SPECIAL EDITION FOR CSEDU STUDENTS

TOUCH-N-PASS EXAM CRAM GUIDE SERIES

CRYPTOGRAPHY

Prepared By

Sharafat Ibn Mollah Mosharraf

CSE, DU

12th Batch (2005-2006)

Table of Contents

CHAPTER 1
INTRODUCTION

1.1	**What is replay attack? Give some examples of replay attack? [*2008. Marks: 1 + 1*]**
1.2	**List and describe categories of Security Services. [*2007. Marks: 5*]**
1.3	**Distinguish between active and passive security attacks and name possible active and passive security attacks. [*In-course 06-07. Marks: 3*]** **ALSO, List the categories of active security attack and passive security attack and explain any one active and any one passive security attack. [*In-course 08-09. Marks: 2 + 3*]**
1.4	**Illustrate and briefly explain any one of the following: [*In-course 06-07. Marks: 2*]** **i. Model for network security** **ii. Network access security model**
1.5	**Illustrate and explain the functions of each component of network security mode. [*In-course 08-09. Marks: 2 + 3*]**

CHAPTER 2
CLASSICAL ENCRYPTION TECHNIQUES

2.1	**Explain Symmetric-Key cryptography model with its ingredients/elements. [*2007. Marks: 4*]**
2.2	**Briefly explain cryptanalysis and brute-force attack. [*2007. Marks: 4*]**
2.3	**What are substitution cipher and transposition cipher? Give example. [*2007. Marks: 2*]** **ALSO, List as many substitution ciphers and as many transposition ciphers as you can and briefly explain any one from each type. [*In-course 08-09. Marks: 1 + 4*]**
2.4	**Distinguish between stream cipher and block cipher and explain n-bit-n-bit block cipher. [*In-course 08-09. Marks: 2 + 3*]**
2.5	**List and briefly define the types of cryptanalytic attacks based on what is known to the attacker. [*In-course 08-09. Marks: 5*]**

CHAPTER 19
MALICIOUS SOFTWARE

19.1	**Explain the principle of operation of a compression virus, and illustrate its operation by the execution of a virus affected program. [*2006. Marks: 2 + 3*]**
19.2	**How does a worm propagate? [*2007. Marks: 2*]**
19.3	**What is Logic Bomb? [*In-course 06-07. Marks: 1*]**
19.4	**What are the typical phases of operations of a virus? [*In-course 06-07. Marks: 2*]**
19.5	**How does Behavior Blocking Software work? [*In-course 06-07. Marks: 1*]**
19.6	**What is DDoS? Differentiate between Direct DDoS attack and Reflector DDoS attack. [*2007. Marks: 1 + 2*]**
19.7	**What is Digital Immune System? Clearly describe the typical steps of Digital Immune System operation. [*2007. Marks: 1 + 4*]**
19.8	**What is the difference between rule-based intrusion detection and statistical anomaly detection? [*2008. Marks: 2*]**

CHAPTER 30 (FOROUZAN), CHAPTERS 3, 5 (STALLINGS)
CRYPTOGRAPHY, AES, DES

30.1	**Explain the steps for generating keys for RSA algorithm, and generate any key-pair using the primes 3 and 11. [*2006. Marks: 2 + 2*]**
30.2	**What is the basic purpose of Diffie-Hellman algorithm? Using this algorithm, how can Eve fool two communicating partners Alice and Bob by creating two keys: one between Alice and herself, and another between herself and Bob? [*2006. Marks: 1 + 5*]**
30.3	**Compare / Distinguish between DES and AES. [*2006. Marks: 2*]**
30.4	**Explain generation technique of round keys for AES. [*In-course 08-09. Marks: 3*]**
30.5	**Illustrate the general structure of the 10-round AES and draw a flowchart showing the operations of each round. [*In-course 06-07. Marks: 2*]** **ALSO, Clearly state the operations of any round. [*In-course 05-06. Marks: 3*]** **ALSO, Name different stages in a common round of AES and clearly explain the operation of any one round. [*In-course 08-09. Marks: 1 + 4*]** **ALSO, Explain the encryption process of AES for any one key-size and list the operations of its common round. [*2006. Marks: 4*]**
30.6	**Distinguish between Cipher Feedback Mode and Output Feedback Mode. [*In-course 06-07. Marks: 3*]** **ALSO, Clearly explain any one of them. [*In-course 05-06. Marks: 3*]**
30.7	**Illustrate one round of DES encryption and (using a flowchart) explain DES function. [*In-course 06-07, 05-06. Marks: 2 + 3*]** **ALSO, Illustrate the internal blocks of operations of one round of DES and explain the internal operations of DES function. [*In-course 08-09. Marks: 2 + 3*]**
30.8	**What is the major advantage of public key cryptography over symmetric key cryptography? [*2008. Marks: 1*]**

