Final Assessment Test – November 2019

VIT Vellore Institute of Technology

Course: CSE4003 - Cyber Security

Class NBR(s): 0787/5584/5586/5733/5739/6712 Slot: A2+TA2

Time: Three Hours Max. Marks: 100

KEEPING MOBILE PHONE/SMART WATCH, EVEN IN 'OFF' POSITION, IS EXAM MALPRACTICE

Answer any TEN Questions

(10 X 10 = 100 Marks)

1. a) Using the extended Euclidean algorithm, find the multiplicative inverse of 7465 mod 2464.

   b) The example used by Chinese to illustrate the CRT was $x \equiv 2 \pmod 3$; $x \equiv 3 \pmod 5$; $x \equiv 2 \pmod 7$. Solve for x.

2. a) Prove or disprove that Z_8 is a field?

   b) Apply Fermat's theorem to find 4^{225} mod 13.

3. Perform MixColumn operation for the following state: 87 6E 46 A6.

4. a) Consider the elliptic curve $E_7(2,1)$; that is, the curve is defined by $y^2 = x^3 + 2x + 1$ with a modulus of p = 7. Determine all the points in $E_7(2, 1)$.

   b) For $E_{11}(1, 7)$, consider the point $G = (3, 2)$. Compute the multiple of G from $2G$ through $4G$.

5. a) Consider two prime numbers p = 17 and q = 11 and public key e = 7. Encrypt the message M = 88 and decrypt the ciphertext using RSA algorithm.

   b) Alice and Bob use the Diffie–Hellman key exchange technique with a common prime q = 157 and a primitive root $\alpha = 5$. If Alice has a private key $X_A = 15$, find her public key Y_A. If Bob has a private key $X_B = 27$, find his public key Y_B. What is the shared secret key between Alice and Bob?

6. a) What is the padding field for sha-512 if the message is of 1600 bits?

   b) Given the Message = "abc". Calculate the value of words w_0, w_1, w_2, w_3 for SHA 512.

   c) Distinguish between HMAC and MAC. How are ipad and opad constants used in HMAC? Do they enhance the security of the algorithm?

7. a) Illustrate Elgamal digital signature using the following values: GF(19), $\alpha = 10$, $X_A = 16$, K = 5. Alice signs a message with m = 14. Show the signing and verification procedure.

   b) DSA specifies that if the signature generation process results in a value of s = 0, a new value of k should be generated, and the signature should be recalculated. Why?

8. Classify the different types of cybercrimes and the provisions of cyber crimes in the IT Act.

9. a) Malware can come under the disguise of genuine software from an official site. Explain how can you identify the malicious software and how the security can be provided?

   b) Describe in detail about identity theft.

10. Explain existing cyber security policies and best practices that are to be followed to protect businesses.

11. Discuss about the security and privacy concerns in online social networks.

⇔⇔⇔