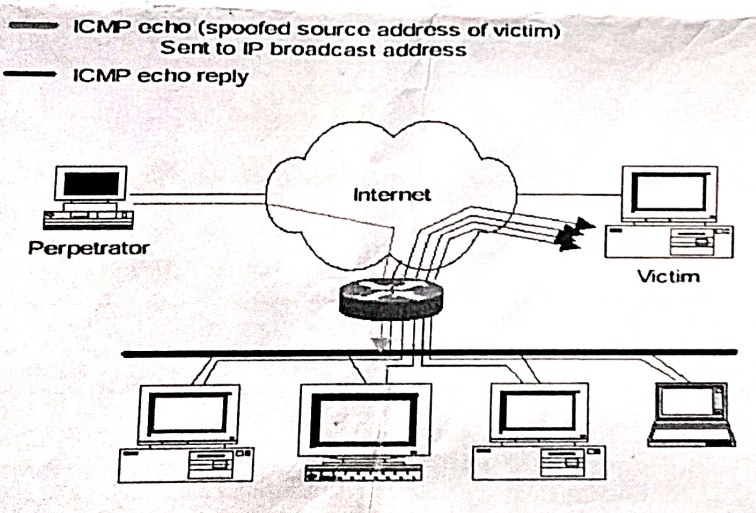
National Forensics Sciences University, Goa Campus
Mid- semester Examination
M.Sc. DFIS - Semester -III

Branch – DFIS **Sem –** III **Date-** /11/2022
Subject Name- Network Security & Forensic **Subject Code-** CTMSDFIS SIII P1
Time- 1.5 Hours **Max. Marks-** 50
Instructions - 1) Answer all questions. 2) Assume suitable data.

Q.1 Attempt all.

		20 Marks
a.	With the help of example, define virtual private network (VPN)? How does it provide the end-to-end security?	5 Marks
b.	Use *Vigenere Cipher* with key ***HEALTH*** to encrypt the message ***"Life is full of surprises".***	5 Marks
c.	Encrypt the following message using *Playfair* cipher. Message: ***quillaja*** Keyword: ***jonquil***	5 marks
d.	Consider the following network scenario:  i. Identify and explain the attack on the above scenario. ii. Also mention the countermeasures to protect this kind of attacks.	5 Marks

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Q.2	Attempt all questions (Q 2(a)- 2 (c)):	**15 Marks**
	a. With reference to ***802.11i***, describe the operation of TKIP and ***CCMP*** protocols?	5 Marks
	b. What is the significance of flow control? Why is it important for the security point of view?	5 Marks
	c. What is the **zero point** of an elliptic curve?	5 Marks
Q. 3	Attempt any **two:**	**8 Marks**
	a. Explain the authentication phase of ***802.11i***.	4 Marks
	b: What is meant by piggybacking? What are its advantages and disadvantages?	4 Marks
	c. What is the significance of **iptable** in the Linux hardening? Also provide the example.	4 Marks
Q.4	Attempt **any one**	**7 Marks**
	a. Use two global prime number ***37*** and ***43***, the value of ***e*** is ***71*** and message ***M= 2***, calculate the *public key*, *private key*, and the corresponding cipher text. Also prove that *RSA* decryption is the inverse of *RSA* encryption.	7 Marks
	OR	
	a. *Alice* and *Bob* wish to swap keys by using *Diffie-Hellman* key exchange algorithm and are agreed on prime ***p* = 23** and base or generator is ***g= 5.*** Calculate the *secret key* of each user and *shared session key* for both the users. Also explain with the same question that how can *Eve* (untrusted third person) exploit *Man-in-Middle attack.*	7 Marks

K	T	M	L	O
V	E	R	A	B
C	D	F	G	H
I/J	N	P	Q	S
U	W	X	Y	Z

Seat No.: _____ Enrolment No._____

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. -DFIS - Semester -III - Jan-2022

Subject Code: CTMSDFIS SIII L1 **Date: /01/2022**

Subject Name: Network Security & Forensic Lab

Time: 45 Minutes **Total Marks: 50**

Instructions:

