## Guru Nanak Dev Engineering College, Ludhiana

### Department of Information Technology

| | | | |
|---|---|---|---|
| Program | B.Tech. (IT) | Semester | 5th |
| Subject Code | PEIT-105 | Subject Title | Cryptography |
| Mid Semester Test (MST) No. | 1st | Course Coordinator | Dr. Sidharath Jain |
| Max. Marks | 24 | Time Duration | 1.30 hrs |
| Date of MST | | University Roll Number | |

Note: Attempt all questions MM: 24

| Q. No. | Question | COs, RBT level | Marks |
|---|---|---|---|
| Q1 | Describe the term Cryptanalysis. | CO1, L2 | 2 |
| Q2 | Draft and organize the model of Secure Communication. | CO1, L4 | 2 |
| Q3 | Explain any two substitution techniques through respective examples. | CO2, L2 | 4 |
| Q4 | Elaborate the importance of Asymmetric Key Cryptography in detail. | CO1, L1 | 4 |
| Q5 | Explain in detail Chinese Remainder Theorm. | CO2, L6 | 4 |
| Q6 | Find the multiplicative inverse of 3 mod 5 using Extended Euclidian's Algorithm. | CO2, L6 | 8 |

Course Outcomes (CO)

*Students will be able*

| | |
|---|---|
| 1 | Understand modern concepts related to cryptography and cryptanalysis. |
| 2 | Analyze and use methods for cryptography and reflect about limits and applicability of these methods. |
| 3 | To define the system to protect determines the security properties that are desired for this system identify the possible threats to these security properties, their likelihood of occurrence and consider possible mitigations against these threats. |
| 4 | Describe and implement of some of the prominent techniques for public-key cryptosystems and digital signature schemes (e.g., Rabin, RSA, ElGamal, DSA, Schnorr) |
| 5 | Explain the notions of public-key encryption and digital signatures and sketch their formal security definitions. |

| RBT Classification | Lower Order Thinking Levels (LOTS) | | | Higher Order Thinking Levels (HOTS) | | |
|---|---|---|---|---|---|---|
| RBT Level Number | L1 | L2 | L3 | L4 | L5 | L6 |
| BT Level Name | Remembering | Understanding | Applying | Analyzing | Evaluating | Creating |

## Guru Nanak Dev Engineering College, Ludhiana

### Department of Information Technology

| | | | |
|---|---|---|---|
| Program | B.Tech (IT) | Semester | 5th |
| Subject Code | PEIT-105 | Subject Title | Cryptography |
| Mid Semester Test (MST) No. | 1st | Course Coordinator | Dr. Sidharath Jain |
| Max. Marks | 24 | Time Duration | 1.30 hrs |
| Date of MST | | Univ. Roll No. | |

MM: 24

Note: Attempt all questions

| Q. No. | Questions | COs, RBT level | Marks |
|---|---|---|---|
| Q1 | Define Digital Certificates in brief with its importance. | CO5, L1 | 2 |
| Q2 | Evaluate the term SSL with an example. | CO5, L5 | 2 |
| Q3 | Determine the importance of Secure Electronic Transaction(SET) & Email security. | CO3, L2 | 4 |
| Q4 | Write a short note on IP Security. | CO4, L3 | 4 |
| Q5 | Explain the concept of Hash Functions and its applications. | CO4, L4 | 4 |
| Q6 | Explain the structure of RSA algorithm in detail. | CO4, L4 | 8 |

*Course Outcomes (CO)*
*Students will be able*

| | |
|---|---|
| 1 | Understand modern concepts related to cryptography and cryptanalysis. |
| 2 | Analyze and use methods for cryptography and reflect about limits and applicability of these methods. |
| 3 | To define the system to protect determines the security properties that are desired for this system identify the possible threats to these security properties, their likelihood of occurrence and consider possible mitigations against these threats. |
| 4 | Describe and implement of some of the prominent techniques for public-key cryptosystems and digital signature schemes (e.g., Rabin, RSA, ElGamal, DSA, Schnorr) |
| 5 | Explain the notions of public-key encryption and digital signatures and sketch their formal security definitions. |

| RBT Classification | Lower Order Thinking Levels (LOTS) | | | Higher Order Thinking Levels (HOTS) | | |
|---|---|---|---|---|---|---|
| RBT Level Number | L1 | L2 | L3 | L4 | L5 | L6 |
| RBT Level Name | Remembering | Understanding | Applying | Analyzing | Evaluating | Creating |

o. of Questions: 09]

Uni. Roll No. .220388]......

S-214

[Total No. of Pages: 01]

Program: B.Tech. (Batch 2018 onward)
Semester: 5
Name of Subject: Cryptography
Subject Code: PEIT-105
Paper ID: 16448
Scientific calculator is Not Allowed.

Time Allowed: 03 Hours

Max. Marks: 60

NOTE:

1) Parts A and B are compulsory
2) Part-C has Two Questions Q8 and Q9. Both are compulsory, but with internal choice
3) Any missing data may be assumed appropriately

## Part – A

Q1. [Marks: 02 each]

a) Define cryptography and cryptanalysis.
b) List the key services provided by secure communication.
c) What are the advantages of modular arithmetic in cryptography?
d) Why is collision resistance important in hash functions?
e) Differentiate between PKCS and PKI.
f) Discuss the collision vulnerability in older hashing algorithms like MD5.

## Part – B

[Marks: 04 each]

Q2. Explain the concept of key management in public-key cryptography.

Q3. Illustrate the role of Kerberos in authentication.

Q4. Solve an example using AES to encrypt a block of plaintext.

Q5. Evaluate the effectiveness of elliptic curve cryptography in resource-constrained devices.

Q6. Justify the use of PGP for email encryption despite the availability of alternatives.

Q7. Critique the use of substitution ciphers in real-world scenarios.

## Part – C

[Marks: 12 each]

8. Demonstrate how to encrypt and decrypt data using DES.

OR

Illustrate the use of Euclidian and Extended Euclidian algorithms in the real-world scenario.

9. Justify the importance of RC4, RC5 and Blowfish in modern cryptographic protocols.

OR

Evaluate the practicality of the Chinese Remainder Theorem in cryptographic systems.

************