Exam Date & Time: 24-Apr-2023 (01:15 PM - 04:30 PM)

CHAROTAR UNIVERSITY OF SCIENCE AND TECHNOLOGY

University Examination April 2023
B.Tech. (IT) - VI
Time: 01:15 pm to 04:30 pm

CRYPTOGRAPHY and NETWORK SECURITY [IT348]

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

Section-I

Answer all the questions. Section Duration: 40 mins

1		

An unknowing user with authorized access to systems in a softwaredevelopment firm installs a seemingly harmless, yet unauthorizedprogram on a workstation without the IT department's sanction.Identify the type of threat that is a result of this user's action. (2)

1)	Unintentional insider threat		2)	Malicious insider threat		3)	Intentional attack vector		4)	External threat with insider knowledge	

2		

Encryption vulnerabilities allow unauthorized access to protecteddata. Which component is subject to brute-force enumeration? (1)

1)	An unsecured protocol		2)	A software vulnerability		3)	A weak cipher		4)	A lost decryption key	

3		

Select the statement which best describes the difference between azero-day vulnerability and a legacy platform vulnerability. (2)

1)	A legacy platform vulnerability is typically unpatchable, while a zero-day vulnerability may be exploited before a developer can create a patch for it.		2)	A zero-day vulnerability is unpatchable, while a legacy platform vulnerability can always be patched, once detected.		3)	A zero-day vulnerability can be mitigated by responsible patch management, while a legacy platform vulnerability cannot likely be patched.		4)	A legacy platform vulnerability can always be mitigated by responsible patch management, while a zero-day vulnerability does not yet have a patch solution.	

4		

An employee is having coffee at an outdoor coffee shop and is nottaking precautions against someone watching their screen whileworking on a company project. A person a few tables over watchesthe employee enter their credentials and then takes photos of thework they are completing with their smartphone. Which form ofsocial engineering is being used in this situation? (1)

1)	Vishing		2)	Lunchtime attack		3)	Shoulder surfing		4)	Man-in-the-middle attack	

5		

Which situation would require keyboard encryption software beinstalled on a computer? (1)

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	

6		

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

1)	A customer gets an email that appears to be from their		2)	An employee gets a call from someone claiming to be in the IT		3)	A company's sales department often has after-hour training sessions, so they order dinner		4)	A customer enters the correct URL address of their bank, which should point to	

	insurance company. The email contains a link that takes the user to a fake site that looks just like the real insurance company site.			department. The caller says there was a problem with the network, so they need the employee's password in order to restore network privileges.			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.			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.	

7 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? (1)

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	

8 Challenge-response authentication can be achieved using ________ . (1)

1)	Symmetric key cipher		2)	Asymmetric key cipher		3)	Keyed hash		4)	All of the above	

9 The DSS signature uses which hash algorithm? (1)

1)	MD5		2)	SHA-1		3)	SHA-2		4)	None	

10 For a client-server authentication, the client requests from theKDC a ________ for access to a specific asset. (1)

1)	token		2)	key		3)	ticket		4)	password	

11 Pretty good privacy (PGP) security system uses_____. (1)

1)	public key cryptosystem		2)	private key cryptosystem		3)	public & private key cryptosystem		4)	none of the above	

12 How many secret key bytes are generated using the Diffie-Hellmanencryption/decryption scheme? (1)

1)	256		2)	871		3)	962		4)	1024	

13 What is the purpose of a web server certificate? (1)

1)	Sign and encrypt email messages.		2)	Guarantee the validity of a browser plug-in.		3)	Provide identification of the certificate authority.		4)	Guarantee the identity of a website.	

14 A Certificate Revocation List (CRL) has a publish period set to 24hours. Based on the normal procedures for a CRL, what is the mostapplicable validity period for this certificate? (2)

1)	26 hours		2)	1 hour		3)	23 hours		4)	72 hours	

15 Which one of the following is not an application hash function? (1)

1)	One-way password file		2)	Key wrapping		3)	Virus Detection		4)	Intrusion detection	

16 Which of the following is not an element/field of the X.509certificates? (1)

1)	Issuer Name		2)	Serial Modifier		3)	Issuer unique Identifier		4)	Signature	

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 "OMVDICVMYADBCOZVNT".Show that how the attacker can use a brute force attack to breakthe additive cipher.

(5)

3

Perform cryptanalysis on the given cipher text using columntransposition. "ETTHEAKIMAOTYCNZNTSG"

(5)

4 1

Perform 1st round encryption of following Plaintext (P) = 11001100using Cipher key (K) =1010101010.

Initial Permutation: 2 6 3 1 4 8 5 7

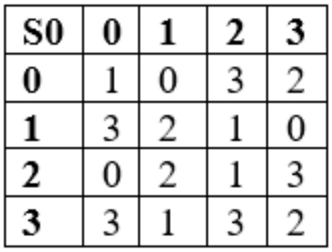
Straight P-Box= 3 5 2 7 4 10 1 9 8 6

Compression P-Box = 6 3 7 4 8 5 10 9

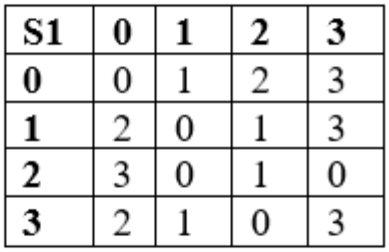
Expansion P-box(E/P8): 4 1 2 3 2 3 4 1

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

List and explain five security services.

(5)

2

What are the capabilities and limitations of the firewall? Explainpacket filtering firewall in detail.

(5)

Section-III

Answer all the questions.

1

In the Diffie-Hellman protocol, g=7, p=23, x=3 and y=5. What arethe values of R1 and R2 & symmetric key?

(5)

[OR] 2

Use the Vigenere cipher with the keyword "HEALTH" to decipher themessage "SMFPBZMYLWHMZYPPKPZI"

(5)

3

What are the services provided by Digital Signature? Explain indetail.

(5)

4

Differentiate between SHA-1 and MD5.

(5)

5

Explain the Encapsulating Security Payload (ESP) with the figure.

(5)

6			Use RSA to encrypt message m=2. Alice uses bob's public key e=37and n=77.	(5)
[OR] 7			What are the minor differences between Kerberos version 4 andKerberos version 5?	(5)

-----End-----