Enrolment No_____

NATIONAL FORENSIC SCIENCES UNIVERSITY
GOA CAMPUS
M.Tech. (AI&DS) - Semester -II Term Assessment-I

Subject Code: CTMTAIDS SII P5 **Subject Name: Network Security**
Date: 01/03/2024 **Total Marks: 25**
Time: 45 Minutes

Instructions:

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

Q1 to Q10 Fill in the blanks/Multiple Choice questions, each for 1 mark (10x1=10)

Select your appropriate answer:

Q 1 MQTT stands for _____. **01 Mark**

Q 2 CoAP stands for _____. **01 Mark**

Q 3 _____ server filters and forward network traffic. **01 Mark**

Q 4 _____is an example of an IoT application focused on healthcare? 01 Mark

Q 5 Which functional building block of IoT architecture focuses on real-time data processing at the device level? **01 Mark**

A) Edge computing B) Cloud computing C) Middleware

D) Communication protocols E) Data analytics

Q 6 What are the fundamental building blocks of IoT architecture? **01 Mark**

A) Sensors, actuators, and cloud computing

B) Databases, servers, and routers

C) Operating systems, programming languages, and APIs

D) Networks, protocols, and firewalls

Q 7 Which wireless technology is commonly used in smart devices for short-range communication? **01 Mark**

A) RFID B) Zigbee C) 5G D) Satellite E) Ethernet

Q 8 Which aspect is NOT a concern regarding IoT security? **01 Mark**

A) Data encryption B) Authentication C) Interoperability

D) Intrusion detection E) Access control

Q 9 What is a characteristic feature of SMART objects in IoT? **01 Mark**

C) Autonomous decision making D) Low power consumption

E) Static behaviour

Q 10 What are SMART objects in the context of IoT?

A) Objects with artificial intelligence

B) Objects with sensors and actuators

C) Objects with virtual reality capabilities

D) Objects with augmented reality features

Q11 to Q15 Descriptive 3 marks for each question (5x3=15)

Q11 Discuss the IoT ecosystem concept. **03 Marks**

Q 12 Differentiate IoT Level 5 and IoT Level 6. **03 Marks**

Q 13 What is the importance of standardization in the IoT domain? **03 Marks**

Q14 Explain the role of Big Data Analytics with respect to smart systems. 03 Marks

Q 15 Read the following scenario of Smart Home Security System Installation and answer the questions below: **03 Marks**

Scenario: Imagine you are a consultant tasked with designing and implementing a comprehensive smart home security system for a client. Your client lives in a large suburban home and wants to integrate various IoT devices to enhance security while maintaining privacy and energy efficiency. They have expressed concerns about cybersecurity and want assurance that their system is secure against potential breaches.

a) Discuss how SMART objects, such as sensors and actuators, will be utilized in the security system.

b) How will these objects interact within the IoT architecture to enhance securi measures?

~END OF PAPER~

National Forensics Sciences University, Goa Campus
Mid- semester Examination

Branch – MTech. AI & DS
Sem – 2
Date - 29-02-2024
Subject Name - Mobile Security and Forensics
Subject Code – CTMSAIDS SII P2
Duration: 45 Min
Max. Marks- 25
Instructions - 1) Answer all questions. 2) Assume suitable data.

Q.1	Multiple Choice Questions (1 mark each)	10 marks
	i. Activity manager: a. Manages views b. Manages intent resolution c. Provide access to graphics d. None of the above	1 mark
	ii. First commercial version of Android 1.0 (with name Alpha), was released in a. August 2008 b. September 2008 c. October 2008 d. November 2008	1 mark
	iii. Google acquired android Incorporation in a. 2004 b. 2005 c. 2006 d. 2007	1 mark
	iv. Activity Manager lies in which layer of android architecture? a. Kernel b. Libraries c. Application Framework d. Applications	1 mark
	v. Resource Manager: a. Manage various event notifications b. Is an interface for setting locations c. Provide access to non-code app resources d. None of the above	1 mark
	vi. Android's native libraries are written in: a. JAVA b. C or C++ c. Python d. Perl	1 mark

	vii. Which is not an Android Application Components: a. Activity b. Service c. Content d. Assembler	1 mark
	viii. Intent cannot be used for: a. Start Activity b. Broadcast Intent c. Start service d. Start application	1 mark
	ix. Which is not a type of intent a. Explicit b. Implicit c. None	1 mark
	x. Sandboxing is: a. isolate applications from each other b. Connect applications	1 mark
Q.2	Answer any 3 questions (3x5 marks each)	15 Marks
	i. What is intent? Explain the types of intent.	5
	ii. Explain the different layers of Android architecture in detail.	5
	iii. What are the four important components of android application.	5
	iv. Explain the binder framework.	5

