SKR/KW/24/2610

Faculty of Science & Technology
Seventh Semester B.Tech. (Information Technology) (CBCS) Examination
CRYPTOGRAPHY AND NETWORK SECURITY
Elective–IV

Time : Three Hours] [Maximum Marks : 70

INSTRUCTIONS TO CANDIDATES

(1) All questions carry marks as indicated.
(2) Solve Question **1 OR** Question No. **2**.
(3) Solve Question **3 OR** Question No. **4**.
(4) Solve Question **5 OR** Question No. **6**.
(5) Solve Question **7 OR** Question No. **8**.
(6) Solve Question **9 OR** Question No. **10**.
(7) Due credit will be given to neatness and adequate dimensions.
(8) Assume suitable data wherever necessary.
(9) Diagrams and chemical equations should be given wherever necessary.
(10) Illustrate your answers wherever necessary with the help of neat sketches.

1. (a) Explain Model of Network Security. 7
   (b) Write the Playfair cipher Algorithm.
   Let the message = "EDUCATION" Key = "WORD"
   Find cipher text using Playfair Cipher. 7

OR

2. (a) What are Attributes of Security ? 7
   (b) Explain Euclidean and Extended Euclidean Algorithm. 7
3. (a) What is Symmetric key Cryptography ? Discuss Block Cipher Principles. 7
   (b) Describe Data Encryption Standard (DES). 7

OR

4. (a) Explain the Key Expansion functions of AES Algorithm. 7
   (b) Write on short note Key Distribution with Diagram. 7

Model Questions

5. (a) Explain the Euler's theorem. 7

(b) State the Chinese Remainder Theorem and find X for the given set of congruent equations

$X \equiv 2 \bmod 3$, $X \equiv 3 \bmod 5$ and $X \equiv 2 \bmod 7$. 7

OR

6. (a) Find the secret key shared between user A and user B using Diffie – Hellman algorithm for the variables $Q = 353$, α (primitive root) $= 3$, $X_A = 45$, $X_B = 50$. 7

(b) Perform decryption and encryption using RSA algorithm with $p = 3$, $q = 11$, $e = 7$ and $m = 5$. 7

7. (a) What is Kerberos ? Explain the different versions of Kerberos. 7

(b) What is hash function ? What are the requirements of hash functions ? 7

OR

8. (a) Explain in detail the operation of Internet Key Exchange with an example. 7

(b) Write short note on X.509 digital certificate format. 7

9. How does PGP provide confidentiality and authentication service for e-mail and file storage applications ? Draw the block diagram and explain its compoments. 14

OR

10. Write short notes on (any **three**) : 14

(i) Firewalls

(ii) Software Vulnerability

(iii) SQL injection

(iv) Electronics payment types.

PRS/KS/24/2900

Faculty of Science & Technology

Seventh Semester B.Tech. Information Technology (C.B.C.S.) Examination

CRYPTOGRAPHY AND NETWORK SECURITY

ELE–IV

Time : Three Hours] [Maximum Marks : 70

INSTRUCTIONS TO CANDIDATES

(1) All questions carry marks as indicated.

(2) Solve Question No. **1 OR** Question No. **2**.

(3) Solve Question No. **3 OR** Question No. **4**.

(4) Solve Question No. **5 OR** Question No. **6**.

(5) Solve Question No. **7 OR** Question No. **8**.

(6) Solve Question No. **9 OR** Question No. **10**.

(7) Assume suitable data wherever necessary.

(8) Illustrate your answers wherever necessary with the help of neat sketches.

