Q1.

a) Give one sentence answers (attempt all parts on one side of a page) **[0.5 x 4 = 2]**

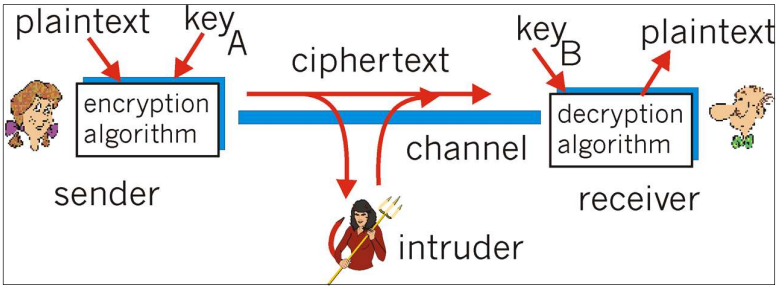
i. **Define the terms:** i) Information Security, ii) Cybersecurity and iii) Network security.
Information security refers to the practice of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Cybersecurity is a subset of information security that specifically focuses on protecting computer systems, networks, and digital devices from cyber threats. Network security is a component of cybersecurity that is concerned with securing computer networks against unauthorized access, attacks, and other threat

ii. **Explain** the linkage between asset, vulnerability, threat and attack.
An asset refers to any valuable resource. A vulnerability is a weakness or flaw in the security of an asset. A threat is any potential danger or harm to an asset, either intentional or accidental. An attack is a deliberate action taken by an attacker to exploit a vulnerability and compromise an asset. Attacks can take many forms, including malware infections, phishing scams, denial-of-service attacks, or physical theft. The goal of information security is to identify and mitigate vulnerabilities and threats to protect assets from attacks.

iii. **Why** an organization needs InfoSec team in addition to Network Security staff in the IT department?
Network Security staff has limited knowledge about i) organization wide risk assessment and security policy create and enforcement and ii) cybersecurity issues like web security, software security and operating system security.

iv. **How** a vulnerability creates an opportunity for an attack?
Vulnerability in application and/or system software, hardware or firmware allows undetected access to system resources that otherwise are not accessible to unauthorized users. For example, the access could be a privileged command prompt on a target node, creation a process undetected, or a favorable change in configuration for future reentry, etc.

b) Draw a compact free-hand labeled diagram of a communication channel between Alice and Bob along with an active attacker Trudy, who has remained passive in the recent past. **Describe** how this attacker violates each entity in the CIA Triad. Give three bullet sentences as your answer on one side of a page. **[3]**

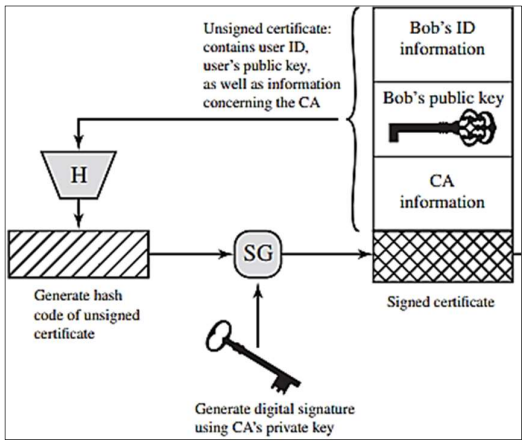


Confidentiality violated as Trudy can read messages, Integrity violated as messages are modified and Availability violated if messages undelivered to Bob due to deletion or making channel compromised even un-operational.

Q2.