1. Attempt all questions.
2. Make suitable assumptions wherever necessary.
3. Figures to the right indicate full marks.

			Marks
Q.1		**Wireshark Experiment**	**25**
		1. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day. For now, you don't need to understand HTTP GET and OK, but reading the textbook may be helpful if you are curious on how they work. 2. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields? 3. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of the website with the RFC? (Hint: the answer is no). What device has this as its Ethernet address? 4. Examine a pair of UDP packets in which the first packet is sent by your host and the second packet is a reply to the first packet. Describe the relationship between the port numbers in the two packets.	
Q.2		Programming Assignment:	**25**
	(b)	1. WAP to demonstrate RSA cryptosystem. 2. WAP to demonstrate Diffie Hellman key exchange algorithm. 3. WAP to demonstrate Caeser Cipher Cryptosystem. 4. WAP to demonstrate Vigenère Cipher Cryptosystem.	

END OF PAPER

Seat No.: _____ Enrolment No. _____

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. (Digital Forensics and Information Security) - Semester - III - Jan-2023

Subject Code: CTMSDFIS SIII P4 EL3 **Date:** 12/01/23

Subject Name: Cloud Security and Forensics

Time: 11:00 AM to 2:00 PM **Total Marks:** 100

Instructions:

1. Write down each question on separate page.
2. Attempt all questions.
3. Make suitable assumptions wherever necessary.
4. Figures to the right indicate full marks.

			Marks
Q.1	(a)	How do you see the cloud computing policy w.r.t. security? Why do we need policy ranking, explain in detail?	06
	(b)	Among IaaS, PaaS, and SaaS which one is least secured and why?	06
	(c)	Discuss in detail about cloud data protection model?	08
Q.2	(a)	Kindly explain defense in depth, how does it make our system secure?	06
	(b)	How separation of duties makes our data secure over the cloud.	06
	(c)	Where and how do we use log parsing, explain with an example?	08
Q.3	(a)	Describe fail-open mode. How does port security used to avoid it? **OR** Explain cloud computing reference architecture in Detail?	10
	(b)	Compare and contrast between Diffie-Hellman and RSA algorithms.	10
Q.4	(a)	Compare signed certificates with self-signed certificates.	06
	(b)	Compare symmetric key and asymmetric key cryptography. Which one is mostly used for web encryption?	06
	(c)	Generate the cipher text for Plain text=19 using RSA algorithm, assuming p=7 and q=17? **OR** Explain any two Hashing algorithms in detail.	08
Q.5	(a)	What difference do you mark the difference between hardening of a system and VAPT?	06
	(b)	What is Hypervisor? Explain advantages and disadvantages.	06
	(c)	What are the issues related to the forensics in cloud computing? Describe.	08

National Forensics Sciences University, Goa Campus
Mid- semester Examination

Branch – M.Sc. Digital Forensic & Information Security Sem – III Date- 17-11-2022
Subject Name- Database Forensics Subject Code- CTMSDFIS SIII P5 EL1
Time- 1.5 Hours Max.Marks- 50
Instructions - 1) Answer all questions. 2) Assume suitable data.

Q.1	**Solve any four**	**20 marks**
	a. Compare the two-tier and three-tier database system architecture.	5 marks
	b. Explain giving examples any five common errors that users make on a network that can contribute to an intrusion in database.	5 marks
	c. Explain the different types of database users	5 marks
	d. Identify and explain any five advantages of using a database approach	5 marks
	e. List and explain any five database models.	5 marks
Q.2	**Attempt all**	15 marks
	a. Describe the process of worm's travel across network. List the different types of worms	5 marks
	b. List any five background processes of an Oracle instance. Describe in detail the functionality of listed processes	5 marks
	c. Identify any three advantages of using a key in database. Briefly explain any four types of keys used in database system.	5 marks
Q. 3	**Attempt Q3a and Q3b**	15 marks
Q.3 a	**Attempt any one**	
Q.3 a	Describe in detail the structured memory of an Oracle instance. Discuss the physical and logical storage structure used in Oracle and their relationship.	8 marks
	OR	
Q.3 a	Consider your team has been assigned the task of creating a relational database. The team has already completed the requirement analysis and designed the Entity Relationship(ER) diagram. Develop a detailed series of steps to generate the tables from the ER diagram.	8 marks
Q.3 b	**Attempt any one**	
Q3 b	Define Malware. Identify and describe in brief the various classification falling under the umbrella of malware.	7 marks
	OR	
Q3 b	Discuss in detail the various components of MySQL architecture	7 marks

