Office Use Only

MONASH University

Semester One 2017
Examination Period
SAMPLE EXAM PAPER SOLUTIONS
Faculty of Information Technology

EXAM CODES:	**FIT2093**
TITLE OF PAPER:	**Introduction to cyber security**
EXAM DURATION:	3 hours writing time
READING TIME:	10 minutes

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

□ Berwick
□ Caulfield
□ Parkville
☑ Clayton
□ Gippsland
□ Other (specify)
☑ Malaysia
□ Peninsula
□ Off Campus Learning
□ Monash Extension
□ Open Learning
□ Sth Africa

During an exam, you must not have in your possession any item/material that has not been authorised for your exam. This includes books, notes, paper, electronic device/s, mobile phone, smart watch/device, calculator, pencil case, or writing on any part of your body. Any authorised items are listed below. Items/materials on your desk, chair, in your clothing or otherwise on your person will be deemed to be in your possession.

No examination materials are to be removed from the room. This includes retaining, copying, memorising or noting down content of exam material for personal use or to share with any other person by any means following your exam.
Failure to comply with the above instructions, or attempting to cheat or cheating in an exam is a discipline offence under Part 7 of the Monash University (Council) Regulations.

AUTHORISED MATERIALS

OPEN BOOK	□ **YES**	☑ **NO**
CALCULATORS	□ **YES**	☑ **NO**
SPECIFICALLY PERMITTED ITEMS **if yes, items permitted are:**	□ **YES**	☑ **NO**

Candidates must complete this section if required to write answers within this paper

STUDENT ID: __ __ __ __ __ __ __ __ DESK NUMBER: __ __ __ __ __

INSTRUCTIONS

1. **There are two parts – Part A has 30 multiple-choice questions (30 marks) and Part B has 7 descriptive questions (70 marks).**
2. **For Part A, please circle the correct choice**.
3. **For Part B, please write the answer in the space provided below the question.**
4. **Total marks - 100. This exam contributes 60% to your result for this unit.**

PART A

There are 30 Multiple Choice questions in this part.
The total marks for this part is 30.
Please choose the one alternative that best completes the statement or answers the question, and CIRCLE the correct answer in the paper.

1. How many different password combinations are possible when a 5-digit password is created based on numbers 0 to 9 and letters a to z (lower case alphabets only)?

   a. 36^5
   b. 5^{36}
   c. 5^5
   d. 36^{36}

2. A _________ approach involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained.

   a. brute-force
   b. triple DES
   c. block cipher
   d. computational

3. With the ________ mode if there is an error in a block of the transmitted ciphertext only the corresponding plaintext block is affected.

   a. ECB
   b. CTS
   c. CBC
   d. TSR

4. The purpose of the _________ algorithm is to enable two users to exchange a secret key securely that then can be used for subsequent encryption of messages and depends on the difficulty of computing discrete logarithms for its effectiveness.

   a. DSS
   b. Diffie-Hellman
   c. Rivest-Adleman
   d. RSA

5. 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. SHA
   b. CTR
   c. RSA

d. MD5

6. The __________ key size is used with the Data Encryption Standard algorithm.
   a. 128 bit
   b. 56 bit
   c. 32 bit
   d. 168 bit

7. Asymmetric encryption can be used for ___________ .
   a. confidentiality
   b. authentication
   c. neither confidentiality nor authentication
   d. both confidentiality and authentication

8. Which of the following would NOT be considered as a element of access control?
   a. Subject
   b. Object
   c. Process
   d. Access right

9. Which of the following would be considered as a subject?
   a. File
   b. Data
   c. Printer
   d. Process

10. Which of the following statements is NOT correct in relation to Discretionary Access Control (DAC)?
    a. Access to information is controlled by the owner of the object.
    b. It can also provide for centralized or distributed security management.
    c. Information is classified based on attributes such as sensitivity, secrecy and confidentiality.
    d. Bell-Lapadula (BLP) Model has a rule using DAC.

11. Which of the following statements is NOT correct referring to Multilevel Security model?
    a. Categorises information by sensitivity and user access is based on their responsibility level.
    b. Information is categorised into classes based on usage patterns.
    c. Bell-Lapadula (BLP) model is a Multilevel Security model.
    d. BLP can combine DAC with MAC.

