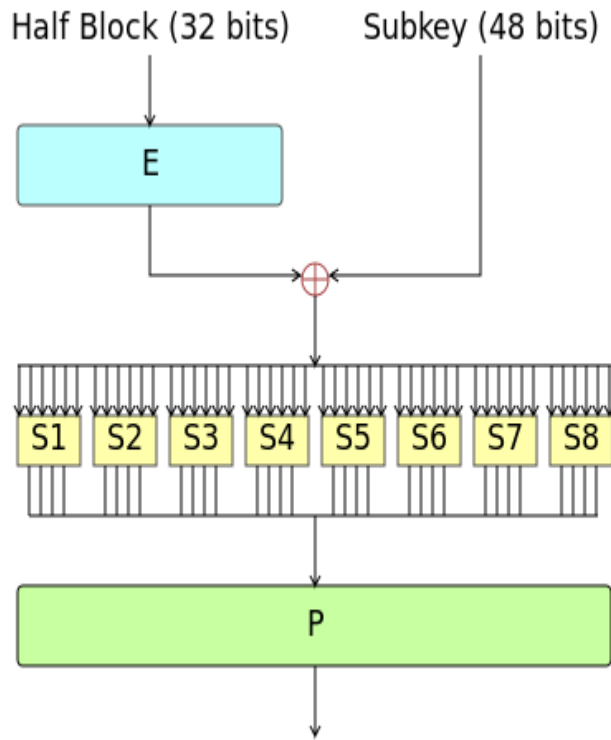


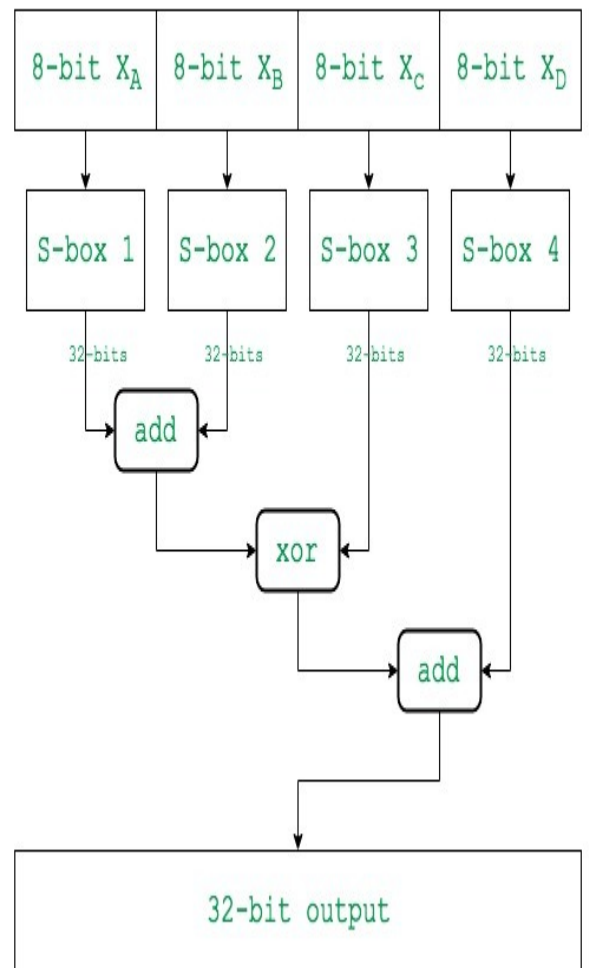
Differences between DES and Blowfish

	DES	Blowfish
Key size	56 bits(effective)	32-bits to 448-bits
Cypher type	Symmetric block cypher	Symmetric block cypher
Block size	64 bits	64 bits
Speed	Slow	Fast
Security	Not secure enough	Secure enough
Number of rounds	16	16
Number of S-boxes	8	4
Structure	Feistel Network	Feistel Network
Sub-Key generation	<p>The diagram illustrates the DES sub-key generation process. It starts with a 64-bit key input to a permutation box PC1. PC1 outputs two 28-bit halves. These are combined with a permutation box PC2 and shifted left (indicated by <<< boxes) to produce