Monash University

Semester One Examination Period 20XX

Faculty of Information Technology
Sample Exam Paper

EXAM CODES:	**FIT3031**
TITLE OF PAPER:	**Information & Network Security**
EXAM DURATION:	2 hours writing time
READING TIME:	10 minutes

THIS PAPER IS FOR STUDENTS STUDYING AT:(tick where applicable)

□ Berwick
☼ Caulfield
□ Pharmacy
☒Clayton
□ Gippsland
□ Other (specify)
□ Malaysia
□ Peninsula
□ Off Campus Learning
□ Enhancement Studies
□ Open Learning
☼ Sth Africa

During an exam, you must not have in your possession, a book, notes, paper, electronic device/s, calculator, pencil case, mobile phone or other material/item which has not been authorised for the exam or specifically permitted as noted below. Any material or item on your desk, chair or person will be deemed to be in your possession. You are reminded that possession of unauthorised materials in an exam is a discipline offence under Monash Statute 4.1.

No examination papers are to be removed from the room.

AUTHORISED MATERIALS

CALCULATORS □ **YES** ☼ **NO**

OPEN BOOK □ **YES** ☼ **NO**

SPECIFICALLY PERMITTED ITEMS □ **YES** ☼ **NO**

INSTRUCTIONS

1. Please answer **ALL** of them.
2. Start the answer to each question on a new page.
3. Write on one side of the paper only.
4. Total marks - 100. This exam contributes 60% to your result for this unit.

Important Disclaimer: Preparing for Your EXAM

*It is advisable to complete your required preparation(s) as quickly as possible and be prepared at least 1 weeks before your exam. The sample exam and coverage can provide **ONLY** sample preparation materials to help you prepare for the exam. The Sample exam Questions above **ARE NOT** designed to provide you with all exam coverage for final exam assessment of your current skill levels, but to orient you to the style of question used in the actual final exam assessment. **DO NOT** treat the sample questions as the **ONLY** scope for your practice exam, or as the actual exam. The final Questions will vary considerably in their content, coverage and the level of difficulty.*

Full Marks:XX marks

There are TWO sections. ANSWER ALL QUESTIONS in both sections in your answer book.

Section A. Multiple Choice. Choose only one answer that best completes the statement.

1. Which of the following algorithm is a symmetric encryption algorithm?

   A. RSA
   B. Diffie-Hellman
   C. SHA-256
   D. DES

2. Which of the following attack(s) is/are active attack?

   (i) Replay
   (ii) Modification of Message
   (iii) Denial-of-Service
   A. (i) only
   B. (i) and (iii)
   C. (ii) and (iii)
   D. All of the above

3. Which of the following statement(s) regarding symmetric encryption is/are not true?

   A. The encryption key is the same as decryption key
   B. Symmetric key encryption is slower than asymmetric key encryption
   C. AES can be speed up using hardware module
   D. All of the above statements are not true

4. Asymmetric encryption can solve the___________problem(s) of symmetric encryption.

   A. key distribution
   B. integrity
   C. efficiency
   D. all of the above

5. Which of the following statement(s) regarding a hash function is/are true?

   (i) The output length of a hash function depends on the input message.
   (ii) It is collision-resistant.
   (iii) It is one-way.
   A. (i) only
   B. (ii) only
   C. (ii) and (iii)
   D. None of the above

6. In IPSec,___________encrypts the whole IP packet.

   A. tunnel mode
   B. transport mode
   C. host-to-host mode
   D. every mode

7. Which of the following issue(s) is/are related to WEP?

   A. No mutual authentication
   B. Directly uses master key
   C. IV value is too small
   D. All of the above

8. ___________is used to secure email.

