

JK Lakshmipat University Jaipur
INSTITUTE OF ENGINEERING AND TECHNOLOGY

End Term Examination (Regular), April 2018
B.Tech. in Computer Science and Engineering, Semester VI

Roll No.....

CSE621: INFORMATION 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. In the _____ mode, IPSec protects information delivered from the transport layer to the network layer.
A) Transport
B) either (a) or (b)
C) Tunnel
D) Neither (a) nor (b)
- ii. Which MAC is used in S/MIME?
A). CMAC with SHA-2
B). HMAC with SHA-1
C). HMAC with MD4
D). HMAC with MD5
- iii. Which of the following is software that allows you to gain administrative rights to someone's computer?
A) A bot
B). A worm
C). A rootkit
D). A Trojan horse
- iv. "When bogus reconfiguration commands are used to affect routers and switches to degrade network performance." Which type of Wireless network threat would you classify this under?
A). Man in the middle attack
B). Malicious Association
C). Network Injection
D). Denial Of Service
- v. 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
- vi. What is a one-way password file?
A). A scheme in which the password is jumbled and stored
B). A scheme in which the password is XOR with a key and stored
C). A scheme in which the hash of the password is stored

- D). A scheme in which the password is passed through a PRF, which is then stored
- vii. Which of the following is independent malicious program that need not any host program
 A) Trap doors B) Trojan horse
 C) Virus D) Worms
- viii. What is the number of operation required to come up with 2 messages having the same message digest in SHA-512?
 A). 2^{256} B). 2^{512}
 C). 2^{1024} D). 2^{128}
- ix. The _____ attack can endanger the security of the Diffie-Hellman method if two parties are not authenticated to each other.
 A) Known Ciphertext attack B) Man-in-the-middle attack
 C) Plaintext attack D) Known Plaintext attack
- x. In the handshake protocol which is the message type first sent between client and server?
 A). Server_hello B) Certificate_request
 C). hello_request D). Client_hello

Q.2 Short answer type questions (4 questions @ 2.5 marks)

10

- Discuss different classes of intruders?
- An ideal password authentication scheme has to withstand a number of attacks. Describe five of these attacks.
- Give features and weakness of Diffie Hellman key exchange algorithm?
- What is importance of confidentiality, Integrity and availability in security management?

Q.3A Alice and Bob use the Diffie-Hellman key exchange technique with a common prime $q=23$ and a primitive root $\alpha=9$.

05

- If Alice has private key $X_A=4$, what is A's public key Y_A ?
- If Bob has private key $X_B=3$, what is B's public key Y_B ?
- What is the shared secret key?

Q.3B What are various internet related threats? Explain the virus related threats and the counter measures applied?

05

Q.4A The following cipher text was encoded using a columnar transposition with keyword "BUBBLES" columns. Decode the message.

05

"SGTEAAN ETTRIOT GESCCRH ILBFEAE DEEETTU OSATYAW PTSTSDR
 OHIPSTO ETTNROE NSRLMRM YSIBTIE OTHAETC ENUTRNE LSETFHD
 IIOWEAE MDLAOHR INLHNSE"

Q.4B	Decrypt the following plaintext using Polyalphabetic (simple) substitution method and also find out Key- "CHMNY UXIZZ IWOMC HAIHN BYGUF QULYZ IWOMI HNBYU NNUWE YL"	05
Q.5A	The following was encrypted with a Playfair Cipher with keyword "BEHAVIOR". Decrypt the Cipher Text to original message. "EO UOKYF ABSQKWNP DXIPAMAAP FU QVH BBCP THVCDB KRC VEPCFYVPV PAIYCOSZ"	05
Q.5B	Answer the following questions on Message authentication: (a) What is message authentication? (b) Define the classes of message authentication function (c) What are the requirements for message authentication?	05
OR		
Q.5B	List the process steps of SHA and Explain the SHA-1 processing of a single 512-bit block and also give the single step operation?	05
Q.6A	Vigenere cipher is under consideration. Use the following tableau with key "ETHICAL" to decrypt the message - "XXJPP OWSZF BTUDX BZIIO ZHMOQ PGMYM JWPTC SEPAC BPXML ZQNP"	05
Q.6B	Draw the IP security authentication header and describe the functions of each field? Also develop applications and advantages of IPSec?	05
Q.7A	Bob has public RSA key ($n = 77$, $e = 13$) Alice wants to send the message $m = 7$ to Bob. She encrypts the message using Bob's public key. What is the value of the cipher text that Alice sends to Bob? Also find out Bob's private key?	05
Q.7B	Why internet banking database should be loaded with Intrusion monitoring software and how internet banking system can be made secure?	05
OR		
Q.7B	How does SET protect payment information from the merchant and how 3D secure is different from SET?	05
Q.8A	Explain the reasons for using PGP? Why E-mail compatibility function in PGP is needed? What are the services provided by PGP services?	10
Q.8B	Write the specific function of MAC in network security and Differentiate MAC and Hash function?	05
OR		
Q.8B	For the DES algorithm, find the output of the final permutation box when the	05

input to the box in hexadecimal is given as: 0x 0810 A4D0 320E 9B00.

- Q.9A What is a firewall and what are its limitations? Why do corporate houses implement more than one firewall for security? 10
- Q.9B When is a demilitarized zone (DMZ) required? And how it is implemented? 05
- OR
- Q.9B Estimate what is the role of intrusion detection system? What are the three benefits that can be provided by the intrusion detection system? 05