Enrollment No.									

KADI SARVA VISHWAVIDYALAYA

B.E. Semester-V Examination (Nov-2016)

SUBJECT CODE: IT-502 SUBJECT NAME: Information security

DATE: 11/11/2016 TIME: 10:30 A.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. Indicate clearly, 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)**	Define security attack and give difference between passive attack and active attack.	**5**
	b)	Encrypt the message "this is a secret message" using playfair cipher, key is "security".	**5**
	c)	Explain different security mechanisms.	**5**
		OR	
	c)	Explain OSI security Architecture.	**5**
Q-2.	**a)**	Define Block Cipher and explain the following terms with respect to block cipher: Diffusion, Confusion, Substitution, Permutation.	**5**
	b)	Draw a figure for Single round of DES algorithm and explain significance of S-Box in DES.	**5**
		OR	
Q-2.	**a)**	Explain CBC and OFB block cipher modes of operation.	**5**
	b)	Explain secrecy and authentication in relation to public key cryptosystems.	**5**
Q-3.	**a)**	Give requirements for public key cryptography.	**5**
	b)	Explain any two arbitrated digital signature techniques.	**5**
		OR	
Q-3.	**a)**	Give different requirements for digital signature.	**5**
	b)	What is hash function? Explain the structure of secure hash code.	**5**

P.T.O

SECTION – 2

Q-4.	a)	Explain Message Exchanges of Kerberos Version 4.	5
	b)	Calculate C using RSA if M=10, p=7, q=13.	5
	c)	What is malicious program and explain any two types of it.	5
		OR	
	c)	Explain the term virus and give different phases of virus.	5
Q-5.	a)	Explain general format of PGP Message.	5
	b)	What is covert channel? Explain its types.	5
		OR	
Q-5.	a)	Explain Firewall characteristics and list the firewall techniques.	5
	b)	Explain S/MIME Content Types.	5
Q-6.	a)	What is MAC? Explain the uses of MAC.	5
	b)	Explain any two intrusion detection systems.	5
		OR	
Q-6.	a)	Explain One time password and Honey pots related to authentication in network security.	5
	b)	What is password management and explain any two password selection strategies.	5

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

KADI SARVA VISHWAVIDHYALAYA

Subject Code: IT-502

Subject Name: INFORMATION SECURITY

Date: 14/11/2014 **Time: 10:30 AM to 1:30 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) Compare conventional encryption with public key encryption. [5]

(B) Define the terms threat and attack. List and briefly define categories of security Attacks. [5]

(C) Construct a Playfair matrix with the key "engineering". And encrypt the message "test this process". [5]

OR

(C) Construct a playfair matrix with the key "occurrence". Generate the cipher text for the plaintext "Tall trees" [5]

Q-2 (A) Define the Caesar cipher. Explain the one time pad scheme. [5]

(B) List and briefly define the security services. [5]

OR

(A) Explain mono alphabetic cipher and poly alphabetic cipher by giving an example [5]

(B) List and briefly define the security Mechanism. [5]

Q-3 (A) Give the steps of RSA algorithm. [5]

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

OR

(A) Calculate cipher text in case of RSA if p=3, q=11, e=3, M=5. [5]

(B) Explain the DES encryption algorithm. [5]

Section-II

Q-4	(A)	Write the Digital Signature Algorithm.	[5]
	(B)	Explain Kerberos in detail.	[5]
	(C)	Explain Substitute Byte Transformation in AES.	[5]
		OR	
	(C)	Explain the operation of secure hash algorithm on 512 bit block.	[5]
Q-5	(A)	Explain man-in-the middle attack with example.	[5]
	(B)	What characteristics are needed in a secure hash function?	[5]
		OR	
	(A)	Write a short note on Viruses and Trapdoors.	[5]
	(B)	Define Cryptography,Substitution,transposition,cryptanalyst,cryptanalysis	[5]
Q-6	(A)	Write a short note on S/MIME.	[5]
	(B)	Explain all types of Firewall.	[5]
		OR	
	(A)	Write a short note on PGP.	[5]
	(B)	Explain Intrusion detection system in brief.	[5]

---End---

En. Roll No. _____

KADI SARVA VISHWAVIDYALAYA

B.E. Semester – V (ATKT) EXAMINATION April-2015

Subject Code:- IT-502 Subject Name:- Information Security

DATE:-21/04/2015 **DURATION:- 3 Hours**

TIME: -10.30 am to 1.30 pm **MARKS:- 70 marks**

Instructions:

1. All questions are compulsory.
2. Make suitable assumptions wherever necessary
3. Figures to the right indicate full marks.
4. Give diagrams wherever required.