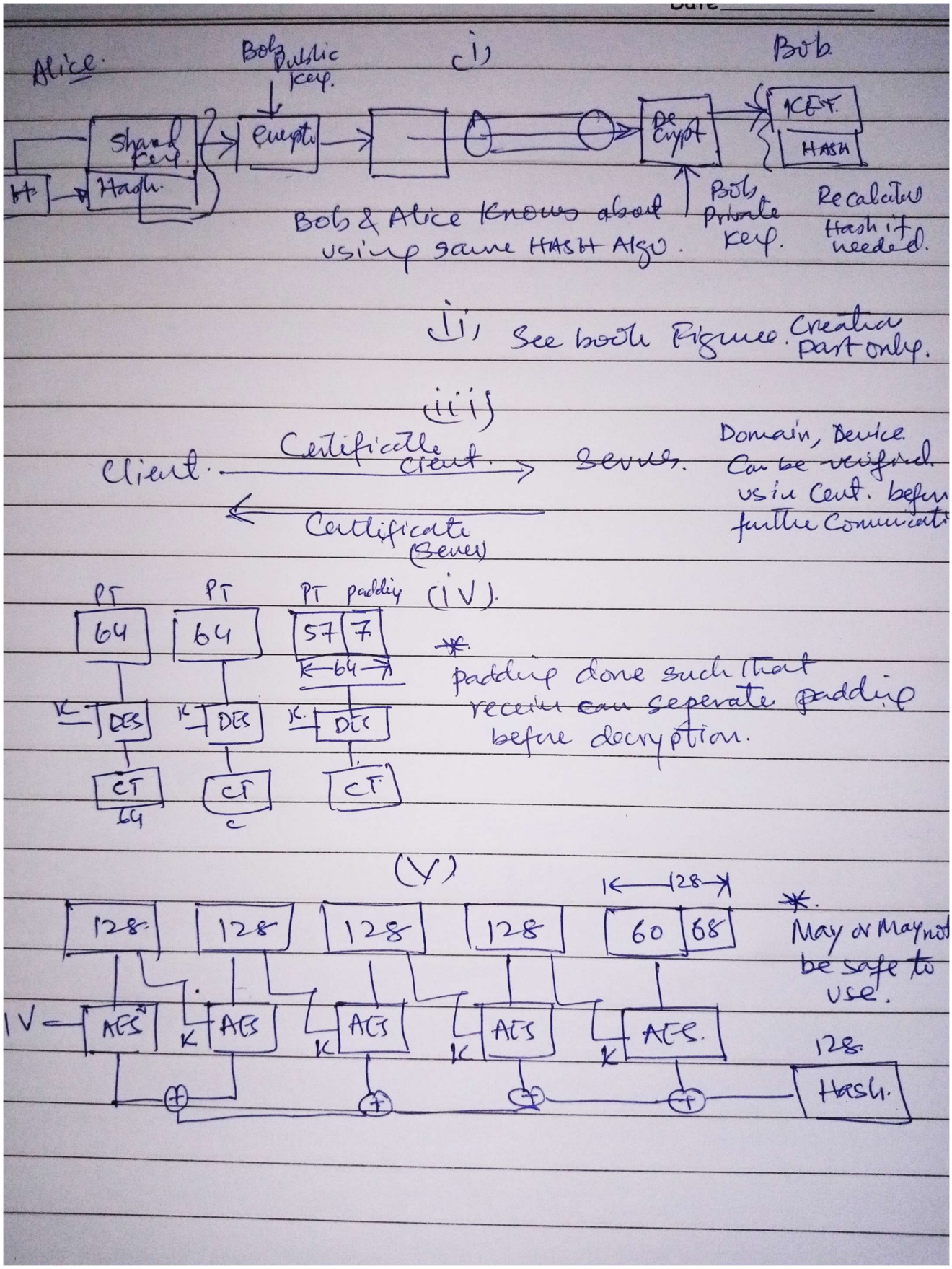
Draw a compact free-hand labeled diagram to explain the following scenarios:
Note: Labels on your diagram will express your knowledge about the underlying principles and methods.

i. Alice sends a "symmetric shared key" confidentially with integrity checking to Bob.
ii. A public certificate creation process.
iii. Exchanges between client and server machines to verify authenticity of each other.
iv. Encryption of a text file of size 185 bits, using DES with block size of 64 bits.
v. Creating of a fixed sized hash from a 700-bits text using AES-128 cipher.



Solution of (ii)

Solution of Q2 part (i), (iii), (iv) and (v).



Q3.

Consider the access control policy of an online entertainment store in Figure 1, which we studied in the class.

```
R1:can_access(u, m, e) ←
   (Age(u) ≥ 17 ∧ Rating(m) ∈ {R, PG-13, G}) ∨
   (Age(u) ≥ 13 ∧ Age(u) < 17 ∧ Rating(m) ∈ {PG-13, G}) ∨
   (Age(u) < 13 ∧ Rating(m) ∈ {G})
R2:can_access(u, m, e) ←
   (MembershipType(u) = Premium) ∨
   (MembershipType(u) = Regular ∧ MovieType(m) = OldRelease)
R3:can_access(u, m, e) ← R1 ∧ R2
```

Figure 1

Now perform the following two tasks:

i. Suppose the store takes user attributes from google.com. **Draw a compact free-hand labeled diagram** of an architecture that can decides to allow or deny access to any user. Explain the parameters u, m and e. **[3]**

