Office Use Only

MONASH University

SAMPLE EXAM - Semester One 2022

Faculty of Information Technology

EXAM CODES:	**FIT2093**
TITLE OF PAPER:	**Introduction to Cyber Security**
EXAM DURATION:	2 hours writing time
READING TIME:	10 minutes

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

Clayton Malaysia

During an exam, you must not have in your possession, a book, notes, paper, electronic device/s, calculator, pencil case, mobile phone, smart watch/device 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, or attempting to cheat or cheating in an exam is a discipline offence under Part 7 of the Monash University (Council) Regulations.

No exam paper or other exam materials are to be removed from the room.

AUTHORISED MATERIALS

OPEN BOOK	□ **YES**	**NO**
CALCULATORS	□ **YES**	**NO**
SPECIFICALLY PERMITTED ITEMS if yes, items permitted are: 5 blank double sided sheets for working.	**YES**	**NO**

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

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

INSTRUCTIONS

- There are two parts to this exam: Part A (30 marks, 15 multiple choice questions) and Part B (70 marks, 4 multiple part short answer questions).
- This exam is worth 60% of your final unit mark.
- Answer all questions in the spaces provided.
- Marks for each question in Part B are indicated at the end of each sub-question.
- The duration of this exam is 130 minutes (2 hours and 10 minutes), which includes a reading time of 10 minutes.

PART A

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. An indirect leakage of information to an attacker by deduction from given information is called ________.
a. masquerade
b. interception
c. repudiation
d. Inference

4. An attack that involve writing or modification is called ________.
a. passive
b. active
c. repudiation
d. disclosure

5. Ensuring that users have access rights that are sufficient for their needs but not more than needed is an application of the principle of ________.
a. Least privilege
a. Input validation
b. Never trusting user input
c. Open design

6. An advantage of biometric authentication compared to passwords is ___________.
a. it avoids the need to memorise a secret
a. it has a lower false positive rate

b. it has a lower false rejection rate
c. none of the above

7. Which of the following is **false** about textbook RSA public key encryption?
a. Decrypting with a private key will undo encryption with the public key
a. Encrypting with a public key will undo decryption with the private key
b. Encrypting with a public key will undo encryption with the private key
c. Encryption with the private key will undo encryption with the private key

8. An advantage of encrypt-then-MAC compared to encryption only could be _______.
a. that encrypt-then-MAC should be faster than encryption only
a. none because encrypt should be enough to protect both confidentiality and integrity
b. that encrypt-then-MAC guarantees both integrity and confidentiality
c. that encrypt-then-MAC is slower to compute than encryption only

9. For long messages, CBC-MAC (CMAC) produces authentication tags that are much shorter than the length of ciphertexts produced by CBC mode of operation for encryption because ___________.
a. CMAC only outputs the last block in the cipher block chain
a. CMAC outputs all the blocks in the cipher block chain
b. CMAC outputs the first block in the cipher block chain
c. CMAC outputs the first 10 blocks in the cipher block chain

10. In the TLS protocol, the perfect forward secrecy property ensures that if an attacker steals a web server's long term private key in time T, then ______.
a. the attacker cannot decrypt all ciphertexts sent to the server at past times T' prior to T (even if the attacker eavesdropped and recorded those ciphertexts)
a. the attacker cannot decrypt all ciphertexts sent to the server at future times T' subsequent to T
b. the attacker cannot decrypt any ciphertexts at any time
c. None of the above

11. In the TLS protocol, the purpose of the handshake sub-protocol is to
a. Establish a shared symmetric key
a. Establish a shared public key
b. Perform symmetric key encryption
c. None of the above'

12. Malicious javascript downloaded to a client's browser from an attacker's website is usually prevented from accessing any client's browser page not on the attacker's domain because of _____.
a. the browser's Same Origin Policy
a. the attacker's good intentions
b. the TLS session encryption
c. None of the above

13. In a reflected XSS attack, the attacker manages to inject malicious javascript into the client's session with a vulnerable server because _____.
a. the server fails to filter out from its response javascript sent in browser's request
a. the server fails to use encryption in its TLS session with the browser
b. the server has an SQL injection vulnerability
c. the server fails use a random salt in its password authentication

14. Which of the following is **false?**
Potential security risks for cloud-hosted databases __________.
a. include exposure of database contents in case of cloud server exposure
a. could be reduced by client-side encryption of the database prior to uploading to the cloud server
b. include unauthorised database access by a rogue cloud server provider employee
c. can be eliminated by using a TLS encrypted session to upload the database to the server

15. An important security property of blockchain systems is that _______.
a. it is infeasible for a dishonest insider to delete past data stored in blockchain
a. it is infeasible for a dishonest insider to insert new data into the blockchain
b. it is infeasible for dishonest insider to read past data stored in blockchain
c. none of the above

END OF PART A

PART B

The total marks for this part is 70.

