|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Roll No |  |  |  |  |  |  |  |  |  |  |  |

PRESIDENCY UNIVERSITY BENGALURU

SCHOOL OF ENGINEERING

MAKE UP EXAMINATION - JULY 2024

|  |  |
| --- | --- |
| **Semester : 6** | **Date : 09/07/2024** |
| **Course Code : CSE3078/CSE215** | **Time : 9.30AM -12.30PM** |
| **Course Name : Cryptography and Network Security** | **Max Marks : 100** |
| **Program : B.Tech** | **Weightage : 50%** |

**Instructions:**

1. *Read all questions carefully and answer accordingly.*
2. *Question paper consists of 3 parts.*
3. *Scientific and non-programmable calculator are permitted.*
4. *Do not write any information on the question paper other than Roll Number.*

|  |  |  |  |
| --- | --- | --- | --- |
| **PART A** | | | |
| **ANSWER ANY 5 QUESTIONS 5Q X 4M=20M** | | | |
| 1 | What is cryptosystem? List the components of crypto system and explain in detail | (CO 1) | [Knowledge] |
|  | | | |
| 2 | Differentiate between block cipher and stream cipher with an example | (CO 1) | [Knowledge] |
|  | | | |
| 3 | Explain why one should avoid selecting Very small or Very large block size in Block Cipher Encryption method | (CO 2) | [Knowledge] |
|  | | | |
| 4 | What is man in the middle attack? Explain | (CO 3) | [Comprehension] |
|  | | | |
| 5 | Draw a block diagram of Message Digest Generation Using SHA-512 | (CO 3) | [Comprehension] |
|  | | | |
| 6 | What is Kerberos? What are its requirements. | (CO 4) | [Comprehension] |
|  |  |  |  |
| 7 | What is SSL? explain | (CO 4) | [Knowledge] |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **PART B** | | | |
| **ANSWER ANY 5 QUESTIONS 5Q X 10M=50M** | | | |
| 8 | 1. List and explain the principles of key management 2. Given the Key a=6, b=9 and the plain text FRIEND. Find the cipher text using Affine cipher technique. | (CO 1) | [Analyze] |
|  | | | |
| 9 | Mr.Alex wants to send a message to his friend as “DANGER LEAVE THE HOUSE AFTER EIGHT” but he wants to send it secretly by encrypting the message. Take key as “FRIEND” and padding as “Q”, and help Alex in sending the message securely by using Playfair cipher | (CO 1) | [Analyze] |
|  | | | |
| 10 | List and explain the Block Cipher design principles | (CO 2) | [Knowledge] |
|  | | | |
| 11 | Differentiate between symmetric and asymmetric key algorithm | (CO 3) | [Knowledge] |
|  | | | |
| 12 | Explain the key generation steps in RSA | (CO 3) | [Comprehension] |
|  | | | |
| 13 | The integer p = 17 is prime. You are the eavesdropper and know that Alice and Bob use the Diffie-Hellman key-exchange with generator α = 3. Assume secret key of a is 12 and b is 14. What is the shared key of Alice and Bob? | (CO 4) | [Analyze] |
|  |  |  |  |
| 14 | With a block diagram explain the benefits of IPSec | (CO 4) | [Knowledge] |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **PART C** | | | |
| **ANSWER ANY 2 QUESTIONS 2Q X 15M=30M** | | | |
| 14 | With a block diagram explain Feistel Network Operation in detail | (CO 2) | [Knowledge] |
|  | | | |
| 15 | Jennifer creates a pair of keys for herself. She chooses p = 397 and q = 401. She calculates n = 159197. She then calculates φ(n) = 158400. She then chooses e = 343 and d = 12007. Show how Ted can send a message to Jennifer if he knows e and n.  Suppose Ted wants to send the message “NO” to Jennifer. He changes each character to a number (from 00 to 25), with each character coded as two digits. He then concatenates the two coded characters and gets a four-digit number | (CO 3) | [Analyze] |
|  | | | |
| 16 | Explain Pretty Good Privacy (PGP) in details | (CO 4) | [Comprehension] |