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) Define linear congruence. What algorithm can be used to solve an equation of type ax ≡ b (mod n)? How can a set of linear equations be solved?

b) Explain the two basic criteria used to validate that a sequence of numbers is random.

c) Explain in brief the basic structure of stream cipher.

d) What is the difference between passive and active security threats? List and briefly define categories of passive and active security attacks?

e) Given p=19, q=23 and e=5, find n, ø(n) and d using RSA cryptography algorithm.

f) Differentiate between data origin authentication and entity authentication.

g) Match the following:

No	Description	No	Security Mechanism
1	A company demands employee identification and a password to let employee log into the company server.	A	routing control
2	A company server disconnects an employee, if he is logged into the system for more than two hours.	B	digital signature
3	A teacher refuses to send students grades by email unless they provide identification assigned by the teacher.	C	access control
4	A bank requires the customer’s signature for a withdrawal.	D	authentication exchange

(7x4)

2.

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

b) 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.

(10+8)

3.

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

b) A small private club has only 100 members. Answer the following questions.

  i) How many secret keys are needed if all members of the club need to send secret messages to each other?

  ii) How many secret keys are needed if everyone trusts the president of the club? If a member needs to send a message to another member, she first sends it to the president; the president then sends the message to the other member.

  iii) How many secret keys are needed if the president decides that the two members who need to communicate should contact him first? The president then creates a temporary key to be used between the two. The temporary key is encrypted and sent to both members.

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

(8+6+4)

4.

a) What are three broad categories of applications of public key cryptosystems? What requirements must a public key cryptosystem fulfill to be a secure algorithm?

b) List four techniques used by firewalls to control access and enforce a security policy.

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

(8+6+4)

5.

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

b) List and briefly define the parameters that define an SSL session state and session connection.

(9+9)

6.

a) Briefly explain the following idea behind the RSA 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.

b) X.800 defines a security service as a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers. List and explain Authentication Access Control, Data Confidentiality, Data Integrity and Non-repudiation services provided by the X.800.

(8+10)

7.

a) 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

b) List and briefly define four techniques used to avoid guessable passwords.

c) 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.

(6+6+6)