National Forensics Sciences University, Goa Campus
Block- Semester Examination
M.Sc. DFIS - Semester -III

Branch – DFIS	**Sem –** III	**LAST DATE: 23 December 2022**
Subject Name- Network Security & Forensic		**Subject Code-** CTMSDFIS SIII P1
Time- 1.5 Hours		**Max. Marks-** 50

Instructions - 1) Answer all questions. 2) Assume suitable data.

Q. N.	Question	Marks
Q.1 (A)	List all types of internetworking devices. Also explain any two application layer devices.	5
(B)	Differentiate the ARP poising and MAC flooding.	5
Q.2 (A)	Construct a Playfair cipher for following: ***Key: Your City Name*** ***Plaintext: Your Name and Surname***	5
(B)	Explain the rotor machine in detail.	5
Q 3 (A)	Consider the following body of e-mail: *Dear UCSC Email User,* *Beginning next week, we will be deleting all inactive email accounts in order to create space for more users. You are required to send the following information in order to continue using your email account. If we do not receive this information from you by the end of the week, your email account will be closed.* **Name (first and last):* **Email Login:* **Password:* Answer the following question on the above scenario: **i.** Identify the type of attack **ii.** How will you prevent this kind of attack?	5
(B)	What is digital signature? What is the use of message digest in Digital Signature?	5
Q 4 (A)	What are the IEEE 802.11 standards for WLAN architectures?	5
(B)	Write short notes on wireless PAN?	5
Q 5	Explain following terms with examples: **(A)** *Relatively Prime* **(B)** Avalanche Effect **(C)** Attack Surface **(D)** Buffer Overflow	10

NATIONAL FORENSIC SCIENCES UNIVERSITY, GOA

SCHOOL OF CYBER SECURITY & DIGITAL FORENSIC

M.Sc. (CYBER SECURITY/DIGITAL FORENSIC & INFORMATION SECURITY)

SEMESTER III

TERM ASSESSMENT – 1

SOCIAL NETWORK ANALYSIS (CTMSDFIS S3-P5)

Date: 22.09.2022 Time: 12:15 to 1:00 PM Max. marks: 25

Q. 1. Multiple Choice Questions (1 mark each) **[10 Marks]**

1. SNA can be described as:
a) study of human relationship by using graph b) study of relationship c) study of graph theory d) All

2. What is a graph diameter?
a) Is the largest number of vertices to be traversed in order to travel from one vertex to another b) Is a way to quantitatively analyze a graph c) Both d) None

3. The degree of a node describes—:
a) its level of connectedness in the network b) its in-degree c) its out-degree d) None

4. A —— is a connection between two nodes.
a) neighborhood b) edge c) degree d) None

5. In a random graph, the presence of a connection between A and B as well as a connection between B and C will not influence the probability of a connection between A and C:
a) true b) false c) true if it is a directed graph d) None

6. A regular graph is a network where each node has the ..... number (k) of neighbors:
a)Even degree b) odd degree c) same degree d)None of these

7. The clustering coefficient of a node:
a) is the number of actual connections across the neighbors of a particular node, as a percentage of possible connections b) degree c) total no. of edges in a given graph d) None

8. Article 21 talks about:
a) Data privacy b) Right to information c) Freedom of speech d) Personal liberty

9. Does social network impact our psychology:

a) True b) False

10. What would be best use of the social network:
a) mass communication b) entertainment c) marketing d) All are correct

2. Answer any 3 questions (3x5 marks each) **[3x5=15 Marks]**

1. Discuss the difference between regular and random graphs?
2. How is social network related with graph theory?
3. Kindly discuss the working mechanism of facebook?
4. Discuss the pros and cons of viral messages.
5. Discuss the role of geo-informatics in social media.

