FALL 2022
CS3002 INFORMATION SECURITY
MID-1 SOLUTION

Instructions:

- Return the question paper. Don't write anything on question paper, except your Roll # & Section #.
- Read each question completely before answering it. There are **08 questions and 2 pages.**
- In case of any ambiguity, you may make assumptions. But your assumptions should not contradict any statement in the question paper. Write your answers only on the answer script.
- Please write all the answers according to the sequence given in the question paper.
- Do not write unnecessary and irrelevant details. Be precise and to the point. Draw a diagram where illustration is required.

Time: 60 minutes **Max. Points**: 15

Question 1: [CLO#1 – C2] [2 points]

Alice wants to send a message to Bob. Alice wants Bob to be able to ensure that the message did not alter on a channel. Outline the steps that Alice and Bob must follow to ensure the integrity of the message by creating and verifying a MAC.

Solution:

• Alice (Sender)

i) Generates message M

ii) Generates MAC = h(M, K) with M and K as input parameters

iii) Sends {M, MAC} to Bob

• Bob (Receiver)

i) Receives {M', MAC} (message denoted as M')

ii) Generates MAC′ = h(M',K) from M'.

iii) Compares MAC′ and MAC

iv) If MAC = MAC′ then Bob knows the message was unchanged in transit

Question 2: [CLO#3 – C4] [2 points]

How does a private key signature ensure non-repudiation? GMail wants every email to be authenticated and protected from modification or tampering while it is in transit from the sender to the receiver. Suppose Alice is sending an email M to Bob. Given GMail's design constraints, what would be a secure way to protect the authenticity and integrity of her email?

Solution:

Private key can only belong to the signer, and signing the hash ensures that the message's integrity can be associated with the private key encryption.

Alice's should send M along with a digital signature on M using Alice's private key. In other words, Alice should send M, S ignK$_{A}$ $^{-1}$ (M). (Signature algorithm)

Question 3: [CLO#4 – C3] [2 points]

A message has 2000 characters. If it is supposed to be encrypted using a block cipher of 64 bits and a character is an 8-bit value, find the size of the padding and the number of blocks.

ANS) Using eight bits for each character, |M| = 8 X 2000 = 16,000 bits. Therefore, we have |M|+|Pad|=0 mod 64 -> |Pad| = -|M| mod 64 -> |Pad| = -16000 mod 64 = 0

This means no padding is needed.

The message is divided into 250 blocks.

Question 4: [CLO#3 – C4] [2 points]

Assume that Arif can observe all messages sent from Sidra to Imran and vice versa. Arif does not have knowledge of any keys but the public key in case of Digital Signature (DS). State whether and how (i) DS and (ii) MAC protect against each attack. The value auth(x) is computed with a DS or a MAC algorithm, respectively.

a. ***(Message Integrity)*** Sidra sends a message x = "Transfer $1000 to Yasir" in the clear and also sends auth(x) to Imran. Arif intercepts the message and replaces "Yasir" with "Arif." Will Imran detect this?
b. ***(Replay)*** Sidra sends a message x = "Transfer $1000 to Arif" in the clear and also sends auth(x) to Imran. Arif observes the message and signature and sends them 100 times to Imran. Will Imran detect this?

ANS)

a) Will be detected with both (i) DS and (ii) MAC.

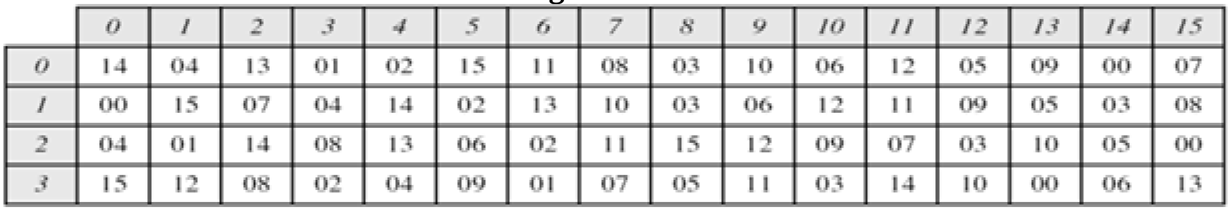
b) Won't be detected by either (use timestamps).

Question 5: [CLO#4 – C4] [1 points]

Show the result of passing the following through S-Box (Figure 1).

a. 001100
b. 110011

Figure 1: S-Box



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

ANS)

(a) 0 0110 0

00 -> 0 0110-> 6

Output = 11 (decimal)

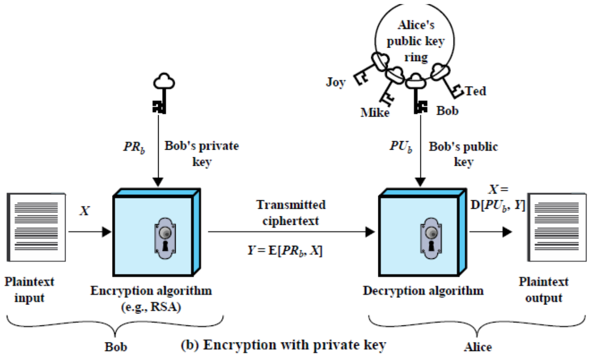
(b) 1 1001 1

11 -> 3 1001 -> 9
Output = 11 (decimal)