   A. SMTP
   B. S/MIME
   C. Telnet
   D. Kerberos

9. Trapdoors are left during the software____________phase.

   A. authentication
   B. certification
   C. development
   D. execution

10. The security of Diffie-Hellman Algorithm relies on the___________problem.

    A. factorization
    B. subset sum
    C. discrete logarithm (DL)
    D. learning with errors (LWE)

11. IPSec is used to secure the____________layer.

    A. application
    B. TCP
    C. IP
    D. physical

12. X.509 is a standard of___________.

    A. digital signature
    B. email security
    C. wireless-LAN security
    D. digital certificate

13. Which of the following activities are examples of Intrusion?
    (i) Cracking password
    (ii) Distributing pirated software
    (iii) Using e-banking service from a web browser in a library public computer during opening hours

    A. (i) and (ii)
    B. (ii) and (iii)
    C. (i) and (iii)
    D. All of the above

14. Which of the following statement(s) describe(s) correctly the difference(s) between a virus and a worm?

    A. A virus cannot be spread without a human action, but a worm has the capacity to travel without any human action.
    B. A virus does not have the dormant phase, but a worm does have.
    C. In the propagation phase, a virus searches for other systems but a worm only searchers for other programs running within the same system.
    D. All of the above are correct

15. Which of the following is/are the limitation(s) of a firewall?

    A. Cannot protect from attacks bypassing it
    B. Cannot protect against internal threat
    C. All of the above are limitations of a firewall
    D. There is no limitation of a firewall

In addition, please go through all the weekly Quizzes we have in the Moodle!

Important Disclaimer: Preparing for Your EXAM

*It is advisable to complete your required preparation(s) as quickly as possible and be prepared at least 1 weeks before your exam. The sample exam and coverage can provide **ONLY** sample preparation materials to help you prepare for the exam. The Sample exam Questions above **ARE NOT** designed to provide you with all exam coverage for final exam assessment of your current skill levels, but to orient you to the style of question used in the actual final exam assessment. **DO NOT** treat the sample questions as the **ONLY** scope for your practice exam, or as the actual exam. The final Questions will vary considerably in their content, coverage and the level of difficulty.*

Section B: Questions & Answers. (XX marks)

1. (a) Briefly explain the following security services:

(i) Confidentiality
(ii) Access Control
(iii) Integrity
(iv) Availability

(b) Which of the above security services (i) – (iv) can a signcryption provide? Explain your answer.

ANSWER:

(a) refer to lecture notes Week 1, pg. 29.

(b) A signrcryption can provide (i), (ii), (iii). A signcryption is a combination of encryption + signature. Confidentiality can be provided by using an encryption. Access control can be provided by using either an encryption or signature. Integrity can be provided by using a signature. Thus a signcryption can provide those services which can be provided by an encryption and signature, that is, (i), (ii) and (iii). However, availability cannot be provided by neither an encryption nor a signature.

2. (a) Which of the following (n,e) pair is a correct RSA public key?

(i) n = 35, e = 3
(ii) n = 85, e = 3

Explain your answer.

(b) For the correct RSA public key in part (a), what is the corresponding private key d? Show your steps.

(c) Use the correct RSA public key in part (a) to encrypt a plaintext m=5. Show your steps.

ANSWER:

(a) (i) n=35 → p=5, q=7. \phi(n) = 4 X 6 = 24. Since gcd(24, 3) is not equal to 1, it is not a valid RSA public key.

(ii) n=85 → p=5, q=17. \phi(n) = 4 X 16 = 64. Since gcd(64,3) = 1, it is a valid RSA public key.
[Refer to lecture notes Week 3, pg. 25]

(b) d.e = 1 mod \phi(n) → 3d = 1 mod 64 → 3d – 1 = 0 mod 64 → 3d - 1= 64N for some integer N → 3d = 64N + 1.
When N=1, 64+1=65 is not divisible by 3.
When N=2, 64X2+1 = 129 which is divisible by 3.
Then we have 3 X 43 = 129 → d = 43.

(c) C = m^e mod n = 5 ^ 3 mod 85 = 125 mod 85 = 40 mod 85.

3. Which Cipher Block Modes of Operations, ECB or CBC, is more commonly used? Give one advantage of using CBC over ECB and one disadvantage of using CBC over ECB.

ANSWER:

CBC is more commonly used.

Advantage: more secure – repeated pattern will not be exposed, provided that a different IV is used.

Disadvantage: encryption of a data block becomes dependent on all the blocks prior to it; or a lost block of data will prevent decoding of the next block of data

[Refer to lecture notes Week 2, pg. 44]

4. Give any FOUR security services that IPSec can provide.

ANSWER:

- Access Control
- connectionless integrity
- Data origin authentication
- Rejection of replayed packet
- Confidentiality / encryption

(any FOUR)

[Refer to lecture notes Week 8, pg. 14]

5. Give THREE possible attacks that involve password capture.

ANSWER:

- watching over shoulder as password is entered
- Using a trojan horse program to collect
- Monitoring an insecure network login
- Extracting recorded info after successful login

(any THREE, or any other reasonable answer)

[Refer to lecture notes Week 9, pg. 23]

6.

