Exam Number: ____________

KADI SARVA VISHWAVIDYALAYA

B.E. 6th (ATKT) EXAMINATION DECEMBER 2023

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

Date: 16/12/2023(Saturday) Time: 12.00 pm to 03.00 pm **Total marks: 70**

Instructions:

1. **Answer each section in separate Answer sheet.**
2. **All questions are compulsory.**
3. **Indicate clearly, the options you attempt along with its respective question number.**
4. **Use the last page of main supplementary for rough work.**

Section-I

Q.1 (A) Explain Active and Passive Attacks with diagram. (5)

(B) Draw and explain Feistel's structure for encryption and decryption. (5)

(C) Differentiate asymmetric key cryptography and symmetric key cryptography. (5)

OR

(C) Prove that Fermat's theorem holds true for p=13 and a=11. (5)

Q.2 (A) Explain DES algorithm with neat Diagram. (5)

(B) What is the multiplicative inverse of (11 mod 13)? (5)

OR

Q.2 (A) Discuss Electronic code book and cipher feedback mode with neat diagrams. (5)

(B) Find the GCD(252,105) using Euclidean's Algorithm. (5)

Q.3 (A) Find Euler's Totient for following: (5)

(i) Φ (8)

(ii) Φ (11).

(B) Perform encryption and decryption using the RSA algorithm for p=3, q=11, e=7, M=5. (5)

OR

Q.3 (A) Explain Encryption and decryption in RSA algorithm. (5)

(B) Discuss Diffie-Hellman key exchange algorithm in detail. (5)

Section-II

Q.4 (A) What characteristics are needed in secure hash function? Explain the concept of simple hash function?

(B) Briefly explain basic uses of MAC.

(C) What are the requirements of digital signature? Explain the concept of arbitrated digital signature?

OR

(C) Explain MD5 Hash Algorithm.

Q.5 (A) Explain differential and linear cryptanalysis.

(B) Write a note on: X.509 Certificate Format.

OR

Q.5 (A) Explain Side Channel Attack.

(B) What is Kerberos? How Kerberos authenticates the users for authorized service access?

Q.6 (A) Discuss SSL architecture in brief.

(B) Differentiate Identity Based Encryption and Attribute Based Encryption.

OR

Q.6 (A) Explain IPSec Protocol.

(B) Explain four stages of a single round in AES.

****

Exam Number:____________

KADI SARVA VISHWAVIDYALAYA

B.E. 6th (REG/ATKT) EXAMINATION APRIL 2023

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

Date: 06/04/2023(Thursday) Time: 10.00 am to 01.00 pm **Total marks: 70**

Instructions:

1. **Answer each section in separate Answer sheet.**
2. **All questions are compulsory.**
3. **Indicate clearly, the options you attempt along with its respective question number.**
4. **Use the last page of main supplementary for rough work.**

Section-I

Q.1 (A) Explain Active and Passive Attacks with diagram. (5)

(B) Draw and explain Feistel's structure for encryption and decryption. (5)

(C) What is the difference between a block cipher and a stream cipher? (5)

OR

(C) List various modes of operations. Explain any three of them briefly. (5)

Q.2 (A) Explain various steps of AES in short. (5)

(B) What is the multiplicative inverse of (11 mod 13)? (5)

OR

Q.2 (A) Explain Encryption and decryption in RSA algorithm. Perform encryption and decryption using the RSA algorithm for p=3, q=11, e=7, M=5. (5)

(B) Find the GCD(252,105) using Euclidean's Algorithm. (5)

Q.3 (A) Find Euler's Totient for following: (5)

(i) Φ (8)

(ii) Φ (7000)

(B) Explain RSA algorithm in detail with suitable example. (5)

OR

Q.3 (A) Prove Fermat's theorem holds true for following: (5)

(i) p = 5 and a = 2

(ii) p = 13 and a = 11

(B) Briefly explain Diffie-Hellman key exchange. Is it vulnerable to man in the middle attack? Justify. (5)

Section-II

Q.4 (A) What is public key cryptography? Differentiate public key cryptography and symmetric key cryptography.

(B) What is message authentication code? What are the requirements for MACs?

(C) Explain the general structure of secure hash functions.

OR

(C) Briefly explain SSL and TLS?

Q.5 (A) Explain Email Security and Role of PGP.

(B) Explain Side Channel Attack.

OR

Q.5 (A) Explain any one approach to Digital Signatures.

(B) Explain Time- Memory Trade-off Attack.

Q.6 (A) What is Kerberos? How Kerberos authenticates the users for authorized service access? (four requirements of Kerberos, TGS).

(B) Briefly explain Attribute-based Encryption (ABE).

OR

Q.6 (A) Briefly explain Identity-based Encryption (IBE).

(B) Illustrate basic concept of Blockchain and Bitcoin.

****

Seat No.								

