B.E./B.TECH. Degree Examination, September 2020

Semester - VIII

CS16701 CRYPTOGRAPHY AND NETWORK SECURITY

(Regulation 2016)

Time: Three hours Maximum : 80 Marks

Answer **ALL** questions

PART A - (8 X 2 = 16 marks)

1. For c = (p+2x) mod 26, where c, p, and x are the ciphertext, the plaintext, and the key, respectively, what is the corresponding decryption? Select all that works.
   a) p = (c+26-2x) mod 26 b)p = (c-x) mod 26 c) p = (c-x) mod 13 d)p = (c-2x) mod 13
2. Triple-DES or 3-DES encryption can be characterized by the following: C=Enc(K3,Dec(K2,Enc(K1,P))). Each keys, K1, K2, K3 are 56-bits-long and are independent to each other (the three-key version). The DES block size is 64 bits. Using the big O notation, which of the following best describe the meet-in-the-middle attacker's encryption/decryption computational effort?
   a) O(2^128)
   b) O(2^56)
   c) O(2^112)
   d) O(2^168)
3. Which of the following statements are true about digital signature?
   a) Digital signature is typically smaller than the data size.
   b) Digital signature is functionally equivalent to message authentication (and is used when symmetric keys are not available)
   c) Digital signature is based on asymmetric/public-key cryptography
   d) Digital signature protects the confidentiality of the data
4. Which among the following is correct?
   i. Network firewalls are a software appliance running on general purpose hardware or hardware based firewall computer appliances that filter traffic between two or more networks.
   ii. Host - based firewalls provide a layer of software on one host that controls network traffic in and out of that single machine
   a) Only i
   b) Only ii
   c) Both i and ii
   d) Both are wrong
5. Find GCD (1970,1066) using Euclid's Algorithm.
6. Why do some block cipher modes of operation only use encryption while others use both encryption & decryption ?
7. In what ways can a hash value be secured so as to provide message authentication?
8. Assume the client C wants to communicate server S using Kerberos procedure. How can it be achieved?

PART B - (4 X16 = 64 marks)

09. (a) Solve the set of Congruences using Chinese Remainder Theorem. Find the value of X. **(16)**

$$X \equiv 1 \bmod 5$$
$$X \equiv 2 \bmod 7$$
$$X \equiv 3 \bmod 9$$
$$X \equiv 4 \bmod 1$$

(OR)

(b) Compare and contrast the traditional security models with suitable examples. **(16)**

10. (a) Using RSA Digital Signature Scheme, let p=5, q=11, n=9 and d=27. Calculate the following: **(16)**

(i) Public key e
(ii) Signature S at the sender

Re-compute the message at the receiver and decide to accept, if both are matching.

(OR)

(b) Consider a scenario of digital world-war and it is decided to use minimum of 192 bit scheme between the superior and the soldier. Identify and explain the algorithm with neat diagram. **(16)**

11. (a) With a neat sketch and process, Explain and demonstrate how MD5 is having extended features than SHA algorithm. **(16)**

(OR)

(b) A cryptosystem uses the private and public keys of the receiver. But, a digital signature uses the private and public keys of the sender. Consider an ElGammal Digital Signature Scheme, Alice sending a message M=120. Alice chooses $p = 3119$, $e_1 = 2$, $d = 127$ and calculates e_2. She also chooses r to be 297. She announces e*1*, e*2*, and p publicly; she keeps d secret. Compute the various stages of outputs at both (i) Signing. (ii) Verifying. **(16)**

12. (a) Design suitable packet filter rule sets to be implemented on the External Firewall and the Internal Firewall to satisfy the aforementioned policy requirements. **(16)**

(OR)

(b) Client and server are mutually authenticated, with neat sketch identify and explain the protocol in detail. **(16)**