(37)

12 May 2023

ſE. (2 Yr) 2nd Semester

ISLAMIC UNIVERSITY OF TECHNOLOGY (IUT)

ORGANISATION OF ISLAMIC COOPERATION (OIC)

Department of Computer Science and Engineering (CSE)

SEMESTER FINAL EXAMINATION **SUMMER SEMESTER, 2021-2022**

DURATION: 3 HOURS **FULL MARKS: 150**

CSE 6291: Information Security

Programmable calculators are not allowed. Do not write anything on the question paper.

Answer **all 6 (six)** questions. Figures in the right margin indicate full marks of questions.

---

1. a) Explain the working mechanism of Ceasar's cipher with a suitable example. What is the major limitation of this method? 6+4

   b) Discuss the key characteristics of Asymmetric/Public Key encryption with an appropriate figure. How does it overcome the limitation of Symmetric/Private Key encryption? 9+6

2. Suppose Alice wants her friends to encrypt email messages using a public-key encryption system before sending the e-mails to her. Assume that computers represent text as long numbers (01 for '*A*,' 02 for '*B*' and so on). That means email message is just a very big number.

   Alice chooses $p = 17$ and $q = 11$.

   a) Find the public key of Alice. The value of public exponent e must be between 10 and 15. 5

   b) Compute the private key of Alice based on the chosen public key. Show the detailed computation. 15

   c) If the plaintext (P) which is to be sent to Alice is 32, what is the ciphertext (C) Alice will receive? 5

3. a) Define the term 'Digital Signature'. How does it work? Explain in detail with a suitable figure. 4+6

   b) Explain the process of the PGP cryptosystem with an appropriate figure. Comment on the significant advantage and disadvantages of PGP Encryption. 9+6

4. a) Define the term 'Cyber Security'. Why is Cyber Security important? 5+5

   b) Discuss the three fundamental concepts of Cyber Security. 15

5. a) Briefly describe the following web-based attacks: 15

      i. Injection
      ii. Session Hijacking
      iii. Phishing
      iv. Denial of Service
      v. Man in the middle attacks

   b) Explain the seven (7) layers of Cyber Security using a suitable figure. 10

6. a) Define the term 'Digital Forensics'. What are the different approaches used for email forensics? Explain accordingly. 5+10

   b) Discuss the major phases of the digital forensics lifecycle. 10