

**M. TECH.-II (INFORMATION TECHNOLOGY) (CBCS – 2015  
COURSE) : SUMMER - 2018**

**SUBJECT: INFORMATION SECURITY**

Day: **Monday**  
Date: **18/06/2018**

**S-2018-3009**

Time: **11.00 AM TO 02.00 PM**  
Max Marks. 60

**N.B.**

- 1) All questions are **COMPULSORY**.
- 2) Figures to the right indicate **FULL** marks.
- 3) Answers to both the sections should be written in **SEPARATE** answer books.

**SECTION - I**

**Q.1 a)** Let  $f(x) = x^4 + x^3 + x^2 + 1$ ,  $g = x^3 + 1 \in f[x]$ . Find g.c.d  $f(g)$  using Euclidean algorithm for polynomials & express the g.c.d in the form  $u(x)f(x) + v(x)g(x)$ . **(06)**

**b)** Define Jacobi symbol with example. **(04)**

**OR**

What is affine cipher transformation? Suppose that an affine cipher  $E(x) = (ax + b) \text{ MOD } 26$  enciphers H as X and Q as Y. Find the cipher (that is determine a and b). **(10)**

**Q.2** What is firewall? Explain the firewall design principles. **(10)**

**OR**

What is intrusion detection? Discuss different approaches to intrusion detection. **(10)**

**Q.3 a)** Why is information security a management problem? **(05)**

**b)** What are data security considerations? **(05)**

**OR**

Explain the role and responsibilities of **(10)**

- i) Data steward.
- ii) Information security committee.
- iii) Chief information security officer.
- iv) Data custodian authorized user.

**SECTION - II**

**Q.4** Describe the process of risk identification in detail. **(10)**

**OR**

What are security threats from insider and outsider attackers? What kind of damage is possible from such type of attackers? **(10)**

**Q.5** Explain continued fraction factoring algorithm. **(10)**

**OR**

Explain 4 possible approaches of attacking on RSA algorithm. **(10)**

**Q.6** What are tasks of information security auditor? Explain. **(10)**

**OR**

Explain the role of backup recovery and virtualization in business continuity and disaster management. **(10)**