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) Compare and contrast attacks on digital signatures with attack on cryptosystem.

b) Distinguish between public and private keys in an asymmetric key cryptosystem. Compare and contrast the keys in symmetric key and asymmetric key cryptosystems.

c) Define cryptographic hash function. Explain three criterions for a cryptographic hash function.

d) Which security mechanism(s) are provided in each of the following cases?
   i) A company demands employee identification and a password to let employee log into the company server.
   ii) A company server disconnects an employee, if he is logged into the system for more than two hours.
   iii) A teacher refuses to send students grades by email unless they provide identification assigned by the teacher.
   iv) A bank requires the customer's signature for a withdrawal.

e) List the main characteristics of the SHA 512 cryptographic hash function.

f) Define a session key and show how a KDC can create a session key between Alice and Bob.

g) AES has a larger block size than DES. Is this an advantage or disadvantage? Explain.

(7x4)

2.

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

b) Compare DES and AES. Which one is bit-oriented? Which one is byte oriented? Why only one substitution table (S box) is needed in AES but several in DES? Why are expansion and compression permutations required in DES, but not in AES?

c) Briefly answer following questions with respect to ElGamal cryptosystem:
   i) What is the one way function in this system?
   ii) What is the trapdoor in this system?
   iii) Define the public and private keys in this system.
   iv) Describe the security of this system.

(4+6+8)

3.

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

b) i) What is the role of compression and encryption in the operation of a virus?
   ii) What is the difference between an unconditionally secure cipher and a computationally secure cipher?

c) Which security service(s) are guaranteed for each of the following methods used to send mail at the post office?
   i) Regular mail
   ii) Regular mail with delivery conformation
   iii) Regular mail with delivery and receipt signature
   iv) Certified mail
   v) Insured mail
   vi) Registered mail

(6+6+6)

4.

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

b) Explain with neat sketch ANSI X9.17 Pseudorandom Number Generator. Which factors contribute to the cryptographic strength of this method?

(8+10)

5.

a) Explain how does symmetric encryption approach used to give assurance to recipient that the message is from the alleged sender using one way authentication function.

b) The exact realization of a Fiestel network depends on the choice of the following parameters and design features: Block size, Key size, Number of rounds, Sub key generation algorithm, Round function, Fast software encryption/decryption, Ease of analysis. Explain significance of each of the parameter.

(9+9)

6.

a) i) Show the result of 3 bit circular left shift on word $(10011011)_2$.
   ii) Show the result of 3 bit circular right shift on the word resulting from part 1.
   iii) Compare the result of part 2 with the original word in part 1. Comment on your answer.

b) Using Fermat's Little theorem, find the results of the following:
   i) $5^{15} \bmod 13$
   ii) $15^{18} \bmod 17$

c) What are the requirements of public key cryptography system? Explain the characteristics of public key cryptography.

(6+6+6)

7.

a) What are the limitations of message authentication? Explain properties and requirements of digital signature.

b) Explain basic structure of stream cipher. List and explain important design considerations for a stream cipher.

c) Encrypt the message "the house is being sold tonight" using Vigenere cipher with key: "dollars". Ignore the space between words. Decrypt the message to get the plaintext.

(6+8+4)