[5254]-670

B.E. (Computer) (Semester - I)

EMBEDDED SECURITY

(2012 Pattern) (Elective - II)

Time : 2½ Hours] *[Max. Marks : 70*

Instructions to the candidates:

1) *Attempt Q1 or Q2, Q3 or Q4, Q5 or Q6, Q7 or Q8, Q9 or Q10.*
2) *Figures to the right indicate full marks.*
3) *Draw neat diagram wherever necessary.*
4) *Assume Suitable data, if necessary.*

Q1) a) Explain EPID (Enhanced Privacy Identification) **[4]**

b) Differentiate between Intel AMT vs. Intel vPro Technology. **[6]**

OR

Q2) a) Explain in brief eBay data breach? **[4]**

b) Explain PAVP with neat diagram? **[6]**

Q3) a) Explain in detail Digital signature algorithm. **[4]**

b) Explain the embedded security and management engine. **[6]**

OR

Q4) a) Explain the boot integrity. **[4]**

b) Write short notes on:

i) Random number generation.

ii) Message Authentication. **[6]**

Q5) a) Differentiate between BIOS and UEFI. **[8]**
b) Explain features of Trusted Platform Module (TPM) **[8]**

OR

Q6) a) Differentiate between Field programmable Fuses vs. Flash Storage. **[8]**
b) What is Intel Boot Guard, Measured Boot, Verified Boot? **[8]**

Q7) a) Explain types and levels of rights protection to protect for content. **[8]**
b) What are Dynamic application Loader security considerations? **[8]**

OR

Q8) a) Explain popular Digital Right Managements (DRMs) used for protecting online media. **[8]**
b) Explain block diagram of Intel's Hardware - Based Content Protection in detail. **[8]**

Q9) a) Write short notes on: **[9]**
    i) Anonymous Authentication.
    ii) Secure Session Establishment.
    iii) Basic utilities of embedded security.
b) Explain the building Blocks for Embedded security? **[9]**

OR

*Q10)*a) Explain Firmware components of security and management engine using neat block diagram? **[9]**
b) Write a short note on: **[9]**
    i) Protected Input and output.
    ii) Software guard extension.
    iii) DAL.

○○○