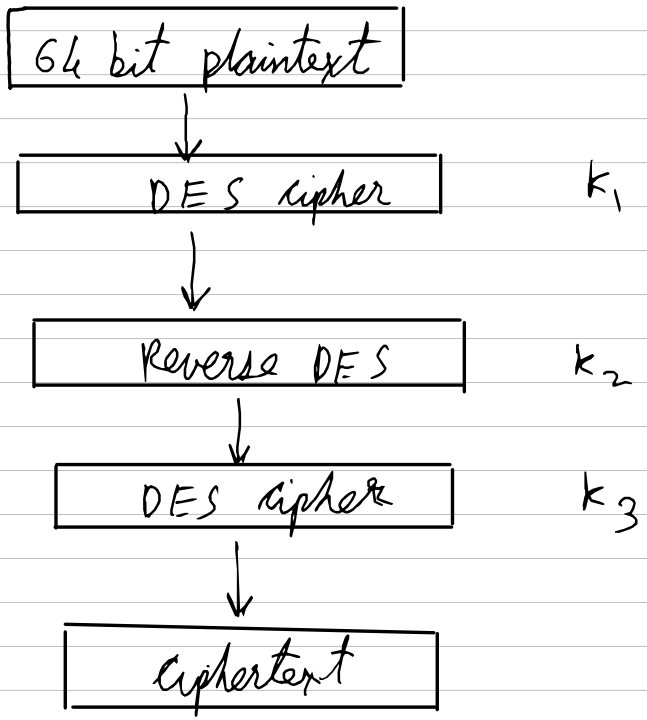
(Q1) Types of DES with diagram

→

One key DES	56 bit key	K_1
Two key DES	2 × 56 bit keys	K_1 K_2
Two key triple DES	2 × 56 bit keys	K_1 K_2' K_1
Three key triple DES	3 × 56 bit keys	K_1 K_2' K_3

