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. Fermat's Little Theorem is a fundamental result in number theory that has significant applications in cryptography. This theorem is essential for various cryptographic algorithms, including RSA encryption.

   a. State Fermat's Little Theorem.

   (4 marks)

   b. Find the remainder when 3^{2024} is divided by 13.

   (6 marks)

   (Total: 10 marks)

2. The GCD plays a vital role in cryptographic techniques, particularly in public-key cryptography. Cryptographic protocols, such as RSA and Diffie-Hellman key exchange, rely heavily on the properties of GCD to ensure secure data transmission and encryption.

   a. Define the Greatest Common Divisor (GCD) of two integers **a** and **b**, not both zero.
   (2 marks)

   b. Find the Greatest Common Divisor (GCD) of 274 and 589 using the Euclidean Algorithm.

   (6 marks)

   c. Based on the GCD in **part (b)**, express it as a linear combination of 274 and 589. Find integers **x** and **y** such that:

   $$274x + 589y = \gcd(274, 589)$$

   (8 marks)

   d. Using your answer from **part (c)**, solve for the integer **k** in the following congruence:

   $$589y \equiv 1 \pmod{274}$$

   where **y** is the integer in **part (c)**.

   (4 marks)

   (Total: 20 marks)

3. In a public-key system using RSA, you are given the following parameters:

   - Two prime numbers: **p = 17** and **q = 23**
   - A public exponent: **e = 7**
   - A plaintext message: **M = 5.**

   a. Determine the modulus **n** and Euler's totient function, **Φ(n).**

   (4 marks)

   b. Given the public key is **(e, n).** Using this public key, determine the encrypted message when **M= 5**

   (6 marks)

   c. Explain how these parameters are used within the RSA framework to enable secure communication.

   (10 marks)

   (Total: 20 marks)

4 Imagine you are tasked with explaining how public key cryptography works to a colleague who understands basic encryption but is unfamiliar with the concept of two different keys.

   a. Describe block diagram that illustrates the process of sending an encrypted message from a Sender (Bob) to a Receiver (Alice) using a public and private key pair. Your diagram must include and clearly label the following components:

   - Alice's Computer (The Receiver)
   - Bob's Computer (The Sender)
   - The Public Key
   - The Private Key
   - The Plaintext Message
   - The Encryption Process
   - The Ciphertext (Encrypted Message)
   - The Insecure Channel (e.g., The Internet)
   - The Decryption Process

   (10 marks)

b. Explain step-by-step process by numbering each step that corresponds to the flow in your diagram in **(a)**.

(6 marks)

c. Determine whether a hacker can intercept the ciphertext and decrypt the message by using the public key.

(4 marks)

(Total: 20 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