CSL-7480 IIT Jodhpur
Minor-2 Cryptography
Time: 1 hour (2:30-3:30 pm, 21 Mar 2024 LHB-105) Sem. 2, 2023-24
Instructor: Somitra Sanadhya
Max. Marks: 15

Note:

1. No queries will be entertained during the test.

1. Explain "Birthday paradox" and its implication on the security of cryptographic hash functions. (2 marks)
2. How can two untrusting parties can toss a fair-coin by sending messages on a public telephone? Explain the method. (2 Marks)
3. Explain Elliptic Curve El-Gamal cryptosystem. Clearly show the process of setting up of the key, encryption, and decryption. (2 marks)
4. (a) The RSA cryptosystem, as covered in the class, uses a modulus n which is a product of two primes. However, it is easy to extend the cryptosystem for multi-prime case in an analogous manner. Let the RSA modulus $n = 120$ and encryption exponent $e = 3$ for multi-prime RSA. Find the decryption exponent d.
   (b) Give one justification for using multi-prime RSA?

   (2+1=3 marks)
5. Let $G = \langle g \rangle = \{(1, g, g^2, \ldots) \bmod 29\}$ be the group used for the El-Gamal encryption for $g = 7$. Let the private key of Alice be 9. Then answer the following:
   (a) What is the public key of Alice?
   (b) If Alice received a ciphertext (3,2) then what is the message being sent to her?

   (1+2 =3 marks)
6. Let $H : \{0,1\}^* \to \{0,1\}^t$ be a hash function, (n, e, d) be the RSA parameters with usual meaning, where (N, e) are public and d is secret. Consider an encryption scheme to encrypt messages $\in \{0,1\}^t$ be defined as follows:

$$\begin{aligned} r &\xleftarrow{\$} \{0,1\}^t \\ \text{Enc}(m) &= (r^e \bmod n, H(r) \oplus m). \end{aligned}$$

   (a) Explain how to decrypt a message from the ciphertext.
   (b) Is the above scheme CCA secure? Prove or disprove.

   (1+2=3 marks)

*****