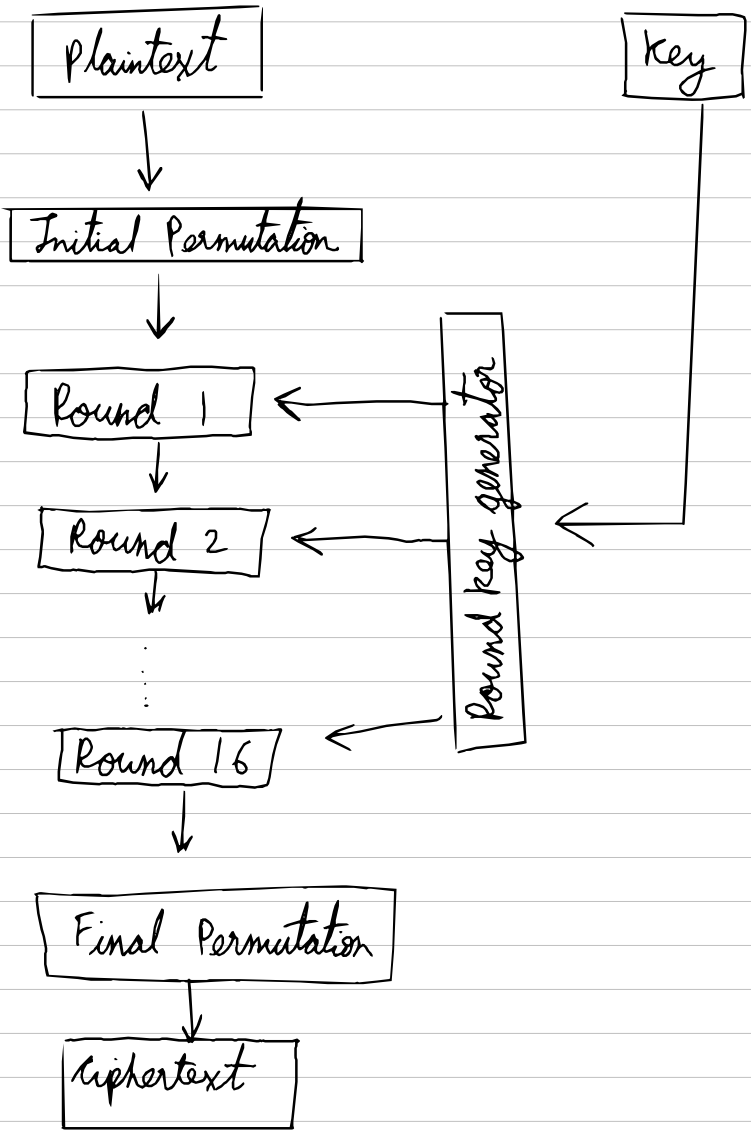
Three key triple DES



(Q2) Explain DES with block diagram

→ i) Symmetric Key algorithm

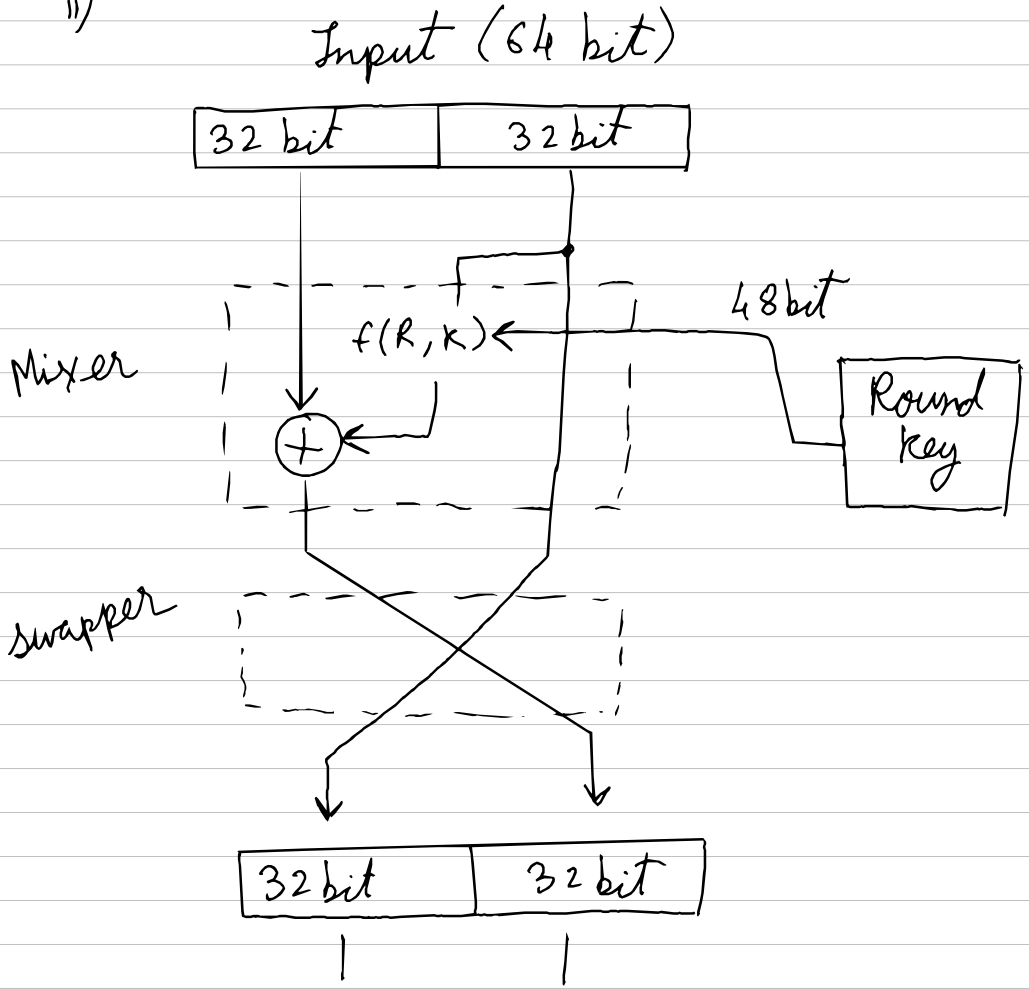
ii) block diagram



(Q3) Explain DES encryption rounds

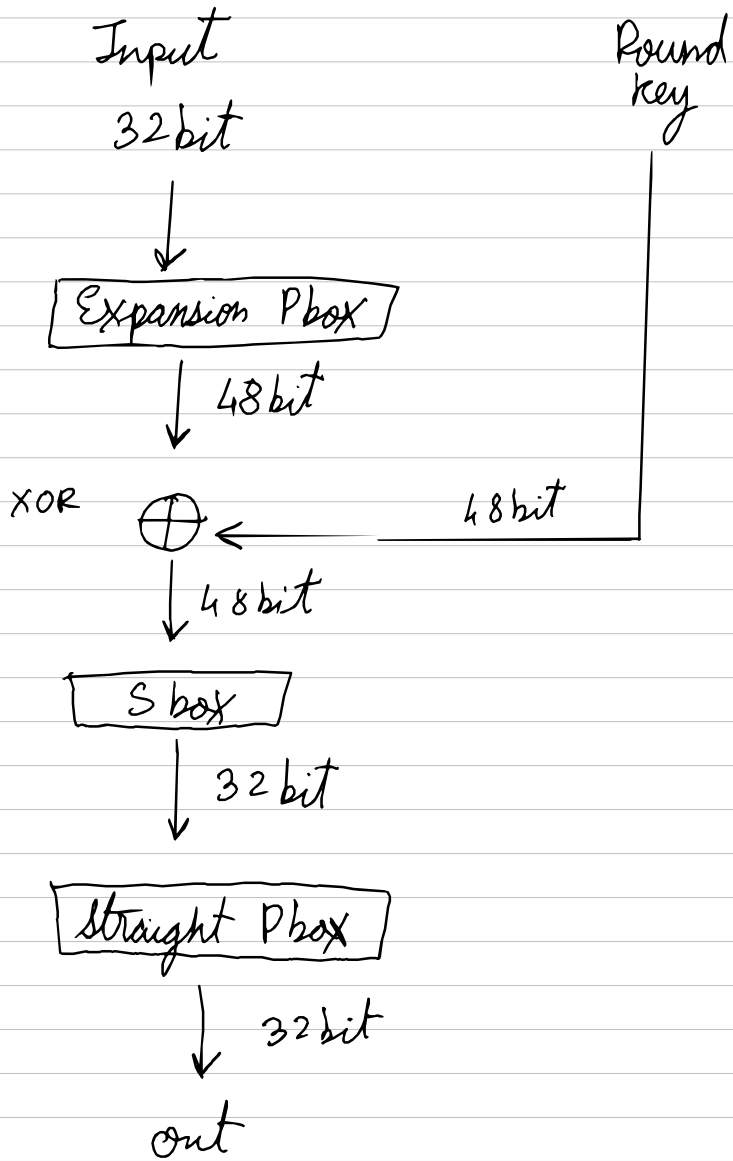
→ i) Feistel cipher algorithm

ii)



