**17P347** (Pages: 2) Name……………………..

Reg. No…………………..

**THIRD SEMESTER M.Sc. DEGREE EXAMINATION, NOVEMBER 2018**

(CUCSS-PG)

**CC17P CSS3 E04c - CRYPTOGRAPHY AND NETWORK SECURITY**

(Computer Science)

(2017 – Admission)

Time: Three Hours Maximum: 36 Weightage

## PART A

Answer ***all*** questions. Each question carries 1 weightage.

1. Define symmetric encryption. List out its ingredients.
2. Describe any two security mechanisms defined in X.800
3. Compare block cipher and stream cipher with example.
4. What are the applications of public key cryptosystem?
5. Define digital signature.
6. What are the services provided by SSL Record Protocol?
7. List out the services provided by IPsec.
8. What is digital immune system?
9. What is statistical anomaly detection?
10. List the DDoS countermeasures.
11. What are the principle elements of an identity management system?
12. In context of Kerberos, illustrate request for service in another realm.

**(12 x 1 = 12 Weightage)**

## PART B

Answer any ***six*** questions. Each question carries 2 weightage.

13. Consider two users A and B. A sends a message to B, meanwhile intruder C manipulates the message. Identify the attack in the above scenario and identify which security service has been compromised and list out its specific security services.
14. What are the advantages of Cipher Block Chaining Mode over Electronic Code Book?
15. Given four words (1 word = 4 bytes) $W_0$=(54,68,61,74),$W_1$=(73,20,6D,79), $W_2$=(20,4B,75,6E),$W_3$=(67,20,46,75). Perform AES key expansion algorithm using RotWord, SubWord and Rcon functions on word $W_3$ and find the solution for $W_4$, $W_5$, $W_6$ & $W_7$.

    [Note: Substitute bytes (SubWord) using following data- 20 as B7, 46 as 5A,75 as 9D and 67 as 85.Given Rcon value as (01,00,00,00)]
16. Illustrate three message authentication approaches using one way hash function.

17. List out the reasons for revocation of X.509 certificate.

18. Define DDoS and its classification.

19. Briefly explain the alert codes used in TLS.

20. How Kerberos version 4 ensures authentication?

21. Describe the countermeasures for worm defense.

**(6 x 2 = 12 Weightage)**

## PART C

Answer any ***three*** questions. Each question carries 4 weightage.

22. Explain in detail about AES Encryption Round function.

23. Explain Diffie-Hellman Key exchange.

24. Write a note on X.509 certificate.

25. Describe SSL Handshake and Change Cipher Spec Protocol.

26. Explain the different types of firewall.

27. Discuss the approaches to intrusion detection.

**(3 x 4 = 12 Weightage)**

*******