CE4-R3: NETWORK SECURITY & CRYPTOGRAPHY

NOTE:

1. **Answer question 1 and any FOUR questions from 2 to 7.**
2. **Parts of the same question should be answered together and in the same sequence.**

Time: 3 Hours **Total Marks: 100**

1.

a) In cryptography, a cipher is an algorithm for performing encryption and decryption — a series of well-defined steps that can be followed as a procedure. Explain with example, what is a substitution cipher.

b) A block cipher operates on blocks of fixed length, often 64 or 128 bits. How output feedback (OFB) mode makes a block cipher into a synchronous stream cipher?

c) The International Data Encryption Algorithm (IDEA) is a block cipher intended as a replacement of Data Encryption Standard. Explain, how does an IDEA operate on 64-bit blocks using a 128-bit key?

d) A pseudorandom process is a process that appears random but it is not. What is a pseudorandom sequence in a pseudorandom process? What is a cryptographically secure pseudorandom sequence?

e) "Strong primes" are prime numbers with certain properties that make their product difficult to factor by specific factoring methods. Explain the properties to be satisfied by the strong prime numbers.

f) S/MIME (Secure / Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of e-mail encapsulated in MIME. Which are the cryptographic security services for electronic messaging applications provided by S/MIME?

g) What is a Secure Electronic Transaction (SET) and why is it failed to win market share as a credit card approved standard?

(7x4)

2.

a) In cryptography, MD5 (Message-Digest algorithm 5) is a widely used cryptographic hash function with a 128-bit hash value. Explain MD5 algorithm and its working in detail.

b) A digital signature or digital signature scheme is a type of asymmetric cryptography used to simulate the security properties of a signature in digital, rather than written form. Discuss the benefits and drawbacks of it?

(10+8)

3.

a) Kerberos is the name of a computer network authentication protocol, which allows individuals communicating over an insecured network to prove their identity to one another in a secured manner. Explain the Kerberos operations in detail.

b) What is IPSec and what are the two modes of IPSec operation? What types of security services are provided by IPSec?

(10+8)

4.

a) Explain the Diffe-Hellman algorithm for establishing a shared secret over an unprotected communication channel. Provide an example to illustrate the working of this algorithm.

b) A Feistel cipher is a block cipher with a particular structure. Explain briefly the basic encryption and decryption operations of it.

c) Briefly explain Euclid's algorithm to determine the greatest common divisor (GCD) of two elements of any Euclidean domain (for example, the integers).

(10+4+4)

5.

a) RC4 is the most widely-used software stream cipher and is used in popular protocols such as Secure Sockets Layer and WEP. Explain, how pseudorandom stream of bits are generated using RC4.

b) X.400 is a suite of ITU-T Recommendations that define standards for Data Communication Networks for Message Handling Systems (MHS).Explain various elements that X.400 address consists of.

(8+10)

6.

a) What is public key infrastructure? Briefly explain the purposes and functions of a public key infrastructure (PKI) in cryptography.

b) X.509 is an ITU-T standard for public key infrastructure (PKI) and specifies standard formats for public key certificates. Briefly explain the structure of the certificate.

c) What is transport layer security? What are the threats from which it prevents an application to communicate across a network?

(4+8+6)

7.

a) Permutation is the rearrangement of objects or symbols into distinguishable sequence. Briefly explain the algorithm to generate permutations.

b) Explain the electronic code book (ECB) encryption mode which allows block ciphers to provide confidentiality for messages of arbitrary length.

c) What is a 'salt' in context of UNIX password management? Explain.

(6+6+6)