Q16. Software Security / Database Security (18 marks)

a. **(9 marks)** A software accounting application was designed to record and store receipts of financial transactions for multiple app users. The app allows a user to upload for storage and display by the app, a .jpg image file of a transaction receipt received by the user. The app uses an API function call to an operating system function called `OpenFile` (see reference material below) to open the user's image file for display.

What kind of vulnerability do you think should this app be tested for? Explain briefly how such a vulnerability might be exploited by an attacker and how to test the app for such vulnerability.

Reference material for part (a):

The `OpenFile` operating system function call takes a file name as an input argument and reads the file header to identify the type of file, then automatically calls the appropriate app to open the file.

b. **(9 marks)** Consider the contents of a prisoner database in the reference material. Explain what kind of protection operation could be done to the data before publishing the view containing attributes Date of Birth and Crime to ensure 2-anonymity, and explain why given the generalised view. Would this operation also respect 2-diversity for the Residence attribute?

Reference material for part (b):

Sex	**Date of Birth**	**Crime**	**Residence**
M	22 Nov 1963	Theft	Melbourne
M	19 Apr 1969	Murder	Sydney
F	14 May 1958	Theft	Sydney
M	5 Feb 1990	Burglary	Brisbane
F	7 July 1991	Theft	Perth
F	15 Mar 1985	Murder	Melbourne
M	3 Dec 1981	Burglary	Sydney
M	28 Jan 1982	Theft	Sydney
F	19 Oct 1978	Manslaughter	Melbourne

M	30 Jun 1966	Manslaughter	Sydney

Answers:

a. A potential vulnerability that should be checked is lack of input validation on the type of file the user uploads to the app. This is especially important because the OpenFile system function called by the app will automatically open the file depending on its file header type. This means that without the app preventing it with appropriate validation checks, if an attacking user uploads, instead of a .jpg image file, an executable file containing malicious code (e.g. .exe on windows), or for instance a spreadsheet file containing a malicious script, it will get automatically executed by the OpenFile function and potentially cause an unauthorized system operation.
To test for this vulnerability, one way is to try to upload such an executable code file instead of the image file and see if it gets executed and produces the expected output. Another way (with access to the app code) is to analyse the code and see what if any validation checks it makes on the input file.

(b) To achieve 2-anonymity using the generalization protection operation on Date of Birth (DOB) and Crime, we need to ensure at least two identical rows exist in the view for every possible generalised value for (DOB,Crime) pairs. One way to achieve this without losing all information is: for DOB, only reveal the category among (1940-1969, 1970-1989, 1990-2009), and for Crime only reveal the category among (Theft/Burglary, Murder/Manslaughter). It gives the following generalised view, showing that 2-anonymity is satisfied.

Sex	Date of Birth	Crime	Residence
	1950-1969	Theft/Burglary	
	1950-1969	Murder/Manslaughter	
	1950-1969	Theft/Burglary	
	1990-2009	Theft/Burglary	
	1990-2009	Theft/Burglary	
	1970-1989	Murder/Manslaughter	
	1970-1989	Theft/Burglary	
	1970-1989	Theft/Burglary	
	1970-1989	Murder/Manslaughter	
	1950-1969	Murder/Manslaughter	

But 2-diversity for residence is not satisfied by this protection method, since both criminals born in 1970-1989 committing Murder/Manslaughter reside in Melbourne and both criminals born in 1970-1989 committing Theft/Burglary reside in Sydney.

Q17. Public key Encryption (18 marks)

(a) With regards to the Diffie-Hellman key exchange:
Explain how Alice and Bob generate their secret and public keys and how they compute the shared secret key in this protocol.
Given public parameters p=23, Alice's public key is A = 5 and Bob's secret key is b=18, use the "square-and-multiply" method to compute the shared secret key that Bob would compute. Show your working. **(12 marks)**

(b) An attacker Marvin eavesdropped on Alice and Bob's Diffie-Hellman key exchange protocol and found that Alice's public key in a Diffie-Hellman key exchange protocol was A = 1 and Bob's public key was B = 3593860232455. The prime p is a 4096-bit prime and g = 5. Explain what is the vulnerability in this scenario and (giving the steps of the attack) how an attacker Marvin can exploit it to efficiently recover the shared secret K Alice and Bob. What is the value of K? (6 marks).

Answer:

(a) The public key of Alice is A = g^a mod p, where a is Alice's secret key, an integer < p. Similarly, public key of Bob is B = g^b mod p, where b is Bob's secret key, an integer < p. Here, p is a prime and g is an integer < p (g and p are public parameters). The shared key is K = g^(a*b) mod p, which Alice can compute as K = B^a mod p and Bob can compute as K = A^b mod p.

