UNIVERSITI POLY-TECH MALAYSIA
UPTM

# FINAL EXAMINATION

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

| | | |
|---|---|---|
| **COURSE** | : | **FUNDAMENTALS OF CRYPTOGRAPHY** |
| **COURSE CODE** | : | **NWC3193** |
| **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. Pease 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*

**ANSWER ALL QUESTIONS.**

1. A healthcare organization is implementing a digital system to store and transmit patient records securely across departments.

   a. Explain **FOUR (4)** main objectives of cryptography and how each objective applies to the healthcare system.
   (8 marks)

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

      i. Plaintext
      (2 marks)

      ii. Ciphertext
      (2 marks)

      iii. Encryption
      (2 marks)

      iv. Decryption
      (2 marks)

   c. Differentiate between symmetric and asymmetric cryptography. Suggest the most suitable approach for real-time patient data transmission with justification
   (4 marks)

(Total: 20 marks)

2. A financial institution detects multiple attempts by attackers to break encrypted transaction data.

   a. Explain the concept of cryptanalysis and its relevance in this scenario.
   (6 marks)

   b. Describe **THREE (3)** types of cryptanalysis attacks and relate each to the scenario.
   (9 marks)

c. Explain how modular arithmetic and prime numbers support secure encryption in financial systems.

(5 marks)

(Total: 20 marks)

3. An e-commerce platform secures customer transactions using public key cryptography.

a. Explain how a public key cryptosystem ensures secure communication between customers and the server

(5 marks)

b. Describe the RSA algorithm including key generation, encryption and decryption in the context of the transaction process.

(10 marks)

(Total: 15 marks)

4 Haji Bakhil Bank is developing a new mobile banking application to be used by millions of customers worldwide. The application must provide:

- Secure communication between mobile devices and the bank server
- Fast transaction processing with minimal delay
- Low power consumption to preserve mobile battery life

The development team is considering replacing the existing RSA-based encryption system with Elliptic Curve Cryptography (ECC) due to performance concerns on mobile devices. As a cybersecurity consultant, you are required to evaluate the suitability of ECC for this system

a. Explain the basic concept of Elliptic Curve Cryptography (ECC) and how it is used to secure communication in the mobile banking application.

(6 marks)

b. Compare ECC and RSA in the context of the Haji Bakhil Bank mobile banking system, focusing on:

- Key size
- Computational efficiency
- Security strength

Explain how these differences impact the performance of the application.

(5 marks)

c. Justify why ECC is more suitable than RSA for the Haji Bakhil Bank mobile banking application.

(4 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 evaluate and 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**