Question Paper

Exam Date & Time: 26-Nov-2022 (09:00 AM - 12:00 PM)

MANIPAL ACADEMY OF HIGHER EDUCATION

MANIPAL INSTITUTE OF TECHNOLOGY
FIFTH SEMESTER B.TECH END SEMESTER EXAMINATIONS, NOV 2022

INFORMATION SECURITY [ICT 3172]

Marks: 50 **Duration: 180 mins.**

A

Answer all the questions.

Instructions to Candidates: Answer ALL questions Missing data may be suitably assumed

1) Mention all the steps necessary for key generation, signing and verification of digital signatures using RSA scheme. (5)

A) Consider p=809, q=751 and d=23. Use RSA scheme and compute public key "e". Then perform the following:

1. Sign and verify a message with M1=100, which is S1
2. Sign and verify the message with M2=50, which is S2.
3. Show that if M=M1*M2=5000 then S=S1*S2.

B) Consider plaintext block of all 0's and key of all 0's and assuming DES is designed for only one round. What will happen if the plain text and the key are complemented? (3)

C) Demonstrate the usage of Salting the password with its necessary requirements. (2)

2) Consider the following digital signature scheme using symmetric encryption technique. For the signature generation of an 'n' bit message, the sender produces 2n, 56 bit secret cryptographic keys:k_1, K_1, k_2, K_2,.....k_n, K_n. The sender also generates two sets of corresponding non secret 64 bit public validation parameters: u_1, V_1, u_2, V_2...u_n, V_n and v_1, V_1, v_2, V_2....v_n, V_n where $v_i=E(k_i, u_i)$ and $V_i=E(K_i,U_i)$. The signature for an input message is produced based on the 'i'th bit of the message where, ki or Ki is attached to the message based on whether message bit is 0 or 1. (If 1st 2 bits of message are 01 then first 2 keys of the signature are k_1, K_2.) (5)

A)

i. Explain how the signature is validated at the receiver side?

ii. Is the technique is safe from any attacks? Justify.

iii. For various messages, how many times the same set of secret keys can be used without any severe problems?

B) Compare the trust model and mesh model of public key Infrastructure. (3)

C) Can a firewall block attacks that use server scripts, such as the attack in which the user could change a price on an item offered by an e-commerce site? Justify your answer. (2)

3) In real life applications, the text to be enciphered is of variable size and normally much larger than the block size defined for modern block ciphers. Modes of operations have been devised to encipher text of any size employing modern block ciphers. Discuss these modes and also evaluation metrics used. (5)

A)

	B)	Suppose Alice chooses p=823 and q=953 and computes n and Ø(n). She chooses e=313 and d=16009. She wants to send the message 19070 to Bob. She sends the message and signature to Bob. Will Bob accept the message? Justify.	(3)
	C)	Differentiate between AES (with 10 rounds) and Whirlpool techniques.	(2)
4)		The problem with Elgamal digital signature scheme is the very large prime p to guarantee that the discrete log problem is intractable in Zp *. This could make signature as large as 2048 bits. Which new scheme is developed based on Elgamal Digital Signature to handle this ? How is this handled?	(5)
	A)		
	B)	In Feige-Fiat-Shamir protocol what is the probability that a dishonest claimant correctly responds to the challenge 15 times in a row.	(3)
	C)	Alice can use only additive ciphers on her computer to send a message to a friend. She thinks that the message is more secure if the message is encrypted twice with a different key. Interpret the implications of above plan? Justify.	(2)
5)		Using Elgamal signature scheme, find the signatures and verify the same, for the following data. Consider p=881, private key=127, random integer=17 and the message to be transmitted is 400. Use the first primitive root for the computation.	(5)
	A)		
	B)	Eve secretly gets access to Alice's computer and using her system types "abcdefghij". The screen displays "CABDEHFGIJ". If the attacker knows that Alice is using a keyed transposition cipher: i. Identify the type of attack Eve is launching. ii. Find out the size of the permutation key.	(3)
	C)	Compare the computation of MAC in SSL and TLS. Which one is more efficient?	(2)

-----End-----