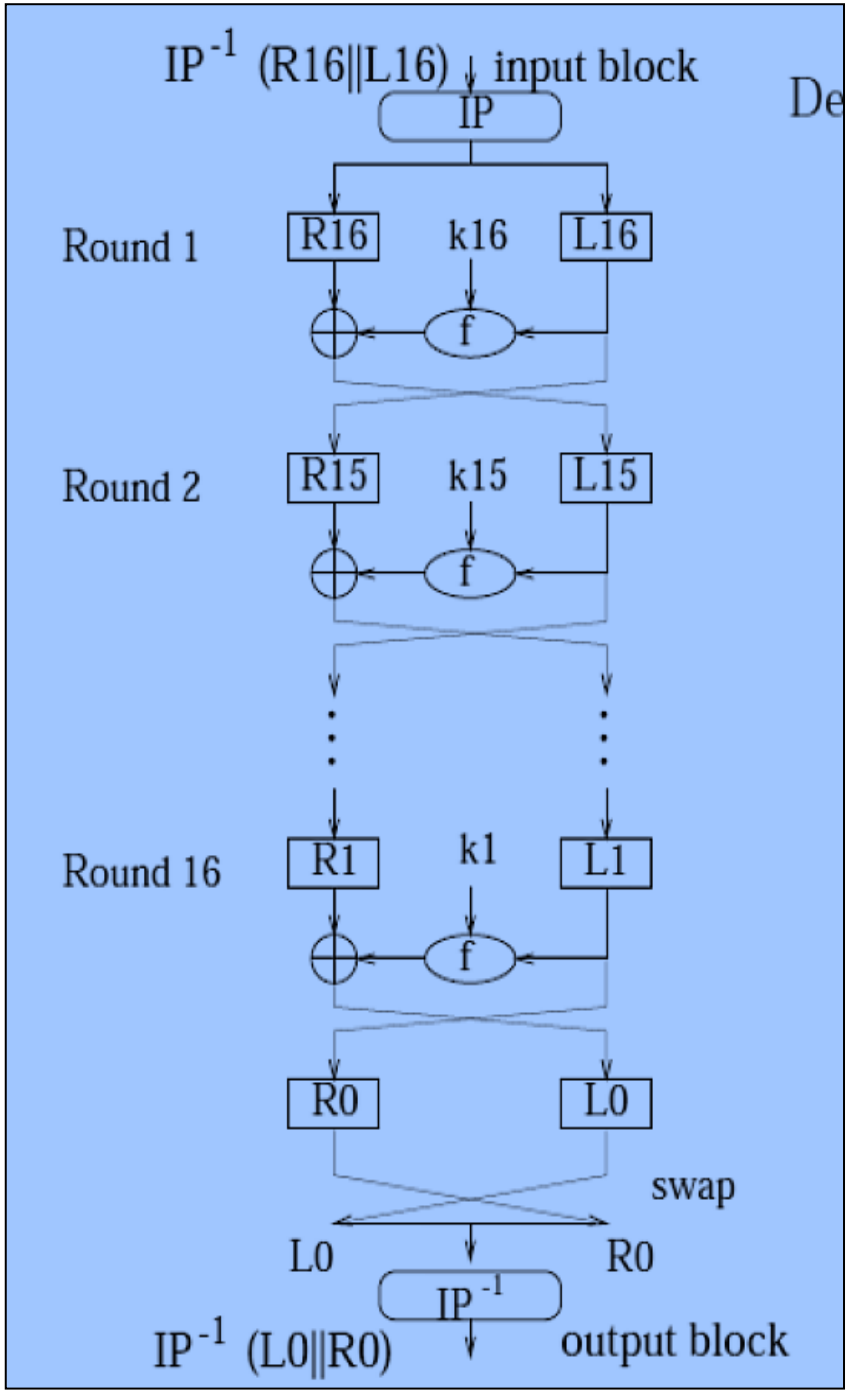
Decrypting DES

- same function to encrypt or decrypt a block.
- The only difference is that the keys must be used in the reverse order. That is, if the encryption keys for each round are K1, K2, K3, . . . , K16, then the decryption keys are K16, K15, K14, . . . , K1,.
- The algorithm that generates the key used for each round is circular as well.
- The key shift is a right shift and the number of positions shifted is 0, 1, 2, 2, 2, 2, 2, 2, 1, 2, 2, 2, 2, 2, 2, 1.

