UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2022/2023

COURSE NAME	:	CRYPTOGRAPHY
COURSE CODE	:	BIS 20404
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	JULY / AUGUST 2023
DURATION	:	3 HOURS
INSTRUCTION	:	1. ANSWER **ALL** QUESTIONS. 2. THIS FINAL EXAMINATION IS CONDUCTED VIA 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 **FOUR (4)** PAGES

Q1 (a) Justify the importance of Feistel cipher.

(3 marks)

(b) Explain the difference between confusion and diffusion. Give **TWO (2)** examples of each related cryptography that are using these theories.

(4 marks)

(c) Explain the purpose of S-boxes in Data Encryption Standard (DES).

(3 marks)

(d) One important property that makes DES secure is that the S-boxes are nonlinear. Given S-box S_1, show that $S1(x1) \oplus S1(x2) \neq S1(x1 \oplus x2)$ for $x1$=111111 and $x2$=100000 to verify the property.

S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Figure Q1(d)

(10 marks)

Q2 Let's consider simplified RC4 algorithm of 4 bytes, rather than full 256 bytes:

```
S-array of length 4, [S0 S1 S2 S3] = [0 1 2 3]
Key, K = [2 5 7 3]
```

Based on the scenario, answer the following questions:

(a) Find the final keystream.

(10 marks)

(b) Using the final keystream in **Q2(a)**, find ciphertext for the following input string as shown in **Figure Q2(b)**.

```
Plaintext, P = [H A L O]
```

Char	A	B	C	D	E	F	G	H	I	J	K	L	M
Decimal	65	66	67	68	69	70	71	72	73	74	75	76	77
Char	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Decimal	78	79	80	81	82	83	84	85	86	87	88	89	90

Figure Q2(b)

(10 marks)

Q3 (a) What are **TWO (2)** security measures does the system offer if Alice transmits an unencrypted message to Bob along with the Message Authentication Code?

(2 marks)

(b) Explain actions that will be done by Bob if an attacker, Eve intercepts a message from Alice to Bob, modifies the message by changing `M` to `N` and then forwards the modified message, with the original MAC attached to Bob.

(4 marks)

(c) Explain actions that will be done by Bob if an attacker, Eve changes a message `M` to `N`, calculates and sends the new MAC based on `N`.

(4 marks)

(d) Discuss what a malicious user can gain and how they perform the attack if the hash function, `H()`, does not have the one-way property.

(4 marks)

(e) Discuss **THREE (3)** properties of a true cryptographic hash.

(6 marks)

Q4 (a) Compute the value of p, q, and $\varnothing(n)$ for an $n = 35$ using Rivest-Shamir-Adleman (RSA) cryptosystem.

(5 marks)

(b) Based on **Q4(a)**, generate a pair of public and private keys for an $e = 5$. Use Euclidean algorithm to find the inverse modulo. Show your work.

(10 marks)

(c) Based on **Q4(b)**, test any other possible values for e.

(5 marks)

Q5 An organization has a Public Key Infrastructure (PKI) for its staffs consisting of a single Certification Authority (CA) and a single Directory Server (DS). Certificates have an expiry time of 1 year. Certificate Revocation Lists are issued frequently.

Based on the scenario, answer the following questions:

(a) Describe the steps taken when Ali joins the organization as a new staff.

(5 marks)

(b) An attacker, Eve steals Ali's private key and Ali does not realize it. Justify how long Eve impersonate Ali after the steal.

(2 marks)

(c) An attacker, Eve steals Ali's private key and Ali realizes this. Describe the steps Ali should takes.

(5 marks)

(d) Describe the benefit of public-key cryptography to online services.

(3 marks)

(e) Justify the reason symmetric key cryptography alone not suitable for online services.

(3 marks)

(f) Propose **ONE (1)** solution to deal with privacy issues in the CA.

(2 marks)

-END OF QUESTIONS –