National Forensics Sciences University, Goa Campus
Mid- semester Examination

Branch – MTech. AI & DS
Sem – 2
Date - 29-02-2024
Subject Name - Mobile Security and Forensics
Subject Code – CTMSAIDS SII P2
Duration: 45 Min
Max. Marks- 25
Instructions - 1) Answer all questions. 2) Assume suitable data.

Q.1	Multiple Choice Questions (1 mark each)	10 marks
	i. Activity manager: a. Manages views b. Manages intent resolution c. Provide access to graphics d. None of the above	1 mark
	ii. First commercial version of Android 1.0 (with name Alpha), was released in a. August 2008 b. September 2008 c. October 2008 d. November 2008	1 mark
	iii. Google acquired android Incorporation in a. 2004 b. 2005 c. 2006 d. 2007	1 mark
	iv. Activity Manager lies in which layer of android architecture? a. Kernel b. Libraries c. Application Framework d. Applications	1 mark
	v. Resource Manager: a. Manage various event notifications b. Is an interface for setting locations c. Provide access to non-code app resources d. None of the above	1 mark
	vi. Android's native libraries are written in: a. JAVA b. C or C++ c. Python d. Perl	1 mark

	vii. Which is not an Android Application Components: a. Activity b. Service c. Content d. Assembler	1 mark
	viii. Intent cannot be used for: a. Start Activity b. Broadcast Intent c. Start service d. Start application	1 mark
	ix. Which is not a type of intent a. Explicit b. Implicit c. None	1 mark
	x. Sandboxing is: a. isolate applications from each other b. Connect applications	1 mark
Q.2	Answer any 3 questions (3x5 marks each)	15 Marks
	i. What is intent? Explain the types of intent.	5 mark
	ii. Explain the different layers of Android architecture in detail.	5 mark
	iii. What are the four important components of android application.	5 mark
	iv. Explain the binder framework.	5 mark

National Forensics Sciences University, Goa Campus

TA-1 Examination

Branch – MTech AI & DS	Sem – II	Date- 28/02/2024
Subject Name- Natural Language Processing	**Subject Code- CTMTAICS SII P3**	**Time- 45 Minutes**
Instructions - 1) Answer all questions.	**2) Assume suitable data.**	**Max.Marks- 25**

Q.1	Answer all.	10 marks
a.	_____ is the main challenge of natural language processing.	
b.	_____ model of NGram model is known as Markov model?	
c.	_____ technique looks at the meaning of the word.	
d.	One hot vector of the term 'pickled' is _____ in the document 'Peter picked a piece of pickled pepper'.	
e.	In linguistic morphology, _____ is the process for reducing inflected words to their root form.	
f.	"Rama loves her mother and Laxman does too", contain _____ type of ambiguity.	
g.	Coreference resolution means _____.	
h.	_____is the stem for the token "bus".	
i.	_____ is the named entity in the document "The head office of Google is in California".	
j.	In a corpus of N documents, one randomly chosen document contains a total of T terms and the term "hello" appears K times in a document. _____ is the value of product of term frequency and inverse document frequency if the term "hello" appears approximately one third of total documents.	
Q2	Answer any three.	3x5 = 15 marks
a.	Calculate Lavenshtein edit distance between the word '**Kitten** and **Sitting**' using dynamic programming algorithm.	
b.	Explain steps of the morphological parser by considering an example. Draw **DFA** for the word **MOOI.**	
c.	Consider the following corpus and answer the following. <S>Thank you so much for your help </S> <S>I really appreciate your help </S> <S>Excuse me, do you know what time it is </S> <S>I really sorry for not inviting you </S>	

	<S>I really like your watch </S> I. Using bigram language model what is the P(like | really). II. Using trigram language model with add one smoothing what is the P(really) III. Calculate the perplexity for trigram <S>I really like your watch </S>
d.	Explain bag of words method. Write steps to convert the document **"This pizza very tasty and affordable. This pizza is not tasty and is affordable. This pizza is very delicious and affordable."** into feature vectors using bag of words method.