Seat No.: 4029 Enrolment No. 006

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. (Digital Forensics and Information Security) - Semester - III - Jan-2023

Subject Code: CTMSDFIS SIII P4 EL3 **Date:** 12/01/23

Subject Name: Cloud Security and Forensics

Time: 11:00 AM to 2:00 PM **Total Marks:** 100

Instructions:

1. Write down each question on separate page.
2. Attempt all questions.
3. Make suitable assumptions wherever necessary.
4. Figures to the right indicate full marks.

			Marks
Q.1	(a)	How do you see the cloud computing policy w.r.t. security? Why do we need policy ranking, explain in detail?	06
	(b)	Among IaaS, PaaS, and SaaS which one is least secured and why?	06
	(c)	Discuss in detail about cloud data protection model?	08
Q.2	(a)	Kindly explain defense in depth, how does it make our system secure?	06
	(b)	How separation of duties makes our data secure over the cloud.	06
	(c)	Where and how do we use log parsing, explain with an exampie?	08
Q.3	(a)	Describe fail-open mode. How does port security used to avoid it? **OR** Explain cloud computing reference architecture in Detail?	10
	(b)	Compare and contrast between Diffie-Hellman and RSA algorithms.	10
Q.4	(a)	Compare signed certificates with self-signed certificates.	06
	(b)	Compare symmetric key and asymmetric key cryptography. Which one is mostly used for web encryption?	06
	(c)	Generate the cipher text for Plain text=19 using RSA algorithm, assuming p=7 and q=17? **OR** Explain any two Hashing algorithms in detail.	08
Q.5	(a)	What difference do you mark the difference between hardening of a system and VAPT?	06
	(b)	What is Hypervisor? Explain advantages and disadvantages.	06
	(c)	What are the issues related to the forensics in cloud computing? Describe.	08

Seat No.: 4732 Enrolment No. 8009

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Digital Forensics and Information Security (Batch:21-23)
Semester - III - Jan-2023

Subject Code: CTMSDFIS SIII P3 **Date: 04/01/2023**
Subject Name: Blockchain and Cryptocurrency
Time: 11:00 AM to 02:00 PM **Total Marks: 100**

Instructions:

1. **Write down each question on separate page.**
2. **Attempt all questions.**
3. **Make suitable assumptions wherever necessary.**
4. **Figures to the right indicate full marks.**

			Marks
Q.1	(a)	Define Blockchain. Differentiate between public and private Blockchain	05
	(b)	What is the difference between hashing and encryption? List all the possible differences	05
	(c)	What is PoW? Explain all the steps involved in PoW	07
Q.2	(a)	How Blockchain is different than the distributed databases?	05
	(b)	How PoW guarantees ledger consistency? Explain in brief **OR** Explain DAO and DAO attack?	05
	(c)	What is Hash function? Write down the properties of good hash function	07
Q.3	(a)	What is Smart Contract? Explain it with example	08
	(b)	Explain the concept of digital signature in Blockchain in detail	08
Q.4	(a)	PoS is more energy efficient than PoW. Justify **OR** What are the limitations of the Blockchain?	05
	(b)	What is Sybil attack? How it can be prevented in Blockchain?	05
	(c)	What is PoB? Compare PoB with PoW in detail **OR** Explain hard forking and soft forking in terms of bitcoin Blockchain	07
Q.5	(a)	What is Gas and Gas limit? Explain all the cases	05
	(b)	Explain the role of Merkle tree in Blockchain	05
	(c)	Explain practical byzantine fault tolerance mechanism	07