12. In UNIX, a file with protection mode 644 (octal) contained in a directory with protection mode 730. Which of the following statements is not correct?
    a. The owner of the file can read this file.
    b. The group users can read this file.
    c. The others can execute this file.
    d. This file may be compromised, because a group user can delete this file and write a new file with the same name.

13. What's the Greatest Common Divisor (GCD) of 748 and 224?
    a. 2
    b. 4
    c. 112
    d. 56

14. What is the Euler Totient value of 91.
    a. 72
    b. 45
    c. 90
    d. 17

15. Which of the following number is multiplicative inverse to 3 in modulo 19?
    a. 13
    b. 16
    c. 30
    d. 5

16. Which of the following groups of numbers are relative prime?
    a. 3 and 6
    b. 15 and 16
    c. 8 and 32
    d. 21 and 35

17. Which of the following statements is NOT correct referring to classical ciphers?
    a. Most of the classical ciphers are designed based on substitution and transposition.
    b. The Caesar cipher is a substitution cipher, named after Julius Caesar.
    c. Rail Fence Cipher uses transposition of alphabets to achieve some confusion effects.
    d. Classical ciphers are easy to be cracked by statistical analysis of alphabets.

18. Which of the following statements is NOT correct referring to modern symmetric ciphers?
    a. Many of block symmetric ciphers use Feistel cipher structure.
    b. Data Encryption Standard (DES) and Advance Encryption Standard (AES) are both block ciphers, but AES is considered to be much more secure than DES.
    c. Symmetric ciphers are more often used for data encryption/decryption for storage and transmission than asymmetric ciphers, because symmetric ciphers have the advantages of less time and resource consumption but achieve the same security levels with less key space compared to asymmetric ciphers.
    d. Both Data Encryption Standard (DES) and Advance Encryption Standard (AES) use Feistel cipher structure.

19. Which of the following statements is NOT true referring to 3-DES cipher?
    a. In the basic method used by 3DES to encrypt plaintext, the data is encrypted, decrypted, and encrypted using three different keys instead of triple encryption for backward compatibility.
    b. If 3 keys used in 3DES are different, the key size is 168 bits. But it achieves only 112-bit security due to meet-in-the-middle attack.
    c. If there are only 2 different key are used in 3DES (the 1st and 3rd key are the same), the key size is 168 bits. But it achieves only 80-bit security due to meet-in-the-middle attack.
    d. AES with a key length of 256 bits has better security than 3DES.

20. Which of the following cryptanalytic attacks on encryption system is less severe than others?
    a. Ciphertext only attack
    b. Known plaintext attack
    c. Chosen ciphertext attack
    d. Chosen plaintext attack

21. Which of the following properties is not considered a property of a stream cipher?
    a. Simpler and faster.
    b. Never reuse stream key.
    c. Long period with no repetitions
    d. Could be more secure than a block cipher with same size key.

22. Which of the following is a countermeasure to protect a database.
    a. Firewall
    b. Authentication
    c. Access control system
    d. All of above

23. Which of the following statements is false regarding public key cryptography?
    a. A message that is encrypted by the private key does not assure confidentiality
    b. Public key encryption algorithms are usually faster than symmetric key encryption algorithms
    c. It is infeasible for an attacker to find the value of private key from the public key
    d. Public key cryptography can be used for authentication

24. Which of the following statements is true regarding public key cryptography?
    a. RSA algorithm is secure because factorizing large composite numbers is computationally infeasible
    b. Diffie-Hellman algorithm is secure against man-in-the-middle attack
    c. The RSA encryption algorithm provides the same level of security with the same key size as symmetric encryption algorithms
    d. Diffie-Hellman algorithm does not require any negotiation to choose public parameters

25. Which of the following features is not a requirement of digital signatures?
    a. Must be a bit pattern based on the message being signed
    b. Must use some unique information of the receiver to protect against forgery
    c. Must be relatively easy to recognize and verify
    d. Must be practical to retain a copy

