Master of Computer Applications
MCAC301: Information Security
Unique Paper Code: 223422303
Semester III
December 2024
Year of Admission: 2023

Time: Three Hours **Max. Marks: 70**

Note: All questions are compulsory. Attempt all parts of a question together. Use of a calculator is allowed.

1 (a) For each of the following assets, assign a *low, moderate, or high* impact level for the loss of confidentiality, availability, and integrity, respectively. Justify your answers. [3]

i. An organization managing public information on its Web server.

ii. A law enforcement organization managing extremely sensitive investigative information.

iii. A financial organization managing routine administrative information (not privacy-related information).

(b) Caesar wants to arrange a secret meeting with Marc Antony at one of two locations, either at the Tiber ("*RIVER*") or at the Coliseum ("*ARENA*"). He sends the ciphertext *EVIRE* to Antony. However, Antony does not know the key, so he tries all possibilities. Where will he meet Caesar? Provide a step-by-step explanation to reach your conclusion. [3]

(c) Give the decryption ~~function~~ table corresponding to the symmetric encryption cryptosystem described by the table below, where $k = m = c = \{0, 1, 2, 3\}$. [4]

		m			
		0	1	2	3
	0	3	0	2	1
k	1	1	3	0	2
	2	2	1	0	3
	3	0	2	3	1

2. (a) Describe the following attack on a cryptosystem: [3]

i. Ciphertext only

ii. Chosen plaintext.

For each, give scenario in which such an attack might be plausible to carry out.

(b) Find the product of bytes 10101111 and 00000011 in $GF(2^8)$. Assume here that field elements are represented using the primitive polynomial $g(x) = x^8 + x^4 + x^3 + x + 1$. [4]

(c) If an encryption function E_K produces the same result as the decryption function D_K, then key K is said to be an involutory (in other words, $E_K(p) = D_K(p)$, for all plaintexts p). Find all involutory keys (K) in the Shift cipher over Z_{26}, over Z_{22}, and over Z_{23}. [3]

3 (a) Alice and Bob agreed to use the Hill Cipher algorithm for the encryption and have shared the key matrix through a secure channel. Bob has already calculated the key matrix K^{-1}, a matrix he will use for the decryption. Find the plaintext message corresponding to the [5]

ciphertext message "*RMCROWQGSVDS*" that Alice has sent to Bob. Provide a step-by-step description.

$$K^{-1} = \begin{bmatrix} 3 & 7 & 1 \\ 24 & 4 & 19 \\ 5 & 4 & 19 \end{bmatrix}$$

(b) The Kerberos protocol has two main components: the Authentication Server (AS) and the Ticket Granting Server (TGS). Explain the functions of these components in detail, including the process of generating and using session keys, and how they interact with each other. [5]

4 (a) Find the results of the following: [6]

i. $16^{-1} mod\ 323$ using Euler's theorem (*Hint:* 323 = 17 × 19)

ii. $320^{23} mod\ 461$ using square and multiply method

iii. $5^{15}\ mod\ 13$ using Fermat's little theorem

(b) Distinguish between a session and a connection. Describe how the master secret is created from the pre-master secret in SSL. [4]

5 (a) In CBC mode, bits 17 and 18 in ciphertext block 9 are corrupted during transmission. Find the possible corrupted bits in the plaintext block 9 and the subsequent plaintext blocks. Will this corruption affect all the subsequent plaintext blocks? [2]

(b) Show why CFB mode creates a nonsynchronous stream cipher, whereas OFB mode creates a synchronous one. [4]

(c) A host receives an authenticated packet with the sequence number 331. The replay window spans from 200 to 263. What will the host do with the packet? What is the window span after this event? [2]

(d) In an organisation comprising of 100 users, what would be the maximum number of keys needed in the case of symmetric encryption and in the case of public-key encryption? [2]

6 (a) Confusion and diffusion are considered as two properties of a secure cipher. Explain how AES adds these two properties to its design. [3]

(b) Let p =17, q = 31, e = 7, and M = 2. Perform encryption using the RSA algorithm. [3]

(c) When DES is used with a *weak key* , then $E_K(E_K(p)) = p$. When we use a pair of keys K_1, K_2 with $K_1 \neq K_2$ such that $E_{K_1}\left(E_{K_2}(p)\right) = p$, then such keys are known as semi-weak keys. [4]

i. How would you describe weak-keys and semi-weak keys, in terms of the round keys they generate?

ii. What is the danger of using semi-weak keys and weak keys? Provide a detailed explanation for your answer.

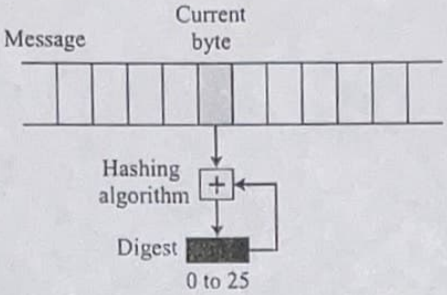
7 (a) Barack periodically comes up with brilliant ideas to stop the financial crisis, provide health care to every citizen, and save the polar bears. He wants to share these ideas with all the cabinet members but also get credit for the ideas. Extending the above approach, he shares a secret key **k** with all the cabinet members. Next, he broadcasts each idea **z** followed by value [2]

h(k||z). Does this approach work or can Tim (a cabinet member) claim that he came up with the ideas instead of Barack? Justify your answer.

(b) Assume we have a very simple message digest. Our unrealistic message digest is just one number between 0 and 25. The digest is initially set to 0. The cryptographic hash function adds the current value of the digest to the value of the current character (between 0 and 25). Addition is in modulo 26. Below Figure shows the idea. [4]

i. What is the value of the digest if the message is "HELLO"?

ii. Why is this digest not secure? Give your answer in terms of the cryptographic hash function criteria.



(c) In the Diffie-Hellman protocol, what happens if x and y have the same value, that is, Alice and Bob have accidentally chosen the same number? Are R1 and R2 the same? Do the session keys calculated by Alice and Bob have the same value? Prove your claims with the help of an example and use g = 7 and p = 23. [4]