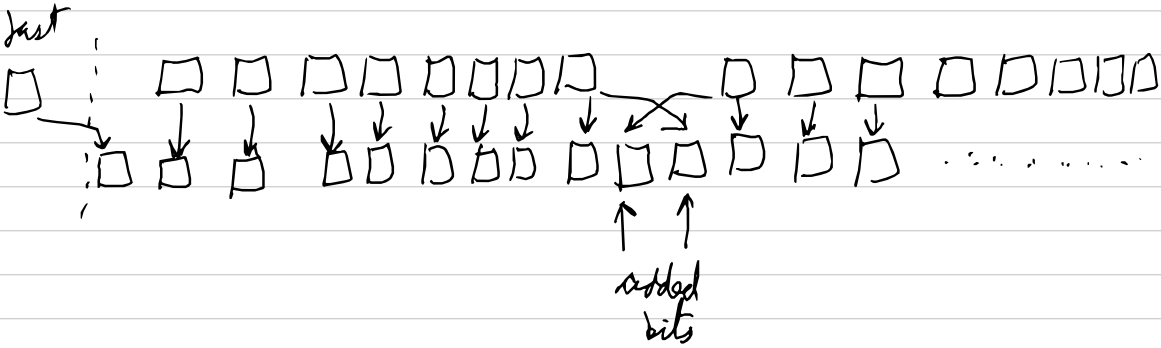
iii) No swapper in last round

(Q4) Explain DES function



(Q5) Explain P box expansion

i) Converts 32 bit to 48 bit



32 = 4 × 8

48 = 6 × 8

} add 2 in every block of 8 bits

iii) Redundant bits are added

32, 1, 2, 3, 4, 5, 6, 7, 8, 9, 8, 9, 10, 11, 12 . . .

