Monash University
Faculty of Information Technology
FIT3031 Information and network security

Class Test

Instructions to Candidates:

1. **First complete this section**

You must complete this section

STUDENT ID:_____

STUDENT NAME : _____

- ☐ **TUTOR NAME : FATHIMA**
- ☐ **TUTOR NAME : SEPEHR**
- ☐ **TUTOR NAME : MALIK**

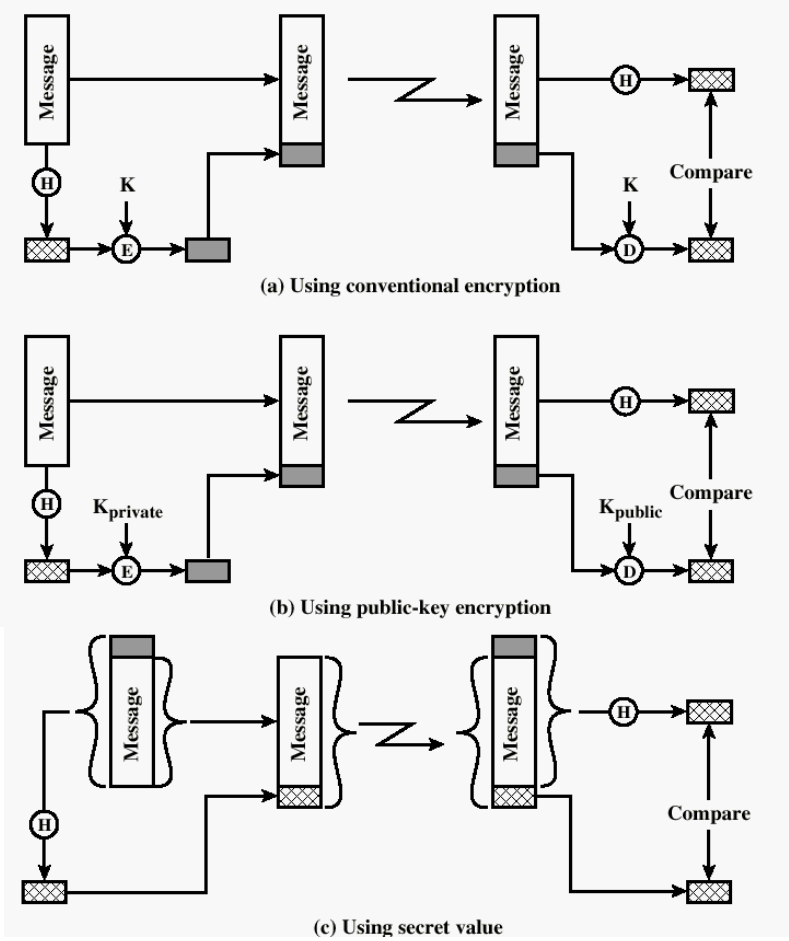
2. **The coverage material from LN01 to LN08 (inclusive of LN08 IP Security).**
3. **There are 2 parts to the test.**
4. **Answer all questions in the space provided in each part.**
5. **Marks are indicated at the beginning of each question.**
6. **This class test is worth 20 % of UNIT marks.**
7. **The duration of this class test is 60 minutes.**
8. **Return this question paper intact.**

Part 1: Answer the following questions in the space provided:

1. **Question-1. (5 + (3+3) = 11 marks)**

   a. With the help of neat diagrams explain any two schemes for message authentication?

   [2 x 2.5 = 5 marks]



Ans:

(a) A hash code is computed from the source message, encrypted using symmetric encryption and a secret key, and appended to the message. At the receiver, the same hash code is computed. The incoming code is decrypted using the same key and compared with the computed hash code.

(b) This is the same procedure as in (a) except that public-key encryption is used; the sender encrypts the hash code with the sender's private key, and the receiver decrypts the hash code with the sender's public key.

(c) A secret value is appended to a message and then a hash code is calculated using the message plus secret value as input. Then the message (without the secret value) and the hash code are transmitted. The receiver appends the same secret value to the message and computes the hash value over the message plus secret value. This is then compared to the received hash code.

(In each of these schemes you will need to explain why each of these schemes provide message authentication.)

