UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
(ONLINE)
SEMESTER II
SESSION 2019/2020

COURSE NAME	:	CRYPTOGRAPHY
COURSE CODE	:	BIS 20404
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	JULY 2020
DURATION	:	2 HOURS 45 MINUTES
INSTRUCTION	:	1. ANSWER **ALL** QUESTIONS. 2. PLEASE MAKE SURE TO CLICK "SAVE ANSWER" BUTTON FOR SUBJECTIVE QUESTIONS.

THIS QUESTION PAPER CONSISTS OF **FOUR (4)** PAGES

TERBUKA

Q1 Show which bucket has high entropy based on Shannon entropy.

- Bucket 1: BAADABAC
- Bucket 2: DBCADACB
- Bucket 3: BAABAAAA

(10 marks)

Q2 (a) Given a block of message in hexadecimal.

[00 04 12 14 12 04 12 00 0C 00 13 11 08 23 19 19]

(i) Convert the block to a state matrix of Advanced Encryption Standard (AES).

(2 marks)

(ii) Apply shiftrows to the state matrix in **Q2(a)(i)**.

(3 marks)

(b) Suppose a message of 100 plaintext blocks is being encrypted with Cipher Block Chaining (CBC) mode. After encryption, the tenth and eleventh ciphertext blocks are swapped.

(i) Calculate how many blocks of plaintext are certain to be correct after decryption.

(2 marks)

(ii) Justify your answer in **Q2(b)(i).**

(3 marks)

Q3 (a) Distinguish **TWO (2)** attacks that can compromise message authenticity.

(5 marks)

(b) In Diffie-Helman key exchange protocol, Alice and Bob agree to choose two numbers $p = 23$ and $g = 5$.

Based on the given information, answer the following questions by providing relevant steps to complete the protocol.

TERBUKA

(i) Compute the value of Bob's private key, X_B if he has a public key, $Y_B = 10$.

(3 marks)

(ii) Compute the value of Alice's private key, X_A if she has a public key, $Y_A = 8$

(3 marks)

(iii) Solve the secret key, K computed by Alice.

(2 marks)

(iv) Solve the secret key, K computed by Bob.

(2 marks)

Q4 Alice wants to use Rivest-Shamir-Adleman (RSA) algorithm to send encrypted messages to Bob. Thus, Bob needs to distribute his public key to Alice before she can encrypt the messages. Bob selects two prime number 17 and 11 as p and q respectively. Then, he selects an exponent $e = 7$ which is coprime to $\emptyset(n)$.

(a) Calculate the value of $\emptyset(n)$.

(1 mark)

(b) Calculate the value of the private key, d.

(5 marks)

(c) Show the pairs of Bob's public and private key.

(3 marks)

(d) Compute its corresponding ciphertext if Alice wants to send a plaintext, $p = 88$ to Bob.

(4 marks)

(e) Show how Bob computes the corresponding plaintext after he receives the ciphertext.

(2 marks)

Q5 Malaysia military department implements a basic Public Key

TERBUKA

Infrastructure (PKI) so that the staffs can communicate among them securely. Suppose that Bob already has his own pair of public key, pk_B and private key, sk_B while the Certificate Authority's (CA) public key is pk_{CA} and the private key is sk_{CA}. In this case, Bob is hired and then asked to go to CA on the first day of his job.

Based on the above case, answer the following questions.

(a) Examine the purpose of CA.

(7 marks)

(b) Examine how the CA can identify Bob as himself.

(2 marks)

(c) Analyse how the CA prevents Bob's certificate from being forged.

(3 marks)

(d) Analyse how other staff can extract Bob's public key from the certificate.

(3 marks)

- END OF QUESTIONS -

TERBUKA