(Q6) Explain Sbox

i) Mixing done (confusion)

ii) 48 bit input converted into 32 bits

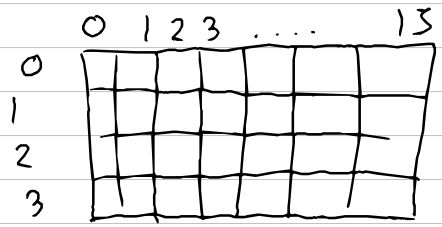
(48 = 8 × 6) ↓

iii) 8 Sboxes are used

iv) converts 6 bit input into 4 bit output

(32 = 8 × 4)

v) lookup table used



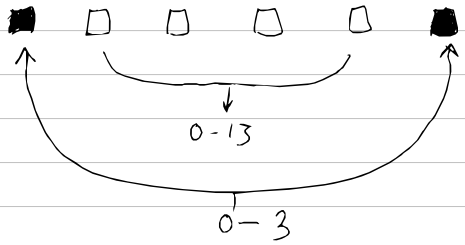


Table entry is the output

(07) AES Vs DES

→	DES	AES
Date	1976	1999
full form	Data encryption standard	Advanced encryption standard
Type of encryption	Confusion + Diffusion	Confusion + Diffusion
Type of cryptography	Permutation substitution	Permutation substitution & bit Mixing
key length	56 bit	128, 192, 256 bit
No of rounds	16	10, 12, 14
block size	64 bit	128 bit
Made by	IBM	duch cryptographers
speed	Slower	Faster
orientation	bit oriented	byte oriented

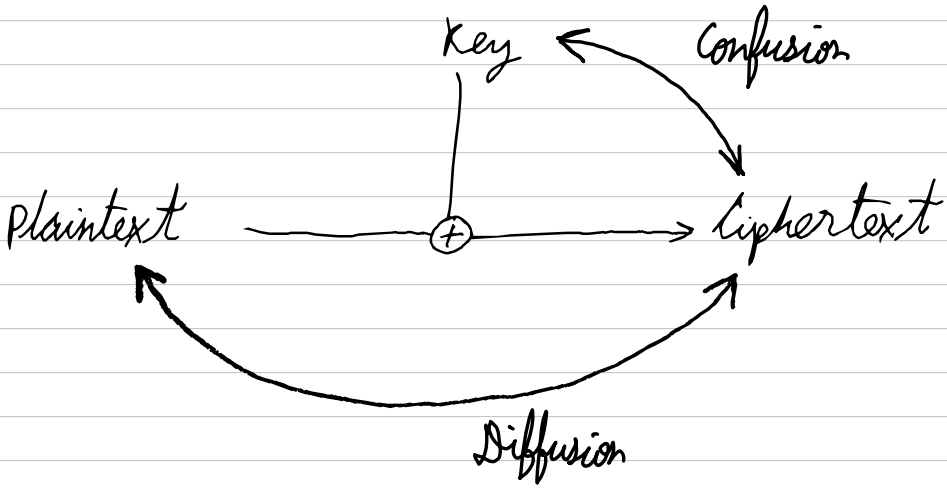
(08) Block vs Stream cipher

Block cipher	Stream cipher
1) Processes entire block	Process bit by bit (byte)
2) Confusion + Diffusion	Only Confusion
3) less vulnerable	More vulnerable
4) Slow	Fast
5) Permutation + substitution	Only substitution
6) Simple design	Complex design
7) eg columnar transposition	eg Caesar cipher

(89) Explain confusion & diffusion

Diffusion → Hide relation between ciphertext & plaintext

Confusion → Hide relation between ciphertext & key



* Confusion is Mandatory for any cipher

(Q10) Explain Cryptanalysis

i) Cryptanalysis is the study of analyzing & decrypting ciphers, codes & encrypted text without using the real key

ii) It is process of finding weaknesses in cryptographic algorithms & decipher the ciphertext without knowing the secret key

Q11 Public key Vs Private key

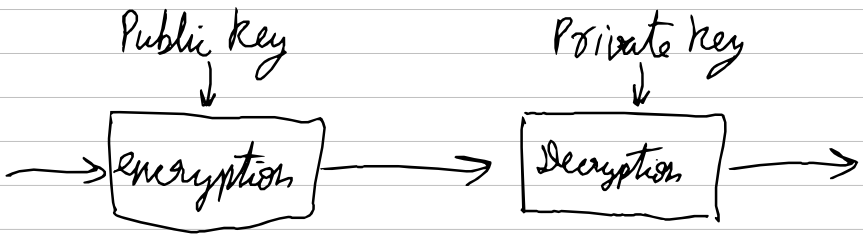
i) In public key cryptography, two types of keys are used seperately for encryption and decryption

