Reg.No. \_\_\_\_\_\_\_\_\_\_\_\_

G:\logo and QP Template\logo 3 Feb 2018 final.tif

**End Semester Examination – Nov/Dec – 2018**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| **Code :** | **14CS2008** | **Duration :** | **3hrs** |
| **Sub. Name :** | **CRYPTOGRAPHY AND NETWORK SECURITY** | **Max. marks :** | **100** |

**ANSWER ALL QUESTIONS (5 x 20 = 100 Marks)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Q. No.** | **Sub Div.** | **Questions** | **Course**  **Outcome** | **Marks** |
| 1. | a. | Analyze the Feistel cipher structure and elaborate Feistel encryption and decryption. | CO1 | 15 |
| b. | List and brief three passive and active attacks. | CO3 | 5 |
| (OR) | | | | |
| 2. | a. | Suppose that the following depicts the input key to the AES algorithm.   |  |  |  |  | | --- | --- | --- | --- | | K0 | K4 | K8 | K12 | | K1 | K5 | K9 | K13 | | K2 | K6 | K10 | K14 | | K3 | K7 | K11 | K15 |   Each Column is denoted as a *word w.* By this way, the input is represented as *w0 w1 w2 w3.* How is the key for round-**4** of AES encryption process generated? (Use appropriate diagram and explain each step) | CO2 | 10 |
| b. | Illustrate the general structure of data encryption standard and elaborate on the single round function of DES. | CO2 | 10 |
|  |  |  |  |  |
| 3. |  | Mr. Dexter wants to set up his own public and private keys. He chooses *p = 7* and *q = 11* with  a. Find **d** so that *ed is congruent to* 1 when divided by *(p-1) (q-1)* if e=13*.*  b. Callie wants to send a message *M = 2* to Dexter. Using Dexter’s public and private keys, calculate the cipher text *C*, and the value of *M* when Alice recovers the message.  c. Explain the appropriate public key encryption/decryption algorithm with all the requirement criteria. | CO2 | 20 |
| (OR) | | | | |
| 4. |  | Examine the ElGamal public Cryptosystem in detail. Perform encryption and Decryption procedure using ElGamal technique for the given data:  **p/q = 23**, **g/α = 7**, **x/xA = 5** for the message **M=3** also the random integer, **k = 3**. | CO2 | 20 |
|  |  |  |  |  |
| 5. | a. | Examine the work flow and application of Kerberos version 5 authentication process. | CO3 | 15 |
| b. | Discuss the advancements of Kerberos version 5 in comparison to version 4 and the attacks its can prevent. | CO3 | 5 |
| (OR) | | | | |
| 6. |  | Explain the authentication service provided by X.509 standard with inclusion of certificates, Certificate Authority hierarchy, certificate revocations and extensions. | CO3 | 20 |
|  |  |  |  |  |
| 7. | a. | Explain IP security architecture using a neat diagram. | CO1 | 10 |
| b. | Discuss in detail about Encapsulating security payload. | CO1 | 10 |
| (OR) | | | | |
| 8. |  | Portray the features of Secure Socket Layer for web security such as SSL Architecture, SSL record protocol, SSL record format and SSL handshake protocol. | CO1 | 20 |
|  | |  |  |  |
|  | | **Compulsory**: |  |  |
| 9. | a. | Discuss the types of intruders. | CO3 | 5 |
| b. | Explain the need and types of firewalls. | CO1 | 15 |