**B. TECH. (CBCS - 2014 COURSE) SEM - VIII (INF. TECH.) :**
**SUMMER - 2018**

**SUBJECT: 3) ELECTIVE – III NETWORK SECURITY & CRYPTOGRAPHY**

Day: **Tuesday** **S-2018-4694** Time: **02.30 PM TO 05.30 PM**
Date: **12/06/2018** Max Marks. : 60

---

**N.B. :**

1) All questions are **COMPULSORY**.
2) Figures to the right indicate **FULL** marks.
3) Assume suitable data, if necessary.
4) Use of non programmable calculator is **ALLOWED**.
5) Draw neat and labeled diagrams **WHEREVER** necessary.

---

**Q.1** List different types of Cipher Techniques and explain any two types in detail. **(10)**

**OR**

**Q.1** State Euclid's algorithm and define how GCD calculated with it? Calculate the GCD of (270, 192). **(10)**

**Q.2** With neat sketch diagram, explain Network Security Model. **(10)**

**OR**

**Q.2** Elaborate on Security Systems Development Life Cycle in detail. **(10)**

**Q.3** Write down Triple DES algorithm and explain it with neat diagram. **(10)**

**OR**

**Q.3** Define and explain various steps involved in Diffie – Hellman key exchange algorithm, with its advantages and disadvantages. **(10)**

**Q.4** Discuss the objectives and Security features of HMAC. Compare HMAC with CMAC. **(10)**

**OR**

**Q.4** How Digital Signature is used for message authentication? Discuss how signing and verification is done using DSS. **(10)**

**Q.5** Describe about X.509 authentication procedures along with its certificate format. **(10)**

**OR**

**Q.5** Explain Secure Electronic Transaction (SET) with suitable example in detail. **(10)**

**Q.6** Write a short note on: **(10)**

**i)** Electronic Mail Security
**ii)** Methods involved in Source Authentication.

**OR**

**Q.6** Express general aspect of Internet key management and distinguish between online and offline key distribution system. **(10)**

* * * * * *

120618-e-engineering-pune