Seat No.								

KADI SARVA VISHWAVIDYALAYA

B.E. Semester-VI Examination (April-2019)

SUBJECT CODE: CE-601 SUBJECT NAME: Cryptography and Network Security
DATE:12/4/2019 TIME: 10:30A.M to 1:30 P.M 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. Indicateclearly, the options you attempted along with its respective question number.
5. Use the last page of main supplementary for rough work.

SECTION –1

Q-1.	**a)**	Perform encryption and decryption using RSA for p=11,q=13,e=11,M=7.	**5**
	b)	Encrypt the message "The Royal Army"using Playfair cipher where key is "cipher".	**5**
	c)	Explain AES with figure.(detailed explanation on individual functional block may not be required)	**5**
		OR	
	c)	Explain single round of DES with figure.	**5**
Q-2.	**a)**	Explain block cipher design principles.	**5**
	b)	Explain Extended Euclidean theorem with one example.	**5**
		OR	
Q-2.	**a)**	Differentiate between block cipher and stream cipher. Explainany two, block cipher modes of operation.	**5**
	b)	State and prove Fermat theorem.	**5**
Q-3.	**a)**	Explain CIA model for network security.	**5**
	b)	Explain any two schemes for distribution of public keys.	**5**
		OR	
Q-3.	**a)**	Explain specific security mechanisms.	**5**
	b)	Explain how we can use public key cryptography for distribution of secret keys.	**5**

P.T.O

SECTION – 2

Q-4.	a)	Explain Content Integrity and Strong authentication in relation with Network security.	5
	b)	Explain any two intrusion detection systems.	5
	c)	Explain PGP services.	5
		OR	
	c)	Explain the format of PGP message.	5
Q-5.	a)	Explain Diffie Hellman Key Exchange algorithm.	5
	b)	What is the need of firewall? Explain types of firewall.	5
Q-5.	a)	Explain Elgamal algorithm.	5
	b)	Explain S/MIME functionalities.	5
Q-6.	a)	Explain Digital signatures.	5
	b)	Explain MD5.	5
		OR	
Q-6.	a)	Explain basic uses of MAC.	5
	b)	Explain SHA-512 with figure.	5

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

Seat No._____ Enrl. No. _____

KADI SARVA VISHWAVIDYALAYA

BE SEMESTER-VI Regular Examination APRIL-2018

Subject Code: CE601

Subject Name: Cryptography and Network Security

Date: 20/04/2018 **Time:10:30 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 option you attempt along with its respective question number.
4. Use the last page of main supplementary of rough work.

Section-I

Q-1 **(A)** Do as directed:

(i) Explain conventional encryption model with neat diagram. [3]

(ii) Explain any one block cipher mode of operation. [2]

(B) Using the playfair cipher and key "cupboard", encrypt the word : "complexity". [5]

(C) Draw the figure and explain the single round of DES algorithm. [5]

OR

(C) Explain the shift row and mix column transformation of AES algorithm [5]

Q-2 **(A)** Differentiate Conventional and Public-key cryptosystem [5]

(B) With figure explain – how the public key cryptosystem can provide authentication. [5]

OR

Q-2 **(A)** List the steps of RSA algorithm. With the value of two prime numbers $p = 11$ and $q = 7$, write one full example of RSA algorithm with the encryption and decryption of a message $M = 4$. [5]

(B) List the steps of Diffie-Hellman algorithm. With the value of common prime $q = 71$ and a primitive root $\alpha = 7$, write one full example of Diffie-Hellman algorithm for key generation along with the private and public keys on each user side. [5]

Q-3 **(A)** List the techniques for distribution of public keys. Explain any one of them. [5]

(B) List and explain the three properties required for securing a hash function. [5]

OR

Q-3 **(A)** Write the ElGamal algorithm. Explain the algorithm with one full example. Consider the values of a common prime $q=71$ and a primitive root $\alpha = 7$. [5]

(B) Explain the Internal and external error control with the help of checksum and encryption mechanism. [5]

Section-II

Q-4 (A) Using extended Euclidean algorithm find [5]

(i) $43^{-1} \bmod 73$

(ii) $395^{-1} \bmod 322$

(B) Calculate Following (for 4th and 5th problem use Fermat's theorem) [5]

(i) $\phi(125)$, (ii) $\phi(9000)$, (iii) $\phi(47)$, (iv) $3^{31} \bmod 7$, (v) $128^{129} \bmod 17$

(C) Prove that if n is an integer number and $n = p*q$, where p and q are prime numbers, then the Euler's totient function value $\phi(n) = (p-1)(q-1)$. [5]

OR

(C) Prove that for any integer number $n^{-1} \bmod (n-1) = 1$ and $(n-1)^{-1} \bmod n = (n-1)$ [5]

Q-5 (A) (i) List and define any three properties of digital signature [3]

(ii) List any two ways to distribute a shared secret key between two users A and B. [2]

(B) Explain the working of Kerberos. [5]