SECTION-I

Q1 A	Give different application of information security.(Any 5)	**[5]**
B	Draw and explain a model for Network Security.	**[5]**
C	Give difference between Active and Passive attacks.	**[5]**
	OR	
C	Explain about Rail-fence technique by giving Example.	**[5]**
Q-2		
A	Give comparison between Symmetric and Asymmetric cryptographic technique.	**[5]**
B	Write a short note on Working of Brute-force attack	**[5]**
	OR	
A	Explain poly-alphabetic cipher in detail.	**[5]**
B	Explain limitation of AES in details	**[5]**
Q-3		
A	Write a program to demonstrate ceaser cipher substitution technique.	**[5]**
B	Let the keyword in play-fair cipher is "keyword". Encrypt a message "Good Morning India" using play-fair substitution technique.	**[5]**
	OR	
A	Discuss DES in detail.	**[5]**
B	What is the purpose of S-box in DES?	**[5]**

SECTION-II

Q-4

A	Give a note on Honeypots.	**[5]**
B	What is firewall? Discus along its types & diagram.	**[5]**
C	What is digital signature? How secure hash function is used to form digital signature.	**[5]**

OR

C	Write a short note on PGP.	**[5]**

Q-5

A	Draw and explain in brief R.S.A. algorithm with example.	**[5]**
B	Explain with example working of Key Management	**[5]**

OR

A	Discus about Intrusion Detecting (IDS).	**[5]**
B	Explain Buffer over flow.	**[5]**

Q-6

A	Working of S/MIME.	**[5]**
B	Give difference between digital Signature and Digital Certificate.	**[5]**

OR

A	Explain working functionality of salami attack.	**[5]**
B	Explain the functions provided by S/MIME.	**[5]**

KADI SARVA VISHWAVIDHYALAYA

Subject Code: IT-502

Subject Name: INFORMATION SECURITY

Date:21/11/2015 **Time: 10:30 AM to 1:30 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)	Explain various types of attack on computer system.	[5]
	(B)	Encrypt the message "Good morning" using the Hill Cipher with the key 9 4 5 7	[5]
	(C)	Construct a playfair matrix with the key "occurrence". Generate the cipher text for the plaintext "Tall trees"	[5]
		OR	
	(C)	What is security mechanism? List and explain various security mechanisms.	[5]
Q-2	(A)	What is transposition technique? Explain types of transposition technique.	[5]
	(B)	Explain single round function of DES with suitable diagram.	[5]
		OR	
	(A)	List various modes of operations of block cipher. Explain any three of them.	[5]
	(B)	Explain the DES encryption algorithm.	[5]
Q-3	(A)	What is KDC? With the help of diagram explain how KDC do key distribution.	[5]
	(B)	Explain RSA algorithm and list the possible approaches to attacking it.	[5]
		OR	
	(A)	What is a nonce in key distribution scenario? Explain the key distribution scenario if A wishes to establish logical connection with B. A and B both have a master key which they share with itself and key distribution center.	[5]
	(B)	Calculate cipher text in case of RSA if p=3,q=11,e=3,M=5.	[5]

Section-II

Q-4	(A)	Explain SHA512 Algorithm.	[5]
	(B)	Explain Kerberos Authentication System.	[5]
	(C)	Write the Digital Signature Algorithm.	[5]
		OR	
	(C)	Illustrate variety of ways in which hash code can be used to provide message authentication.	[5]
Q-5	(A)	Write a note on Digital Signature.	[5]
	(B)	What is cryptographic checksum or message authentication code? Describe the three situations in which message authentication code is used.	[5]
		OR	
	(A)	What is MAC? Explain HMAC algorithm.	[5]
	(B)	Explain Man-in-the Middle attack.	[5]
Q-6	(A)	Write Short note on PGP.	[5]
	(B)	What is Trapdoors? Explain Salami attack.	[5]
		OR	
	(A)	Write Short note on S/MIME.	[5]
	(B)	Write a note on types of Firewall.	[5]

---End---