Exam Date & Time: 01-Jul-2023 (01:15 PM - 04:30 PM)

CHAROTAR UNIVERSITY OF SCIENCE AND TECHNOLOGY

University Examination July-2023
B.Tech (IT)-VI
01:15 p.m. to 4:30 p.m.

CRYPTOGRAPHY and NETWORK SECURITY [IT348]

Marks: 70 **Duration: 195 mins.**

Section-I

Answer all the questions. Section Duration: 40 mins

1 $\phi(187) =$ _____ (2)

1) 160 2) 120 3) 140 4) 186

2 Find out whether 9 is a Quadratic Residue in Z11*or not. (2)

1) Yes 2) No

3 Key domain of affine cipher _____ in Z26. (2)

1) 312 2) 26 3) 12 4) 25

4 In hashing, a fixed-length message digest is created out of_____ length message. (2)

1) variable 2) fixed

5 lcm(5,10) * gcd(5,10) = _____ (2)

1) 50 2) 10 3) 5 4) 500

6 Do we need padding if the length of the original message is alreadya multiple of 1024 bits? (2)

1) Yes 2) No

7 Analyze the following attacks to determine which best illustrates apharming attack. (2)

1) A customer gets an email that appears to be from their insurance company. The email contains a link that takes the user to a fake site that looks just like the real insurance company site.

2) An employee gets a call from someone claiming to be in the IT department. The caller says there was a problem with the network, so they need the employee's password in order to restore network privileges.

3) A company's sales department often has after-hour training sessions, so they order dinner delivery online from the restaurant across the street. An attacker is able to access the company's network by compromising the restaurant's unsecure website.

4) A customer enters the correct URL address of their bank, which should point to the IP address 172.1.24.4. However, the browser goes to 168.254.1.1, which is a fake site designed to look exactly like the real bank site.

8 The Data Encryption Standard (DES) uses a key generator to generatesixteen _____ bit round keys. (2)

1) 48 2) 64 3) 20 4) 24

9			Which situation would require keyboard encryption software beinstalled on a computer?									
	1)	To protect against spyware		2)	To set up single sign-on privileges		3)	To comply with input validation practices		4)	For the purpose of key management		(2)
10			A system administrator downloads and installs software from avendor website. Soon after installing the software, theadministrator's computer is taken over remotely. After closerinvestigation, the software package was modified, probably while itwas downloading. What action could have prevented this incidentfrom occurring?									(2)
	1)	Validate the software using a checksum		2)	Validate the software using a private certificate		3)	Validate the software using a key signing key		4)	Validate the software using Kerberos		

Section-II

Answer all the questions.

1			Calculate the Mix column example of AES for the given data. $\begin{bmatrix}2&3&1&1\\1&2&3&1\\1&1&2&3\\3&1&1&2\end{bmatrix} * \begin{bmatrix}d4\\bf\\5d\\30\end{bmatrix} = \begin{bmatrix}??\\66\\81\\e5\end{bmatrix}$	(5)
2			The attacker has intercepted the cipher text "UVACLYFZLJBYL". Showhow an attacker can use a brute force attack to break the additivecipher.	(5)
3			Encrypt the message using Playfair cipher "The house is being soldtonight" with the key "MONARCHY".	(5)
4	1		Perform 1st round encryption of following Plaintext (P) = 1111 1111using Cipher key (K) =11111 11111. Initial Permutation: 2 6 3 1 4 8 5 7 Straight P-Box= 3 5 2 7 4 10 1 9 8 6 Compression P-Box = 6 3 7 4 8 5 10 9 Expansion P-box(E/P8): 4 1 2 3 2 3 4 1 Straight P-box(P4): 2 4 3 1	(10)

S0	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	2

S1	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

	[OR] 2	1	Write a short note on Authentication Header protocol (AH).	(5)
		2	Write a short note on X.509 certificate revocation format.	(5)

Section-III

Answer all the questions.

1			Write a short note Diffie-Hellman protocol.	(5)
[OR] 2			Discuss the electronic mail system.	(5)
3			What are the minor differences between Kerberos version 4 andKerberos version 5?	(5)
4			Find all multiplicative inverse pairs in Z26*.	(5)
5			Use RSA to encrypt message m=19 and show the decryption of thecipher text. Alice uses Bob's public key e=5, p=7, and q=17.	(5)
6			Use an affine cipher to encrypt the message "hello" with the keypair (7, 2).	(5)
[OR] 7			List and explain five security services.	(5)

-----End-----