OR

Q-5 (A) (i) Explain the "Append padding bits" operation of MD5. [3]

(ii) Explain the usage of Nonce in secure data transmission [2]

(B) Explain how Kerberos support inter-realm authentication. [5]

Q-6 (A) Explain PGP. [5]

(B) Explain IPSec. [5]

OR

Q-6 (A) Explain Firewall. [5]

(B) Explain the approaches for Intrusion Detection. [5]

BEST OF LUCK

Seat No._____ Enrl. No. _____

KADI SARVA VISHWAVIDYALAYA

BE SEMESTER-VI Examination April-2017

Subject Code: CE601

Subject Name: Cryptography and Network Security

Date: 17-04-17 **Time:** 10:00 to 1:00 **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 Answer following Questions **[15]**

(A) List and explain various types of active and passive attacks. [5]

(B) Draw and explain the conventional encryption model used for security. [5]

(C) Write extended Euclidean algorithm. [5]

OR

(C) Write the Euclidean algorithm and show the steps to find gcd (1970, 1066). [5]

Q-2 Answer following Questions **[10]**

(A) Explain Fermat theorem. [5]

(B) Explain play fair cipher with suitable example. [5]

OR

Q-2 Answer following Questions **[10]**

(A) Explain hill cipher with suitable example. [5]

(B) Compare public key and private key cryptography. Also list various algorithms for each. [5]

Q-3 Answer following Questions **[10]**

(A) Explain single round function of DES with suitable diagram. [5]

(B) List various modes of operations of block cipher. Explain any two of them. [5]

OR

Q-3 Answer following Questions **[10]**

(A) Explain key expansion process in AES algorithm. [5]

(B) Explain Kerberos in brief. [5]

Section-II

Q-4 Answer following Questions **[15]**

(A) Write the steps of RSA algorithm. [5]

(B) Explain Deffie Hellman key exchange scheme in detail. [5]

(C) Briefly explain Elliptic Curve Cryptography. [5]

OR

(C) Discuss public key cryptosystem. [5]

Q-5 Answer following Questions **[10]**

(A) Explain MD5 Algorithm. [5]

(B) Write short note on: Message Authentication Code. [5]

OR

Q-5 Answer following Questions **[10]**

(A) Draw and explain the general structure of secure hash algorithm. [5]

(B) List and explain schemes for the distribution of public keys. [5]

Q-6 Answer following Questions **[10]**

(A) Explain types of Firewalls. [5]

(B) Briefly describe IDS. [5]

OR

Q-6 Answer following Questions **[10]**

(A) Explain the general format of Pretty Good Privacy (PGP) message. [5]

(B) Write short note on: Digital Signature. [5]

KADI SARVA VISHWAVIDYALAYA

B.E SEMESTER VI EXAMINATION (OCTOBER 2016)

SUBJECT CODE: CE 601 **SUBJECT NAME: Cryptography and Network Security**

DATE: 20/10/2016 TIME: 2.00PM TO 5.00PM TOTAL MARKS: 70

Instructions:

1. Answer each section in separate Answer sheet.
2. Use of scientific Calculator is permitted.
3. Al 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 (All Compulsory)

(A) List and briefly define the security services. 05

(B) What is cryptography? Briefly explain the model of Asymmetric Cryptosystem. 05

(C) Explain Steganography in detail. 05

OR

(C) Construct a playfair matrix with the key "occurrence". Generate the cipher text for the plaintext "Tall trees". 05

Q:2 (A) Draw and Explain the Single Round of DES algorithm. 05

(B) What is Double DES? Explain the meet-in-the-middle Attack. 05

OR

(A) Define the terms diffusion and confusion. What is the purpose of S-box in DES? 05

(B) Write the Euclid's algorithm and show the steps of Euclid's algorithm to find gcd(1970,1066). 05

Q:3 (A) State and Explain Euler's totient function. 05

(B) Why mode of operation is defined? Explain the block cipher modes of operation. 05

OR

(A) Explain the following with reference to modular arithmetic. 05

1. Set of Residues
2. Congruence
3. Additive and Multiplicative inverse.

(B) State and Prove Euler's Theorem with the help of an example. 05

SECTION 2

Q:4 (All Compulsory)

(A) Explain PGP message generation. . 05

(B) Explain Honeypots in detail. 05

(C) Perform encryption and decryption using the RSA algorithm for p=3,q=11, e=7, M=5. 05

OR

(C) What is a virus? Explain different types of viruses. 05

Q:5	(A)	Discus the ways in which public keys can be distributed to two communication parties.	05
	(B)	Write a short note on application-level gateways.	05
		OR	
	(A)	Write HMAC algorithm.	05
	(B)	Explain any two approaches for Intrusion detection.	05
Q:6	(A)	Explain the functions provided by S/MIME.	05
	(B)	Explain packet filtering router in case of firewall.	05
		OR	
	(A)	Write the Digital Signature Algorithm	05
	(B)	Explain Kerberos in detail.	05

Best of Luck

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]

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---