UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2017/2018

COURSE NAME	:	CRYPTOGRAPHY
COURSE CODE	:	BIS 20404
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	JUNE / JULY 2018
DURATION	:	3 HOURS
INSTRUCTION	:	ANSWER **ALL** QUESTIONS

THIS QUESTION PAPER CONSISTS OF **NINE (9)** PAGES

SECTION A

Instruction: Choose the BEST answer for each of the following questions.

Q1 The equation $a \equiv b \ (mod\ n)$ means ______________.

A. $a + kb = n$ for some integer k
B. $a - kb = n$ for some integer k
C. $a + b = kn$ for some integer k
D. $a - b = kn$ for some integer k

Q2 If $a = 7$, then $a^{-1}\ mod\ 17$ is ______________.

A. 20
B. 7
C. 1
D. 5

Q3 If $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} (mod\ 2)$ then ______________.

A. A^{-1} does not exist
B. $A^{-1} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \ (mod\ 2)$
C. $A^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \ (mod\ 2)$
D. $A^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \ (mod\ 2)$

Q4 The exclusive OR (XOR) operation is equivalent to ______________.

A. multiplication modulo 2
B. addition modulo 2
C. the logical AND operation
D. negation of the logical OR operation

Q5 The period of a Vigenère cipher can be estimated by ___________.

A. computing the autocorrelation profile of the ciphertext
B. using the Kasiski method
C. computing the index of coincidence
D. all of the above

Q6 If the character frequencies in a ciphertext are the same as those of its corresponding plaintext then it is likely that the cryptosystem used was _________.

A. a transposition cipher
B. a simple substitution cipher
C. a Vigenère cipher
D. the one time pad

Q7 The encryption of a general linear cipher is defined as $j \equiv ai + b \ (mod\ n)$ where j is the ciphertext output, i is the plaintext input and (a, b) are key values. A linear cipher is a type of ____________.

A. substitution cipher
B. transposition cipher
C. Caesar cipher
D. one time pad

Q8 A certain linear cipher is defined by an encryption of the form $j \equiv ai + b \ (mod\ 26)$ where j is the ciphertext output, i is the plaintext input (a, b) are key values. The number of possible distinct keys for this cipher is ____________.

A. 26
B. $26^2 = 676$
C. 26 x 12 = 312
D. 26 x 25 = 650

Q9 Man-in-the-middle attack can endanger security of Diffie-Hellman method if two parties are not __________.

A. authenticated
B. joined
C. submit
D. encrypted

Q10 The maximum entropy of a message set with 32 message is ___________.

A. 5 bits
B. 32 bits
C. 8 bits
D. 4 bits

Q11 A certain cryptosystem has 2^{64} randomly chosen keys and is used to encrypt a language with 4 bits of redundancy per character. Its unicity distance is ________.

A. 60 characters
B. 16 characters
C. 32 characters
D. 64 characters

Q12 The unicity distance of a cipher may be increased by ____________.

A. decreasing the length of the key
B. decreasing the redundancy in the plaintext
C. making the encryption algorithm more complex
D. all of the above

Q13 If the plaintext for the Vernam one time pad is 00101 and the key is 10101 then the ciphertext is ________________.

A. 0100110011
B. 1000110011
C. 10000
D. 00101

Q14 Which of the following is **NOT** a requirement for a sequence to be called Golumb-random?

A. Approximately half the bits in a period should be 1.
B. In any period approximately half the runs should have length 1.
C. For every run of 0 bits there should be a run of 1 bits of the same length.
D. The out-of-phase autocorrelation function is constant.

Q15 Given a recurrence relation of a Linear Feedback Shift Register (LFSR) is $Z_{t+5} = Z_{t+2} \oplus Z_t$, and the first five bits output are 10001, the next two output bits will be ________.

A. 00
B. 01
C. 10
D. 11

Q16 Which one of the following statement about block ciphers is **TRUE**?

A. Plaintext is encrypted one block at a time, under a time-varying function of the key.
B. When using Cipher Block Chaining (CBC) mode, if the same block occurs at different block positions in the plaintext then the corresponding ciphertext blocks will also be the same.
C. When using Electronic Codebook (ECB) mode, if the same block occurs at different block positions in the plaintext then the corresponding ciphertext blocks will also be the same.
D. A block cipher used in ECB mode is effectively a stream cipher.

Q17 Which one of the following statements about hash functions is **TRUE**?

A. A hash function takes an input message of any length and produces an output of variable length.
B. A hash function never creates collisions.
C. Given a particular hash function and the hash value of a message, it is easy to compute the corresponding message.
D. Given a particular hash function and a message, it is easy to compute the corresponding hash value of the message.

Q18 You receive a message, *M*, and the hash value of the message, *H*, computed using the MD5 hash function. Which of the following statements about *H* is **TRUE**?