ii) Public key → used for encryption
Private key → used for decryption

iii) Public key → acts as unique identifier
→ known to everyone
eg email id

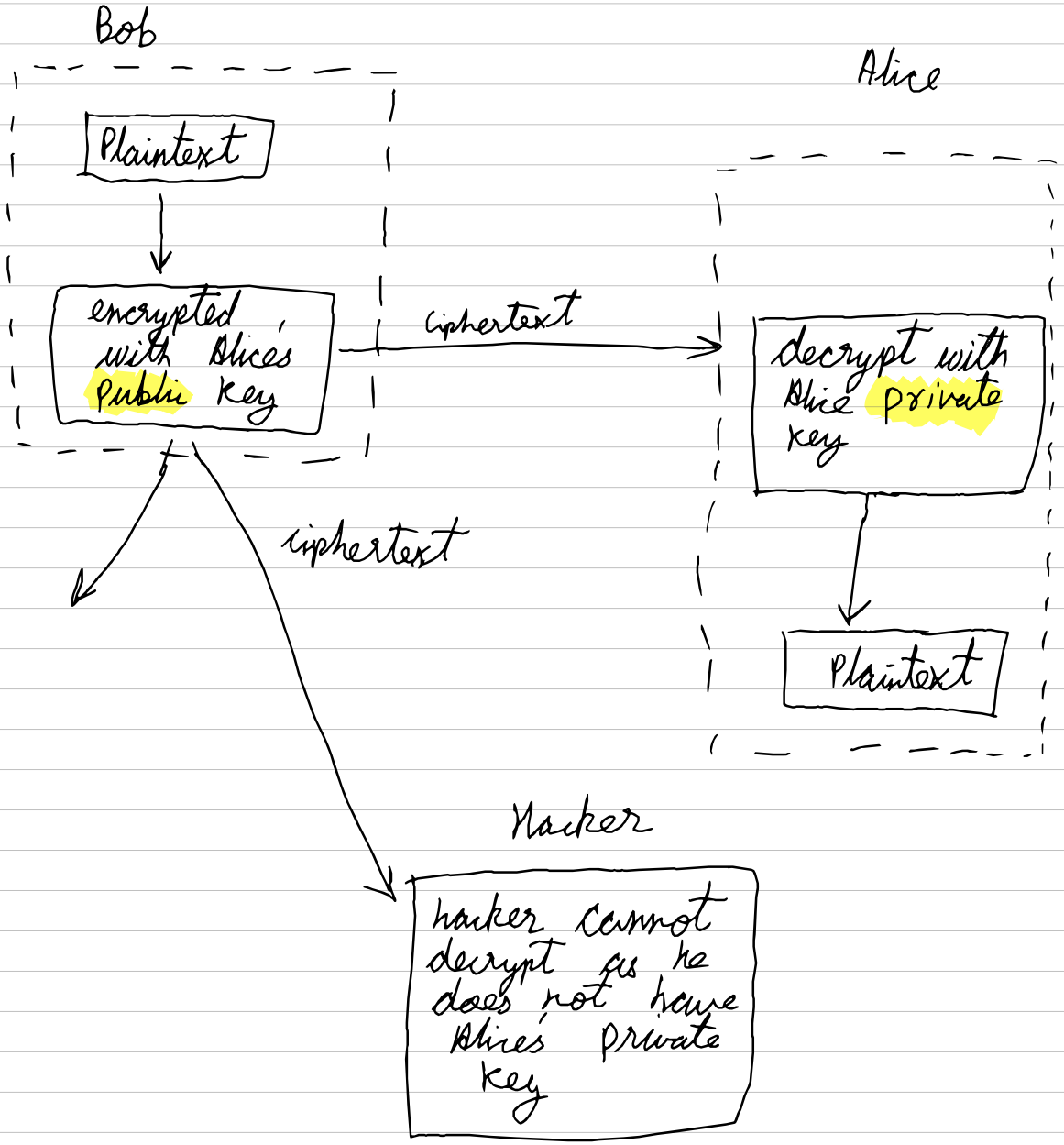
iv) Private key → acts as a password
→ known only by the owner
→ eg password

v) Sender encrypts data with recievers public key. Only the reciever can decrypt it with their private key



(Q12) Explain public key cryptosystem with diagram

→ i) Asymetric keys → public + Private



Q13) Explain digital signatures in public key cryptosystem with diagram

→ i) Used to ensure Bob is the sender

ii) Since only Bob has private key, it can be verified that bob is the sender from bobs public key.

(Q11) Explain digital certificates & PKI
Public key Infrastructure

→ i) PKI (Public key Infrastructure) is a set of technologies, policies & procedures that are used to create & manage digital certificates

ii) A digital certificate is public key & identity that is bound together and signed by a certificate Authority

iii) A certificate Authority (CA) is a trusted third party.

iv) Digital certificates ensure

i) Authenticity → document has come from BOB

ii) Integrity → Is not tampered with