UNIVERSITI POLY-TECH MALAYSIA
UPTM

FINAL EXAMINATION

BACHELOR OF INFORMATION TECHNOLOGY (HONOURS) IN CYBER SECURITY

COURSE	:	**FUNDAMENTALS OF CRYPTOGRAPHY**
COURSE CODE	:	**NWC3373 / 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. Modern cryptography techniques include algorithms and ciphers that enable the encryption and decryption of information, such as 128-bit and 256-bit encryption keys.

   a. Explain the primary security objectives provided by cryptography.

   (4 marks)

   b. Describe how cryptography protects communication over public networks.

   (3 marks)

   c. Differentiate between classical and modern cryptography in terms of design and security strength.

   (3 marks)

   d. Explain the relationship between **plaintext, ciphertext, encryption algorithm**, and **key.**

   (5 marks)

   e. Explain why modern cryptographic systems rely on keeping the key secret rather than the algorithm.

   (5 marks)

   (Total: 20 marks)

2. Cryptanalysis evaluates the security of cryptographic systems. It requires strong mathematic and analysis on the ciphertext.

   a. Explain why understanding attack models is important when designing secure cryptographic systems.

   (4 marks)

   b. Explain the following attack models.

      i. Ciphertext-only attack.

      (3 marks)

      ii. Brute-force attack.

      (3 marks)

c. Explain the importance of modular arithmetic in encryption systems.

(3 marks)

d. Describe the role of large prime numbers in public key cryptography.

(3 marks)

e. Describe the concept of computational hardness and why it determines practical security.

(4 marks)

(Total: 20 marks)

3. Upon ensuring security on the message, Ali wants to send a confidential message to Siti using a public key cryptosystem. From its third-party key distribution center, it generates RSA key pair using $p = 13$ and $q = 19$ to be used by Ali and Siti for the data transmission.

a. Explain how Ali should use Siti's keys to ensure confidentiality during transmission.

(3 marks)

b. Suppose Ali encrypts the message using his own private key. Explain what security service is achieved and why confidentiality is not guaranteed.

(3 marks)

c. Calculate the modulus **n** and Euler's Totient **Φ(n).**

(3 marks)

d. The organization propose to use $e = 18$ as public exponent. Explain whether this is valid choice by referring to the mathematical requirement of RSA.

(3 marks)

e. Without performing full calculations, explain why knowing **n** alone does not easily reveal the private key in real-world RSA implementations.

(3 marks)

(Total: 15 marks)

4 A software company distributes updates signed using RSA digital signatures. The RSA parameters used by the third party KDC are $e = 5$, $n = 91$. A message with value of 3 has been sent into the network.

a. Explain how a receiver verifies that the software truly comes from the company using the company's public key.

(3 marks)

b. The company signs a hash of the file instead of the full file. Explain **TWO (2)** reasons why hashing is performed before RSA signing.

(4 marks)

c. Compute the ciphertext with the given parameter.

(4 marks)

d. Justify why reversing encryption without the private key is difficult.

(4 marks)

(Total: 15 marks)

5. A Malaysian university deploys a secure authentication infrastructure to protect its Learning Management System (LMS), lab servers, and remote VPN access.

The architecture includes:

- Symmetric encryption for internal service communication
- Public key infrastructure for external authentication
- Kerberos for Single Sign-On (SSO)
- Diffie-Hellman for session key establishment

You are appointed as a security consultant to evaluate and explain the design.

a. Explain how public key distribution improves scalability compared to symmetric key distribution in a large campus network.

(4 marks)

b. The following exchange has occurred:
   - Lecturer sends $A = g^a \bmod p$
   - Server sends $B = g^b \bmod p$

   Explain how both sides obtain the same shared secret. ***(Note: No long arithmetic required.)***

(8 marks)

c. Determine the role of the Key Distribution Center (KDC) including the Authentication Server (AS) and Ticket Granting Server (TGS).

(8 marks)

d. Describe the authentication process from login until a service ticket is obtained.

(10 marks)

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

END OF QUESTION PAPER