Q.6	(a)	Differentiate between Symmetric and Asymmetric Cryptography. Explain any one asymmetric cryptographic algorithm in brief	08
	(b)	Explain role of Blockchain in Medical Record Management System **OR** What is Quantum Computing? Explain its need in Blockchain	08

END OF PAPER

L

S	HY	HJ	M
60	60	40	-
40	40	-	-
-	-	-	-
	40	50	-

D

S	HY	HJ	M
40	40	40	
40	40	40	
40	40	50	40
		50	

Seat No.: _____ Enrolment No. _____

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Cyber Security - Semester - III - Jan-2023

M.Sc. Digital Forensics - Sem III - Jan 2023

Subject Code: CTMSCS SIII P5 EL1 , CTMSDFIS SIII P5 EL1 **Date: 16/01/2023**

Subject Name: Social Network Analysis

Time: 11:00 to 2:00 **Total Marks: 100**

Instructions:

1. **Write down each question on separate page.**
2. **Attempt all questions.**
3. **Make suitable assumptions wherever necessary.**
4. **Figures to the right indicate full marks.**

			Marks
Q.1	(a)	Explain difference between social media and social network.	05
	(b)	What do you mean by Google Dorks?	05
	(c)	Write a note on different social network platforms.	07
Q.2	(a)	What do you mean by metadata. Explain with example.	05
	(b)	Write a note on cyber psychology.	05
	(c)	Explain email forensics. Explain email header tracking and tracing.	07
Q.3	(a)	Explain OSINT with its types.	08
	(b)	Write a case study on fake social media profile investigation.	08
Q.4	(a)	Write a short note on API and its benefits in Social Network investigation.	05
	(b)	Explain terms person profiling and organization profiling through social media intelligence.	05
	(c)	What do you mean by fake news? How can the fake news related incident can be investigated through social network analysis?	07
Q.5	(a)	Explain the term social engineering using social media.	05
	(b)	What do you mean by data breach? How data breach dumps can helpful in collecting intelligence?	05
	(c)	Explain graph theory with nodes, edges, unidirectional and bi-directional linkages.	07
Q.6	(a)	Discuss security and privacy functionality in different social network platforms for hardening the security of any user account.	08
	(b)	Write a brief note on surface web, deep web and dark web.	08

END OF PAPER

Blockchain and Cryptocurrency Lab Exam

Solve any three

Timing 10:30 to 1:30

Date: 18/01/2023

Q.1 Amit received following threatening mail.

With one click, I can send your morphed video to all your friends via email, social networks and instant messengers. I can also publish access to all your emails and instant messengers that you use. In addition, I found a lot of interesting things that I was able to publish on the Internet and send to friends. If you don't want me to do it, send me 1450 $ (US dollar) in my bitcoin wallet.

My BTC wallet address:

bc1q7cuazm24zgraqd92zxqw4kzqzv2z7kwscuey79

can you trace the location, URL , IP address, and exact location of the attacker.

Q.2 Find the following bitcoin wallet IDs are malicious or not. If yes then trace location, URL , IP address, and exact location of the attacker.

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

bc1qxtnjfvrfk3x90np6rx9726d5llg84c3n2jzh7a

bc1qd9sk4msyvw7tpr444czcd9c0c7k9pgqtlmcd0f

bc1qsww0rqcusj9rte73sttr8sfhc4cce8xhv2trt4

bc1q0x35pfvhe9r7rnzexpccwypw60692tej9qd30h

bc1q3a0jy6y42j6zlmq0407qq4p55p6t6ymrzu7aw8

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Q.3 Implement smart contract to solve owner tenant problem. You can write logic in any language.

Q.4 Implement the smart contract to solve military logistic supply chain management challenges.

Q.5 Implement smart contract for IPL auction.

Q.6 Implement smart contract for the university degree certification system.