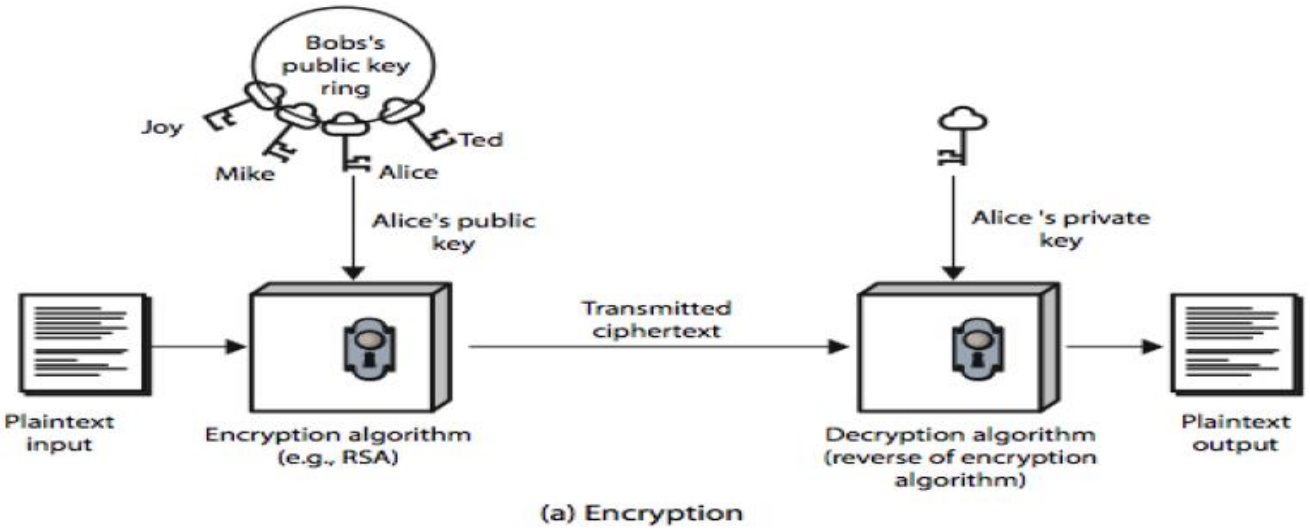

IP-1 (R16||L16)
input block
IP
Round 1
R16
k16
L16
f
Round 2
R15
k15
L15
f
Round 16
R1
k1
L1
f
R0
L0
swap
L0
R0
IP-1
IP-1 (L0||R0)
output block

Block vs. Stream Ciphers

Block cipher	Stream cipher
process messages in into blocks, each of which is then en/decrypted	process messages a bit or byte at a time when en/decrypting
Error propagation	Low error propagation
Slowness	Speed of transformation
High Diffusion	Low diffusion
Immunity to insertions	Susceptibility to attacks on integrity

Public-Key Cryptography

- public-key/two-key/asymmetric cryptography involves the use of two keys:
  - a public-key, which may be known by anybody, and can be used to encrypt messages, and verify signatures
  - a private-key, known only to the recipient, used to decrypt messages, and sign (create) signatures
- is asymmetric because those who encrypt messages or verify signatures cannot decrypt messages or create signatures



Public-Key Characteristics: -

- it is computationally infeasible to find decryption key knowing only algorithm & encryption key
- it is computationally easy to en/decrypt messages when the relevant (en/decrypt) key is known
- either of the two related keys can be used for encryption, with the other used for decryption (for some algorithms)

Public-Key Applications: -

- can classify uses into 3 categories:
  - encryption/decryption (provide secrecy)
  - digital signatures (provide authentication)
  - key exchange (of session keys)
- some algorithms are suitable for all uses, others are specific to one

Security of Public Key Schemes: -

- like private key schemes brute force exhaustive search attack is always theoretically possible
- but keys used are too large (>512bits)

Diffie-Hellman

- first public-key type scheme proposed by Diffie & Hellman in 1976 along with the exposition of public key concepts.
- Based on the difficulty of computing discrete logarithms of large numbers.

Public Parameter Creation
A trusted party chooses and publishes a (large) prime p and an integer g having large prime order in $\mathbb{F}_p^*$.

Private Computations	
Alice	**Bob**
Choose a secret integer a.	Choose a secret integer b.
Compute $A \equiv g^a \pmod{p}$.	Compute $B \equiv g^b \pmod{p}$.

Public Exchange of Values	
Alice sends A to Bob	$\longrightarrow A$
$B \longleftarrow$	Bob sends B to Alice

Further Private Computations	
Alice	**Bob**
Compute the number $B^a \pmod{p}$.	Compute the number $A^b \pmod{p}$.
The shared secret value is $B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \pmod{p}$.	