2 x 2.5 marks = 5 Marks (includes 1.5 marks each for diagram + 1 marks for explanation)
Any two of these three schemes

b. For the 8-bit CFB (Cipher Feedback) mode with each encrypt block consisting of 128-bit AES as shown in Figure below:

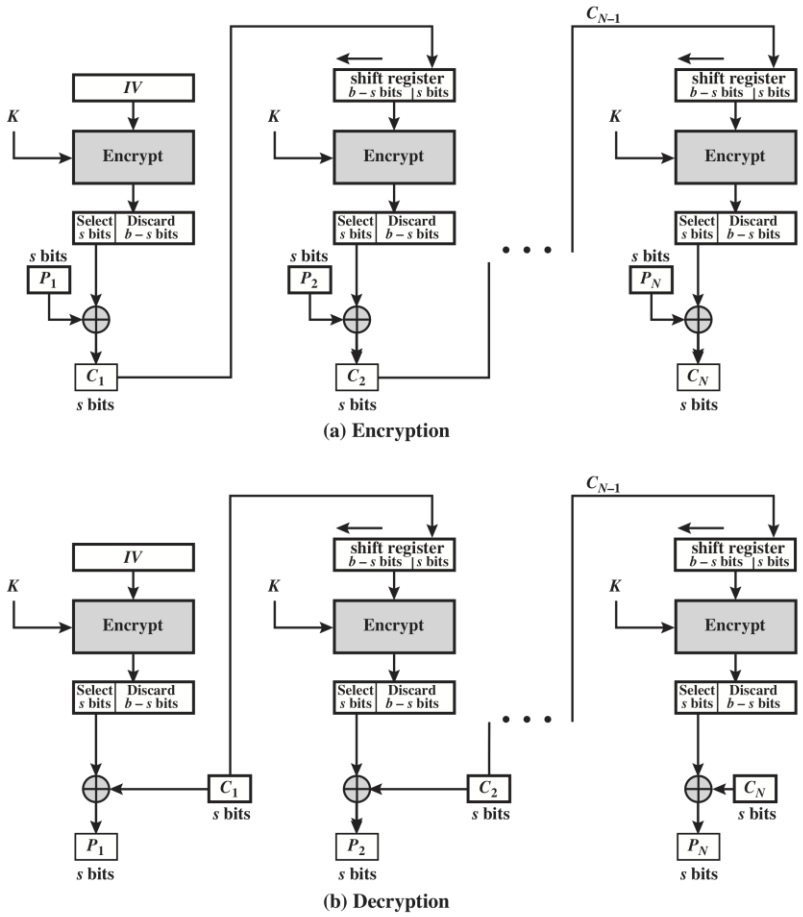


Figure 1: s-bit Cipher Feedback (CFB) Mode

i. Identify which decrypted plaintext blocks $\mathbf{P_x}$ will be corrupted if there is an error in block $\mathbf{C_4}$ of the transmitted ciphertext giving reasons. **[3 marks]**

If there is, an error in the transmitted C_4 only then this will affect the decrypted $\mathbf{P_4}$ and $\mathbf{P_5}$, as both these plaintext blocks depend on the transmitted C4. In addition, the transmitted C4, which is in error also corrupts the least significant eight bits of the 128-bit shift register. This will remain in the shift register for 16 blocks (128/8 = 16) thus corrupting blocks P5 to P20. Hence, here you have decrypted message blocks P4 to P20 corrupted if the transmitted C4 is in error.

[1.5 mark for correct answer, 1.5 mark for the reason/explanation]

ii. Assuming that the ciphertext contains of **N** blocks, and there was a bit error in the source version of $\mathbf{P_3}$, identify through how many ciphertext blocks this error is propagated giving reasons.

[3 marks]

17 plaintext characters are affected. The plaintext character corresponding to the ciphertext character is obviously altered. In addition, the altered Ciphertext character enters the shift Register and is not removed until the next 16 Characters (128/8 = 16) Are processed.

