

JK Lakshmipat University Jaipur
INSTITUTE OF ENGINEERING AND TECHNOLOGY

End Term Examination (Backlog), May-2019
B. Tech. in Computer Science and Engineering, Semester VI

Roll No.....

CSE 621 : Information Security

Time: 3 hours

Max. Marks: 100

Instructions to students:

1. Do not write anything other than your roll number on question paper.
2. Assume suitable data wherever required and mention it clearly.
3. Writing appropriate units, nomenclature, and drawing neat sketches/schematics/flow chart wherever, required are an integral part of the answer. NO SCIENTIFIC OR OTHER TYPES OF CALCULATORS ALLOWED IN THIS EXAM PAPER TO THE STUDENTS. NO LOG BOOKS ALLOWED FOR THIS EXAM.

- Q.1 Objective type - (multiple choice questions) [*Only one option is correct*]: 10
- i.) The most secure symmetric cipher of the following options:
 - A.) AES
 - B.) RSA
 - C.) Triple DES
 - D.) None of the Above Options are Correct.
 - ii.) The most commonly used public key cryptographic algorithm is:
 - A.) El Gamal
 - B.) AES
 - C.) RC6 Cipher
 - D.) RSA
 - iii.) What is not true about Hash Functions?
 - A.) Non - Collision Resistance
 - B.) Non - Irreversible Functions
 - C.) Non - Compression Functions
 - D.) All of the Above Options are Correct.
 - iv.) The purpose of a MAC algorithm is to provide:
 - A.) Authentication
 - B.) Authorization and Availability
 - C.) Non-Repudiation
 - D.) Confidentiality and Privacy
 - v.) Which one of these is based on the principles of Public Key Cryptography and PKI:
 - A.) Hashed - MAC
 - B.) Electronic Code Block (ECB)
 - C.) Digital Signature Standard (DSS)
 - D.) Cyber Block Chaining (CBC)

- vi.) Original Message after being transformed is called as:
 - A.) Plain Text
 - B.) Cipher Text
 - C.) Decrypted Text
 - D.) None of the above
- vii.) OTP (One Time Pad) is a type of:
 - A.) Public Key Cipher
 - B.) Hybrid Cipher
 - C.) Private Key Cipher
 - D.) Classical Cipher
- viii.) PGP is a protocol/ technique used for:
 - A.) Web Application Security
 - B.) Client Side Security
 - C.) Email Security
 - D.) Server Side Security
- ix.) The technique which is used to exchange keys in symmetric key cryptography by the parties involved in secure communication is called:
 - A.) Diffie-Hellman Key Exchange Mechanism
 - B.) Public Key Distribution
 - C.) Private Key Distribution
 - D.) All of the above options are correct
- x.) Which one of these are features of Systems Security:
 - A.) Intrusion Detection Systems
 - B.) Intrusion Prevention Systems
 - C.) Firewalls and DMZ
 - D.) All of the above options are correct

Q2 Short answer type questions:

- i. Given the two prime numbers $p=11$, and $q=17$; calculate the value of $\phi(n)$ and also describe the key generation algorithm in RSA using the above given information. ($e = 7$). Also find the Decryption Key. 10
- ii. Encrypt the given plain text 'T' or 't' using RSA. The give data is; the two prime number $p=2$, and $q =3$, encryption key (PU) = {5, 6}. Elucidate, is the given data enough to encrypt using RSA algorithm. If not then why? And if Yes then Encrypt the plain text. 5

- Q.3A Describe the DES algorithm mathematically and in your own words. Describe its structure and it's working. What is the importance of DES function? 10
- Q.3B What are Birthday Attacks? How do they work? Give examples to support your answer. 5
- Q.4A What do you understand by SSL (Secure Socket Layer)? How is it Implemented? What is Open SSL? 10
- Q.4B Describe the structure of X.509 Digital Certificate. 5
- OR
- Q.4B What do you understand by the term 'KERBEROS' and PGP with respect to security of data and messages? Give examples to support your answer. 5
- Q.5A Differentiate between MAC and HMAC. List Five differences with examples to better explain your answer. What do you understand by SHA or Secure Hashing Algorithm? Give Examples in support of your answer. 10
- OR
- Q.5A What do you understand by IP Security? Elaborate on it with the help of examples. What is VPN (Virtual Private Network)? Differentiate VPN and IPsec. 10
- Q.5B What do you understand by a Group? What do you understand by a Field? Differentiate between them. Also, differentiate between prime numbers and relative prime numbers. (*Hint: These are Mathematical Terms relating to Number Theory and Group Theory in Mathematics*). 10
- Q.6 Explain in detail with the help of examples Fermat's Theorem and Euler's Theorem. 10
- Q.7 Explain in detail with the help of examples the Chinese Remainder Theorem. 10
- Q.8 Write Short Notes on the following (give examples to support your answer): 10
- i) Cryptanalysis
 - ii) Steganography
 - iii) Stream and Block Ciphers

10

11

12