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 do you understand by security attacks, security mechanism and security services? Explain and define each of them.

b) Cryptographic algorithms and protocols can be grouped into four main areas. Briefly explain each of them.

c) Define the following terms.
   i) Cipher
   ii) Deciphering
   iii) Cryptography
   iv) Cryptanalysis

d) Fill in the blanks by choosing the appropriate options given.
   1. Modular arithmetic is a kind of integer arithmetic that reduces all numbers to one of a fixed set [0,…, n -1] for some number n. Any integer outside this range is reduced to _____ in this range by taking the remainder after division by n.
   2. A field is a set of elements on which two arithmetic operations (addition and multiplication) have been defined and which has the properties of ordinary arithmetic, such as closure, associativity, commutativity, distributivity, and having both additive and multiplicative _____.
   3. Finite fields are important in several areas of cryptography. A finite field is simply a field with a finite number of elements. It can be shown that the order of a finite field (number of elements in the field) must be a power of a prime p^n, where n is a _____ integer.
   4. Finite fields of order p^n, for n > 1, can be defined using arithmetic over _____. Choose the appropriate answer from [one, largest, inverses, mod, numbers, positive, negative, polynomials, smallest, greatest, two]

e) What is Advanced Encryption Standard (AES)? What are the four separate functions it uses during each full round?

f) A mode of operation is a technique for enhancing the effect of a cryptographic algorithm or adapting the algorithm for an application. What are the five modes of operation have been standardized by NIST for use with symmetric block ciphers such as DES and AES?

g) A number of network security algorithms and protocols based on cryptography make use of random binary numbers. Give any two examples and explain in brief.

(7x4)

2.

a) What are the different uses of random numbers in network security algorithm?

b) What do you understand by divisibility? Explain the Division algorithm in detail.

(8+10)

3.

a) To overcome the security deficiencies of ECB, a technique in which the same plaintext block, if repeated, produces different ciphertext blocks. A simple way to satisfy this requirement is to use the cipher block chaining (CBC) mode. Explain CBC with example.

b) Euclidean algorithm is a simple procedure for determining the greatest common division of two positive integers. Explain the algorithm in details.

(10+8)

4.

a) Differentiate between:
   i) TRNG = true random number generator
   ii) PRNG = pseudo random number generator
   iii) PRF = pseudo random function

b) In the context of communications across a network, what are the different types of attacks that can be identified? List each of them and explain in brief.

(9+9)

5.

a) Explain the processing steps of any SHA logic. Explain each step in detail.

b) Briefly explain the generic model of Digital Signature process.

(12+6)

6.

a) A simple public-key algorithm is Diffie-Hellman key exchange. This protocol enables two users to establish a secret key using a public-key scheme based on discrete logarithms. Explain the algorithm in detail.

b) What are the security requirements for cryptographic Hash function?

(12+6)

7.

a) Explain the EIGamal Cryptosystem in detail with example. Also demonstrate why this scheme will work?

b) Briefly explain the symmetric encryption scheme.

(10+8)