KADI SARVA VISHWAVIDYALAYA

B.E. Semester-VI Examination (December-2022)

SUBJECT CODE: CE603-N **SUBJECT NAME: Cryptography and Network Security**
DATE: 14/12/2022 **TIME: 10.00 A.M. to 1:00 P.M.** **TOTAL MARKS: 70**

Instructions:
1. Answer each section in separate Answer Sheet.
2. All questions are compulsory.
3. Indicate clearly, the options you attempted along with its respective question number.
4. Use the last page of main supplementary for rough work.

SECTION – 1

Q-1. A) Explain Security Services in detail. [5]

B) Draw and explain the model for network security. [5]

C) Explain Feistel Cipher Structure. [5]

OR

C) Explain the difference between active and passive attack using any example. [5]

Q-2. A) Draw and explain the structure of AES Encryption algorithm. [5]

B) List the block cipher modes of operation. Which one is simplest and why? [5]

OR

Q-2. A) Explain single round function of DES with suitable diagram. [5]

B) Explain Cipher feedback mode of operation in detail with figure. [5]

Q-3. A) Explain Extended Euclidian Algorithm. [5]

B) Users A and B use the Diffie-Hellman key exchange technique with common prime q = 71 and a primitive root α = 7. [5]
a.) If user A has private key X_A = 5,
what is A's public key YA?
b.) If user B has private key X_B = 12, what is B's
public key YB?
c.) What is the shared secret key?

OR

Q-3. A) Find the encryption of "*DEMONETIZATION* "using playfair algorithm. Use the secret key "MODI". [5]

P.T.O

B) Perform encryption and decryption using the RSA algorithm for p=3; q=11; e=7; M=5 [5]

SECTION – 2

Q-4. A) Write a short note on Steganography. [5]

B) Describe the desired properties of a Hash function. [5]

C) Explain Triple DES with two keys. [5]

OR

C) Differentiate between Private Key cryptography and Public key cryptography. [5]

Q-5. A) Write a short note on Kerberos. [5]

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

OR

Q-5. A) Explain Digital Signature Standard. [5]

B) Explain One-time pad technique. [5]

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

B) Explain IP Security Architecture. [5]

OR

Q-6. A) What is Transport Layer Security? Explain in detail. [5]

B) Write about fermat's theorem. [5]

******BEST OF LUCK******

Seat No.								

KADI SARVA VISHWAVIDYALAYA

B.E. Semester-VI Examination (April-2022)

SUBJECT CODE: CE603-N **SUBJECT NAME: Cryptography and Network Security**
DATE: 12/04/2022 **TIME: 12.30 P.M. to 3:30 P.M.** **TOTAL MARKS: 70**

Instructions:
1. Answer each section in separate Answer Sheet.
2. All questions are compulsory.
3. Indicate clearly, the options you attempted along with its respective question number.
4. Use the last page of main supplementary for rough work.

SECTION – 1

Q-1. A) Explain Security Services in detail. [5]

B) Explain Euler's Theorem in detail. [5]

C) Explain Feistel Cipher Structure. [5]

OR

C) Explain Steganography in detail. [5]

Q-2. A) Describe SubBytes, ShiftRows, MixColumns and AddRoundKey in AES (Advanced Encryption standard). [5]

B) Explain Electronic code Book block cipher mode of operation in detail with figure. [5]

OR

Q-2. A) Explain single round function of DES with suitable diagram. [5]

B) Explain Cipher feedback mode of operation in detail with figure. [5]

Q-3. A) Find the multiplicative inverse of following using extended Euclidean algorithm. [5]
(1) 50 mod 71
(2) 43 mod 64

B) Users A and B use the Diffie-Hellman key exchange technique with a common prime q = 71 and a primitive root $\alpha = 7$. [5]
a.) If user A has private key XA = 5,
what is A's public key YA?
b.) If user B has private key XB = 12, what is B's
public key YB?
c.) What is the shared secret key?

OR

Q-3. A) Encrypt the following message using playfair cipher. [5]

P.T.O

Message: INSTRUMENTS Keyword: MONARCHY

B) Perform encryption and decryption using the RSA algorithm for p=3; q=11; e=7; M=5 [5]

SECTION – 2

Q-4. A) Differentiate Conventional Encryption vs. Public-Key Encryption. [5]

B) Explain X.509 Certificate Format. [5]

C) Explain Triple DES with two keys. [5]

OR

C) Explain SHA- Secure Hash Algorithm. [5]

Q-5. A) Write a short note on Kerberos. [5]

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

OR

Q-5. A) Explain Digital Signature Standard. [5]

B) Describe the desired properties of a Hash function. [5]

Q-6. A) What is Blockchain? Explain advantages and Disadvantages of Blockchain. [5]

B) Explain IP Security Architecture. [5]

OR

Q-6. A) What is Transport Layer Security? Explain in detail. [5]

B) Explain Attribute-based encryption. [5]

********BEST OF LUCK********