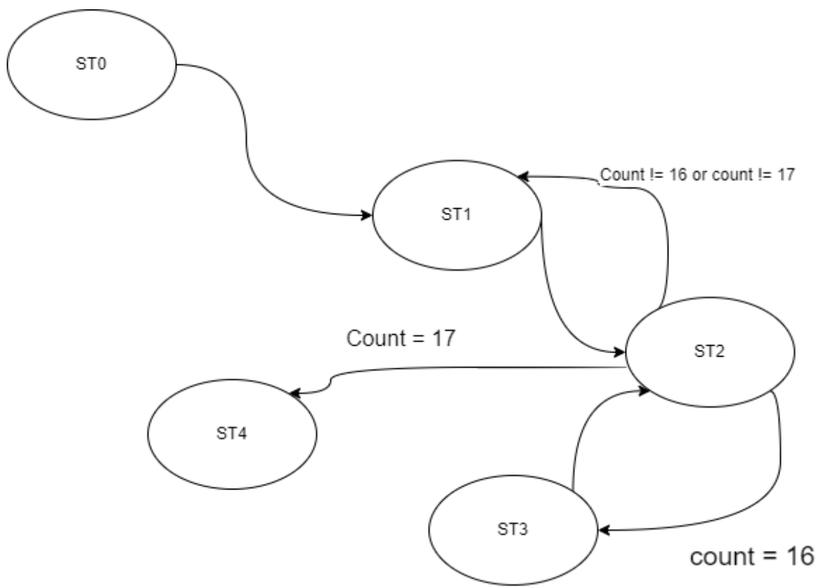
Encryption datapath



F-function datapath



State Diagram



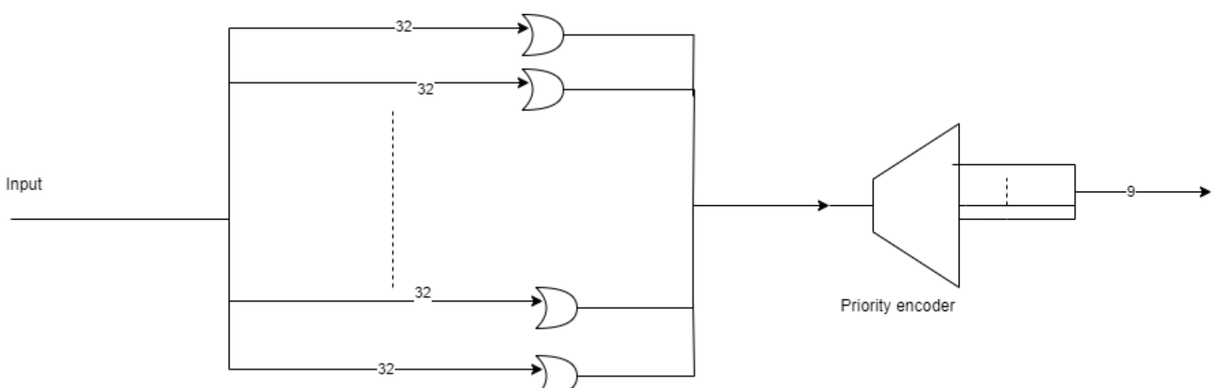
Control table

INSTRUCTIONS	STATE ENCODING	SIGNALS									
		Load P	Load K	Load RL	Load RR	Load PL	Load PR	Mux 1	Mux 2	Mux 3	Output
Input plain text, mode and key	000	0	1	1	1	0	0	0	0	0	0
Enable round registers	001	0	0	1	1	0	0	1	1	X	0
Enable key and Pi registers	010	1	1	0	0	0	0	X	X	1	0
Enable left post-processing register	011	0	0	0	0	1	0	X	X	X	0
Enable right post-processing register	100	0	0	0	0	0	1	X	X	X	0

