

CONFIDENTIAL

MAY 2026/SET A/NWC3373



FINAL EXAMINATION

**BACHELOR OF INFORMATION TECHNOLOGY (HONOURS) IN
CYBER SECURITY**

COURSE : FUNDAMENTALS OF CRYPTOGRAPHY

COURSE CODE : NWC3373

DURATION : 3 HOURS

INSTRUCTIONS TO CANDIDATES:

1. This question paper consists of **FIVE (5)** short essay questions.
2. Answer **ALL** questions in the Answer Booklet provided.
3. Please check to make sure that this examination pack consists of:
 - The Question Paper
 - An Answer Booklet
4. Do not bring any material into the examination hall. Electronic calculator is allowed.
5. Please write your answer using permanent ink.

MYKAD/PASSPORT NO : _____
ID.NO : _____
LECTURER : _____
SECTION : _____

DO NOT OPEN THIS QUESTION PAPER UNTIL YOU ARE TOLD TO DO SO

This question paper consists of 5 printed pages including the front page

CONFIDENTIAL

ANSWER ALL QUESTIONS.

1. A healthcare organization is planning to implement an electronic medical record (EMR) system that allows doctors, nurses, and administrators to access patient information through a centralized network. The management is concerned about protecting sensitive patient records from unauthorized access and cyberattacks.

- a. Describe the role of cryptography in securing information systems. Explain how cryptography contributes to the protection of confidentiality, integrity, authentication, and non-repudiation within the healthcare system.

(8 marks)

- b. Define the following terms and **relate each to the scenario**:

- i. Plaintext

(2 marks)

- ii. Cryptographic key

(2 marks)

- iii. Cipher

(2 marks)

- c. *"The organization is worried that attackers may attempt to recover patient information without possessing the encryption key."*

Describe the concept of cryptanalysis and discuss **TWO (2)** common objectives of cryptanalysts when attacking encrypted information.

(6 marks)

(Total: 20 marks)

2. An online banking institution plans to develop a secure transaction platform. Before selecting cryptographic algorithms, the security team needs to understand the mathematical foundations used in modern cryptography.

- a. Discuss the importance of mathematics in cryptography. Explain how mathematical operations contribute to the security of cryptographic algorithms.

(6 marks)

- b. Modular arithmetic is frequently used in cryptographic systems.
Given:

$$17 + 25 \bmod 13$$

Calculate the result and show your working.

(4 marks)

- c. Explain the significance of the following mathematical concepts in modern cryptography:

i. Prime numbers

(2 marks)

ii. Modular arithmetic

(2 marks)

iii. One – way functions

(2 marks)

- d. Differentiate between brute-force attacks and cryptanalytic attacks. Your answer should include the approach used, required knowledge, and potential effectiveness.
(4 marks)

(Total: 20 marks)

3. A multinational company intends to implement secure communication between its headquarters and branch offices. The company is considering adopting a Public Key Infrastructure (PKI) solution.

- a. Describe the basic concept of a public key cryptosystem. Explain how public and private keys are used during encryption and decryption processes.

(6 marks)

- b. Compare symmetric key cryptography and public key cryptography in terms of:

i. Scalability

(2 marks)

ii. Performance

(2 marks)

- c. Explain how public key cryptography supports digital signatures and non-repudiation in electronic business transactions.

(5 marks)

(Total: 15 marks)

- 4 An e-commerce company plans to secure customer transactions and digital communications. The security architect is evaluating RSA and Elliptic Curve Cryptography (ECC).

- a. Describe the RSA cryptographic algorithm and explain its key generation, encryption, and decryption processes.

(7 marks)

- b. Discuss the fundamental concept of Elliptic Curve Cryptography (ECC).

(3 marks)

- c. Compare RSA and ECC in terms of key size and computational efficiency. Based on the analysis, recommend which algorithm is more suitable for resource-constrained environment

(5 marks)

(Total: 15 marks)

5. Megah Holdings Berhad is a multinational company with offices across Asia, Europe, and North America. The company is deploying a secure internal communication system to support:

- Confidential communication between branches
- Secure employee authentication for internal systems
- Safe exchange of encryption keys over public networks

However, the IT security team has identified several challenges:

- Difficulty in securely distributing symmetric keys across multiple locations
- Risk of impersonation attacks during user authentication
- Need for secure communication without pre-sharing keys

As a cybersecurity consultant, you are required to explain appropriate cryptographic solutions for this system.

- a. Explain the challenges of symmetric key distribution faced by Megah Holdings Berhad and how these challenges can be addressed using a Key Distribution Center (KDC).

(8 marks)

- b. The company decides to implement a Public Key Infrastructure (PKI).

Describe how public key distribution works in this system, including the roles of:

- Digital certificates
- Certificate Authority (CA)

Relate the answer to how employees in different countries can trust each other's public keys.

(6 marks)

- c. To prevent unauthorized access, Megah Holdings Berhad implements Kerberos authentication for internal login systems.

Explain how Kerberos works in this environment by describing:

- The role of the Authentication Server (AS)
- The Ticket Granting Server (TGS)
- The use of tickets and session keys

Illustrate how an employee securely accesses a service without repeatedly entering credentials.

(8 marks)

- d. For secure communication between branches that have never interacted before, the system uses Diffie-Hellman Key Exchange.

Explain how Diffie-Hellman enables two branches to securely establish a shared secret over an insecure network.

(8 marks)

(Total: 30 marks)
(TOTAL: 100 MARKS)

END OF QUESTION PAPER

