

**DAFFODIL INSTITUTE OF INFORMATION TECHNOLOGY (DIIT)**  
**BSc. (Hons) in CSE 4<sup>th</sup> Year 8<sup>th</sup> Semester 14<sup>th</sup> Batch**  
**Computer and Network Security**  
**Course Code: CSE-423**  
**Mid-Term Examination, 2018**

Time – 1 hour & 20 minutes

Full marks – 40

*[N.B. – the figures in the right margin indicate the full marks. Answer any **four** questions of the following segment.]*

- |    |    |  |     |
|----|----|--|-----|
| 1. | a) | Define Computer security, network security and internet security | 2.5 |
|    | b) | Describe public key cryptography with diagram.                   | 5   |
|    | c) | Define Hill Cipher and Auto key cipher.                          | 2.5 |
| 2. | a) | Discuss different types of security attacks.                     | 5   |
|    | b) | Plaintext: MOURNDAY  | 5   |
|    |    | Key: RIP   |     |
|    |    | Find the cipher text using poly-alphabetic cipher.               |     |
| 3. | a) | Describe Block cipher v stream cipher.                           | 4   |
|    | b) | Describe a single round of DES with diagram.                     | 6   |
| 4. | a) | Discuss different types of security goals.                       | 5   |
|    | b) | Define feistel cipher structure with diagram.                    | 5   |
| 5. | a) | Discuss model for network access security with diagram.          | 5   |
|    | b) | Describe triple DES with two keys.                               | 3   |
|    | c) | What is secret key cryptography?                                 | 2   |
| 6. | a) | What are ECB and OFB with diagram?                               | 6   |
|    | b) | Describe plaintext, cipher text, cryptanalysis, and cryptology.  | 4   |