

JK Lakshmipat University Jaipur
INSTITUTE OF ENGINEERING AND TECHNOLOGY

End Term Examination (Regular), April- May 2016
M.Tech in Computer Science Engineering, Semester II



Roll No.....

MTCS202: COMPUTER AND NETWORK SECURITY

Time: 03 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.

Q.1A Objective type multiple choice questions (10 questions @ 1 mark)

10

- i. The linear cryptanalysis can find DES key knowing
 - A. 2^{47} bits of known plaintext
 - B. 2^{46} bits of known plaintext
 - C. 2^{45} bits of known plaintext
 - D. 2^{43} bits of known plaintext
- ii. The hash function Whirlpool is based on components of which algorithm?
 - A. DES
 - B. Triple-DES
 - C. AES
 - D. Serpent
- iii. The difficulty of attacking RSA is based on the difficulty of:
 - A. Finding a discrete logarithm value
 - B. Finding the prime factors of a composite number
 - C. Inversion problem in finite fields
 - D. Multiplication of big integers
- iv. In the firewall terminology, DMZ denotes:
 - A. Data Moving Zombie
 - B. Data Management Zone
 - C. Demilitarized zone
 - D. Demonized protection
- v. OAEP (Optimal Asymmetric Encryption Padding) is a technique applied to:
 - A. PKI
 - B. Diffie-Hellman
 - C. ECC
 - D. RSA
- vi. According to the OSI security architecture, "Security service" is:
 - A. PKI
 - B. A security database server
 - C. A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization.
 - D. A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
- vii. Which algorithms for digital signatures are used in S/MIME?
 - A. ECC and RSA
 - B. DSS and RSA
 - C. ECC and DSS
 - D. ECC and Diffie-Hellman
- viii. An S-box satisfies the following criterion: For a 1-bit input change, at least n output bits change. We say that the S-box satisfies the
 - A. Bit change criterion
 - B. Bijection criterion
 - C. Diffusion criterion
 - D. Guaranteed avalanche criterion
- ix. In computing the Message Authentication Codes both parties have to use

- A. the public key of the other party B. a shared secret key
C. two different secret keys D. the private key of the other party
- x. Which three functional areas are provided by IPSec?
A. Authentication, Confidentiality, and Key management
B. Authentication, Error detection, and Error correction
C. Authentication, Key generation, and Certificate exchange
D. Encryption, Decryption, and Certificate validation
- Q.2 Short answer type questions (4 questions @ 2.5 marks) 10
- i. What is a Feistel structure?
ii. Assuming that the 25 symbols a b c d e f g h i/j k l m n o p q r s t u v w x y z are randomly assigned to the cells of a 5 X 5 square, how many such squares are possible?
iii. What are the properties that digital signature must have?
iv. How big can be the key in AES, how many rounds have AES for each key, and how big is the block?
- Q.3A Users A and B want to establish a secret key using Diffie-Hellman key exchange protocol using a common prime $q=353$, a primitive root $\alpha=3$, A's secret key $X_A=97$ and B's secret key $X_B=233$. Compute 05
i. A's public key, Y_A
ii. B's public key, Y_B
iii. A's and B's common secret key, K
- Q.3B Determine the Playfair square for the following message that was enciphered with a Playfair cipher. 05
FZTOZ DGRNB ASCOQ YDOBK RZXXX CNTFD ULNZD LYZNG HVTZT
LUBDY UQOPY DNBQE RPSOK MMZQA XCIYD OZPCP UOZNO NCIXC
QKNVY DFOOH EN
The plaintext message begins "Australian coast watchers." (During World War II, the Australian coast watchers used Playfair ciphers.)
- Q.4A What are the five principal services provided by pretty good privacy? 05
Q.4B List three approaches to secure user authentication in a distributed environment? 05
- Q.5A Perform encryption and decryption using RSA Alg. for the following. $P=7$, $Q=11$, $e=17$, $M=8$. 05
Q.5B What is proof of submission delivery in network security applications? 05
- OR
- Q.5B True or false: The larger the size of the key space, the more secures a cipher? 05
Justify your answer.
- Q.6A Decode the following messages(Shift) which is encrypted using Caesar cipher 05
Adiy evhzn wjiy
- Q.6B Differentiate public key and conventional encryption? 05

Q.7A	How IPsec does offer the authentication and confidentiality services?	05
Q.7B	How does PGP provide confidentiality and authentication services for email and file storage applications?	05
OR		
Q.7B	What are the different between SSL version 3 and TLS?	05
Q.8A	What are viruses, worms and Trojan horse? Explain the various related threats and the counter measures applied?	10
Q.8B	What are the weakness of password and explain how should they be designed to avoid abusing a system?	05
OR		
Q.8B	Discuss the different types of firewall and its configurations.	05
Q.9A	Write short notes on: (Any Two) i) S/MIME ii) Kerberos iii) IP Security Architecture.	10
Q.9B	Why is SHA more secure than MD5?	05
OR		
Q.9B	What are the three benefits provided by IDS (Intrusion Detection System)?	05