26. Which of the following attacks cannot be mitigated by Message Authentication Code?
    a. Masquerade
    b. Replay
    c. Interception
    d. Modification

27. Which of the following statements is false regarding Message Authentication Codes?
    a. Can be used to assure the integrity of the message
    b. Can provide a kind of authenticity of the message
    c. Can be created by combining a hash function with a shared secret
    d. Can be used to resolve a dispute about the origin of a message

28. Which protocol is responsible for key establishment in HTTPS?

a. VPN
b. TLS Handshake
c. TLS Record
d. TCP/IP

29. With respect to public key encryption, which of the following is true of a server's public key when transferring data across the Internet to a client computer?
a. Client computers when transferring encrypted data from that particular server use it.
b. The server uses it to decrypt information sent by a client.
c. All clients and servers use the same public key when transferring encrypted data on the Internet.
d. It is not a very secure method of encryption, because every computer is aware of a recipient's public key value and can decrypt the data.

30. Why is the destination port important in a firewall rule?
a. It identifies a particular server that should be blocked/allowed.
b. It identifies an application program outside the internal network that should be blocked/allowed.
c. It enables encryption of traffic through the firewall.
d. It identifies a service running on a server behind the firewall that should be blocked/allowed.

PART B

The total marks for this part is 70.
Answer all the questions in this booklet itself.
Please write your answer after the question in the space provided.

1. (4+(4+2+2) = 12 marks)

   a. Identify two important properties an encrypted message should have? Define each one of them and describe one method to implement each one. (4 marks)

   The two important properties an encrypted message should have are confusion & diffusion.

   In diffusion, the statistical structure of the plaintext is dissipated into long range statistics of the ciphertext. This is achieved by having each plaintext digit affect the value of many ciphertext digits, which is equivalent to saying that each ciphertext digit is affected by many plaintext digits. This is achieved by the use of complex permutation algorithms.

   Confusion seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible, again to thwart attempts to discover the key. Thus, even if the attacker can get some handle on the statistics of the ciphertext, the way in which the key was used to produce that ciphertext is so complex as to make it difficult to deduce the key. This is achieved by the use of a complex substitution algorithm.

   b. Tracy, a web developer, has recently developed a web site for a large accounting firm which requests a username and password from clients for entering into the web site and accessing their information. She has used a challenge-response protocol and only the message digests of the password are stored in the back-end database. All of the clients' confidential information is stored in encrypted format; the associated key is stored in the same table as the passwords, and the back-end database is only accessible via web server. Tracy forgot to check the entered values in the username and password fields which will permit an attacker to perform a SQL injection attack (which only requires some knowledge in the database) against the back-end database and effectively recover the content of any table in the database in the returned web page by the web server.

      i. Identify an asset, the threat to the asset, the likelihood, the consequence, and the level of the risk. **Justify your answer.** **(4 marks)**

Asset	Threat	Likelihood	Consequence	Risk Level
Client's confidential data	Attacker/hacker/Web application vulnerability	Likely/almost certain	Catastrophic/Doomsday	Extreme
Justification:				

1.The likelihood is likely/almost certain, as the firm is a large accounting firm that makes it a big target for monetary gain. Performing a SQL injection attack also does not require an extensive knowledge in specific area, which increases the chance of the attack.

2.The consequence is catastrophic/doomsday as the table that contains the passwords and the associated keys can be recovered and the keys then can be used to decrypt the clients' confidential information. This could lead to massive lawsuits, and loss of clients that could threaten the future of the firm.

3.The risk level is extreme based on the likelihood and the consequence.

ii. Luckily Gary, the firm's Chief Information Officer, hires a penetration test team to try to hack into the firm's IT infrastructure; they discover Tracy's mistake during their tests. Which risk treatment approach has Gary chosen?

(2 marks)

Reduce the likelihood by finding the vulnerabilities in the IT infrastructure. This will also affect the risk level.

iii. Gary also asks Tracy not to store the keys in the back-end database and to use a public key mechanism for clients to provide the required symmetric key. Which risk treatment approach does Gary use?

(2 marks)

Reduce the consequence since even if the back-end database is compromised the confidential information is still in encrypted format.

