Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2014/2015

COURSE NAME	:	CRYPTOGRAPHY
COURSE CODE	:	BIS 20404
PROGRAMME	:	2 BIS
EXAMINATION DATE	:	JUNE 2015 / JULY 2015
DURATION	:	3 HOURS
INSTRUCTION	:	ANSWER **ALL** QUESTIONS

THIS QUESTION PAPER CONSISTS OF **SIX (6)** PAGES

Q1 (a) A transposition cipher permutes characters usually in a fixed period d and with permutation f.

(i) How many possible permutations of length d are available for encryption? Explain your answer.

(5 marks)

(ii) What is the key that both sender and receiver need prior to communication?

(2 marks)

(b) **Figure Q1(b)** is an autocorrelation diagram output from **Cryptool** for a ciphertext 1 and ciphertext 2.

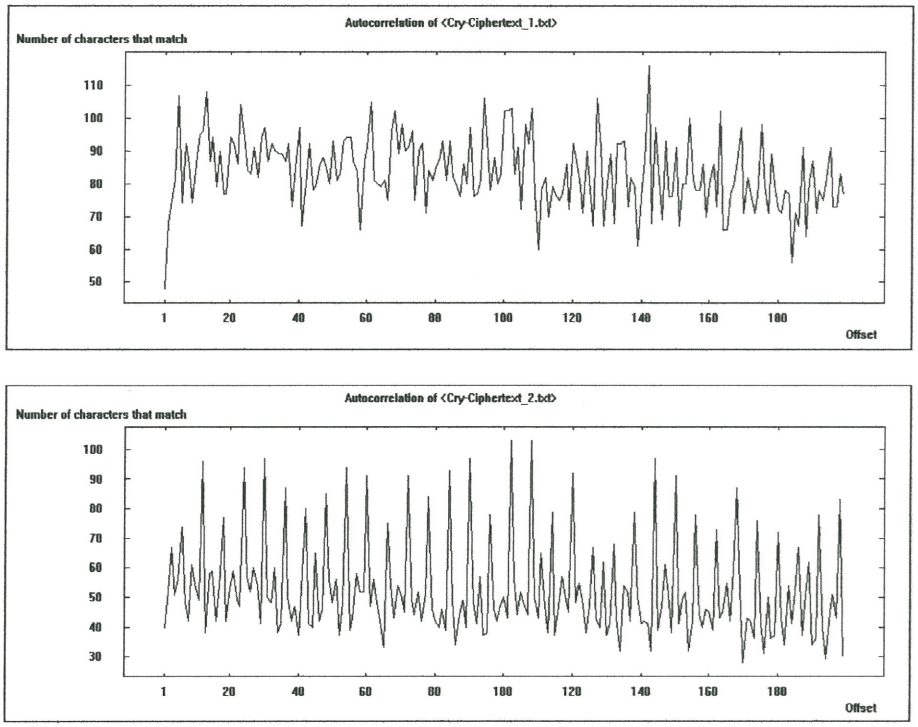

Figure Q1 (b)

Explain how these plots allow you to distinguish which ciphertext is the simple substitution and which one is the Vigenère cipher.

(4 marks)

(c) In the 2 X 2 Hill cipher, encryption follows the equation $C = KP$ where C is the ciphertext matrix, K is the key matrix, and P is the plaintext matrix. Suppose that $K = \begin{pmatrix} 1 & 2 \\ 26 & 2 \end{pmatrix}$ and Assume that the alphabet is encoded as A = 0;B = 1;…; ▽ = 26.

(i) Calculate the inverse key matrix, K^{-1}

(4 marks)

(ii) Encrypt the plaintext "ABCD".

(4 marks)

(d) Consider a message set with three possible plaintexts M_1, M_2 and M_3. Their probabilities are $\Pr(M_1) = \Pr(M_3) = 1/4$ and $\Pr(M_2) = 1/2$. Assume that messages and keys are chosen independently of each other and keys are chosen with equal probability. Suppose there are 4 possible ciphertexts C_1, C_2, C_3, C_4. A cipher is defined by the following table which shows how each plaintext message M_i is encrypted using each key K_i.