A. It provides confidentiality for *M*.
B. It provides a means for verifying that *M* has not been altered accidently.
C. It provides a means for verifying that *M* has not been altered intentionally.
D. It provides a means for authenticating the sender of *M*.

Q19 A group of six people (let's call them Alice, Bob, Carol, Dave, Ed and Frank) wish to communicate with each other using symmetric key cryptography. How many distinct symmetric keys will the group need, so that any two people can communicate securely?

A. 6.
B. 12.
C. 15.
D. 30.

Q20 An important aspect of key management is the protection of cryptographic keys. Which of the following statements regarding key protection is **FALSE**?

A. Asymmetric public keys need protection against unauthorised disclosure.
B. Asymmetric private keys need protection against unauthorised disclosure.
C. Symmetric keys need protection against unauthorised disclosure.
D. All keys need protection against unauthorised modification.

(40 marks)

SECTION B

Q21 Batu Pahat Clinic wants to create a secure system to store the patient records. Confidentiality and integrity are two basic security requirements by the authority of Batu Pahat Clinic. The password is encrypted using RC4. The integrity of the patient records are checked using SHA256. Maslan is the security software programmer who is assigned to design the secure system for Batu Pahat Clinic. Figure **Q21(a)** shows the database design.

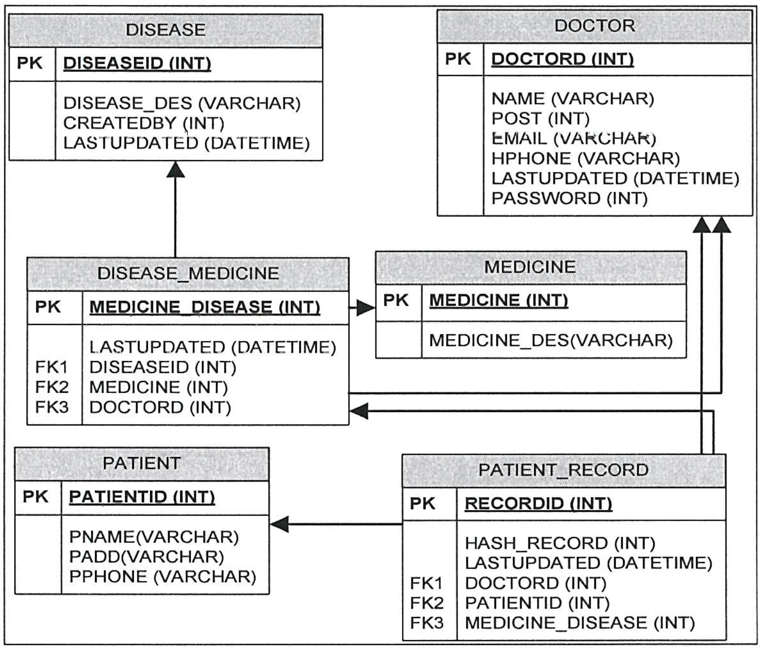

FIGURE Q21(a)

(a) In Figure **Q21(a)**, the output of confidentiality and integrity respectively cannot be stored. Discuss the design flaws.

(4 marks)

(b) Recommend possible solutions to address the limitations discussed in **Q21(a)**.

(2 marks)

(c) Suggest the possible attack that can compromise the confidentiality of the system. Provide the solution to encounter the attack.

(4 marks)

(d) Suggest **TWO (2)** hash functions that can provide better security compare to SHA256.

(2 marks)

Q22 Explain **THREE (3)** basic properties of hash functions.

(3 marks)

Q23 Explain **THREE (3)** differences between hash function and message authentication code (MAC).

(6 marks)

Q24 (a) Explain why encryption is usually much faster than decryption in the RSA.

(2 marks)

(b) Explain why decryption process slower than encryption process in the RSA.

(2 marks)

(c) The RSA cryptosystem uses a modulus n which is the product of two primes numbers p and q. Suppose that the values $p = 5$ and $q = 7$ are used.

(i) Justify the reason where the value $e = 3$ cannot be used for the public exponent in this case.

(2 marks)

(ii) Calculate the private exponent d, where $e = 5$.

(4 marks)

(iii) Calculate the value of ciphertext where the message $m = 3$.

(2 marks)

(e) Explain how randomness is usually included for RSA encryption.

(2 marks)

Q25 (a) Suppose the parameter $p = 13$, $g = 3$, and private key $x = 7$ are used for ElGamal signature scheme.

(i) Compute the public key, y.

(2 marks)

(ii) Compute a valid signature if $m = 4$, where $k = 7$.

(10 marks)

(b) Suppose that Alice and Bob use an *asymmetric* cipher (example: 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?

(3 marks)

(ii) Which messages is Carol able to access?

(3 marks)

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

(3 marks)

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

(4 marks)

- END OF QUESTION -