B.E.(Information Technology) Seventh Semester (CBS)

Computer System Security

P. Pages : 2 **AHK/KW/19/2347**

Time : Three Hours * 1693 * Max. Marks : 80

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. Solve Question 11 OR Questions No. 12.
8. Due credit will be given to neatness and adequate dimensions.
9. Assume suitable data whenever necessary.
10. Illustrate your answers whenever necessary with the help of neat sketches.

1. a) Explain the basic model of network security with suitable diagram. **6**

b) Explain the working of AES algorithm with neat diagram. **8**

OR

2. a) Explain the play – fair substitution technique convert the following text to cipher using "MONARCHY" as a keyword. "It was disclosed yesterday". **8**

b) Distinguish between monoalphabetic cipher & polyalphabetic cipher. **3**

c) Explain rail fence cipher technique with example. **3**

3. a) Explain the IDEA cipher in detail with neat diagram. **7**

b) Explain Chinese Remainder Theorem with example. **6**

OR

4. a) Explain subkey, s-box generation and round structure of Blow – fish with neat diagram. **7**

b) Distinguish between differential and linear cryptanalysis. **6**

5. a) Explain RSA algorithm in detail. Perform encryption and decryption using following data. **8**
$P = 3, q = 11, d = 7, m = 5$

b) What is an elliptic curve. Elaborate in brief. **5**

OR

6. a) Explain Diffie – Hellman key exchange – algorithm in detail. **8**

b) Explain Hash function authentication requirements. **5**

7.	a)	Explain HMAC algorithm in detail.	**7**
	b)	What are the uses of Kerberos? Explain Kerberos's V4	**6**

OR

8.	a)	Explain digital signatures & authentication protocol digital signature.	**7**
	b)	What is the purpose of X. 509 authentication services? Describe the format of X. 509 certificate & certificate revocation.	**6**
9.	a)	Explain Radix – 64 conversion with the help of example.	**6**
	b)	Explain S/ MIME architecture with neat diagram.	**7**

OR

10.		Explain the architecture of AH (Authentication Header) and Encapsulating security payload with suitable diagram and data packets.	**13**
11.	a)	Explain SSL (Secure Socket Layer) and TLS (Transport Layer Security Protocol in detail.	**9**
	b)	Basic concept of web security & requirements.	**5**

OR

12.	a)	Write short note on.	**9**
		i) System security.	
		ii) Viruses & worms.	
		iii) Trusted system.	
		iv) DOS.	
	b)	Explain concept of Secure Electronic Transaction (SET).	**5**

****