{1.5 Mark for correct answer, 1.5 marks for explanation]

2. Question-2. (3 + 4 = 7 marks)

a. When a Client (C) presents a service granting ticket (SGT) to a server (S) in a system that uses Kerberos to provide the authentication service, the client must also attach an authenticator to prove that he is the legitimate holder of the ticket. How can the server (S) verify that the authenticator belongs to the ticket's legitimate holder? **[3marks]**

The authenticator contains the client's identity and a timestamp. These are encrypted with the session key that is known to the client and the server. [1 mark]

So a client that will create a valid authenticator has to have this session key, which has been provided by the TGS (Ticket Granting Server) to the client and the server via a ticket that has been encrypted with a key known to the TGS and the server. [1 mark]

Since the TGS has checked the client's legitimacy (using the ticket provided by the Authentication Server (AS)), S is sure that the client with the session key is legitimate as he is the only one who is able to create a valid authenticator with his identity. [1 mark]

b. What are the requirements for the use of a public-key certificate scheme? **[4 Marks]**

1. Any participant can read a certificate to determine the name and public key of the certificate's owner.
2. Any participant can verify that the certificate originated from the certificate authority and is not counterfeit.
3. Only the certificate authority can create and update certificates.

4. Any participant can verify the currency of the certificate.

(1 MARKS FOR EACH POINT)

4. Question-3. (3 + 3 = 6 marks)

a. Explain how PGP achieves public key management. **[3 marks]**

Rather than relying on certification authorities, in PGP every user is a CA. [1 mark]

A user can sign keys for users they know directly. [1 mark]

They form a "web of trust" and can trust keys others have signed if they have a chain of signatures to them. [1 mark]

c. You have just received an email with the digital signature of a certain Bill Thornton using PGP. Unfortunately, you have never exchanged a public key with any Bill Thornton. It happens that Richard Branson has signed Bill's key and John Fraser, whom you completely trust has signed Richard's key. What can you say about the validity of Bill Thornton's key?**[3 marks]**

Since Richard Branson's key is signed by John Fraser whom you trust (i.e. in the web of trust it is indicated that you already have complete trust in John Fraser who signed Richard Branson's key), [1 mark]

So you can consider his key as being valid. [1 mark]

However, you do not know how much trust John has in Richard Branson, therefore, you cannot validate Bill Thornton's key. [1 mark]

5. **Question-4: [2 x 3 =6 marks]**
   a. Consider the following threats to Web security and describe/explain how a particular feature of SSL in each case provides a countermeasure.

   i) Replay Attack: Earlier SSL handshake messages are replayed. **[2 marks]**

Answer:

Replay Attack: This is prevented by the use of nonces.

The replay attack is countered through the usage of a timestamp in the server authentication process. The client will check to see if the server's certificate is valid and during that process, a timestamp would be used to verify that the messages are not old.

Replay Attack: This is prevented by the use of **nonces**. Both client and server use nonces when they send session keys. Before the message is signed the content of the message is hashed along with the nonces and they are attached to the message. The Handshake Protocol makes sure messages are sent and received with a signature hash.

ii) **Man-in-the-Middle Attack:** An attacker interposes during key exchange, acting as the client to the server and as server to the client. **[2 marks]**

Answer:

Man-in-the-Middle Attack: This is prevented by the use of public-key certificates to authenticate the correspondents.

The client application checks the server domain name specified in the server certificate is the same as the actual domain name of the server. If they are not the same, the authentication fails.

Man-in-the-Middle Attack: This is prevented by the use of public-key certificates to authenticate the correspondents. The checking if the domain name in server's certificate matches the domain name of the server itself. This step makes sure that the server is in the same network address specified by domain name in the certificate. This step alone protects from this attack although it is not part of SSL.

iii) **Password sniffing:** Passwords in HTTP or other application traffic are eavesdropped. **[2 marks]**

Answer:

Password Sniffing: User data is encrypted. The application message is encrypted, so the password transmission is protected.

Password Sniffing: User data is encrypted.

With SSL, key-management is handled well because short-term session keys are generated using random hash number generators. Each direction of communication generates independent keys for the connection as well as for each instance of the connection.

END OF PART 1

FIT3031 Sum-Semester B, 2017 Class

Test Part 2

(10 +10 + 10 = 30 marks)

TRUE/FALSE. Write 'T' if the statement is true and 'F' if the statement is false.

