C8-R4: INFORMATION SECURITY

NOTE:

1. **Answer question 1 and any FOUR from questions 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) What are the key principles of security? Explain with help of an example.

b) What is access control? How different is it from availability?

c) A message has 2000 characters. If it is supposed to be encrypted using a block cipher of 64 bits, find the size of the padding and the number of blocks.

d) Compare DES and AES. Which one is bit oriented? Which one is byte oriented?

e) List important design consideration for a stream cipher. Why is it not desirable to reuse a stream cipher key?

f) Random numbers play an important role in the use of encryption for various network security applications. These applications give rise to two distinct requirements for a sequence of random numbers: randomness and unpredictability. Explain the importance of each requirement in network security applications.

g) Define a trapdoor one way function and explain its use in asymmetric key cryptography.

(7x4)

2.

a) Using the Euclidean algorithm, find the greatest common divisor of the following:
   i) 300 and 42
   ii) 88 and 220

b) What is triple DES? What is triple DES with two keys? What is triple DES with three keys?

c) In Cipher Feedback Mode (CFB), how many blocks are affected by a single bit error in transmission?

(6+6+6)

3.

a) Define linear congruence. What algorithm can be used to solve an equation of type $ac \equiv b \pmod{n}$? How can we solve a set of linear equations?

b) Distinguish between message integrity and message authentication.

c) Find the results of the following, using Fermat's little theorem.
   i) $5^{15} \bmod 13$
   ii) $15^{1} \bmod 17$

(4+6+8)

4.

a) Rita has a long message to send. She is using monoalphabetic substitution cipher. She thinks that if she compresses the message, it may protect the text from single-letter frequency attack. Does the compression help? Should she compress the message before the encryption or after the encryption? Defend your answer.

b) Which parameters and design choices determine the actual algorithm of a Feistel cipher?

c) Distinguish between a session and a connection in SSL protocol. List the four protocols in SSL with their purpose.

(4+7+7)

5.

a) Use the playfair cipher to encipher the message “The key is hidden under the door pad”. The secret key can be made by filling the first and part of the second row the word “GUIDANCE” and filling the rest of the matrix with the rest of the alphabet.

b) What are the requirements of public key cryptography system? Explain the characteristic of public key cryptography.

c) Compare the digital signature and conventional signature with respect to following four parameters: Inclusion, Verification, Relation, and Duplicity.

(6+6+6)

6.

a) Distinguish between differential and linear cryptanalysis. Which one is a chosen plaintext attack? Which one is a known plaintext attack?

b) List the main features of the SHA-512 cryptographic hash function. What kind of compression function is used in SHA – 512?

c) List and briefly define types of cryptanalytic attacks based on what is known to the attacker.

(4+8+6)

7.

a) In the Diffie- Hellman protocol, what happens if x and y have same value, that is Rita and Shyam have accidentally chosen the same number? Are R1 and R2 the same? Do the session keys calculated by Rita and Shyam have the same value? Give an example to prove your claims.

b) Give example of replay attacks. List and explain three general approaches to dealing with replay attacks.

c) Differentiate between statistically random numbers and pseudo random number. Write and explain the ANSI X9.17 Pseudorandom Number Generator.

(6+6+6)