T.E. (IT) (Sem-V) (CBCGS) (R-20-21)

Computer Network Security

90324

C C Scher

University of Mumbai

Examinations Summer 2022

Time: 2hour 30 minutes | Max. Marks: 80

Q1.	**Choose the correct option for following questions. All the Questions are compulsory and carry equal marks**
1.	In which of the following cipher the plain text and cipher text does not have same number of letters
Option A:	Keyword cipher
Option B:	Vigenere cipher
Option C:	Hill cipher
Option D:	Additive cipher
2.	What is the value of ipad in HMAC structure
Option A:	00111110
Option B:	00110010
Option C:	10110110
Option D:	01110110
3.	Which of the following modes of operation in DES used is for operating short data
Option A:	ECB
Option B:	CBC
Option C:	OFB
Option D:	CFB
4.	Which of the following operations are false for each round in the AES algorithm i)Substitute bytes ii) Shift columns iii)Mix rows iv) XOR round key
Option A:	i only
Option B:	ii,iii,iv
Option C:	ii and iii
Option D:	only iv
5.	A firewall protects which of the following attacks
Option A:	Denial of service
Option B:	Phishing
Option C:	Eavesdropping
Option D:	Shoulder surfing
6.	To assess the host's state,the ___often consults backend systems
Option A:	Supplicants
Option B:	Network access server
Option C:	Policy server
Option D:	Access requestor
7.	Which one of the following is not a higher layer SSL protocol
Option A:	Change cipherspec protocol
Option B:	Alert protocol

2E055FAEAB5384883030BDD25535FCC7

Option C:	Handshake protocol
Option D:	Alarm protocol
8.	What is the software called which when get downloaded on computer,scans your hard drive for personal information and your internet browsing habits
Option A:	Malware
Option B:	Keyloggers
Option C:	Spyware
Option D:	Trapdoors
9.	_____are computer programs that are designed by attacker to get administrative access to your computer
Option A:	Trapdoors
Option B:	Spyware
Option C:	Malware
Option D:	Rootkits
10.	An analysis method used by some IDS that looks for instances that are considered normal behavior
Option A:	Stateful Inspection
Option B:	Anomaly Detection
Option C:	Evasion
Option D:	Pattern Matching

Q2	**(20 Marks)**
A	**Solve any Two** **5 marks each**
i.	Enlist security goals. Discuss their significance
ii.	What is the significance of a digital signature on a certificate ?Justify
iii.	Compare and contrast HMAC and CMAC
B	**Solve any One** **10 marks each**
i.	Encrypt "This is the final exam" using playfair cipher using the key "Guidance"
ii.	Explain different types of denialof service attacks

Q3	**(20 Marks)**
A	**Solve any Two** **5 marks each**
i.	How does IPSec help to achieve authentication and confidentiality?Justify the need of AH and ESP
ii.	Explain different methods of IDS?State capabilities and challenges in IDS
iii.	What is network access control?Discuss the elements present in this context
B	**Solve any One** **10 marks each**
i.	Perform encryption and decryption using RSA algorithm with p=7,q=11,e=17 and M=8
ii.	What is SSL protocol ?Explain

Q4	**(20 Marks)**
A	**Solve any Two** **5 marks each**
i.	Write short note on :Email Security
ii.	Explain network security model in detail with neat diagram
iii.	What are block cipher modes describe any two in detail
B	**Solve any One** **10 marks each**
i	Show how a Kerberos protocol can be used to achieve single sign on in distributed systems
ii.	What is a firewall?explain different types of firewalls

2E055FAEAB5384883030BDD25535FCC7