Seat No: ________

Kadi Sarva Vishwavidyalaya

B.E. (C.E.) Semester – VI Nov 2015

Sub code: CE-601 **Subject: Cryptography and Network Security**
Date: 06/11/2015 **Time: 10.30 am to 1.30 pm** **Max.Marks:70**

Instruction:

(1) Answer each section in separate Answer sheet
(2) Use of Scientific calculator is permitted
(3) All questions are compulsory.
(4) Indicate clearly, the options you attempted along with its respective question number
(5) Use the last page of main supplementary for rough work.

Section – I

Q.1

[A] Explain the Model of Network Security [5]

[B] Explain RSA algorithm with example [5]

[C] ax + by = gcd (a,b) is stated in the extended Euclidean algorithm. Computer x and y for a = 1239 and b = 735. [5]

OR

[C] Compute the following: [5]

i. 12+18(mod 9)
ii. 3*7(mod 11)
iii. (103 (mod 17))*(42 (mod 17)) (mod 17)
iv. 103*42 (mod 17)
v. 72 (mod 13)

Q.2

[A] Discuss the difference between symmetric key and public key cryptography [5]

[B] Explain MD5 Message Digest algorithm [5]

OR

Q.2

[A] Explain Kerberos [5]

[B] Write about Modes of Operations namely: ECB, Counter and OFB and compare their strengths. [5]

Q.3

[A] Write about the strengths and weaknesses of S-Box in DES [5]

[B] Find public key and private key using RSA for following data: p=7 q=13 e= 5. Also encrypt the letter "z". [5]

OR

Q.3

[A] Write about Firewalls and honeypots. [5]

[B] Describe various access control mechanisms in Network Security [5]

Seat No: ________

Section – II

Q.4

[A] Differentiate between active and passive attacks [5]

[B] Ceaser cipher is vulnerable to which type of attack? Explain with an example supporting your claim [5]

[C] Compute 3^{31} (mod 7) and 29^{25} (mod 11) [5]

OR

[C] Explain Eulers theorem with example [5]

Q.5

[A] Write about Digital Signatures [5]

[B] Explain Elliptic Curve Cryptography in detail using diagrams [5]

OR

Q.5

[A] Write a note on block cipher design principles. [5]

[B] Write about AES key generation technique. [5]

Q.6 [A] Write about email security and the role of PGP [5]

[B] Write about SHA [5]

OR

Q.6

[A] Explain rail-fence cipher [5]

[B] Write about the need of authentication in network communication [5]

Seat No. _______ Enrl. No. ________________

KADI SARVA VISHWAVIDYALAYA

BE SEMESTER-VI Regular Examination APRIL-2015

Subject Code: CE - 601

Subject Name: Cryptography and Network Security

Date: 27/04/2015 **Time: 10:30 AM to 01:30 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 of rough work.

Section-I

Q-1 **(A)** Differentiate between Elgamal encryption and Diffie Hellman Key Exchange [5]

(B) Write about the design of S-BOX and its use in DES [5]

(C) Explain the following with suitable example: [5]
Rail-Fence Cipher
Monoalphabetic Cipher

OR

(C) Draw and explain conventional model of cryptography. [5]

Q-2 **(A)** Explain AES key generation algorithm. [5]

(B) Give brief overview of Kerberos [5]

OR

(A) Explain the terms with example [5]
Integrity, Non Repudiation

(B) Explain MD5. [5]

Q-3 **(A)** Explain how Group property P (dot) I ≡ P is satisfied in Elliptic Curve Cryptography. [5]

(B) Differentiate between public key cryptography and symmetric key cryptography. [5]

OR

(A) How access control is achieved in Network Security. [5]

(B) Explain with example: Honeypots, Firewalls [5]

Section-II

Q-4 **(A)** Give the public and private key combination in RSA for n=33, e=7. Also encrypt plaintext m=2. [5]

(B) Encrypt "ACT" using hill cipher. Key matrix is as follows [5]

6	24	1
13	16	10
20	17	15

(C) Find secret key in diffie hellman key exchange for following data [5]

Prime number = 23, base = 5 secret integer for sender= 6 and secret integer for receiver = 15

OR

(C) Write about fermat's theorem and the concept of generators. Also briefly describe the concept of discrete logarithm derived from fermat's theorem. [

Q-5 **(A)** Encrypt "rahi" with playfair using key "mendacious" [5]

(B) Find 5^{1001} mod 11 [5]

OR

(A) Write about possible cryptanalytic attacks on ceaser cipher. [5]

(B) Explain PGP. [5]

Q-6 **(A)** Discuss various Modes of operations in symmetric key cryptography. [5]

(B) Write about digital signatures. [5]

OR

(A) Explain SHA. [5]

(B) How is "man in the middle attack" conceived while exchanging secret key using public key cryptography? [5]

---x---