(a) What are the two default policies of packet filtering firewall?

(b) Give TWO advantages and THREE disadvantages of using packet filtering firewall over application level gateway firewall.

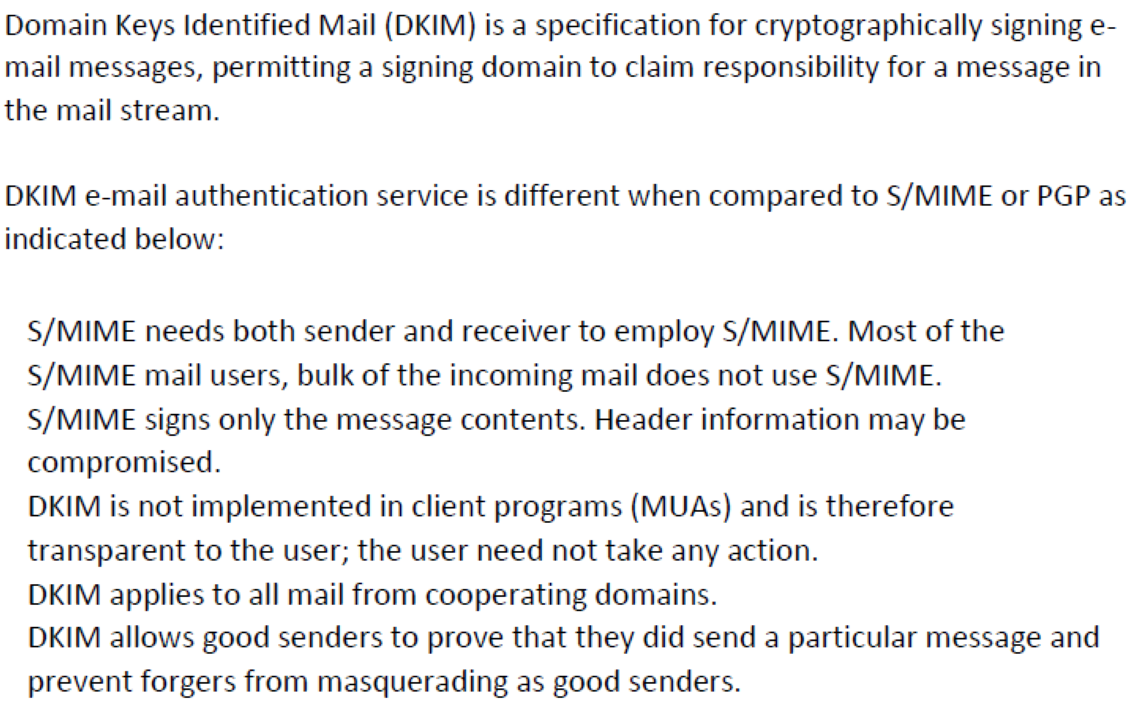
ANSWER:

(a) Discard, Forward

(b) Refer to lecture notes Week 11, pg. 19-20

7.

a) What is Domain Keys Identified Mail (DKIM)?
b) How is the DKIM e-mail authentication service different when compared to S/MIME or PGP? Give TWO differences.



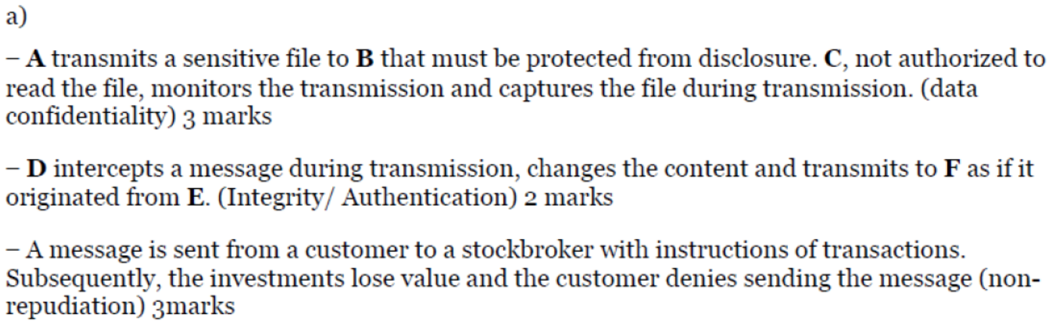
Domain Keys Identified Mail (DKIM) is a specification for cryptographically signing e-mail messages, permitting a signing domain to claim responsibility for a message in the mail stream.

