

JK Lakshmipat University Jaipur
INSTITUTE OF ENGINEERING AND TECHNOLOGY

End Term Examination (Regular), April- May 2015
B.Tech. in Computer Science and Engineering, Semester VI

Roll No.....

CSE621: 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. Pretty good privacy (PGP) is used in
 - a) browser security
 - b) email security
 - c) FTP security
 - d) none of the mentioned
- ii. Which one of the following is a cryptographic protocol used to secure HTTP connection?
 - a) stream control transmission protocol (SCTP)
 - b) transport layer security (TSL)
 - c) explicit congestion notification (ECN)
 - d) resource reservation protocol
- iii. The attackers a network of compromised devices known as
 - a) Internet
 - b) Botnet
 - c) Telnet
 - d) D-net
- iv. Cryptographic hash function takes an arbitrary block of data and returns
 - a) fixed size bit string
 - b) variable size bit string
 - c) both (a) and (b)
 - d) none of the mentioned
- v. One way to limit hostile sniffing on a LAN (Local Area Network) is by installing:
 - a) An Ethernet switch
 - b) A firewall
 - c) An Ethernet hub
 - d) A CSU/DSU (Channel Service Unit/Data Service Unit)



- vi. Wireless Application Protocol (WAP) has several layers. Which of the following is the security layer?
- Wireless Security Layer (WSL)
 - Wireless Transport Layer (WTL)
 - Wireless Transport Layer Security (WTLS)
 - Wireless Security Layer Transport (WSLT)
- vii. SSH uses _____ to authenticate the remote computer.
- public-key cryptography
 - private-key cryptography
 - both (a) and (b)
 - none of the mentioned
- viii. This type of virus is activated when a user runs an application such as a word processor or spreadsheet.
- Macro-virus
 - Trojan virus
 - Boot-sector virus
 - Email virus
 - Worm
- ix. Which of the following devices is used to monitor network traffic, including DoS attacks in real time?
- A host-based Intrusion Detection System
 - A network-based Intrusion Detection System
 - A router-based Intrusion Detection System
 - A server-based Intrusion Detection System
- x. IPSec is designed to provide the security at the
- | | |
|----------------------|------------------|
| a) transport layer | b) network layer |
| c) application layer | d) session layer |
- Q.2 Short answer type questions (4 questions @ 2.5 marks) 10
- What is Replay attack?
 - What is misfeasor?
 - Is the outer IP header in an IPSEC communication encrypted why or why not?
 - What is a Trojan Horse?
- Q.3A What is the difference between digital certificate and digital signature? 05
- Q.3B Why PGP does generate signature before applying compression? 05
- Q.4A After which message, and following, which computation in SSL, is the client certain that he/she talking to authentic server? 05
- Q.4B How KERBEROS supports authentication in distribution system And which type of network environment is not suitable for KERBEROS services? 05



Q.5A	User A and B uses the Diffie Hellman key exchange technique with a common prime $q=71$ and a primitive root $a=7$. If user A has private key $X_A=5$, what is A's public key Y_A ?	05
Q.5B	How does a network based IDPS is different from host based IDPS (Intrusion detection and prevention system)?	05
OR		
Q.5B	What is the importance of secure socket layer?	05
Q.6A	Explain how a man-in-the-middle attack on a Wi-Fi network can be defeated?	05
Q.6B	Whatever is accomplished by a firewall can also be accomplished by IDS (Intrusion Detection System) yes or no Justify?	05
Q.7A	Suppose a directory that stores digital certificates is broken into, and the certificates in the directory are replaced by bogus certificates, will the user be able to identify these certificates are bogus or not and how?	05
Q.7B	Identify and define the three elements associated with AAA services?	05
OR		
Q.7B	What functionality is provided by a PKI?	05
Q.8A	A Mid-sized organization wishes to deploy a public key infrastructure. Do you recommend that they use digital certificates or identity based cryptography or a hybrid? Clearly justify your recommendations?	10
Q.8B	Is S/MIME an abstracted system for general MIME type encryption, whereas PGP is more for email? Why would I want to choose one over the other, or can I use both at the same time?	05
OR		
Q.8B	What is dual signature and what is its purpose?	05
Q.9A	The following message was received by Admin:- 14, 26, 27, 17, 05, 09, 12, 09, 13, 16 If the message is encrypted by using RSA Algorithm, with the following values $N=33$ and $D=7$ then find the original plain text in Alphabets. (Note:- value 1 =A, 2 =B.....25=Y, 26=Z)	10
Q.9B	What are security threats to internet banking system and how internet banking can be made safe?	05
OR		
Q.9B	What are the three benefits provided by IDS (Intrusion Detection System)?	05