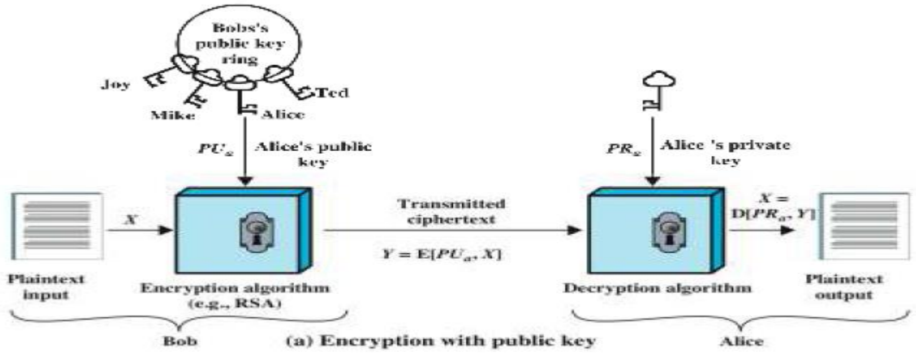
Question 6: [CLO#1 – C2] [2 points]

Illustrate (labelled diagram only) a public-key cryptosystem depicting the concepts of digital signature and confidentiality.

Solution:



Digital Signature



Confidentiality

Students need to combine the above two mechanisms by applying digital signature first and encryption of message (confidentiality) after it.

Question 7: [CLO#4 – C4] [2 points]

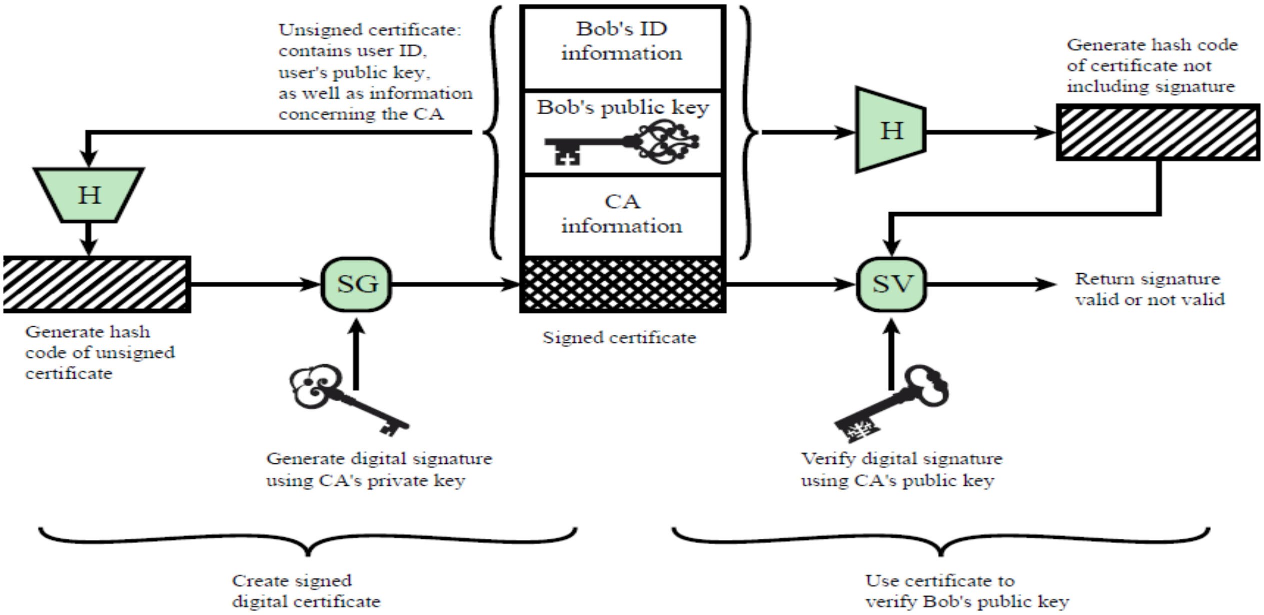
Let ***H(M)*** be a cryptographic hash function. Is it possible to use a hash function as an encryption algorithm for confidentiality? Is it possible for the attacker to find '***M***' if ***H(M)*** is known? Give valid reasons for your answer.

ANS) No because hash function is irreversible. It is not computationally feasible as hashes are one-way functions. However, an attacker can tell if the same message is sent twice as hashes are deterministic. An attacker could also test a guess at 'M'.

Question 8: [CLO#1 – C2] [2 points]

Illustrate (labelled diagram only) the process generation and verification of a public-key certificate.

Solution


Unsigned certificate:
contains user ID,
user's public key,
as well as information
concerning the CA
Bob's ID information
Bob's public key
CA information
H
Generate hash code of certificate not including signature
H
SG
SV
Return signature valid or not valid
Generate hash code of unsigned certificate
Signed certificate
Generate digital signature using CA's private key
Verify digital signature using CA's public key
Create signed digital certificate
Use certificate to verify Bob's public key

****