DEPARTMENT OF INFORMATION TECHNOLOGY

JIS COLLEGE OF ENGINEERING, KALYANI

Stream: IT-3B **Paper Name & Code: IT602 (Computer Networks)**

Topic: Network Security & Cryptography

1. What is **Cryptography**? Classify the model of cryptography.

2. Explain the different types of attacks and terminologies relevant to Network security:
   - ***a. Confidentiality***
   - ***b. Integrity***
   - ***c. Authenticity***
   - ***d. Non-repudiation***
   - e. ***Denial of Service*** (***DoS***)
   - f. ***Man-in-Middle*** (***MiM***) attack
   - ***g. Brute-force attack***

3. Explain the basic functional architecture of a symmetric cryptographic system.
   a. Advantage of **symmetric cryptography**
   b. Disadvantages of **symmetric cryptography**
   c. Give three examples of **symmetric cryptography** algorithms commonly in use

4. Explain the basic functional architecture of an asymmetric cryptographic system.
   a. What do you mean by **public key**?
   b. What do you mean by **private key**?
   c. Advantage of **asymmetric cryptography**
   d. Disadvantages of **asymmetric cryptography**
   e. Give three examples of asymmetric cryptography algorithms commonly in use

5. How can you check **authenticity** of a message using **asymmetric cryptography**? Explain with a neat sketch.
6. What is **Digital signature**? How does it ensure **authenticity** of a message?
7. How do you check **integrity** of a message?
8. How does **Message Digest** help detect a possible tampering in a message?
9. What do you mean by **Digital Envelop** and **Digital finger print**?
10. What do you mean by **IP spoofing**?
11. What do you mean by **Digital Certificates**? What is the full form of **PKI** and **KDC**?