	M_1	M_2	M_3
K_1	C_1	C_2	C_2
K_2	C_2	C_4	C_3
K_3	C_3	C_1	C_4
K_4	C_4	C_2	C_1

(i) Analyze why this cipher does not provide perfect secrecy?

(4 marks)

(ii) Draw a similar encryption table for a different cipher, defined on the same messages, which *does* provide perfect secrecy.

(2 marks)

Q2 (a) **Figure Q2(a)** is Linear Feedback Shift Register (LFSR).

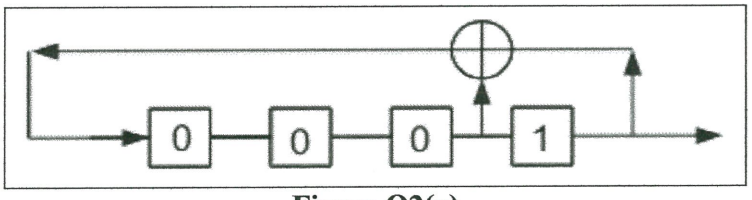

Figure Q2(a)

(i) Outline the recurrence relation defined by this LFSR.

(2 marks)

(ii) Calculate the next 20 symbols output by this LFSR.

(2 marks)

(iii) Determine the maximum possible period of the sequence output by any LFSR of this length?

(2 marks)

(iv) Determine the linear complexity of the sequence output by this LFSR

(1 marks)

(b) Consider the following (toy) cipher, which is a three-rounds iterated block cipher with a block length of 8 bits and a key length of 8 bits. Work through the steps required to encrypt the plaintext block P = 01010101 using key K = 11000011. The cipher is a substitution-permutation in which each S-box operates on sub-blocks of 2 bits.
Thus m = 4 and l = 2.

- The permutation π_S is defined by the following table:

Input block	00	01	10	11
Output block	10	00	01	11

- The permutation π_P is defined by the following table where the block bits are labelled from 0 to 7:

Input position	0	1	2	3	4	5	6	7
Output position	3	6	0	5	2	1	7	4

The key schedule is defined by K1 = K, K2 = K1 << 2, K3 = K2 << 1 where << 1 denotes cyclic shift left by one position and << 2 denotes cyclic shift left by two positions.

(9 marks)

(c) Alice wants to send a message to Bob. Alice wants Bob to be able to ensure that the message did not change in transit. Briefly outline the cryptographic steps that Alice and Bob must follow to ensure the integrity of the message by creating and verifying a MAC.

(6 marks)

(d) State **THREE (3)** security properties of hash functions.

(3 marks)

Q3 (a) Suppose that an RSA public key is chosen with primes $p = 17$ and $q = 19$. Suppose that the public key $e = 11$ is used.

(i) Find the value of d.

(10 marks)

(ii) Find the ciphertext value for $M = 5$ and $M = 14$.

(4 marks)

(iii) Decrypt the ciphertext and verify that the correct value is recovered.

(4 marks)

(b) The Diffie-Hellman key agreement algorithm allows two entities to establish a shared secret key without requiring the use of a secure channel. That is, they can establish a shared secret key even though the messages they send may be observed by others.

(i) What sort of mathematics is required to perform Diffie-Hellman key agreement?

(2 marks)

(ii) One problem with this scheme is that each entity has no assurance about the identity of the entity they are communicating with. What sort of attack is possible as a result of this problem?

(5 marks)

Q4 (a) Suppose that Alice and Bob use an *asymmetric* cipher (say, RSA) to communicate confidentially. They have their public keys in a file that is available on the corporate network. Another employee, Carol, wants to know what they are communicating. Carol cannot break the RSA algorithm, but is able to access and alter the file containing their public keys.

(i) How does altering the public keys help Carol to gain access to the confidential communications between Alice and Bob?

(6 marks)

(ii) Which messages is Carol able to access?

(3 marks)

(iii) Explain how a *digital certificate* can be used to provide a solution to this problem.

(4 marks)

(iv) Can you trust a digital certificate? Justify your answer.

(4 marks)

(v) Is a *digital signature* the same as a *digital certificate*? Justify your answer.

(4 marks)

(b) State **ONE (1)** advantage and **ONE (1)** disadvantage if applying quantum cryptography.

(4 marks)

- END OF QUESTION -