UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2022/2023

COURSE NAME	:	MULTIMEDIA SECURITY TECHNOLOGY
COURSE CODE	:	BIM 33403
PROGRAMME CODE	:	BIM
EXAMINATION DATE	:	JULY / AUGUST 2023
DURATION	:	3 HOURS
INSTRUCTION	:	1. ANSWER ALL QUESTIONS. 2. THIS FINAL EXAMINATION IS CONDUCTED VIA **CLOSED BOOK.** 3. STUDENTS ARE **PROHIBITED** TO CONSULT THEIR OWN MATERIAL OR ANY EXTERNAL RESOURCES DURING THE EXAMINATION CONDUCTED VIA CLOSED BOOK.

THIS QUESTION PAPER CONSISTS OF **TEN (10)** PAGES

TERBUKA

Q1 Which of the following is an example of a vulnerability in a multimedia system?

A. A strong password policy.
B. The use of encryption to protect data.
C. Uncompressed content delivered thru unsecured network.
D. The use of two-factor authentication.

(1 mark)

Q2 Which of the following authentication factors are the same?

i. What you are
ii. Inherence
iii. What you have
iv. Biometric

A. i, ii and iii
B. i, ii and iv
C. ii, iii and iv
D. i, iii and iv

(1 mark)

Q3 How would you apply biometric authentication to secure a multimedia file on a recent smart mobile device?

A. Use a fingerprint scanner to authenticate the user before allowing access to the file.
B. Use a password or passphrase to restrict access to the file.
C. Use a public key encryption algorithm to encrypt the file.
D. Use steganography to hide the file on a different file system.

(1 mark)

Q4 Which of the following is used to apply encryption to secure a multimedia transmission over the internet?

A. Use a secure socket layer (SSL) or transport layer security (TLS) encryption protocol.
B. Use steganography to hide the data in the transmission.
C. Use a hash function to compress the data.
D. Use a digital signature to authenticate the data.

(1 mark)

TERBUKA

Q5 What is the difference between symmetric and asymmetric encryption?

1. Symmetric encryption requires more keys when complexity increases than asymmetric encryption.
2. Symmetric encryption is slower than asymmetric encryption.
3. Asymmetric encryption is used for data at rest while symmetric encryption is used for data in motion.
4. Asymmetric encryption is more vulnerable to attacks than symmetric encryption.

(1 mark)

Q6 Which of the following best describes the concept of steganography?

A. Encrypting a message with a secret key.
B. Hiding a message within another message or file.
C. Breaking a message into smaller pieces and sending them separately.
D. Preventing unauthorized access to a system with biometric authentication.

(1 mark)

Q7 What is the difference between a virus and a Trojan horse?

A. A virus is a type of malware while a Trojan horse is a type of hardware.
B. A virus spreads by infecting other files while a Trojan horse disguises itself as a legitimate file.
C. A virus is always harmful while a Trojan horse can be harmless or harmful.
D. A virus is only spread through email while a Trojan horse can be spread through multiple channels.

(1 mark)

Q8 Password-based authentication main drawback is that passwords can easily be cracked or guessed. Which of the following is a guideline to defeat potential Brute Force attacks to crack or guess the passwords?

i. Limit login attempts
ii. Use CAPTCHA
iii. Strong password policies
iv. Multi-factor authentication

A. i, ii and iii
B. i, iii and iv
C. ii, iii and iv
D. All of the above.

(1 mark)

TERBUKA

Q9 How would you apply digital watermarking to an image to verify its authenticity?

A. Embed a unique identifier into the image.
B. Encrypt the image with a secret key.
C. Compress the image using a lossy algorithm.
D. Add a signature to the image.

(1 mark)

Q10 Which of the following is **NOT** a potential vulnerability in a digital watermarking system?

i. The watermark can be easily detected and removed by an attacker.
ii. The watermark can be embedded in the multimedia data without affecting its quality.
iii. The watermarking algorithm used is too complex, leading to slow processing times.
iv. The watermarking system is incompatible with certain types of multimedia data.

A. i, ii and iii
B. ii, iii and iv
C. i, ii and iv
D. ii and iv

(1 mark)

Q11 Which of the following statements about CIA model in the context of a Maybank financial system is **FALSE**?

A. The model can be used to identify potential vulnerabilities in the financial institution's security system.
B. The model can be used to determine the most important component for the financial institution's security needs.
C. Availability is not a concern for financial systems as they are typically closed systems.
D. Confidentiality is of utmost importance for financial systems to protect sensitive customer information.

(2 marks)

TERBUKA

Q12 Which of the following is an example of a denial of service (DoS) attack on an online content-subscription system such as HBO Go and Disney Hotstar?

A. An attacker steals login credentials and gains access to a system.
B. An attacker intercepts and modifies data in transit.
C. An attacker floods a system with traffic to disrupt its normal operation.
D. An attacker uses a key logger to record keystrokes on a user's computer.

(2 marks)

Q13 How would you apply the strategy to protect any UTHM campus network from unauthorized access to copyrighted video stored in the data centre?

A. Use a firewall to filter incoming and outgoing network traffic.
B. Use steganography to hide the data on a different network.
C. Use a digital signature to authenticate the data.
D. Use a hash function to compress the data.