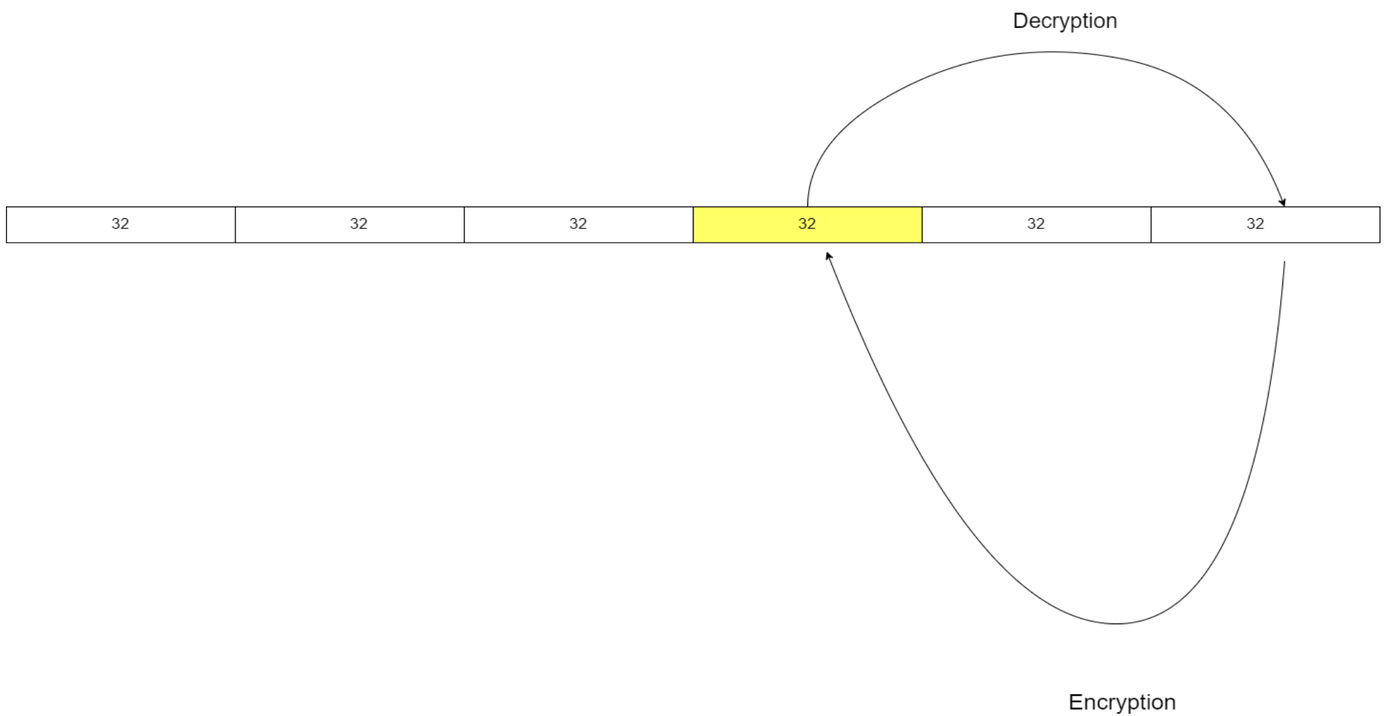
Implementation Table

CURRENT STATE	NEXT STATE			
	COUNT ≠ 16		COUNT ≠ 17	
	0	1	0	1
000	001	001	001	001
001	010	010	010	010
010	001	011	001	100
011	010	010	010	010
100	100	100	100	100

Key evaluator



Combinational shifter



References

- Shneier B.(1995, September). The blowfish encryption algorithm-one year later. *shneier.com*. Academic: The Blowfish Encryption Algorithm—One Year Later - Schneier on Security
- Abhay Bhat.(2023, July 6). Blowfish algorithm with examples. *geeksforgeeks.org*. Blowfish Algorithm with Examples – GeeksforGeeks
- Arifuzzaman Munaf.(2020, December 1).Blowfish encryption algorithm [Video]. YouTube. (1269) BLOWFISH ENCRYPTION ALGORITHM - YouTube

The End