Enrolment No._____

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. -DFIS - Semester -III - Jan-2022

Subject Code: CTMSDFIS SIII L1 **Date: /01/2022**

Subject Name: Network Security & Forensic Lab

Time: 45 Minutes **Total Marks: 50**

Instructions:

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**

			Marks
Q.1		**Wireshark Experiment**	**25**
		1. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day. For now, you don't need to understand HTTP GET and OK, but reading the textbook may be helpful if you are curious on how they work. 2. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields? 3. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of the website with the RFC? (Hint: the answer is no). What device has this as its Ethernet address? 4. Examine a pair of UDP packets in which the first packet is sent by your host and the second packet is a reply to the first packet. Describe the relationship between the port numbers in the two packets.	
Q.2		Programming Assignment:	**25**
	(b)	1. WAP to demonstrate RSA cryptosystem. 2. WAP to demonstrate Diffie Hellman key exchange algorithm. 3. WAP to demonstrate Caeser Cipher Cryptosystem. 4. WAP to demonstrate Vigenère Cipher Cryptosystem.	

END OF PAPER

National Forensics Sciences University, Goa Campus
Mid- semester Examination

Branch – MSc DFIS / MSc CS | Sem –III | Date- 18/11/2022

Subject Name-Advanced Computer Forensics Subject Code- CTMSCS SIII P4 EL1 & CTMSDFIS SIII P4 EL2

Time- 1.5 Hours | Max. Marks- 50

Instructions - 1) Answer all questions. 2) Assume suitable data.

Q.1	Solve any four	20 marks
	a. Write a short note on windows object.	5 marks
	b. Which information does object header contains?	5 marks
	c. Draw and explain the architecture of the system call.	5 marks
	d. Explain pool tag algorithm.	5 marks
	e. How to analyse process from memory dump.	5 marks
Q.2	**Attempt all**	**15 marks**
	a. Enlist any five windows object with their description.	5 marks
	b. Write down the process handle analysis objectives	5 marks
	c. What are the objectives of the event log analysis?	5 marks
Q. 3	Attempt a and b	15 marks
Q.3 a	Attempt any one	
	1) Discuss dynamic storage allocation strategies and write short note on the external and internal fragmentation.	8 marks
	OR	
	2) Write down suitable volatility plugin for the following scenarios i) To get a list of processes that were running at the time a RAM dump captured. ii) To examine the environment variables set by a process. iii) Plugin to list registry hives, including their path on disk. iv) Plugin for determining network connections in Windows systems	8 marks
Q.3 b	Attempt any one	
	1) Which data can be found in the registry?	7 marks
	OR	

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Digital Forensics and Information Security- Semester - III - Jan-2023

Subject Code: CTMSDFIS SIII P2 **Date: 06/01/2023**

Subject Name: IoT Security and Forensics

Time: 11:00 AM to 2:00 PM **Total Marks: 100**

Instructions:

1. **Write down each question on separate page.**
2. **Attempt all questions.**
3. **Make suitable assumptions wherever necessary.**
4. **Figures to the right indicate full marks.**

			Marks
Q.1	(a)	Which are the different components of IoT? Explain it with respect to any one IoT application.	05
	(b)	Give classifications of sensors and actuator. Give two examples of each category.	05
	(c)	Draw IoT protocol stack and explain each layer in brief.	07
Q.2	(a)	Write characteristics of M2M technology and differentiate between M2M & IoT.	05
	(b)	What is SNMP? Write its limitations.	05
	(c)	Which are the different types of IoT nodes? Explain its behavior in WSN.	07
		OR	
	(c)	Which are the different IoT enabling technologies? Explain importance of any two with respect to Smart City.	07
Q.3	(a)	Why interoperability is required for IoT system? Explain with its key points.	08
	(b)	Which protocol is used in messaging applications? Explain its architecture in detail.	08
		OR	
	(b)	Which protocol is used in resource constraint application? Explain its architecture in detail.	08
Q.4	(a)	Write importance of IoT security with respect to any one IoT application.	05
	(b)	Differentiate between MQTT & CoAP.	05
	(c)	What are the major components of MQTT protocol? Explain its working in detail.	07
Q.5	(a)	Which are the different attack surfaces in IoT system? Explain each attack surface along with its attack vector.	05