1. (a) Explain different attacks and compare two types of attack. 5

(b) Explain Simplified DES Algorithm. 5

(c) Find ciphertext of " Security model " using hill cipher technique. 4

OR

2. (a) Solve and find ciphertext using playfair Technique Plaint text is "Information Technology and key is computer. 7

(b) Explain OSI network Security model. 4

(c) Explain different Transposition Techniques used for cryptographic algorithms. 3

3. (a) Explain meet in middle attack and triple DES in detail. 5

(b) Explain Session key master key and centralized key control and decentralized key control. 9

OR

4. (a) Solve using Extended Eucliadian algorithm gcd(161,28). 5

(b) Explain RC4 in detail. 4

(c) Explain any 3 block cipher Principles. 5

5. (a) Explain RSA algorithm in detail with example. 9

(b) Explain Fermats theorem. 5

Model Questions

OR

6. (a) Solve and find value of X Using Chinese Remainder Theorem : 7

X = 1mod 5

X = 1mod 7

X = 3mod 11

(b) Explain Diffehellman Key Exchange algorithm. 7

7. (a) What are different authentication requirement and functions ? 7

(b) Compare MD5, SHA1, RIPEMD 160. 7

OR

8. (a) Give design of MD5 Algorithm. 7

(b) Explain Kerberos. 7

9. (a) What are Firewalls ? Explain different types of Firewalls. 6

(b) Illustrate with example Phishing. 4

(c) Explain role of Intrusion Detection in network security. 4

OR

10. (a) Illustrate PGP and relate it with web of Trust. 6

(b) Write short notes on **(any three)** : - 8

(i) SQL Injection

(ii) Electronic Payment Types

(iii) SSL

(iv) Bufferoverflow

B.Tech. (Information Technology) Seventh Semester (C.B.C.S.)

Program Elective-IV : Cryptography & Network Security

P. Pages : 2 **PSM/KW/23/2900**

Time : Three Hours Max. Marks : 70

Notes : 1. All questions carry marks as indicated.
2. Solve Question 1 OR Questions No. 2.
3. Solve Question 3 OR Questions No. 4.
4. Solve Question 5 OR Questions No. 6.
5. Solve Question 7 OR Questions No. 8.
6. Solve Question 9 OR Questions No. 10.
7. Due credit will be given to neatness and adequate dimensions.
8. Assume suitable data whenever necessary.

1.	a)	Elaborate model of Network security with respect to OSI security model.	**7**
	b)	Explain Playfair Encryption technique and encrypt the following message. **Keyword:** OCCURRENCE **Plain text:** I AM INDIAN	**7**
		OR	
2.	a)	Explain Caesar cipher encryption in detail. Decrypt the following cipher text and find the key of encryption by using Caesar cipher encryption technique. **Cipher Text:** LTTI RTWSNSL	**7**
	b)	Explain network security principles in detail.	**7**
3.	a)	Explain the working of DES algorithm in detail.	**9**
	b)	Explain the working of RC4 algorithm.	**5**
		OR	
4.	a)	Explain key distribution scenario with labelled diagram. Define master key and session key in Hierarchical key control.	**8**
	b)	Describe key generation of AES algorithm.	**6**
5.	a)	Explain RSA algorithm in details. Perform encryption and decryption, where p = 17; q = 11; e = 7; M = 88.	**7**
	b)	Explain man in middle attack in detail.	**7**
		OR	
6.	a)	Describe Diffie-Hellman key exchange algorithm in detail.	**7**
	b)	Explain Elliptic curve cryptography in detail.	**7**

Model Questions

7.	a)	Explain the working of MD-5 Hash algorithm in detail.	**7**
	b)	What is the purpose of X.509 authentication service? Describe the format of X.509 certificate and certificate Revocation.	**7**
		OR	
8.	a)	Describe Kerberos version 4 with the help of suitable diagram.	**9**
	b)	Write a short note on Hash function? Give the basic uses of hash function.	**5**
9.	a)	Explain secure socket layer Architecture in detail.	**7**
	b)	Explain design principles of firewall and discuss types of firewalls.	**7**
		OR	
10.	a)	Explain the working of PGP in detail.	**7**
	b)	What do you mean by "Intrusion detection system" and "Intrusion prevention system".	**7**

****