DKIM e-mail authentication service is different when compared to S/MIME or PGP as indicated below:

- S/MIME needs both sender and receiver to employ S/MIME. Most of the S/MIME mail users, bulk of the incoming mail does not use S/MIME.
- S/MIME signs only the message contents. Header information may be compromised.
- DKIM is not implemented in client programs (MUAs) and is therefore transparent to the user; the user need not take any action.
- DKIM applies to all mail from cooperating domains.
- DKIM allows good senders to prove that they did send a particular message and prevent forgers from masquerading as good senders.

8. Answer the following questions:

a) Explain any two examples of security violations that can be experienced in the transmission of information over the network. For each example given, name the type of security service that applies to such violations.
b) There are two major concerns with regards to where to implement the security mechanisms designed to combat security violations. Briefly explain these two concerns.
c) Explain briefly polymorphic virus and metamorphic virus?(Ref: Lecture)
d) List the six main security services defined by the X800 OSI security architecture?(Ref: Lecture)

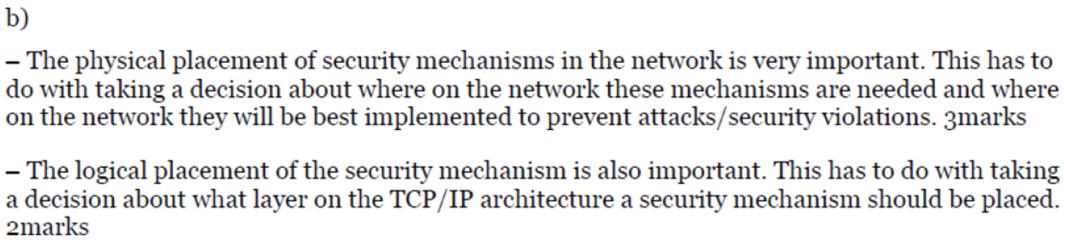


a)

– **A** transmits a sensitive file to **B** that must be protected from disclosure. **C**, not authorized to read the file, monitors the transmission and captures the file during transmission. (data confidentiality) 3 marks

– **D** intercepts a message during transmission, changes the content and transmits to **F** as if it originated from **E**. (Integrity/ Authentication) 2 marks

– A message is sent from a customer to a stockbroker with instructions of transactions. Subsequently, the investments lose value and the customer denies sending the message (non-repudiation) 3marks



b)

– The physical placement of security mechanisms in the network is very important. This has to do with taking a decision about where on the network these mechanisms are needed and where on the network they will be best implemented to prevent attacks/security violations. 3marks

– The logical placement of the security mechanism is also important. This has to do with taking a decision about what layer on the TCP/IP architecture a security mechanism should be placed. 2marks

9.

a) Suppose Bob chooses n=35 as his RSA modulus and chooses e=7 as his public key exponent so that his public key (n, e) = (7, 35). Calculate his private key exponent d.

b) In asymmetric encryption, a sender can deny his public key and a hacker can create a false key to impersonate someone. Explain how it can be ensured that the public key belongs to the entity that it claims it belongs to?

a) n=5x7=35,

So, p=5 and q =7

Hence, ø(N)= (5-1)(7-1)=24.

The private key exponent, d should satisfy: de mod ø(N)=1

dx7mod24=1

dx7/24 should give a remainder of 1, thus d=7.

Private key = (7, 35).

b) A trusted body is required to certify public key. The trusted body is the Certification Authority (CA) which certifies the public key of any user.

- user A generates his/her public key and submits to CA for certification
- CA determines identity and background of A
- CA appends time stamp to public key, generates hash code and encrypts with CA's private key.
    - This constitutes the signature of CA
    - hash code ensure that public key is unaltered
- Signed public key of A is now available for presentation
- Any one equipped with CA's public key can authenticate A's authenticity

10.

a) What hash function is used in PGP and what is the length of the message digest? What is the use of detached signature supported by PGP?

b) Why does PGP generate a signature before applying compression?

