Cryptography Sem-V IT

University of Mumbai

Program: Information Technology (CBCGS)

Curriculum Scheme: Rev 2016

Examination: TE Semester V

Course Code: 1T01225 and Course Name: 32404 / / Cryptography & Network Security

Time: 2 hours Max. Marks: 80

Q1.	**Choose the correct option for following questions. All the Questions are compulsory and carry equal marks**
1.	Number of rounds in DES is
Option A:	15
Option B:	16
Option C:	17
Option D:	18
2.	if e=3 and n=35 and ciphertext is 22 generated by Bob what is the corresponding plaintext using cyclic attack
Option A:	12
Option B:	6
Option C:	8
Option D:	9
3.	In the following messages which one can be used to preserve the integrity of a document or a message.
Option A:	Message summary
Option B:	Message digest
Option C:	encrypted message
Option D:	Plaintext
4.	What is the number of round computation steps in the SHA-256 algorithm?
Option A:	80
Option B:	76
Option C:	64
Option D:	70
5.	Hashed message when enncrypted is called as
Option A:	Physical signature
Option B:	digital signature
Option C:	electronic signature
Option D:	handwritten signature
6.	Needham–Schroeder Protoco forms the basis for
Option A:	DES
Option B:	KERBOSE
Option C:	RSA
Option D:	AES
7.	Which of the following is the valid key size of RSA used for Signature scheme
Option A:	448
Option B:	568
Option C:	1296
Option D:	1024
8.	In which layer of TCP/IP Protocol congestion and Flow control Mechanism take place

Option A:	Application
Option B:	Transport
Option C:	Data link
Option D:	Network
9.	Packet Filter Firewall is also called as
Option A:	Policy filter
Option B:	Analysis filter
Option C:	Policy router
Option D:	Screening filter
10.	In Kerberos, _____ shares a unique password with every user in the system.
Option A:	Authentication server
Option B:	Ticket granting ticket
Option C:	Ticket granting server
Option D:	File Server

Q2 (20 Marks)	**Solve any Four out of Six** **5 marks each**
A	*Define ARP spoofing with example.Compare wwith IP spoofing.*
B	*What is significance of digital signature on digital certificates?Justify*
C	*Compare and contrast HMAC and CMAC.*
D	SHA provides better security than MD Justify
E	Explain IPSec
F	Explain Stegnography

Q3 (20 Marks)	**Solve any Two Questions out of Three 10 marks each**
A	*Explain Transpositional ciphers with illustrative example.*
B	*What are block cipher modes.Describe any two in details*
C	*Explain different types of DOS attacks.*

Q4 (20 Marks)	
A	**Short notes on any Two** **5 marks each**
i.	*SSL/TLS*
ii.	*Email Security*
iii.	Port scanning
B	**Attempt any one** **10 marks**
i.	*Explain Kerbose in details*
ii.	*What is firewall? Explain different types of firewalls and list their advantages.*