Q1.

Give **two-sentence** answers **without making any diagrams**.

a) Define public-key. How keys are different in symmetric and asymmetric cryptography?
In asymmetric cryptography, a pair of keys is generated. One key is the private (secret) key and the other key is required to be shared with the public (everybody). In contrast, symmetric encryption works with one key that is strictly shared with sender and receiver.

b) State each term of the acronym CIA in the CIA triad. Give real-world examples for each term.
Confidentiality: Sending messages between Alice and Bob, which cannot be disclosed, to an adversary.
Integrity: The contents of the message can be changed by the adversary.
Availability: Infrastructure and other facilities needed in communication are ready and in working condition should Alice and Bob want to communicate.

c) Give an example of a vulnerability in a house that creates an opportunity for an attack.
i) A weak boundary wall OR
ii) A mechanical lock on the door with a compromise design OR
iii) A compromised security system that can be exploited remotely to open the main gate and other doors.

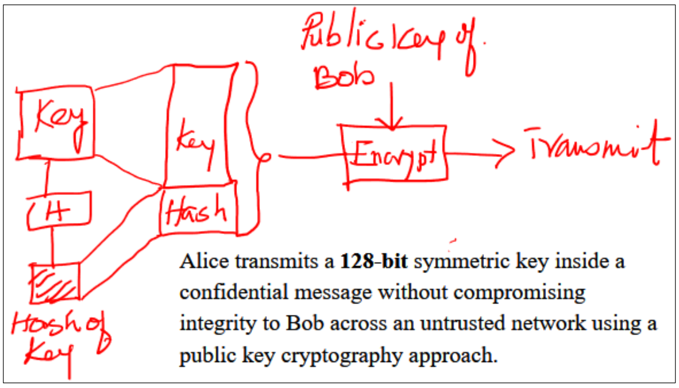
d) How lack of authenticity of a fund transfer message cause financial loss to the sender?
An adversary can forge the identity of any account holder (without his/her knowledge) and transfer funds to an account of his/her choosing. Digital signatures prevent this and assure authenticity.

e) How do the slow hashing function and salt help the password authentication scheme in the UNIX operating system?
The slow hashing function makes brute force and dictionary attacks computationally hard (i.e. time-consuming and resource-intensive). Salting ensures that identical passwords have different hashs in the password database (thwarting rainbow table attacks).

Q2.

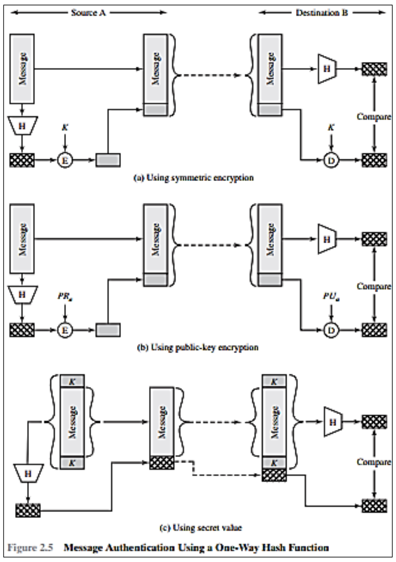
Draw a compact free-hand labeled diagram to explain the following scenarios:

a) The 128-bit symmetric key is the message. Alice will encryption the message + hash with Bob's public key.



Alice transmits a **128-bit** symmetric key inside a confidential message without compromising integrity to Bob across an untrusted network using a public key cryptography approach.

Q2 part (a)



(a) Using symmetric encryption

(b) Using public-key encryption

(c) Using secret value

Figure 2.5 **Message Authentication Using a One-Way Hash Function**

Related to part (a) and (c) or Q2

b) Substitution operation in AES.