Subkey 1 (48 bits). This process repeats to produce Subkey 2, ..., Subkey 15, and Subkey 16 (all 48 bits).</p>	$P[0] = P[0] \text{ xor } 1\text{st } 32\text{-bits of input key}$ $P[1] = P[1] \text{ xor } 2\text{nd } 32\text{-bits of input key}$ <p>.</p> <p>.</p> <p>.</p> $P[i] = P[i] \text{ xor } (i+1)\text{th } 32\text{-bits of input key}$ <p>(roll over to 1st 32-bits depending on the key length)</p> <p>.</p> <p>.</p> <p>.</p> $P[17] = P[17] \text{ xor } 18\text{th } 32\text{-bits of input key}$ <p>(roll over to 1st 32-bits depending on key length)</p>

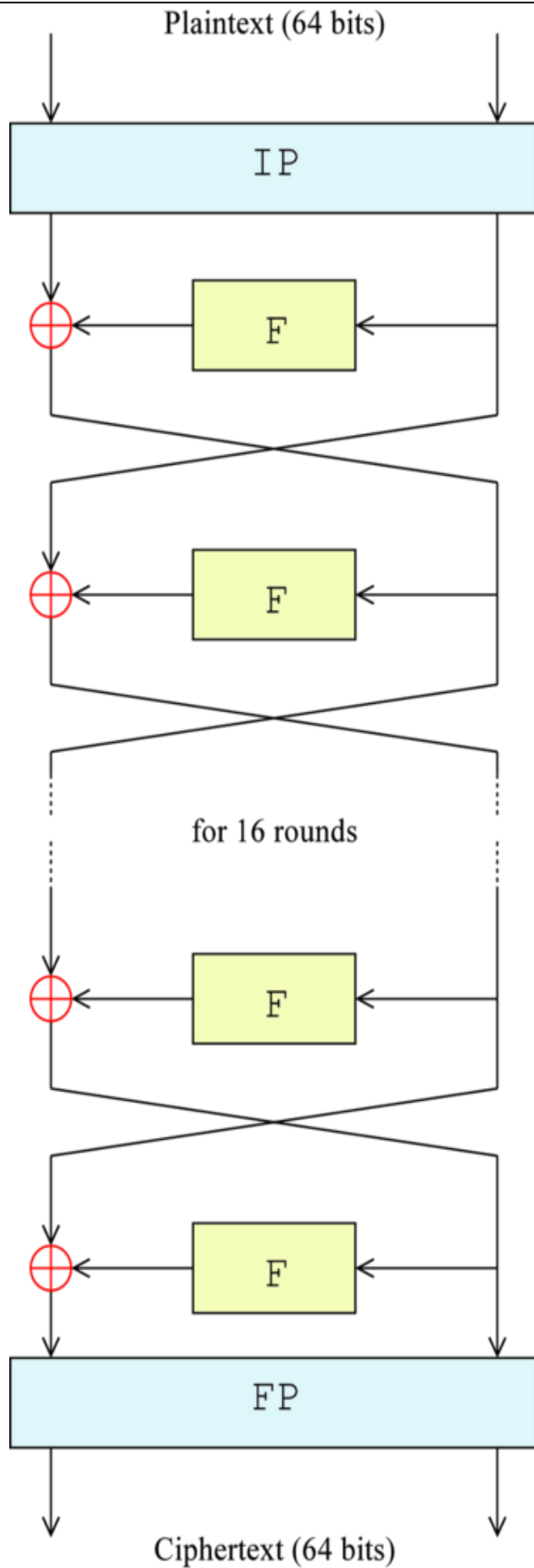
Feistel function



Flow-diagram of function "F"



Encryption Algorithm



Encryption

