Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058, India
(Autonomous College Affiliated to University of Mumbai)

End Semester Examination

Nov 2017

Max. Marks: 100 Duration: 3 hr
Class: B.E Semester: VII
Course Code: CPC 702 Cryptography & System Security Branch: Computer
Name of the Course: [redacted]

Instruction:

(1) All questions are compulsory
(2) Draw neat diagrams
(3) Assume suitable data if necessary

Q No.		Max. Marks	CO
Q.1 a	Explain in detail Public key infrastructure ?	10	CO4
	OR		
Q.1 a	What is digital signature ? Explain Elgamal Digital signature algorithm ?	10	CO4
Q.1 b	Use the playfair cipher to encrypt the message " attack cancelled on Monday, wait for next message" Keyword used is " morning "	05	CO1
Q.1 c	Explain non malicious program errors with examples ?	05	CO5
	OR		
Q.1 c	Write a note on Operating System Security ?	05	CO3
Q.2 a	Explain transposition cipher in detail ?	05	CO1
	OR		
Q.2 a	What is crypt analysis ? Explain Different Crypt analysis attacks ?	05	CO1
Q.2 b.	Explain packet sniffing and packet spoofing ?Explain Session hijacking attack?	10	CO3
Q.2 c	What is Firewall ? Explain different types of firewall ?	05	CO3
Q.3 a	How a key is shared between two parties using Diffie Hellman Key exchange algorithm with example ? What is the drawback of this algorithm ?	10	CO2
	OR		
Q.3 a	In RSA System the public key(e,n) of user A is defined as (7.187). If the plaintext is P= 88. Decrypt plaintext ?.	10	CO2
Q.3 b	Is SHA is Secured ? Explain secure hash algorithm in detail ?	10	CO2
Q.4 a	What are the disadvantages of symmetric key cipher ? Explain in detail working of AES Cipher in detail?	10	CO2

Q.4 b	Write in breif about i. Deniel of Service ii. CAST- 128	10	CO2
Q.5 a	How Security to transport layer is provided using SSL ?	10	CO5
Q.5 b	Explain SET protocol for mobile payment in detail	10	CO5
	OR		
Q.5 b	How authentication and confidentiality are achieved using IPSec?	10	CO5