## M. TECH.-II (INFORMATION TECHNOLOGY) (CBCS – 2015 COURSE) : WINTER - 2017

## SUBJECT : INFORMATION SECURITY

Day : **Thursday**
Date : **30/11/2017**

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

**W-2017-2815**

---

**N.B. :**

1) All questions are **COMPULSORY**.
2) Figures to the right indicate **FULL** marks.
3) Draw neat diagram **WHEREVER** necessary.

---

**Q.1** **a)** What is Fermat's Little theorem? **(06)**
Suppose. n = 7 and p=19 then prove Fermat's Little theorem.

**b)** What are properties of Fermat's Little theorem? **(04)**

**OR**

What is Hill cipher crypto-analysis? Differentiate Affine and Hill cipher techniques? **(10)**
Suppose the plain text 'Friday' is encrypted using a Hill cipher with m = 2 to give the cipher test 'PQCFKU'. Find K.

**Q.2** Differentiate between authentication and authorization. What are various ways of achieving authentication? Explain. **(10)**

**OR**

What are basic components of Intrusion Detection System (IDS)? Explain different types of IDS. **(10)**

**Q.3** What is Internet security policy? Why do we need it also explain employee internet usage policy. **(10)**

**OR**

What is intellectual property (IP)? Is it offered the same protection in every country of the world? Explain intellectual property rights included. **(10)**

**Q.4** How does a threat to information security differ from an attack? **(10)**

**OR**

Explain components of risk identification. Also differentiate between quantitative and qualitative risk control practices. **(10)**

**Q.5** Explain RSA algorithm and state approaches for breaking RSA algorithm. **(10)**

**OR**

Explain elliptic curve architecture. **(10)**

**Q.6** Explain the concept of information security audit. What are various principles of information security audit? **(10)**

**OR**

Explain various computer forensic techniques and tools. **(10)**

* * * * *