No. of Printed Pages : 2

SEAT No._____

[21A]

SARDAR PATEL UNIVERSITY

T.Y.B.Sc : SEMESTER – VI

INFORMATION TECHNOLOGY

US06CINT05: Information Security

Date: 08-04-2017 **Time: 10:00am to 01:00pm** **Max. Marks: 70**

Q.1 Multiple choice of Question: **10**

[1] _____ is the original message or data that is involved into the algorithm as input.
- a) Plaintext
- b) Simpletext
- c) Ciphertext
- d) None of these

[2] A _____ cipher replaces one symbol with another.
- a) Monographic
- b) Substitution
- c) Transposition
- d) None of these

[3] A transposition cipher _____ symbols in a block of symbols.
- a) Re permutes
- b) Subtract
- c) Permutes
- d) None of these

[4] The full form of CBC is _____
- a) Chaining Block Cipher
- b) Cipher Block Chaining
- c) Chipher Bookcode
- d) None of these

[5] DES stands for _____
- a) Data Encryption Standard
- b) Data Encryption Scheme
- c) Data Encryption System
- d) None of these

[6] _____ is not authorized person to use the computer.
- a) Masquerader
- b) Misfeasor
- c) Clandestine user
- d) None of these

[7] MAC stands for _____
- a) modification authentication code
- b) modification authorized code
- c) message authentication code
- d) None of these

[8] A _____ can use a pair of asymmetric keys.
- a) message integrity
- b) message authentication
- c) digital signature
- d) None of these

[9] In _____ IPSec protects the original IP header.
- a) Active mode
- b) Tunnel mode
- c) Transport mode
- d) None of these

[10] The _____ protocol provides security at the application layer.
- a) Pretty Good Privacy
- b) IPSec
- c) SSL/TLS
- d) None of these

(PTO)

Q.2	**Answer the following questions in short (Any 10) :**	20
	[1] Define the terms: PlainText, Cryptanalysis.	
	[2] Define system services. Also write down its categories.	
	[3] List the fundamental principles of cryptography.	
	[4] Define: Trojan Horse and Logic Bomb	
	[5] Define: Backdoor and Trap Door	
	[6] Write a difference between DES and AES.	
	[7] How HMAC is generated?	
	[8] List the various ways for public key distribution.	
	[9] Draw the diagram for creation of MAC.	
	[10] Explain IPSec protocol in brief.	
	[11] Write a difference between SSL vs. TLS.	
	[12] Draw the diagram for tunnel mode.	
Q.3	[A] Explain substitution cipher in detail.	5
	[B] Explain transposition cipher in detail.	5
	OR	
Q.3	Write a detail note on Security Attack.	10
Q.4	[A] Explain Virus Structure in detail.	5
	[B] Explain application for public key cryptosystem.	5
	OR	
Q.4	[A] Write a detail note on Data Encryption Standard.	5
	[B] Explain different cipher modes in detail.	5
Q.5	[A] Write a detail note on Message authentication.	5
	[B] Explain various attacks performed on password.	5
	OR	
Q.5	Explain entity authentication methods in detail.	10
Q.6	Explain in detail the types of firewall.	10
	OR	
Q.6	[A] Explain various services performed by SSL.	5
	[B] Explain Encapsulating Security Payload protocol in detail.	5

—x—