2 **(1+2+2+3 = 8 marks)**

Morris, a freelance black hat hacker, has stolen Cornelia's hard drive to recover password-protected files of her patients' information.

i. In order to recover the password for the files which type of attack does Morris need to perform?

(1 mark)

Offline dictionary attack/ offline brute force attack.

a. If Cornelia has chosen her password from a-z, A-Z, 0-9, and the set {!,@,#,$,%,^,&,*,~,?} (Comma and curly brackets are not part of the character set) and the password length is 8 characters then what is the total number of passwords required for a brute force attack?

(2 marks)

26+26+10+10=72

Total number of passwords=72^8

b. If Morris knows that the password starts with an alphabet character then what is the total number of passwords? **(2 marks)**

$52*72^7$ (for the first position 52 choices and the other seven position each 72 choices)

c. If Morris can check 9 passwords in one microsecond how long will it take on average to recover the password (in each b and c circumstances)? **(3 marks)**

b) $72^8/9*2=9*8*72^7/9*2=4*72^7$ micro seconds

c) $52*72^7/9*2=52*9*8*72^6/9*2=208*72^6$ micro seconds

5. (4+2+2+2 = 10 marks)

a. Briefly describe the difference between Discretionary Access Control (DAC) and Mandatory Access Control (MAC). How does Role Based Access Control (RBAC) relate to DAC and MAC? **(1.5 + 1.5 + 1 = 4 marks)**

1. Discretionary access control (DAC) controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do. This policy is termed *discretionary* because an entity might have access rights that permit the entity, by its own volition, to enable another entity to access some resource.

2.**Mandatory access control (MAC)** controls access based on comparing security labels (which indicate how sensitive or critical system resources are) with security clearances (which indicate system entities are eligible to access certain resources). This policy is termed *mandatory* because an entity that has clearance to access a resource may not, just by its own volition, enable another entity to access that resource.

3.**Role-based access control (RBAC)** controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles. RBAC may have a discretionary or mandatory mechanism.

b. Calculate the value of 24^{200} mod 7 (show few steps). **(2 marks)**

24^{200} mod 7 =

= $(3 \times 8)^{200}$ mod 7

= $[(3^2 \bmod 7)^{100} \times (8 \bmod 7)^{200}]$ mod 7

= $[(9 \bmod 7)^{100} \times (8 \bmod 7)^{200}]$ mod 7

=2^{100} mod 7=2 x 2^{99} mod 7

= 2 x $[(8 \bmod 7)^{33} \bmod 7]$ mod 7 = 2

c. What is the greatest common divisor of 1000 and 29? **(2 marks)**

29 is a prime number and only has 1 and 29 as the factors.

1000 = $10^3 = 2^3$ X 5^3 = 1 X 2^3 X 5^3

Only common factors = 1;

GCD(1000, 29) = 1;

d. What is the Euler's totient ϕ of 77? **(2 marks)**

$\phi(77) = \phi(7X11) = 6X10 = 60$

4. (4+[2+2+2] = 10 marks)

   a. Briefly explain Diffie-Hellman key exchange.

   Two parties each create a public-key(Y), private-key (X) pair and communicate the public key to the other party. The keys are designed in such a way that both sides can calculate the same unique secret key, K based on each side's private key and the other side's public key and the shared global parameters, prime number q and its primitive root, α. You may use the following equations to illustrate the point.

   - $Y_A = \alpha^{X_A} \bmod q$ (A's public key, obtained from A's private key and global values)
   - $Y_B = \alpha^{X_B} \bmod q$ (B's public key)
   - $K = Y_B^{X_A} \bmod q$ (which A computes) $= Y_A^{X_B} \bmod q$ (which B computes)

   b. Users A and B use the Diffie-Hellman key exchange technique with a common prime q=7, primitive root α= 2;

   - X_A= 4 (A's private key), what is $Y_A = \alpha^{X_A} \bmod q$ (A's public key)?

     $Y_A = \alpha^{X_A} \bmod q = 2^4 \bmod 7 = 2X(8 \bmod 7) \bmod 7 = 2$

   - If $Y_B = \alpha^{X_B} \bmod q$ (B's public key) = 4, what is the shared secret session key?