(2 marks)

Q14 Assume there is 15 staff in the UTHM Data Centre. Calculate the number of keys required using the most suitable cryptography mechanism, to support private communication between staff.

A. 100
B. 105
C. 15
D. 30

(2 marks)

Q15 What is the output of the program that used an encryption based on transposition with the key value is shift right of 3, and if the user inputs the message "`HELLO`"?

A. "`KHOOR`"
B. "`HELLU`"
C. "`KHOOU`"
D. "`GDKKN`"

(2 marks)

TERBUKA

Q16 What is the cipher text produced by encrypting the message "`HELLO`" using a Rail Fence cipher with 2 rails?

A. `HLELO`
B. `HLOEL`
C. `HLLOE`
D. `HOELL`

(2 marks)

Q17 Given a password with 3 characters. Each character can be a number from 0 to 9. Calculate the password complexity.

A. 999
B. 1000
C. 739
D. None of the above.

(2 marks)

Q18 Select the correct output for the following code snippet that demonstrates encryption.

```
int x=0; char c = ‘F’;
x = c - 3;
printf(“%c”,x);
```

A. `C`
B. `D`
C. `c`
D. `d`

(2 marks)

Q19 When conducting multimedia forensic analysis for FSKTM multimedia laboratories, which of the following tools would be used to extract hidden data from a multimedia file?

A. Hex Editor
B. Window Defender
C. Norton Antivirus
D. WinZip

(2 marks)

TERBUKA

Q20 When selecting an audio watermarking solution such as AWT2, which of the following factors would be most important to consider in terms of security?

A. The speed of the solution in encoding and decoding watermarks.
B. The size of the watermark that can be embedded in the multimedia data.
C. The complexity of the watermarking algorithm used.
D. The amount of storage space required for the watermarked data.

(2 marks)

Q21 Questions **Q21(a) - Q21(d)** are based on the following scenario:

Deepfake technology utilizes artificial intelligence to make fake videos. For example, Wombo is a lip-syncing app that lets you transform yourself or others into a singing face. Another example, Deepfakes Web is a service that lets you create deepfake videos on the web. It uses deep learning to absorb the various complexities of face data. Currently, these deepfake technologies are being used for fun, however, they can be a medium of security threat.

(a) Discuss **ONE (1)** issue of deepfake videos in relation to intellectual property (IP).

(3 marks)

(b) Discuss **TWO (2)** potential crimes from the misuse of deepfake technology.

(4 marks)

(c) Discuss **TWO (2)** relevant strategies to secure or protect your photos/videos from being used in a deepfake video.

(4 marks)

(d) Discuss **TWO (2)** ways to detect deepfake videos.

(4 marks)

TERBUKA

Q22 Questions **Q22(a)** - **Q22(e)** are based on the following scenario.

Netflix is a popular streaming service that provides users with access to a vast library of movies and TV shows. One of the key challenges for Netflix is to protect its content from piracy and unauthorized access. To address this challenge, Netflix plans to employ various content protection measures.

(a) Suggest **ONE (1)** potential challenge that Netflix faces in protecting its content from piracy and unauthorized access.

(2 marks)

(b) Suggest **ONE (1)** solution to track content distribution and prevent unauthorized copying of the content.

(2 marks)

(c) Suggest **ONE (1)** solution to control access to and use of its digital content, ensuring that only authorized users with a valid subscription can access the content.

(2 marks)

(d) Discuss **ONE (1)** reason to deploy hardware-based security modules over software-based solutions for a subscription-based streaming service like Netflix.

(3 marks)

(e) Discuss **ONE (1)** solution for each principle to ensure confidentiality, integrity and availability principles of the CIA model are guaranteed.

(6 marks)

TERBUKA

Q23 Questions **Q23(a) - Q23(i)** are based on **Figure Q23**.

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

int main()
{
    char message[100];
    int key, i;

    printf("Enter a message to encrypt: ");
    fgets(message, 100, stdin);

    printf("Enter key: ");
    scanf("%d", &key);

    for (i = 0; message[i] != '\0'; ++i)
    {
        if (message[i] >= 'a' && message[i] <= 'z')
        {
            message[i] = message[i] + key;

            if (message[i] > 'z')
            {
                message[i] = message[i] - 'z' + 'a' - 1;
            }
        }
        else if (message[i] >= 'A' && message[i] <= 'Z')
        {
            message[i] = message[i] + key;

            if (message[i] > 'Z')
            {
                message[i] = message[i] - 'Z' + 'A' - 1;
            }
        }
    }

    printf("Encrypted message: %s", message);

    return 0;
}
```

Figure Q23

(a) State the purpose of this C code.

(2 marks)

(b) Suggest the type of cipher being used.

(2 marks)

(c) State the maximum length of the input message.

(2 marks)

TERBUKA

(d) Discuss the purpose of the `key` variable used.

(2 marks)

(e) Suggest the exact range of the `key` variable.

(2 marks)

(f) Discuss what happens if the shifted value of a character goes beyond '`z`'.

(2 marks)

(g) Discuss what happens if the user inputs a message containing only a symbol.

(2 marks)

(h) Discuss what happens if the user inputs a message with more than the maximum length of characters.

(2 marks)

(i) Given the message to encrypt is '`you`' and the `key` value is 5, illustrate the output.

(4 marks)

- END OF QUESTIONS –

TERBUKA