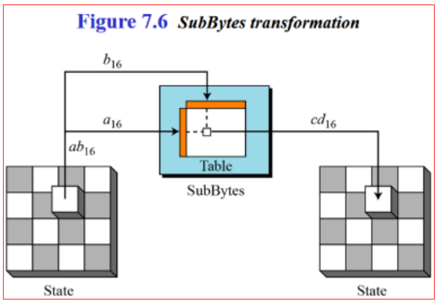
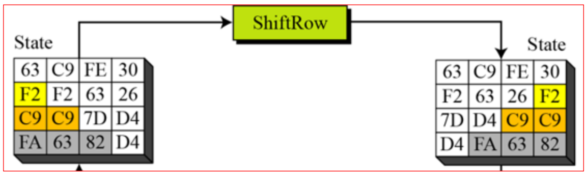


Figure 7.6 ***SubBytes transformation***

Q2 part (c)



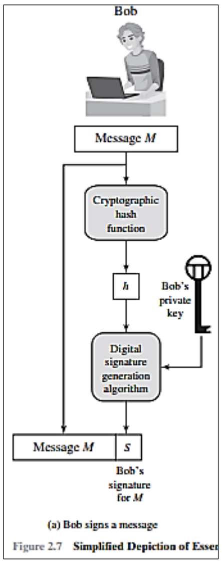
63	C9	FE	30
F2	F2	63	26
C9	C9	7D	D4
FA	63	82	D4

63	C9	FE	30
F2	63	26	F2
7D	D4	C9	C9
D4	FA	63	82

This is permutation not substitution. Give 25% marks.

c) Bob digitally signs a message and sends it to a group of people ensuring integrity but not confidentiality.

The digital signature generated by encrypting the message hash using Bob's private key. The digital signature verification algorithm takes Bob's public to ensure authenticity and integrity of the message.


Bob
Message M
Cryptographic hash function
h
Bob's private key
Digital signature generation algorithm
Message M
S
Bob's signature for M

(a) Bob signs a message

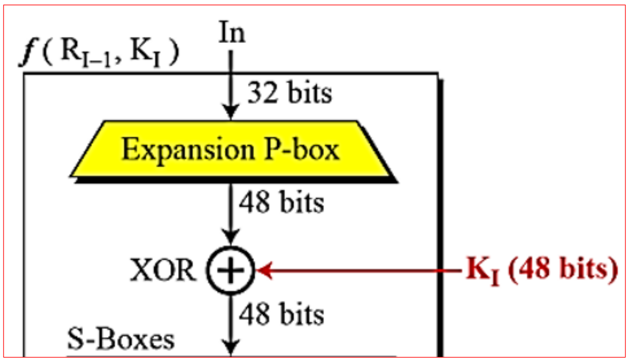
Figure 2.7 **Simplified Depiction of Esser**

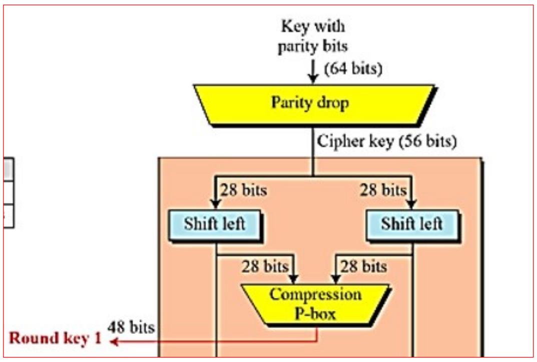
Q2 part (c)

d) XORing of the 54-bit key inside a Feistel function while utilizing DES.

The 54-bit was a typo (goes unnoticed). It was 64-bit to check students' recall of DES key generation algorithm. Student should have identified it as per the following DES key generation diagram.

100% marks: To student drawn Feistal function XORing with 48 bits and clearly identify that round key is 48-bits.

