Master of Computer Applications

MCAC302: Information Security

Unique Paper Code: 223401302

Semester III
OBE Examination, Nov./Dec.-2021
Year of Admission: 2020

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

Note: Attempt any four questions. All questions carry equal marks.

Q.1 Why is modular arithmetic used in cryptography? Alice often needs to encipher plaintext made of both letters (A to Z) and digits (0 to 9). If she uses an additive cipher, what is the key domain? 3 marks

Confusion and diffusion are considered as two properties of a secure cipher. Differentiate between these two. Further, explain how AES adds these two properties to its design. 8 marks

Distinguish between passive and active security attacks. Consider an ATM which asks users to provide a card or an account number to deposit cash. Give examples of confidentiality, integrity, and availability requirements associated with the system, and, in each case, indicate the degree of importance of the requirement. 6.5 marks

Q.2 S-boxes are generally used to provide non-linearity in a modern block cipher. How does IDEA cipher achieve the non-linearity though it does not use any S-Box? Suppose Simplified-IDEA is used to encrypt the 16-bit plaintext message 1001110010101100 using the 32-bit key 11011100011011110011111. Show the intermediate result obtained after round one 9.5 marks

What is the purpose of Linear feedback shift register? Create a linear feedback shift register with 8 cells in which $b8 = b7 + b6 + b3 + b0$. 5 marks

Differentiate between *men-in-the-middle* and *meet-in-the-middle* attack. 3 marks

Q.3 Alice devised a new cipher scheme in which she writes out the plaintext, by rows, in m × n matrix. Here, m and n are two positive integers. Then form the ciphertext by taking the columns of these rectangles. For example, for plaintext 8.5 marks

"$MEETAT\ FIRSTANDPINEATMIDNIGHT$", the ciphertext is "$TTEIERIDMIPITNTHFDMTESNNAAAG$."

a) Determine the value of m and n used in the devised cipher scheme.
b) Describe how Bob would decrypt a ciphertext string (given values for m and n)
c) Decrypt the following ciphertext, which was obtained by using this method of encryption:
$VOHMIAEAXYATED$

What are the ways in which secret keys can be distributed to two communicating Parties? In a simple protocol using a KDC, what happens if the ticket for Bob is not encrypted using the Bob's key K_B, but is encrypted instead by K_{AB}. 5 marks

Determine the following: 4 marks

a) $145^{102}\ mod\ 101$ using Fermat's little theorem
b) $38^{-1}\ mod\ 180$ using Extended Euclidean algorithm

Q.4 When DES is used with a weak key K, then $E_k(E_k(p)) = p$. When we use a pair of keys $K1, K2,$ such that $E_{k1}(E_{k2}(p)) = p$, then such keys are known as semi-weak keys. 9.5 marks

a) How would you describe weak-keys and semi-weak keys in terms of the round keys they generate?
b) What is the danger of using semi-weak keys and weak keys? Provide a detailed explanation for your answer.
c) What is the probability of randomly selecting a weak, a semi-weak, or a possible weak key in DES?

In Cipher Feedback Mode (CFB), bits 3 to 6 in block 11 are entirely corrupted during transmission. The size of the plaintext or ciphertext block is 8 bits. Find the possible corrupted bits in the following plaintext blocks if DES is used. 5 marks

Why is Caesar cipher substitution technique vulnerable to a brute-force cryptanalysis? 3 marks

Q.5 Give reason for the following: 9.5 marks

a) CFB mode creates a nonsynchronous stream cipher, but OFB mode creates a synchronous one.
b) There is no need of ciphertext stealing in CFB, OFB and CTR modes.

Encrypt the message UNIVERSITYOFDELHI using the Hill Cipher with key matrix 5 marks

$A = \begin{bmatrix} 03 & 02 \\ 02 & 07 \end{bmatrix}$.

Differentiate Asymmetric cryptography with Symmetric cryptography. How are these two techniques combined to make a more secure cryptosystem? 3 marks

Q.6 Consider an RSA cipher with prime p=3 and q=11, encryption exponent e = 7, and correspondence A=0, B=1, C=2,..Z=25. Use this cipher to encrypt BOONE. Further, decrypt 27,2,29,10,16,7 which was formed using this technique. 9.5 marks

Sherlock and his friend are playing a cryptography game. Sherlock's friend gives him a ciphertext "CIW" and tell the plaintext is "yes" which is obtained by using the shift cipher. Now, the friend gave him another ciphertext "$FILIEPXLCERHLETTC$". Sherlock immediately found the actual meaning of the ciphertext. What type of attack did Sherlock launch here? What is the plaintext. Further, Encrypt the obtained plaintext using Playfair cipher using the key "$LOCKDOWN$" 5 marks

Explain why modes of operation are needed if modern block ciphers are to be used for encryption. Find the possible corrupted bits in the plaintext in CTR mode if blocks 4 and 5 are entirely corrupted. 3 marks