(a) SHA-1 160 bit message length.

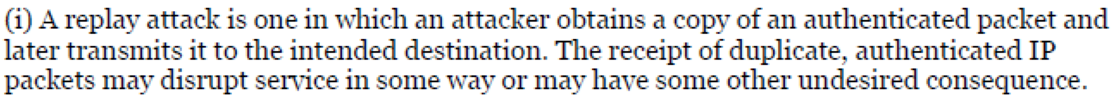
A detached signature is useful in several contexts. A user may wish to maintain a separate signature log of all messages sent or received. A detached signature of an executable program can detect subsequent virus infection. Finally, detached signatures can be used when more than one party must sign a document, such as a legal contract. Each person's signature is independent and therefore is applied only to the document. Otherwise, signatures would have to be nested, with the second signer signing both the document and the first signature, and so on.

(b)

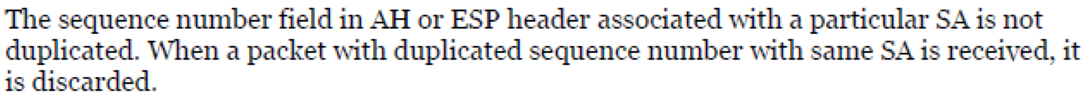
- The sender needs to store only the uncompressed message and the signature for future verification
    - Otherwise, compressed message needs to be store as well
- There are different compression algorithms and different versions of the same algorithm
    - If compression is done after encryption, all PGP implementation must use the same version of the same algorithm
- It strengthen the security as cryptanalysis on compressed message is more difficult

11.

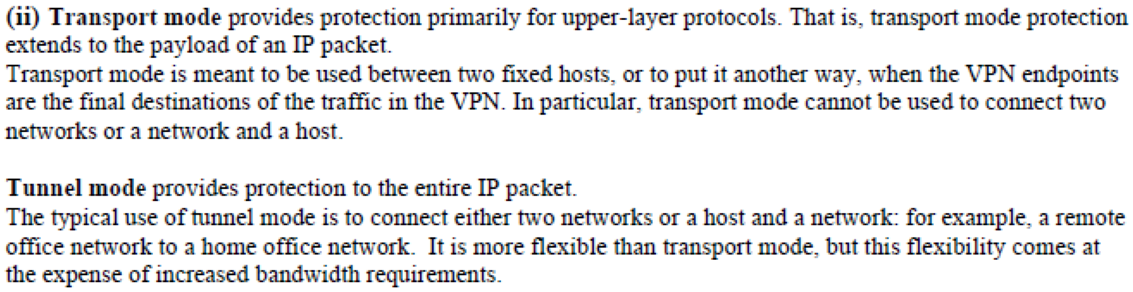
a) In relation to IPSec, answer the following:
   i. Explain how IPSec can prevent a replay attack.
   ii. Explain the difference between transport and tunnel mode operation of IPSec? When is it suitable to use each of the above modes of operation?



(i) A replay attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination. The receipt of duplicate, authenticated IP packets may disrupt service in some way or may have some other undesired consequence.



The sequence number field in AH or ESP header associated with a particular SA is not duplicated. When a packet with duplicated sequence number with same SA is received, it is discarded.



(ii) Transport mode provides protection primarily for upper-layer protocols. That is, transport mode protection extends to the payload of an IP packet.
Transport mode is meant to be used between two fixed hosts, or to put it another way, when the VPN endpoints are the final destinations of the traffic in the VPN. In particular, transport mode cannot be used to connect two networks or a network and a host.

Tunnel mode provides protection to the entire IP packet.
The typical use of tunnel mode is to connect either two networks or a host and a network: for example, a remote office network to a home office network. It is more flexible than transport mode, but this flexibility comes at the expense of increased bandwidth requirements.

12.

a) What security areas are addressed by IEEE 802.11i? Briefly describe the four IEEE 802.11i phases of operation.
b) What is the difference between an SSL connection and an SSL session?
c) Describe services that are provided by the SSL Record Protocol.

(a): IEEE 802.11i addresses four main security areas: authentication, key management, data confidentiality & data integrity.