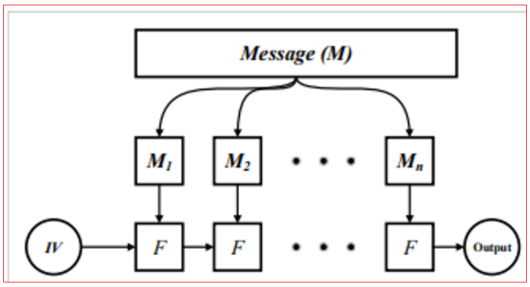




Q2 part (d)

e) Generating a fixed-sized hash from a 700-bit text using Merkle-Damgard construction.

The function F can be implemented using DES or AES encryption where IV is the Initial Vector (secure random bits). Assume that we use AES-128 so the message is divided into 128-bit chunks named M1, M2, M3, M4, and M5 totaling 640 bits. The last 60 bits along with a padding of 68 bits form M5. They will generate a fixed 128-bit hash of a 700-bit message.



Q2 part (e)

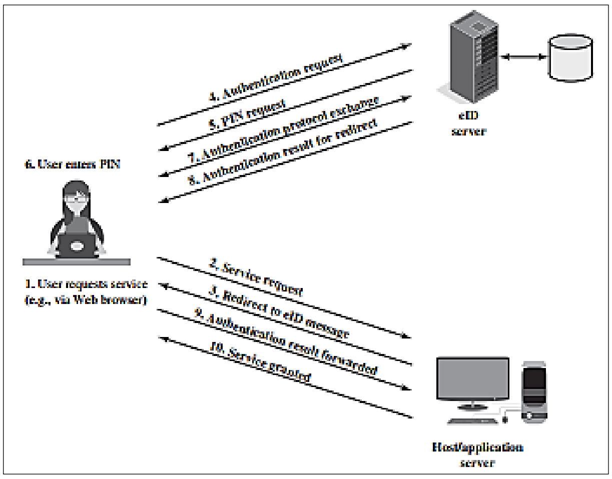
Q3.

a) How do you determine a user's identity while doing THREE different types of authentications? **[1.5]**

There are four general means of authenticating a user's identity, which can be used alone or in combination:

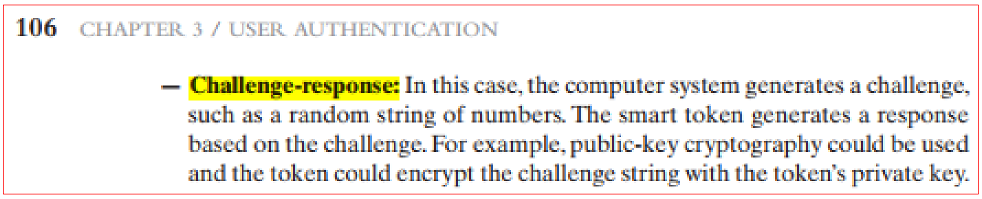
1. Something the individual knows: Examples include a password, a personal identification number (PIN), or answers to a prearranged set of questions.
2. Something the individual possesses: Examples include electronic keycards, smart cards, and physical keys. This type of authenticator is referred to as a token.
3. Something the individual is (static biometrics): Examples include recognition by fingerprint, retina, and face. Or Something the individual does (dynamic biometrics): Examples include recognition by voice pattern, handwriting characteristics, and typing rhythm.

b) Illustrate all stakeholders and protocol exchanges while doing eID authentication. **[1.5]**


4. Authentication request
5. PIN request
7. Authentication protocol exchange
8. Authentication result for redirect
eID server
6. User enters PIN
1. User requests service (e.g., via Web browser)
2. Service request
3. Redirect to eID message
9. Authentication result forwarded
10. Service granted
Host/application server

Q3 part (b) – textual answers will not be given any marks

c) How the values of challenge and response are computed in the challenge-response authentication between a smart device and a computer. **[2]**



106 CHAPTER 3 / USER AUTHENTICATION

— **Challenge-response:** In this case, the computer system generates a challenge, such as a random string of numbers. The smart token generates a response based on the challenge. For example, public-key cryptography could be used and the token could encrypt the challenge string with the token's private key.

Q3 part (c) – award marks in case of text or diagram

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