Synpat C

BHARATIYA VIDYA BHAVAN

SARDAR PATEL INSTITUTE OF TECHNOLOGY

MUNSHI NAGAR, ANDHERI (WEST), MUMBAI – 400 058.

Subject: Cryptography and ~~Network~~ System Security

Class: B. E COMPUTERS **Semester: VII**

Course Code: CPC 702 **Marks : 100**

Q.1 a.	Definition of Public key Infrastructure	1M
	Components of PKI	
	• Certificate authority	2M
	• Registration authority	2M
	• PKI Clients	1M
	• Validity Details	2M
	• Public Key Certificate	2M

Expalnation of earch term in detail

OR

Q.1 a.	Definition of digital Signature	2M
	Explanation of ELgamal DSA in detail stepwise	
	Key generation	2M
	Signature generation	2M
	Verification	4M

Q.1 b	Playcipher rules	1M
	Stepwise solution	3M
	Correct answer	1M

Q.1 c	non Malicious Program errors	
	• Buffer overflow with example	1.5M
	• Incomplete mediation	1.5M
	• Time of check to time of use	2M

Expalnation of earch term in detail

OR

Q.1 c	**Operating System Security (In Short)**	
	• Memory Address protection	2M
	• File protection	1.5M
	• User Athentication	1.5M

Expalnation of each term in detail

Q.2 a Definition of transposition cipher 1M
Stepwise solution of transposition cipher 2M
example of transposition cipher 2M

OR

Q.2 a Definition of Cryptanalysis attack 1M

- Plaintext only attack 1M
- Ciphertext only attack 1M
- Known plaintext only attack 1M

Known ciphertext only attack 1M

Q.2 b Defination of packet snipping 1M
Defination of packet spoofing 1M
Defination Session Hijacking with example 1M
Session Fixation with example 1.5M
Session Side jacking with example 2M
Cross site scripting with example 2M
Malware with example 1.5M

Q.2 c Defination of Firewall 1M
types of firewall

- Packet filtering gateway with example 1M
- Application Proxy with example 1M
- Statefull inspection firewall with example 1M
- Guard with example 1M

Q.3 a Key Exchange of Diffie Hellman Algorithm Stepwise 5M
example of Diffie Hellman Algorithm Stepwise 3M
Drawbacks of algorithm 2 M

OR

Q.3 a (use extended Euclidian method)
Factors of n p=17, q=11 1M
Calculation $\Phi(n)=160$ 2M
find Value of d=23 5 M
CT= 11 2M

Q.3 b NO. Explanation of not vulnerable to cryptanalysis attack 2M
SHA block structure (Neat and labelled) 4M
explanation of working of SHA in detail with fiestel structure 4M

Q.4 a Disadvantages of symmetric key cipher 2M
AES block structure (Neat and labelled) 4M
explanation of working of AES in detail (fiestel Structure) 4M

Q.4 b	i . Definition of DoS	1M
	classification of DoS attacks	2M
	types od DoS attacks	2M
	ii. CAST 128 block structure (Neat and labelled)	2M
	explanation of working of CAST 128 in detail (fiestel Structure)	3M
Q.5 a	**TLS protocol and** handshake protocol	3M
	Stepwise Client ans server Communication	5M
	record protocol detail	2M
Q.5 b i.	SET protocol Importance	2M
	SET participents	4M
	SET interaction steps	4M

OR

Q.5 b	Athentication Header and Encapsulating security payload Protocol	2M
	Transport Mode	2M
	Tunnel mode	2M
	Confidentiality – Athentication Algorithm	2M
	Authentication- Encryption Algorithms	2M