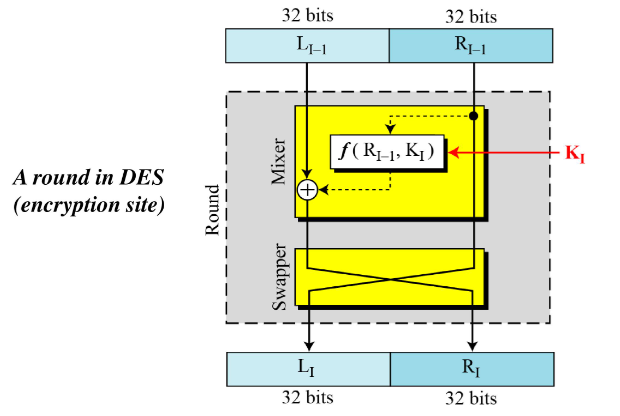


**Group A**

Q1



Q2

XOR does not leak information about plaintext, output is 1 or 0, both with 50% chances.

XOR is a self-inverse function, add the key to encrypt, add it back to decrypt.

Q3

Most important sections are below. 1 mark each

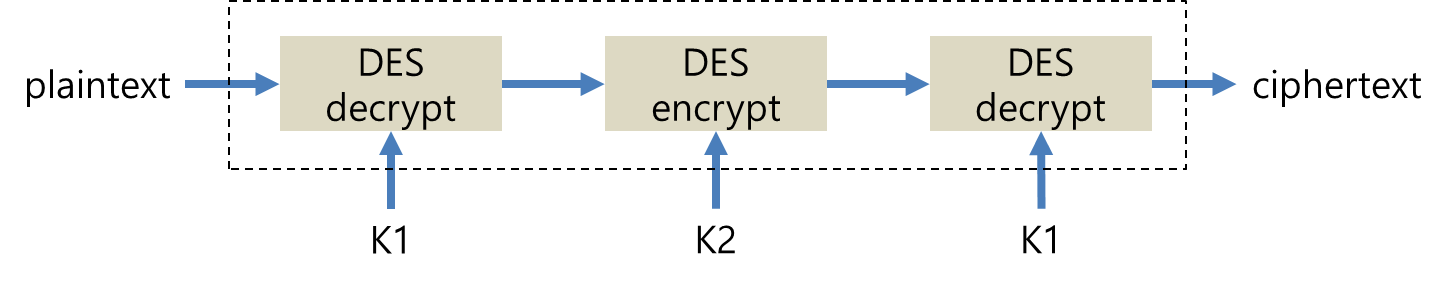
* Subject’s identity and public key
* CA’s identity
* Expiry date
* CA’s Digital signature

**Group B**

Q1

Can use two keys, or three different keys.

Note the order and function of each block: decrypt, encrypt, decrypt



Q2

Any one

* Output is the combination of 1’s and 0’s distributed variably with a proportion of 50% each
* A single bit change in input must change the output by at least 50%
* Collision resistance: It must be difficult to find two different messages m1 and m2 that yield the same hash code.

Q3

Recipient’s public key is used for RSA encryption, and private key for decryption. When sender asks for the recipient’s public key, the attacker may send their own key instead. This way attacker will be able to decrypt the message with their own private key.

Q4

In addition to validity, receiver must check: (1.5 each)

* Is the certificate signed by a trusted CA?
* has the certificate been revoked?