LNMIIT/B. Tech/CSE-CCE/PE/2018-19/EVEN/CSE3112

The LNM Institute of Information Technology

Department of Computer Science & Engineering

Cryptograhic Algorithms (CSE3112)
Mid-term Examination

Time: $1\frac{1}{2}$ hours(02.00-3.30PM) Date:26/02/2019 Maximum Marks: 30

1. Prove that the **RSA** cryptosystem is insecure against a `Chosen Ciphertext Attack`(CCA). In particular the adversary Eve can choose a ciphertext $\tilde{c} \in \mathbb{Z}_n^*$ different from the original ciphertext say c of the plain text message m such that the knowledge of the plain text $\tilde{m} = D_k(\tilde{c})$ allows to compute $m = D_k(c)$. [6]

2. (a) Write an algorithm to mount `Cyclic Attack` on **RSA** Cryptosystem where the ciphertext $c = m^e \bmod n$ *i.e* encryption is the permutation of the message space $\{0, 1 \ldots n-1\}$. [3]

   (b) Let us assume that, there is a communication between Alice and Bob. Alice uses **RSA** cryptosystem for privacy of message, how does the adversary Eve can perform `Factorization Attack` on the cryptosystem to obtain the Alice's private key? [3]

3. (a) Write the algorithm of generalized **ElGamal Encryption Scheme** and its proof of correctness. [3]

   (b) Evaluate the computational cost of encryption. [1]

   (c) Which of the following random exponent k_1 or k_2 can be chosen to sped up the encryption process? Justify your answer. [2]

   - $k_1 =$ 001110000010001001
   - $k_2 =$ 001110000010001111

4. Write **Digital Signature Algorithm** and prove that `Signature verification` works. [6]

5. *How Known-messsage Attack can be mount against* **RSA Signature scheme** ? in particular the adversary *intercepted two message and signature pairs* (m_1, s_1) and (m_2, s_2) and can able to generate a new signature s *on message* m *which make fool to the verifiers believing that it is the signature of the signer on* m. Where $m = m_1 \times m_2 \bmod n$. [6]

****END***