Seat No. _____

KADI SARVA VISHWAVIDYALAYA

BE SEMESTER-VI (Computer Engineering) Examination April - 2024

Subject Name: Cryptography and Network Security
Subject Code: CE603-N

Date: 04/04/2024 **Time: 12:00 pm to 03:00 pm** **Total Marks: 70**

Instructions:
1. Answer each section in separate answer sheet.
2. Use of scientific calculator is permitted.
3. All questions are Compulsory.
4. Indicate clearly, the option you attempt along with its respective question number.
5. Use the last page of main supplementary for rough work.

Section-I

Q-1 (A) Decrypt the plaintext "attack" using Hill cipher for the given key = $\begin{vmatrix} 2 & 3 \\ 3 & 6 \end{vmatrix}$ [5]

(B) Draw the general structure of AES and briefly explain it. [5]

(C) Describe and illustrate the Chinese Reminder Theorem. [5]

OR

(C) Find the gcd of following number pairs using Euclidean algorithm. [5]
1) 24140 and 6409
2) 3997 and 2947

Q-2 (A) Explain Playfair Cipher substitution technique in detail. Find out cipher text for the following given key and plaintext. [5]
Key = COMPUTER
Plaintext= COMMUNICATE.

(B) Explain the triple DES scheme with two keys and three keys. [5]

OR

Q-2 (A) What are different security attacks. describe any two in brief. [5]

(B) Why mode of operation is defined? Explain the block cipher modes of Operation. [5]

Q-3 (A) Calculate the multiplicative inverse of **550 mod 1769** using the Extended Euclidean Algorithm. [5]

(B) Perform the encryption and decryption using the RSA algorithm for the following p=13, q= 11, e = 13, M=13 [5]

OR

Q-3 (A) Explain Euler's totient function and Find the results of following: [5]
1) $\phi(97)$ 2) $\phi(35)$ 3) $\phi(28)$ 4) $\phi(43)$

(B) Explain Elliptic curve cryptography [5]

Section-II

Q-4 (A) Describe the desired properties of Hash function. [5]

(B) Explain differential cryptanalysis in detail. [5]

(C) Briefly explain Diffie-Hellman key exchange. [5]

OR

(C) User A and B use the Diffie-Hellman key exchange technique with common prime $q = 71$ and a primitive root $\alpha = 7$. [5]

1) If user A has private key $X_A = 5$, what is A's pubic key Y_A ?
2) If user B has private key $X_B = 12$, what is B's pubic key Y_B ?
3) What is the shared secret key?

Q-5 (A) Explain PGP message generation [5]

(B) What do you mean by Bitcoin Cryptocurrency? Explain in detail. [5]

OR

Q-5 (A) Explain Kerberos in detail. [5]

(B) What is Blockchain technology, describe various security features of blockchain technology in brief. [5]

Q-6 (A) Explain IP Security architecture. [5]

(B) Explain digital signature standard. [5]

OR

Q-6 (A) Describe the functions provided by S/MIME. [5]

(B) Explain Message Authentication Code in detail [5]

----------**All The Best** ----------