Enrolment No._____

NATIONAL FORENSIC SCIENCES UNIVERSITY
GOA CAMPUS
M.Sc. Cyber Security - Semester -II Term Assessment-I

Subject Code: CTMSCS SII P1
Date: 28/02/2024 **Subject Name: Network Security**
Time: 45 Minutes **Total Marks: 25**

Instructions:

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

Q1 to Q10 Fill in the blanks/Multiple Choice questions, each for 1 mark (10x1=10)

Select your appropriate answer:

Q 1 _____layer of the OSI model is responsible for establishing, maintaining, and terminating connections between systems? **01 Mark**

Q 2 _____attack floods a network with a large volume of bogus traffic to disrupt normal operation? **01 Mark**

Q 3 _____ server filters and forward network traffic. **01 Mark**

Q 4 _____ attack involves sending fraudulent emails to trick individuals into revealing sensitive information? **01 Mark**

Q 5 Transport layer aggregates data from different applications into a single stream before passing it to _____ layer.

Q 6 What is the primary purpose of a Network Operations Center (NOC)? **01 Mark**

(i) Monitor and manage network infrastructure
(ii) Block malicious traffic
(iii) Investigate security incidents
(iv) Assign IP addresses to devices on a network
(v) All of these.

Q 7 In Three-Way Handshaking process, the situation where both the TCP's issue an active open is _____ **01 Mark**

(i) Mutual open
(ii) Mutual Close
(iii) Simultaneous open
(iv) Simultaneous close
(v) Never Close.

Q 8 What is the main function of a Firewall in a network? **01 Mark**

(i) To filter and control network traffic based on security rules
(ii) To route data packets between different networks
(iii) To provide dynamic IP addressing
(iv) To enhance network performance
(v) All of the above

Q 9 Which protocol is used by mail servers to send and receive emails? **01 Mark**

i) SMTP
ii) POP3
iii) IMAP
iv) SNMP

Q 10 What is the purpose of a SIEM system? **01 Mark**

i) To prevent unauthorized access to a network

ii) To manage DNS requests

iii) To monitor and analyze security events

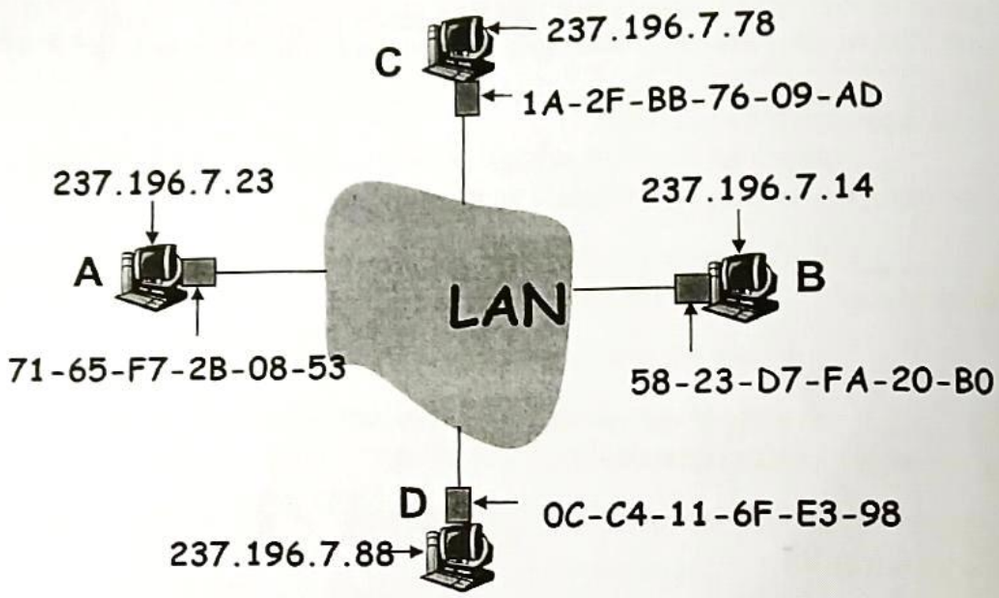
iv) To assign IP addresses to devices on a network

