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

 ****

**Presidency University**

**Bengaluru**

 **SCHOOL OF** COMPUTER SCIENCE AND ENGINEERING

**Make-Up Examinations, July 2024**

**Course Code**: CSE 3078

**Course Name**: Cryptography and Network Security

**Program** : B.Tech (CCS)

**Date**: 19-07-2024

**Time**: 01:30 PM – 04:30 PM

**Max Marks**: 100

**Weightage**: 50%

 **Instructions:**

1. *Read the all questions carefully and answer accordingly.*
2. *Do not write any matter on the question paper other than roll number.*

**Part A [Memory Recall Questions]**

**Answer all the Questions. Each question carries** 0**2 marks. (**10**Qx 2M=** 2**0M)**

1. List out any 4 security services defined by OSI security architecture (C.O.No.1) [Knowledge]

2. What are the benefits of IP Security? (C.O.No.4) [Knowledge]

3. Mention two scenarios where you need to have filler characters in playfair cipher (C.O.No.1) [Knowledge]

4. Find 117 mod 13. (C.O.No.2) [Comprehension]

5. Which key is used for deriving and verifying Digital signature. (C.O.No.3) [Knowledge]

6. What are the keys used by PGP? (C.O.No.4) [Knowledge]

7. Define Commutative group in number theory. (C.O.No.2) [Knowledge]

8. Differentiate between the block and stream cipher. (C.O.No.1) [Knowledge]

9. Explain the purpose of s-boxes in DES algorithm. (C.O.No.2) [Knowledge]

10.Define public key cryptography. (C.O.No.3) [Knowledge]

 **Part B [Thought Provoking Questions]**

**Answer all the Questions. Each question carries** 10 **marks. (**5**Qx**1**0M=**5**0M)**

11. Encrypt the message “WINTER” using hill cipher with the following key matrix

 K = $\begin{matrix}12&15&8\\7&10&10\\4&19&22\end{matrix}$ (C.O.No.1) [Comprehension]

12. a) calculate 28-1 mod 161 using extended euclidean algorithm.

 b) calculate GCD(27, 2265) using euclidean algorithm. (C.O.No.2) [Comprehension]

13. Given two prime numbers 11 and 17. Calculate the encryption and decryption key using RSA algorithm (C.O.No.3) [Comprehension]

14. Answer the following with respect to AES Algorithm.

(a). List all the operations involved in AES algorithm.

(b). How many times these operations will be performed for 128 bits plaintext and 128 bits key?

(c). Explain concept of shift\_rows operation in detail. (C.O.No.2) [Comprehension]

15. Explain Kerberos authentication mechanism in detail with suitable diagram. (C.O.No.4) [Comprehension]

**Part C [Problem Solving Questions]**

**Answer all the Questions. Each question carries** 15 **marks. (**2**Qx**15**M=**3**0M)**

16. User Alice and Bob use the Diffie-Hellman key exchange technique with a common prime

q = 11 and a primitive root ɑ = 2.

* 1. Show that 2 is a primitive root of 11.
	2. If user A has public key YA = 9, what is A’s private key XA?
	3. If user B has public key YB = 3, what is B’s Private key XB?
	4. What is the shared secret key?

 (C.O.No. 3) [Application]

17. Using Chinese Remainder Theorem find the value of x for the given set of congruent equations
x≡ 1(mod5)
x≡ 2(mod7)
x≡ 3(mod9)
x≡ 4(mod11)

 (C.O.No. 2) [Application]