- **Discovery**: An AP uses messages called Beacons and Probe Responses to advertise its IEEE 802.11i security policy. The STA uses these to identify an AP for a WLAN with which it wishes to communicate. The STA associates with the AP, which it uses to select the cipher suite and authentication mechanism when the Beacons and Probe Responses present a choice.
- **Authentication**: During this phase, the STA and AS prove their identities to each other. The AP blocks non-authentication traffic between the STA and AS until the authentication transaction is successful. The AP does not participate in the authentication transaction other than forwarding traffic between the STA and AS.
- **Key generation and distribution**: The AP and the STA perform several operations that cause cryptographic keys to be generated and placed on the AP and the STA. Frames are exchanged between the AP and STA only Protected data transfer: Frames are exchanged between the STA and the end station through the AP. As denoted by the shading and the encryption module icon, secure data transfer occurs between the STA and the AP only; security is not provided end-to-end.
- **Connection termination:** The AP and STA exchange frames. During this

phase, the secure connection is torn down and the connection is restored to the original state.

(b) The following services are provided
Confidentiality: The Handshake Protocol defines a shared secret key that is used for conventional encryption of SSL payloads.
Message Integrity: The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC). The method used for these are:
Fragmentation - fragments the data in manageable block size (16KB or less)
Compression – optional, must be lossless, SSLv3 (TLS) does not specify any compression algorithm
Integrity protection - compute MAC on the compressed data using SHA-1,MD; uses a shared secret key negotiated in handshake protocol
Encryption - compressed message and MAC are encrypted using symmetric encryption algorithm; Algorithm permitted: IDEA, RC2, RC4, DES, 3DES, Fortezza
Append SSL record header

13.

a) List and briefly define three classes of intruders.
b) Having an Intrusion Detection System (IDS) in a network is crucial for ensuring security. What are the benefits that can be provided by an intrusion detection system?
c) What are the characteristics of stealth and polymorphic viruses that make them difficult to detect? Name two advanced antivirus techniques.

(a)

- **Masquerader**: 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.
- **Misfeasor**: A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges.
- **Clandestine user**: An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.

(b)

- If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system before any damage is done or any data are compromised. Even if the detection is not sufficiently timely to preempt the intruder, the sooner that the intrusion is detected, the less the amount of damage and the more quickly that recovery can be achieved.
- An effective intrusion detection system can serve as a deterrent, so acting to prevent intrusions.
- Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility.

(c)
Stealth virus:

- explicitly designed to hide from virus scanning programs;
- b)actively hides any change it has made to the hard disk;
- The virus takes over system functions that are used in reading files or system sectors.

Polymorphic virus:

- mutates with every infection, making "signature" detection impossible appearance and size changes;
- difficult to detect by scanning as each copy looks different;
- needs more than one method of viral detection.

Two advance anti-virus techniques:

- Generic Decryption;
- Digital Immune System

14. Firewalls are a viewed as a means to protect internal networks from external networks. In relation to this, explain the following:

    a) List three design goals for a firewall.
    b) What is a DMZ network and what types of systems would you expect to find on such networks.
    c) What is the difference between an external and internal firewall?

(a)

- All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Various configurations are possible, as explained later in this section.
- Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies, as explained later in this section.
- The firewall itself is immune to penetration. This implies that use of a trusted system with a secure operating system.

(b)

- Between internal and external firewalls are one or more networked devices in a region referred to as a DMZ (demilitarized zone) network. Systems that are externally accessible but need some protections are usually located on DMZ networks. Typically, the systems in the DMZ require or foster external connectivity, such as a corporate Web site, an e-mail server, or a DNS (domain name system) server.

(c)

- An external firewall is placed at the edge of a local or enterprise network, just inside the boundary router that connects to the Internet or some wide area network (WAN). One or more internal firewalls protect the bulk of the enterprise network.

In addition, please go through all the tutorials solutions we have in the Moodle!

Important Disclaimer: Preparing for Your EXAM

*It is advisable to complete your required preparation(s) as quickly as possible and be prepared at least 1 weeks before your exam. The sample exam and coverage can provide **ONLY** sample preparation materials to help you prepare for the exam. The Sample exam Questions above **ARE NOT** designed to provide you with all exam coverage for final exam assessment of your current skill levels, but to orient you to the style of question used in the actual final exam assessment. **DO NOT** treat the sample questions as the **ONLY** scope for your practice exam, or as the actual exam. The final Questions will vary considerably in their content, coverage and the level of difficulty.*