Exp : 284 30

(U19CS012)

Department of Computer Science and Engineering, SVNIT, Surat.
End-Semester Examinations, May 2022
B Tech – III – 6th Semester
Global Elective Course: Cryptography (CS362)

Date: 6th May, 2022 Time: 12:00 to 15:00 Max Marks: 50

Note: Each question carries 5 marks.

1. In RSA, an entity sends the same message, m, to three parties, X, Y, and Z, each encrypted with their respective public keys. Assume that the public key moduli of the three parties are n_x, n_y, and n_z. The encryption key in each case is 3.
Analyze the security of the above scenario. Identify the attack and design/suggest suitable solution to prevent the attack.

2. Explain Diffie-Hellman key exchange protocol for two parties. Design the same protocol for more than two (let us say three) parties.

3. Let A = (2,4) and B = (8,5) be two points on the elliptic curve $y^2 = x^3 + 2x + 4$ over F_{13}. Compute points A+B and 2A for the given curve.

4. "The objective of Message Authentication Codes (MAC) and Digital Signature is to ensure message authentication and integrity." Then why do we have these two different techniques? Identify the application scenario that uses MAC and the scenario that uses digital signature.

5. Do each of the following inverses exist? If yes, what are they? If no, explain why not.
$102^{-1} \pmod{411}$
$77^{-1} \pmod{411}$

6. Can you think of a ring of size 9 (i.e. there are 9 elements in the ring). You should clearly define the ring operations, + and * . Is that ring also a field? Why or why not?

7. We have studied two uses of the cryptographic hash – in computing the MAC and the digital signature. Think and elaborate upon any two other applications of the cryptographic hash.

OR

What is the number of messages that need to be created (variations of the malicious message and the innocent message) so that the birthday attack is successful with a probability more than 0.5? Explain your answer.

8. Which of the following is/are true and why? The Initialization Vector (IV) in CBC mode should be,
a) a constant known only to sender and receiver
b) a non-secret constant
c) a random variable known only to sender and receiver
d) a non-secret random variable

OR

A single bit error occurs in exactly one block of ciphertext during transmission. How will this affect the recovery of plaintext in each of the following modes?
ECB, CBC, CFB, Counter

9. Give at least one application scenario for which a block cipher is more appropriate and an application scenario where a stream cipher is more appropriate. Justify your answer.

10. Do the security assessment of One time pad cipher. Is it perfectly secure? What are the implementation issues in One time pad cipher?