     $K = Y_B^{X_A} \bmod q$

     $K = 4^4 \bmod 7 = 4$

   - What is XB, B's private key?

     $Y_B = \alpha^{XB} \bmod 7 = 4 = 2^2 \bmod 7; X_B = 2$

5. (10 marks)
Figure 1 illustrates six methods in which a hash code can be used to provide message authentication. Explain each of the six methods.

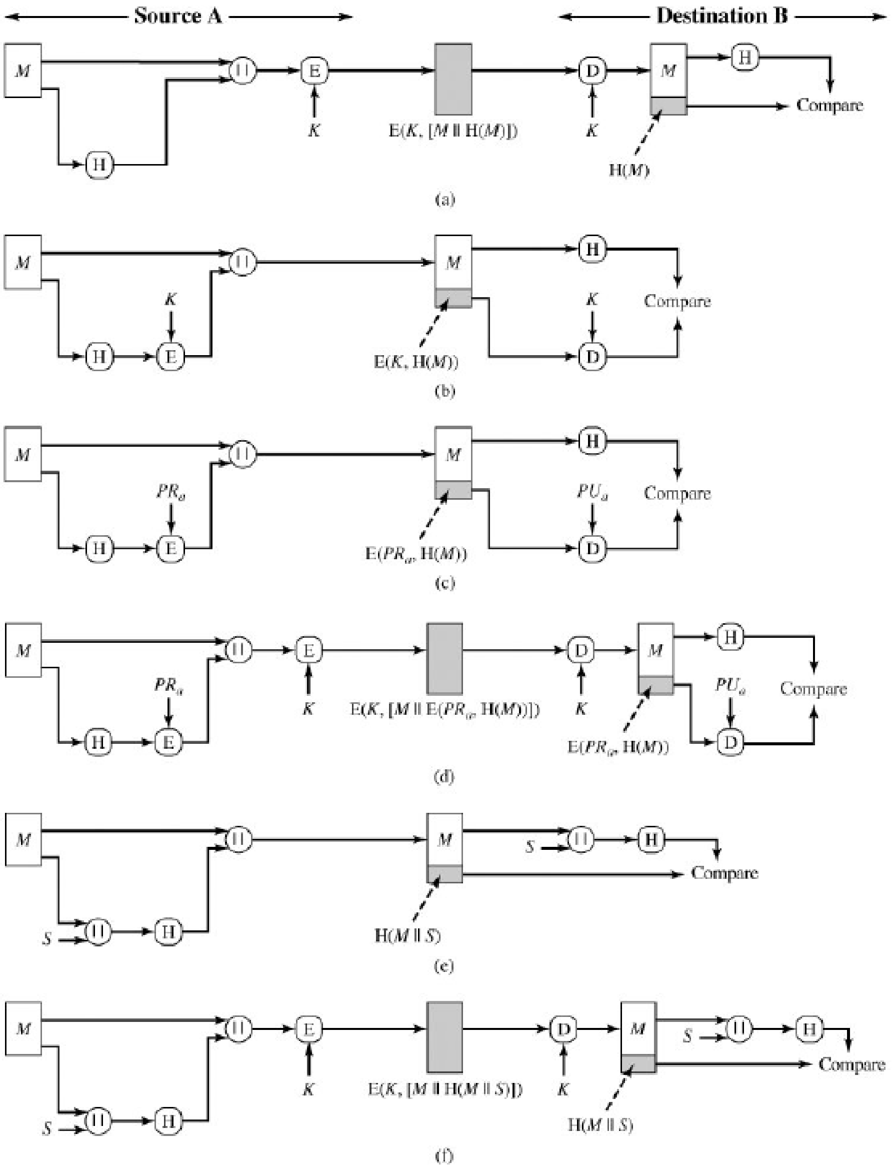

Figure 1 Basic Uses of Hash Function

Figure 1 illustrates a variety of ways in which a hash code can be used to provide message authentication, as follows:

a. The message plus concatenated hash code is encrypted using symmetric encryption.

