ASUTOSH COLLEGE

4th Semester Examination 2021-2022

B.Sc. Hons. in Computer Science (Under University of Calcutta)

Paper Name: Information Security

Paper Code: CMS-A-SEC-B-4-1-TH

The figures in the margin indicate full marks. Candidates are required to give their answers in their own words as far as practice

Time: 2 Hrs Full Marks: 30

Group-A

1. Answer the following questions (any 4): 1.5x4=6
   a. What is steganography?
   b. Are all stream ciphers monoalphabetic? Explain.
   c. State the difference between Symmetric and Asymmetric Key Cryptography.
   d. What are the features of polygram substitution cipher?
   e. What is meet in the middle attack?
   f. Compare diffusion and confusion.
   g. What do you mean by Packet Sniffing?

Group-B

(Answer any 4)

2. What do you mean by One-Time-Pad? Why this cipher technique is highly secure? how it is differing from Book Cipher? 3+1+2

3. What are the key principles of information security? What are" Replay Attacks" give an example? 4+2

4. Suppose we have a plain text message "balloon", now encrypt the message with the help of Play Fair Cipher technique using the key "MONARCHY". 6

5. Define Digital Signature. What are the advantages to use the digital signature? Write the differences between MD5 and SHA algorithms. 1+2+3

6. Explain ECB and CTR modes of operation 3+3

7. Draw the general structure of DES and explain the encryption process. 6
8. Explain the working of Vignere Cipher and discuss the security value of it. 6
9. Write down the difference between Stream cipher and Block Cipher. 6