Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2018/2019

COURSE NAME	:	CRYPTOGRAPHY
COURSE CODE	:	BIS 20404
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	JUNE / JULY 2019
DURATION	:	3 HOURS
INSTRUCTION	:	ANSWER **ALL** QUESTIONS

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

Q1 (a) Given a one-time pad encryption with the message, m_0 = attack at dawn and c_0 = 61747461636b206174206461776e (the plaintext letters are encoded as 8-bit ASCII and the given ciphertext is written in hex.

What would be the one time pad encryption of the message, m_1 = attack at dusk under the same one-time pad key? Show your solution.

(10 marks)

(b) Consider a 3-bit version of RC4 with the following algorithm.

```
//Creation of initial state and key
for (i= 0 to 7)
{
    S[i]=i
    T[i]=Key[i mod KeyLength]
}
//Initial permutation of S
j=0
for (i=0 to 7)
{
    j = (j + S[i] + T[i]) mod 8;
    swap(S[i],S[j]);
}
```

If the `plaintext = 32071553` and the `key = 31415`, compute the first **FOUR (4)** outputs of the initial permutation.

(10 marks)

Q2 (a) Diffentiate **TWO (2)** advantages between Advanced Encryption Standard (AES) and Data Encryption Standard (DES).

(5 marks)

(b) State **FIVE (5)** modes of operation in modern block ciphers.

(5 marks)

(c) Illustrate the precise consequences of a 1-bit error in a single block of ciphertext for Cipher Block Chaining (CBC) block cipher mode using an appropriate diagram.

(5 marks)

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

How many blocks of plaintext, after decryption, are certain to be correct? Justify your answer.

(5 marks)

Q3 (a) Alice can use Message Authentication Code (MAC) or digital signature to provide two similar security properties but they also have several differences that give them advantage to one another.

Discuss **ONE (1)** similarity and **ONE (1)** difference between MAC and digital signature.

(5 marks)

(b) Alice wants to send a message to Bob and she wants Bob to be able to verify that the message has not changed in transit. For this, they use a MAC function with a shared secret key, K for generating and verifying a MAC value.

(i) Discuss the protocol that Alice must follow to ensure the integrity of the message by creating the MAC.

(5 marks)

(ii) Discuss the protocol that Bob must follow to ensure the integrity of the message by verifying the MAC.

(5 marks)

(c) Discuss a cryptographic hash function.

(5 marks)

Q4 (a) In Diffie-Helman key exchange protocol, Alice and Bob agree to choose two numbers $p = 23$ and $g = 7$. Then, Alice chooses her secret number, $x = 3$ and Bob chooses his secret number, $y = 6$.

Based on the given information, calculate the answers by providing relevant steps to complete the protocol.

(i) What is the public value, R_1 computed by Alice which sent to Bob?

(2 marks)

(ii) What is the public value, R_2 computed by Bob which sent to Alice?

(2 marks)

(iii) What is the secret key, K_1 computed by Alice?

(2 marks)

(iv) What is the secret key, K_2 computed by Bob?

(2 marks)

(b) 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 7 and 11 as p and q. Then, he selects an exponent $e = 13$ which is coprime to $\emptyset(n)$ and $n = pq$.

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

(2 marks)

(ii) Calculate the value of the private key where $e \times d = 1 \; mod \; \emptyset(n)$.

(3 marks)

(iii) What are Bob's public and private key?

(2 marks)

(iv) Imagine that Alice wants to encrypt the plaintext, m = 5, calculate its corresponding ciphertext.

(2 marks)

(v) After Bob receives the ciphertext, show how he computes the corresponding plaintext.

(3 marks)

Q5 (a) A military department implements a basic Public Key Infrastructure (PKI) so that the staffs can communicate among them securely. In this case, Bob is hired and then asked to go to Certification Authority (CA) on the first day of his job.

Suppose that Bob already has his own pair of public key, pk_B and private key, sk_B while the CA's private key is sk_{CA}. Discuss how the CA generates the signed certificate, $cert_B$ for Bob. Use the appropriate diagram to describe the procedure.

(10 marks)

(b) Describe **FIVE (5)** differences between classical and quantum cryptography.

(10 marks)

- END OF QUESTIONS -