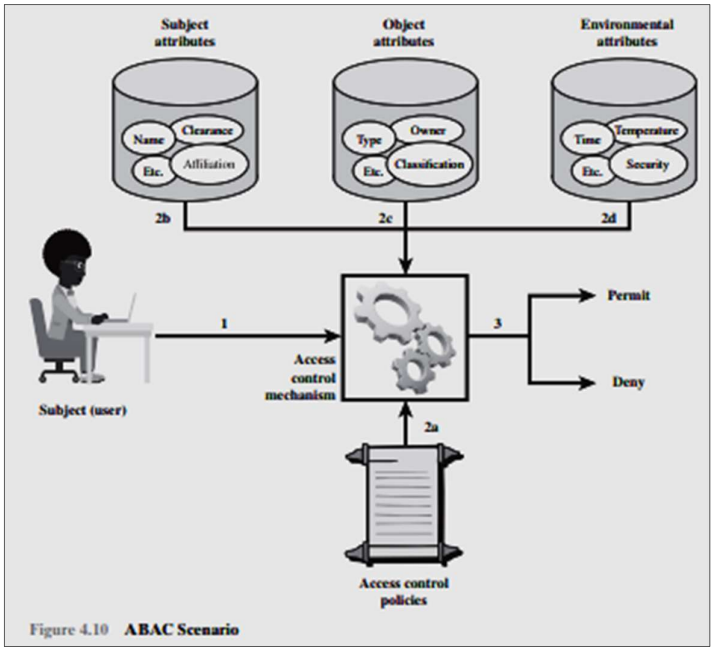


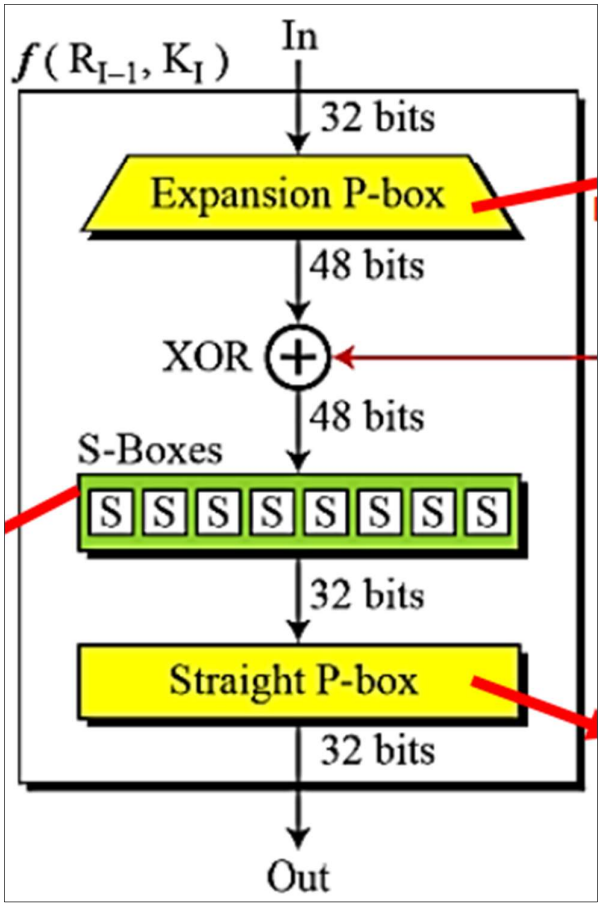
Figure 4.10 **ABAC Scenario**

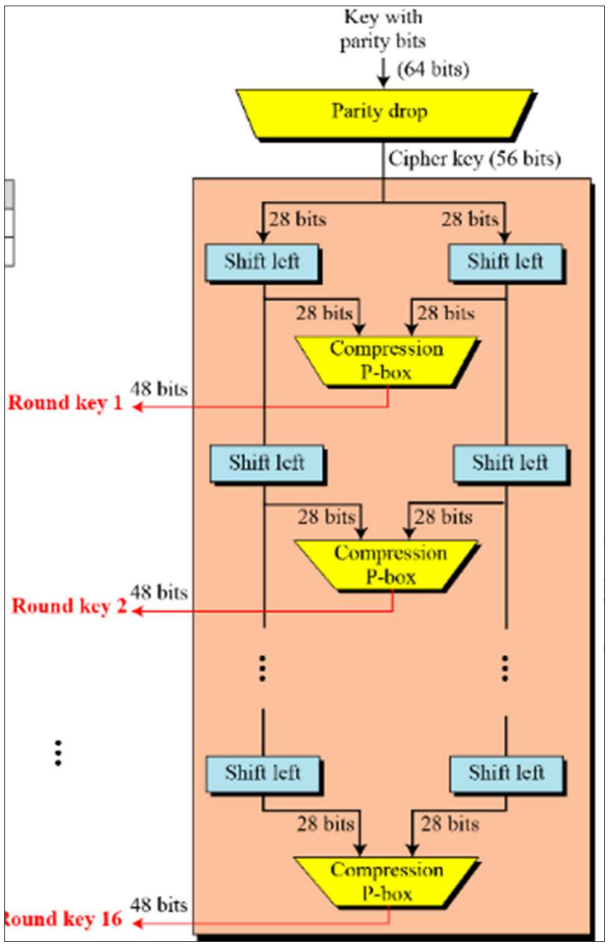
ii. **Change the policy in Figure 1** to allow access to under thirteen users only when social security number of their guardian is in the database. **[2]**

The social security number of minor might not be available from google.com therefore the store's web portal need to ask and store it while registering the minor user.

Modify under 13 part of R1 → R1: Age(u) < 13 AND Rating(m) ∈ {G} AND SSN_Gardian(u) Ɛ QueryDB (u))

Bonus Question. Draw a labeled diagram of the inner working of i) Feistel function and ii) the key generator of DES cipher.
Note: Attempt this only if you think that you cannot score more than 3.5 marks in Q2.





----------(O)----------