CHAPTER 31 (FOROUZAN)
NETWORK SECURITY

31.1	**What do you understand by message non-repudiation? Explain the role of a trusted center for message non-repudiation. [*2006. Marks: 1 + 3*]**
31.2	**Illustrate the process of creation and verification of message authentication code. [*2006. Marks: 2*]**
31.3	**What is digital signature? Explain the uses of hash functions for generating and verifying digital signature. [*2006. Marks: 1 + 4*]**
31.4	**Discuss the relationship between digital signature, digital certificate authority and public key infrastructure. [*2006. Marks: 5*]**
31.5	**Can you use a secret (symmetric) key to both sign and verify a digital signature? Justify your answer. [*2007. Marks: 3*]**
31.6	**In Kerberos Protocol, what are the steps that Alice (user requesting service) should follow to communicate/receive services from three different servers: Bob, Eve and Trudy? [*2007. Marks: 5*]**
31.7	**What purpose does the authenticator in a Kerberos message serve? Detail one flaw Merritt and Bellovin identified in its design. [*2008. Marks: 1 + 2*]**
31.8	**How does digital signature provide message non-repudiation? [*2008, 2007. Marks: 3*]**
31.9	**What is digital signature? State the requirements for digital signature. [*2008, 2007. Marks: 5*]**
31.10	**What are the threats with direct digital signature scheme? [*2008. Marks: 1*]**
31.11	**Clearly describe the steps for generating any one RSA key-pair using the prime numbers 5 and 11. [*In-course 06-07. Marks: 3*]**
31.12	**Suppose Bob chooses two prime numbers 7 and 11. How can he determine the RSA keys? Show the procedure and determine a key pair. [*In-course 05-06. Marks: 3 + 2*]**
31.13	**Distinguish between message authentication code and message digest. [*In-course 06-07. Marks: 2*]**
31.14	**Explain how a digital signature provides message integrity and message authentication services. [*In-course 08-09, 06-07. Marks: 3*]**
31.15	**How can a session key be created between Alice and Bob using any method? [*In-course 06-07. Marks: 2*]**
31.16	**Explain the uses of different Kerberos servers. [*In-course 06-07. Marks: 3*]** **ALSO, Using an illustration, explain the purpose of authentication server and ticket granting server of Kerberos version 4. [*In-course 08-09. Marks: 3*]**
31.17	**Distinguish between message authentication and entity authentication. Explain entity authentication using symmetric key cipher or asymmetric key cipher. [*In-course 05-06. Marks: 2 + 3*]**
31.18	**What do you understand by a trusted center? [*In-course 05-06. Marks: 1*]**
31.19	**Distinguish between modification detection code and message authentication code. [*In-course 08-09. Marks: 2*]**
31.20	**Using an illustration explain the principle of operation of SHA-1 or any other hash algorithm. [*In-course 08-09. Marks: 3*]**

