

**PE-519-CV-19**  
**M.Sc. COMPUTER SCIENCE (4<sup>th</sup> Semester)**  
**Examination, June 2022**  
**Paper-II**  
**SECURITY & CRYPTOGRAPHY**

**Time : Three Hours]**

**[Maximum Marks : 80**  
**[Minimum Pass Marks : 29**

---

**Note :** Answer from both the Sections as directed. The figures in the right-hand margin indicate marks.

---

**Section-A**

**1. Answer the following multiple choice type questions.** **1x10=10**

- (a) The.....is the message after transformation.  
i). Cipher text    ii). Plaintext    iii). Secret-text    iv). None of these
- (b) User cipher is an example of.  
i). Poly-alphabetic cipher    ii). Mono-alphabetic cipher  
iii). Multi-alphabetic cipher    iv). Bi-alphabetic cipher
- (c) A DES function has .....components.  
i). 2    ii). 3    iii). 4    iv). 5
- (d) ECB and CBC are.....ciphers  
i). Block    ii). Stream    iii). Field    iv). None
- (e) Which of these in a public-key cryptography method.  
i). RSS    ii). RAS    iii). RSA    iv). RAA
- (f) The SSL divides the data into blocks of .  
i).  $2*6$     ii).  $2*14$     iii).  $2*20$     iv).  $2*24$
- (g) A proxy firewall filter is at the.  
i). Physical Layer    ii). Application Layer  
iii). Data Link Layer    iv). Network Layer
- (h) In affine block cipher systems if.  $f(m_1) = Am + t$ , what is  $f(m_1 + m_2)$   
i).  $f(m_1) + f(m_2) + t$     ii).  $f(m_1) + f(m_2) + 2t$   
iii).  $f(m_1) + t$     iv).  $f(m_1) + f(m_2)$
- (i) Author names for message authentication codes is cryptographic.....  
i). Code break    ii). Code sum    iii). Check sum    iv). Check out
- (j) AES has.....different configurations:  
i). Two    ii). Three    iii). Four    iv). Five

**2. Answer the following short answer type questions:** **2x5=10**

- (a) What is secret Key?
- (b) What is Key distribution?
- (c) What is hash function?
- (d) What is SET?
- (e) What is Intrusion in system?

**Section-B**

**12x5=60**

**Answer the following long answer type questions:**

**3. Explain TCP/IP model.**

**OR**

**Explain mathematical tools of cryptography.**

**4. What is DES? Explain strength of DES? How it differs from AES?**

**OR**

**Explain block cipher design principal.**

**5. Explain various key management techniques.**

**OR**

**Explain Hash and MAC algorithm.**

**6. What is user authentication? What are its principle? What is remote user authentication?**

**OR**

**Explain email-security in detail.**

**7. Explain IDPS in detail.**

**OR**

**What is firewall? How it works? Explain the difference in firewall & antivirus.**