b. Only the hash code is encrypted, using symmetric encryption.

c. Only the hash code is encrypted, using public-key encryption and using the sender's private key.

d. If confidentiality as well as a digital signature is desired, then the message plus the public-key-encrypted hash code can be encrypted using a symmetric secret key.

e. This technique uses a hash function but no encryption for message authentication. The technique assumes that the two communicating parties share a common secret value S. A computes the hash value over the concatenation of M and S and appends the resulting hash value to M. Because B possesses S, it can recompute the hash value to verify.

f. Confidentiality can be added to the approach of (e) by encrypting the entire message plus the hash code

6. (3+3+4=10 marks)

a. What are the three broad categories of applications of public-key cryptosystems?

The three broad categories of applications of public-key cryptosystems are:
1. Encryption/decryption: The sender encrypts a message with the recipient's public key.
2. Digital signature: The sender "signs" a message with its private key. Signing is achieved by a cryptographic algorithm applied to the message or to a small block of data that is a function of the message.
3. Key exchange: Two sides cooperate to exchange a session key. Several different approaches are possible, involving the private key(s) of one or both parties.

b. What security requirements must RSA public-key cryptosystem fulfil to be a secure algorithm?

i. The value of the modulus n should be very large that brute force attack would take a very long time for the adversary to guess the message m, which is < n, and thus compute the private key, d

ii. The security of RSA is based on the factorization problem and hence it should be computationally infeasible to factorise or split a large number to its prime factors.

c. Discuss the features of a good one-way hash function with respect to its application to digital signatures.

a. Can be applied to any size of data: files and messages with arbitrary sizes can be signed
b. Produces a fixed-length output: overhead of signature for transmission or storage is low and the verification process is easier
c. Fast and efficient algorithm: signature generation and verification should be fast and efficient (low overhead in terms of processing time)
d. One-way feature: infeasible to get back message from the hash value and thereby infeasible to get back the message from the digital signature
e. Hard to find collisions: it should be infeasible to find two inputs that will be hashed into the same value, thereby preventing forging of digital signatures for two different messages.

7. (5+5=10 marks)

   a. Assume an employee of a company is travelling and wants to use her laptop to access a server placed in the internal network of a company. How can a VPN be used to provide secure access to the server in the company network without making the server directly accessible from outside the network? Which protocol can be used to implement this concept. Name the entities involved in establishing the secure connection between the laptop and the internal network and protecting the internal network from other access. Discuss if this mechanism is sufficient to protect data on the server from malicious access. Mention at least two security mechanisms that might improve security in addition to the VPN.

A Virtual Private Network established an authenticated and encrypted tunnel between the laptop and the VPN gateway. The laptop is now virtually part of the internal network and can get access as if it was physically connected to the company network.

Possible protocols are TLS and IPSec.

Entities involved are the VPN client on the laptop, the VPN gateway and a firewall blocking other traffic.

The VPN only protects traffic between the laptop and the VPN gateway. Packets within the internal network are not protected. Furthermore, the VPN will not provide any access control to the server. Thus, it is necessary to provide user authentication and access control on the server side. Furthermore, a transport layer security protocol (TLS) or application layer security protocol would protect traffic from attacks within the company network.

   b. A user accesses a discussion forum on a web-server. She needs to login to the server and a session is established. Explain how a badly implemented forum might be used by an attacker to run a Cross-site scripting attack to steal the active session from the user. Show the different steps of the attack. What is the name for this particular XSS attack?

The attacker will register with the server and is then able to post to the forum himself. He can include active content (e.g. JavaScript) in his post. Then, if a user accesses this post to the forum, the active content might be executed as if it was coming from the server. Thus, it could get access to the session information and forward this information to the attacker, enabling him to steal the session.

The steps are:
1. Attacker posts message containing attack code to the forum.
2. User logs in.
3. User reads forum message posted by the attacker.
4. Server responds with attackers JavaScript.
5. JavaScript is executed in user’s browser.
6. User’s browser sends session information to the attacker
7. Attacker hijacks user’s currently active session.

This attack is called a *stored XSS attack,* because the attack code is stored on the server side.