Seat No.

Total No. of Pages : 3

OCT-NOV 2025 WINTER EXAMINATION

1154 B.Tech. CBCS

Sub. Name: Information Security

Sub. Code: 80798/81037

Day and Date: Friday ,12-12-2025 **Total Marks: 70**

Time: 02:30 PM To 05:00 PM

Instructions:
1. **All questions are compulsory**
2. **Draw neat labelled diagrams wherever necessary**
3. **Figures to the right indicate full marks**
4. **Use of Scientific calculator is allowed**

Q1) Solve MCQs. (2 Marks Each) **[14]**

A. ---------- Is To Protect Data And Passwords **[2]**

A. Encryption
B. Authentication
C. Authorization
D. Non Repudiation

B. Encryption is currentlyconfinedto key management and ---------- public key **[2]**

A. Digital signature
B. Encryption decryption
C. Signature applications
D. None of these

C. A varietyof approaches has been proposedfor the digitalsignature function. These approaches fall into two categories _____. **[2]**

A. Direct and arbitrated
B. Indirect and arbitrated
C. Direct and indirect
D. None of the above

D. Pretty Good Privacy (PGP) provides ---------- **[2]**

A. confidentiality, integrity, and authenticity.
B. integrity, availability, and authentication
C. availability, authentication, and non-repudiation.
D. authorization, non-repudiation, and confidentiality

E. At the lower layer of SSL, a protocol for transferring data using a variety of pre defined cipher and authentication combinations called the ……. **[2]**

A. SSL handshake protocol
B. SSL authentication protocol
C. SSL record protocol
D. SSL cipher protocol

F. Point out the correct statement. **[2]**

A. Parameterized data cannot be manipulated by a skilled and determined attacker
B. Procedure that constructs SQL statements should be reviewed for injection vulnerabilities
C. The primaryform of SQL injection consists of indirect insertion of code
D. None of the mentioned

G. ----------Prevents Either Sender Or Receiver From Denying A Transmitted Message **[2]**

A. Non Repudiation
B. Data Integrity
C. ActiveAttack
D. Passive Attack

Q2) Solve any 2 of the following (7 Marks Each) **[14]**

a. Explain different types of attacks with example. **[7]**

b. Explain X.800 Security services. **[7]**

c. Explain applications and requirements of public key cryptography. **[7]**

Q3) Solve any 2 of the following (7 Marks Each) **[14]**

a. Explain RSA algorithm with example. **[7]**

b. Explain arbitrated and direct digital signature. **[7]**

c. Explain RSA and DSS approaches to digital signature? **[7]**

Q4) Solve any 2 of the following (7 Marks Each) **[14]**

a. Explain 5 services of PGP. **[7]**

b. What is MIME And S/MIME. **[7]**

c. Explain SSL Architecture. **[7]**

Q5) Solve any 2 of the following (7 Marks Each) **[14]**

a. Explain SSL Record Protocol. **[7]**

b. Explain DOS and DDOS attack. **[7]**

c. Explain ARP Spooing with neat diagram. **[7]**

End Of Question Paper

Important Note for Chief Exam Officer / SRPD Coordinator / Sr Supervisor/ Student -
This Question Paper may be distributed for following Subjects as common code.
सदरची प्रश्नपत्रिका खालील विषयांकरिता वितरित करता येईल.

1] (101) Bachelor of Engineering (81037) Information Security Part 3 SEM 5
2] (1154) B.Tech. CBCS (80798) Information Security Part 3 SEM 5