ASUTOSH COLLEGE

4th Semester Examination 2021-2022

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

Paper Name: Information Security

Paper Code: CMS-G-SEC-B-X-2-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): 4x1.5=6
   a. What is Cryptography?
   b. Difference between Passive Attack and Active Attack?
   c. What do you mean by private key and public key?
   d. What is "Worm"?
   e. Write down the difference between monoalphabetic and polyalphabetic cipher.
   f. What are the limitations of ECB mode of operation?
   g. What is avalanche effect?

Group-B

(Answer any 4)

2. State the differences between Symmetric and Asymmetric Key Cryptography. What is the role of Cryptanalyst? 4+2

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

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

5. Write a short note (**Any 2**):
   a. Packet Sniffing
   b. One-Time-Pad Technique
   c. RSA algorithm
   d. Firewall

6. Explain Feistel cipher with a neat diagram. 6
7. Draw the general structure of DES and explain the decryption process. 6
8. Compare Stream Cipher and Block Cipher. 6
9. Explain the encryption and decryption process of CBC and CFB modes of operation. 3+3