1. A loss of confidentiality is the unauthorized modification or destruction of information._____False_____
2. Patient allergy information is an example of an asset with a moderate requirement for integrity. ._____False_____
3. The primary advantage of a stream cipher is that stream ciphers are almost always faster and use far less code than do block ciphers. ._____True_____
4. One desirable property of a stream cipher is that the ciphertext be longer in length than the plaintext._____False_____
5. Because of the mathematical properties of the message authentication code function it is less vulnerable to being broken than encryption. ._____True_____
6. Cryptographic hash functions generally execute slower in software than conventional encryption algorithms such as DES. ._____False_____
7. The security of the Diffie-Hellman key exchange lies in the fact that, while it is relatively easy to calculate exponentials modulo a prime, it is very easy to calculate discrete logarithms. ._____False_____
8. The automated key distribution approach provides the flexibility and dynamic characteristics needed to allow a number of users to access a number of servers and for the servers to exchange data with each other. ._____True_____
9. If an opponent captures an unexpired service granting ticket and tries to use it they will be denied access to the corresponding service._____False_____
10. Transport mode provides protection to the entire IP packet. ._____False_____

MULTIPLE CHOICE. Choose the one alternative that best completes the statement or answers the question.

1. Verifying that users are who they say they are and that each input arriving at the system came from a trusted source is _____.
   A) confidentiality
   B) authenticity
   C) accountability
   D) integrity

2. A _____is an individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account.
   A) Clandestine User
   B) Misfeasor
   C) Sniffer
   D) Masquerader

3. _____mode requires only the implementation of the encryption algorithm and not the decryption algorithm.
   A) DKS
   B) CTR
   C) ECB
   D) CBC

4. Authentication applied to the entire original IP packet is _____.
   A) cipher mode
   B) transport mode
   C) security mode
   D) tunnel mode

5. If the analyst is able to get the source system to insert into the system a message chosen by the analyst, a _____attack is possible.
   A) known plaintext
   B) chosen plaintext
   C) chosen ciphertext
   D) ciphertext only

6. It is computationally infeasible to find any pair (x, y) such that $H(x) = H(y)$. A hash function with this property is referred to as _____
   A) collision resistant
   B) preimage resistant
   C) weak collision resistant
   D) one-way

7. The most widely accepted and implemented approach to public-key encryption, _____is a block cipher in which the plaintext and ciphertext are integers between 0 and $n - 1$ for some n.
   A) RSA
   B) MD5
   C) SHA
   D) CTR

8. The _____knows the passwords of all users and stores these in a centralized database and also shares a unique secret key with each server.

A) management server
B) key distribution server
C) ticket server
D) authentication server

9. Once the authentication server accepts the user as authentic it creates an encrypted _____which is sent back to the client.

A) password
B) ticket
C) key
D) access code

10. _____provides secure, remote logon and other secure client/server facilities.

A) SSH
B) HTTPS
C) SLP
D) TLS

SHORT ANSWER. Write the word or phrase that best completes each statement or answers the question.

1. An intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system is an _____ **attack** _____.

2. A _____**Passive**_____attack attempts to learn or make use of information from the system but does not affect system resources.

3. A _____ **digital signature**_____is data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery.

4. An encryption scheme is __ **computationally secure**____if the cost of breaking the cipher exceeds the value of the encrypted information and/or the time required to break the cipher exceeds the useful lifetime of the information.

5. Protection against active attack (falsification of data and transactions) is known as _____**message authentication**_____

6. Bob uses his own private key to encrypt the message. When Alice receives the ciphertext she finds that she can decrypt it with Bob's public key, thus proving that the message must have been encrypted by Bob. No one else has Bob's private key and therefore no one else could have created a ciphertext that could be decrypted with Bob's public key. Therefore the entire encrypted message serves as a ____ **digital signature**_____.

7. The ____ **SSL Record Protocol** ____takes an application message to be transmitted, fragments the data into manageable blocks, optionally compresses the data, applies a MAC, encrypts, adds a header, and transmits the resulting unit in a TCP segment.

8. The WAP Programming Model is based on three elements: the client, the original server, and the _____ **gateway** _____.

9. The key legitimacy field, the signature trust field and the owner trust field are each contained in a structure referred to as a ___ **trust flag byte** _____.

10. IPsec policy is determined primarily by the interaction of two databases: The security policy database and the ____ **security association database (SAD)** _____.

END OF CLASS TEST