Department of Computer Science and Engineering – SVNIT Surat
Mid Semester Examinations, March 2023
B Tech III (CSE) – Semester VI
Course: Information Security & Cryptography (CS302)

Time: 90 minutes (13th March 2023 – Monday – 1100 to 1230) Max. Marks: 30

Instructions:
1. Answer all questions.
2. Figures to the right indicate maximum marks.

Q1 A Answer the following.

1. Use a phrase "Smith captioned Aussy much better than Cummins to defeat India" to define a key of 5x5 Playfair cipher. Encrypt message "India at WTC" using this Playfair cipher. **03**
2. Encrypt the text "meet me at ten pm near gate" using Rail Fence Cipher (of depth 2) and Caesar cipher with key 2. **02**

Q1 B Answer the following (any two) **03**

1. Discuss security of One-time-pad. What is two-time pad?
2. How ChatGPT can threaten information security?
3. Discuss Jefferson cylinder.

Q2 A Answer the following (any three) **06**

1. What are the Side Channel Attacks? Discuss Timing attack and its countermeasures.
2. How Cryptographic hash function can be used for message authentication and in software licensing?
3. List classical and modern Steganography techniques.
4. List properties of cryptographic hash function (CHF). How CHF can be constructed from a symmetric key block cipher?
5. List critical infrastructures. What was Stuxnet?

Q2 B Answer the following (any one): **04**

1. Discuss AES and its design.
2. Discuss SHA1 and its design.

Q3 A Answer the following (any two): **08**

1. Alice and Bob agreed to use the RSA algorithm for the secret communication. Alice securely chooses two primes, p=5 and q=11 and a secret key d=7. Find the corresponding public key. Bob uses this public key and sends a ciphertext 18 to Alice. Find the plain text.

2. Consider a Diffie Hellman scheme with a common prime q = 11 and primitive root $\alpha = 2$.
   i. Show that 2 is a primitive root of 11.
   ii. If user A has public key YA = 9, what is A's private key?
   iii. If user B has public key YB = 3, what is the shared secret key K, shared with A

3. State the Chinese Remainder theorem and find the value of x for the given set of congruent equations using Chinese Remainder theorem.
   $x \equiv 1 (\text{mod } 5)$
   $x \equiv 2 (\text{mod } 7)$
   $x \equiv 3 (\text{mod } 9)$

Q3 B Answer any two of the following:

1. Illustrate man in the middle attack on Diffie Hellman key exchange algorithm. 04
2. Find gcd(240, 46) using Extended Euclid's Algorithm.
3. Define Confusion and Diffusion. How they are useful in designing ciphers?

****