	ALSO, How does SHA-1 create message digest? [*2007. Marks: 3*]
31.21	**What do you understand by challenge-response method of entity authentication? Using an illustration, explain any one such method for entity authentication. [*In-course 08-09. Marks: 1 + 2*]**
31.22	**What is the purpose of a digital certificate? List at least five fields of a digital certificate using X.509 standard. [*In-course 08-09. Marks: 2*]**
31.23	**List possible attacks on fixed passwords and explain salting a password. [*2006. Marks: 1 + 3*]** **ALSO, Explain dictionary attack on fixed passwords. [*In-course 08-09. Marks: 2*]** **ALSO, How can a system prevent a guessing attack on a fixed password? [*2007. Marks: 1*]** **ALSO, How does salted password make dictionary attack more difficult? [*2007, In-course 08-09. Marks: 2*]**
31.24	**What is Hash function? Mention the requirements for hash function. [*2008. Marks: 5*]**
31.25	**Briefly explain MD5 hash algorithm. [*2008. Marks: 5*]**
31.26	**In what order should the signature function and the confidentiality function be applied to a message and why? [*2008. Marks: 2*]**

CHAPTER 32 (FOROUZAN)
SECURITY IN THE INTERNET

32.1	**How does ESP of IPSec provide source authentication, data integrity and privacy services for communication between two users? [*2006. Marks: 6*]**
32.2	**How does IPSec provide source authentication and data integrity for communication between two users? [*2007. Marks: 5*]**
32.3	**What is a virtual private network? How can IPSec in the tunnel mode provide authentication, integrity and privacy services for a virtual private network? [*2006. Marks: 1 + 3*]**
32.4	**What are the techniques to achieve secure email transactions along with sender's identity? [*2006. Marks: 5*]**
32.5	**Differentiate between Transport mode and Tunnel mode of IPSec Protocol. [*2007. Marks: 2*]**
32.6	**Differentiate between Authentication Header Protocol and Encapsulating Security Payload Protocol in IPSec. [*In-course 06-07. Marks: 3*]** **ALSO, Differentiate between authentication data of AH and ESP of IPSec. [*In-course 08-09. Marks: 2*]**
32.7	**What is the purpose of firewall? Differentiate between packet filter and proxy firewall. [*2007. Marks: 1 + 3*]**
32.8	**What is R64 conversion? Why is R64 conversion useful for an email application? [*2008. Marks: 1 + 1*]**
32.9	**How does PGP use the concept of trust? [*2008. Marks: 2*]**
32.10	**What services are provided by SSL record protocol? [*2008. Marks: 2*]**
32.11	**State any four services of SSL. [*In-course 06-07. Marks: 2*]**
32.12	**What is dual signature and what is its purpose? [*2008. Marks: 1 + 1*]**
32.13	**What is the purpose of Proxy Firewall? [*In-course 06-07. Marks: 1*]**
32.14	**What is VPN? Why is it needed? [*In-course 06-07. Marks: 1 + 1*]**
32.15	**What is the purpose of Handshake protocol in SSL? [*In-course 06-07. Marks: 1*]**
32.16	**How does SSL create Cryptographic Secret? [*In-course 06-07. Marks: 2*]**
32.17	**Explain the operation of any one of the following: [*In-course 08-09. Marks: 3*]** **i. Authentication Header Protocol of IPSec in transport mode.** **ii. Encapsulating Security Protocol of IPSec in transport mode.**
32.18	**Point out the security services required when a customer shops online using WWW. [*In-course 08-09. Marks: 2*]**
32.19	**Explain any one of the following: [*In-course 08-09. Marks: 3*]** **i. Security association of IPSec** **ii. Security parameters of SSL**
32.20	**Using an appropriate illustration, explain how authentication and confidentiality services are provided by PGP for secure email. [*In-course 08-09. Marks: 5*]**
32.21	**What is Hybrid Network? Why is it needed? [*2007. Marks: 1 + 1*]**
32.22	**Why should you include a message authentication code (MAC) with a message? What is the difference between a MAC and an HMAC? [*2008. Marks: 1 + 1*]**
32.23	**Explain Hand-Shake protocol for web security approaches. [*2008. Marks: 4*]**