For the example parameters, the shared secret key K that Bob computes is K = A^b mod p = 5^18 mod 23. To compute K using square and multiply algorithm ,

- Write 18=(10010)_2 in binary
- Start with 5.
- Square: 5^2 mod 23 = 25 mod 23 = 2. Since bit 2 = 0, don't multiply.
- Square: 2^2 mod 23 = 4. Since bit 3 = 0, don't multiply.
- Square: 4^2 mod 23 = 16. Since bit 4 = 1, multiply: 16 * 5 mod 23 = 80 mod 23 = 11.
- Square: 11^2 mod 23 = 121 mod 23 = 6, since bit 5 = 0, don't multiply.
- Result: K = 5^18 mod 23 = 6.

(b) The large numbers for B and p are irrelevant (the 4096-bit p means that Discrete log problem is hard to compute for a random secret key). However, the vulnerability is that Alice chose a non-random bad value for her public key A = 1 (secret key a = 0). With this bad value, the shared secret K is *always* K = 1 regardless of Bob's key and the value of g and p, because K = A^b mod p = 1^b mod p = 1. So Marvin can just set K = 1 and therefore knows the shared secret secret. To avoid this problem, Alice must choose a random secret key a in the range (1,…,p-1) for a sufficiently large p.

Q.18 Web Security/Security Protocols (18 marks)

a. **(9 marks)** Charlie owns an online shop selling house goods. Daniela is a customer of Charlie's shop and exploits an SQL injection vulnerability in Charlie's web server to discover the credit card details of other customers of Charlie's shop. She also exploits this vulnerability to modify her own account balance in Charlie's shop from $10 to $1000 without paying. Categorise the type of attack and identify which two security properties are violated in the performed attack.

b. **(9 marks)** Daniela is a customer of an online shop with URL `https://myhousegifts.com` selling house goods, and she pays for her purchased goods using her credit card. Marvin, an attacker, found out that Daniela's web browser implements the TLS protocol with the following vulnerability: in the TLS handshake phase, the web browser always accepts the web server's certificate (i.e. it doesn't give a warning to Daniela if the server's certificate signature is invalid). Explain how Marvin can exploit this vulnerability to steal Daniela's credit card number. Your answer should describe the steps that Marvin should perform in his attack, and any assumptions you need to make.

Answers:

a. Attack 1 (SQLi): type: active; violated security property: confidentiality. Attack 2 (Modify account balance): type: active; violated security property: integrity.

a. Man in the middle Attack part 1:

- Assume Marvin can intercept Daniela's web browser requests to myhousegifts.com.
- In handshake phase, Marvin responds with a fake certificate for myhousegifts.com containing Marvin's self generated public key for which Marvin knows the corresponding private key.
- Due to the vulnerability in Daniela's browser, Marvin's fake cert will not raise an error.
- Daniela's browser will encrypt a TLS record phase session key with Marvin's pub key, which Marvin can decrypt.

Attack part 2:

- We assume Marvin can imitate the real myhousegifts.com web server pages (e.g. by performing his own session with the real myhousegifts.com server and forwarding Daniela's browsing queries to the web page and the responses from the server) to allow Daniela to purchase a product.
- When completing her purchase Daniela will then enter her credit card number to make a purchase, and Marvin will intercept and decrypt it with his session key.

Q19 User Authentication/Message Integrity> (16 marks)

Assume passwords are selected from four-character combinations of 26 alphabet characters. Assume that an adversary is able to attempt passwords at a rate of one per second.

(a) First, assuming that no feedback is given to the adversary until each attempt has been completed, what is the expected time to discover the correct password?
Second, assume that feedback to the adversary is given flagging an error as each incorrect character is entered, what is the expected time to discover the correct password? **(8 marks)**

(b) A software developer Bob developed the following Message Authentication Code (MAC) BobMAC based on the AES block cipher E. Given a message M with 128-bit blocks M_1,...,M_N and an AES key K, the MAC tag T on M consists of T=(IV, C), where IV is a 128-bit string chosen independently at random for each message and C is computed as follows:

T= E(K,IV) XOR M_1 XOR M_2 … XOR M_N .

Explain whether you think BobMAC is a secure message authentication code under a known message attack. If so, explain why it is difficult to forge. If not, explain how an attacker could efficiently break its unforgeability under a known message attack. **(7 marks)**

(a)
Solution:
First question: Average number of attempts until success = 0.5 * (number of possible 4 letter passwords), N = 0.5 * (26)^4 → Average success time @ 1 attempt/sec = N sec = ≈ 126 hours. (on average)
Second question: Expect 13 tries (on average) for each digit. → T = 13 × 4 = 52 seconds.

b. No, it’s not secure. (Example attack: Given a tag T = (IV,C), where C= E(K,M) XOR M_1 on a 1-block message M_1, and another 1-block message M’_1, an attacker can forge a valid tag T’ = (IV’,C’) for M’_1 as follows: set IV’ = IV and set C’ = C XOR M_1 XOR M’_1.

END OF EXAM