UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2023/2024

COURSE NAME	:	CRYPTOGRAPHY
COURSE CODE	:	BIS 20404
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	JULY 2024
DURATION	:	3 HOURS
INSTRUCTIONS	:	1. ANSWER ALL QUESTIONS 2. THIS FINAL EXAMINATION IS CONDUCTED VIA ☐ Open book ☒ 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 **SEVEN (7)** PAGES

PART A

Instructions: Choose the BEST answer.

Q1 What is the purpose of the initial permutation in DES?

(a) To spread out the input bits and provide diffusion.

(b) To reverse the order of the input bits.

(c) To reduce the number of rounds in the algorithm.

(d) To increase the speed of encryption.

(1 mark)

Q2 What are some weaknesses of DES?

(a) Small key size, vulnerability to brute force attacks, susceptibility to differential cryptanalysis and not secure for modern standards.

(b) Large key size and immunity to brute force attacks.

(c) Vulnerability to other types of attacks and high computational efficiency.

(d) Resistant to differential cryptanalysis and secure for modern standards.

(1 mark)

Q3 What is a Pseudorandom Number Generator (PRNG) in the context of stream ciphers?

(a) A random number generator that produces truly random numbers.

(b) An algorithm that generates a sequence of numbers used as a keystream to encrypt plaintext into ciphertext.

(c) A non-deterministic algorithm that generates random numbers.

(d) An algorithm that generates a fixed sequence of numbers for encryption.

(1 mark)

Q4 The **BEST** concept of feedback in stream ciphers is ________________.

(a) refers to the process of providing comments on the encryption process

(b) involves using the output of the decryption algorithm as input for subsequent encryption rounds

(c) the mechanism by which the encryption key is generated

(d) involves using the output of the encryption algorithm as input for subsequent encryption rounds

(1 mark)

Q5 How is a Message Authentication Code (MAC) generated and verified?

(a) By using a public key with the message directly.

(b) By encrypting the message with a symmetric key.

(c) By sending the message in plain text.

(d) By combining a secret key with the message using a cryptographic hash function.

(1 mark)

Q6 How does a hash function ensure data integrity?

(a) By compressing the data.

(b) By generating a fixed-size hash value based on the input data.

(c) By encrypting the data using a secret key.

(d) By randomly shuffling the data.

(1 mark)

Q7 What is the most common use of the Diffie-Hellman algorithm?

(a) To secure the exchange of keys.

(b) To generate signatures.

(c) To encrypt and decrypt messages.

(d) To provide certificates.

(1 mark)

Q8 Which of the following numbers **CANNOT** be used as a public key?

(a) 3

(b) 27

(c) 7

(d) 11

(1 mark)

Q9 To obtain a certificate from a certificate authority, the user must present ___________.

(a) proof of identity

(b) public and private keys

(c) password and public key

(d) proof of identity and public key

(1 mark)

Q10 Which of the following is **NOT** a requirement for digital certificates?

(a) Any entity can read the certificate to determine the name and the public key of the certificate owner.

(b) Only authorized entities can send requests to check the certificate validity.

(c) Any entity can ask the validation authority to check the certificate validity.

(d) Only the CA can issue a digital certificate.

(1 mark)

PART B

Q11 Alice wants to send a message to Bob. Alice wants Bob to ensure that the message did not change in transit.

(a) Outline cryptographic steps that Alice must follow to ensure the integrity of the message by creating MAC.

(6 marks)

(b) Outline cryptographic steps that Bob must follow to ensure the integrity of the message by verifying a MAC.

(8 marks)

(c) What is the difference between a MAC and a hash function?

(4 marks)

Q12 Answer the following questions based on **Figure Q12.1**.

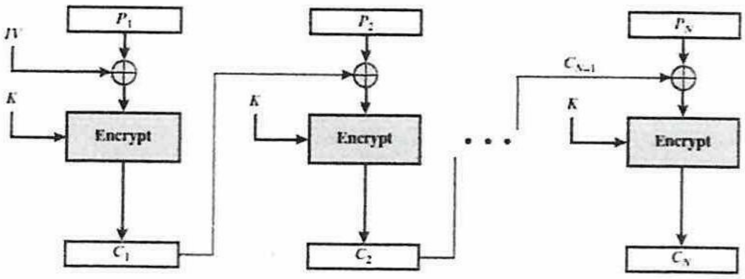

Figure Q12.1

(a) If an error occurred in the transmitted C1, are any blocks beyond P2 affected? Explain your answer.

(4 marks)

(b) Suppose there is a bit error in the source version of P1. Explain how this error is propagated.

(4 marks)

(c) Discuss whether it is possible to perform encryption and decryption in parallel on multiple blocks of plain text in Cipher Block Chaining (CBC) mode?

(4 marks)

Q13 In DES, the input to S-BOX 8 is 000000. What is the output in decimal and binary? Show your calculations based on **Figure Q13.1**.

S_8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Figure Q13.1

(6 marks)

Q14 Consider a Linear Feedback Shift Register (LFSR) with a degree, $m = 4$, and the feedback path, $p3 = 0, p2 = 0, p1 = 1, p0 = 1$.

(a) Create a LFSR with 4 cells in which $p4 = p3 \oplus p0$ for 16 clock cycles.

(10 marks)

(b) Design a LFSR circuit for the encryption in stream cipher.

(4 marks)

(c) Explain **TWO (2)** common attacks on LFSR.

(4 marks)

Q15 Answer **ALL** questions:

(a) Compute the value of p, q, and $\phi(n)$ for an $n = 77$ using Rivest-Shamir-Adleman (RSA) cryptosystem.

(4 marks)

(b) Based on **Q15(a)**, generate a pair of public and private keys for an $e = 13$.

(10 marks)

(c) Based on **Q15(b)**, test any other possible values for e.

(4 marks)

Q16 Answer **ALL** questions:

(a) Suppose that Bob already has a pair of public key, pk_B and private key, sk_B while the Certificate Authority's (CA) public and private key are pk_{CA} and sk_{CA} respectively. Using the correct notations, apply a digital certificate to protect Bob's public key.

(10 marks)

(b) Imagine that Eve knew Bob's public key and certificate. Identify if she can use the known information to exchange data with Alice, pretending to be Bob.

(4 marks)

(c) Discuss if Eve can change Bob's certificate and include her public key in place of Bob's, and then send the certificate to Alice.

(4 marks)

- END OF QUESTIONS -