Q11 to Q15 Descriptive 3 marks for each question (5x3=15)

Q11 Discuss the differences between IDS and IPS in terms of detection and prevention mechanisms. **03 Marks**

Q 12 Differentiate the Non repudiation, Eavesdropping, and Masquerading. **03 Marks**

Consider the following Network: **(for Q 13-14)**



Q 13 Consider the above network topology, **User A** wants to communicate with **User B**. Explain the explain ARP protocol with respect to this scenario. Further consider **User C** as the attacker and explain the any ARP attack in the same topology. **03 Marks**

Q14 With respect to the same network topology, highlight the all-possible attack vectors and attack surfaces. **03 Marks**

Q 15 Read the following scenario and answer the questions below: **03 Marks**

Scenario: A medium-sized company operates a network infrastructure consisting of multiple offices interconnected through a Wide Area Network (WAN). The company's network includes servers for various services, such as DNS, DHCP, email, and applications. Recently, the company experienced a series of DDoS attacks that disrupted its operations and caused financial losses.

a) Identify potential vulnerabilities in the company's network infrastructure that could have been exploited to launch the DDoS attacks.

b) Recommend preventive measures and countermeasures to enhance the company's network security and mitigate the impact of future DDoS attacks.

~END OF PAPER~

National Forensics Sciences University, Goa Campus
TA-1 Examination

Program Name – M.Tech. (AI&ML)	Sem – II	Date- 28.02.24
Subject Name- Advanced Machine Learning for Cyber Security & Forensic		Subject Code- CTMSAIDS SII P1
Time- 45 minutes		Max. Marks- 25
Instructions - 1) Answer all questions. 2) Assume suitable data.		
Q.1	Multiple Choice Questions (1 mark each)	10 marks
	1a What is Machine learning? A) The autonomous acquisition of knowledge through the use of manual programs B) The selective acquisition of knowledge through the use of manual programs C) The autonomous acquisition of knowledge through the use of computer programs D) The selective acquisition of knowledge through the use of computer programs	1 mark
	1b. How many types of Machine Learning Techniques? A) 3 B) 5 C) 7 D) 9	1 mark
	1c. Machine learning is a subset of_____ A) Data Learning B) Deep Learning C) Artificial Intelligence D) None of the above	1 mark
	1d. Machine Learning is a field of AI consisting of learning algorithms that_____ A) At executing some task B) Over time with experience C) Improve their performance D) All of the above	1 mark
	1e. What is true about Machine Learning? A) Machine Learning (ML) is that field of computer science B) ML is a type of artificial intelligence that extract patterns out of raw data by using an algorithm or method. C) The main focus of ML is to allow computer systems learn from experience without being explicitly programmed or human intervention. D) All of the above	1 mark
	1f. Data points have negetive residual A) if they are below the regression line B) if they are above the regression line	1 mark

	C) if the regression line actually passes through the point D) None of the above	
	1g. In linear regression, we try to _____ the least square errors of the model to identify the line of best fit. A) Change B) Maximize C) Minimize D) None of the above	1 mark
	1h. Which of the following is not a supervised learning? A) PCA B) Naive Bayesian C) Linear Regression D) Decision Tree	1 mark
	1i. How do you handle missing or corrupted data in a dataset? A) Drop missing rows or columns B) Assign a unique category to missing values C) Replace missing values with mean/median/mode D) All of the above	1 mark
	1j. Identify the type of learning in which labeled training data is used. A) Reinforcement learning B) Unsupervised learning C) Supervised learning D) Semi unsupervised learning	1 mark
Q.2	Answer any 3 questions (3x5 marks each)	15 Marks
	i. Differentiate between Supervised, Unsupervised and Reinforcement Learning	5 marks
	ii. What are the important objectives of machine learning?	5 marks
	iii. Explain Hypothesis class with example.	5 marks
	iv. Explain VC dimension with example.	5 marks

Seat No. _____ Enrolment No. _____

NATIONAL FORENSIC SCIENCES UNIVERSITY

Master of Technology, AI and DS (specialization in Cyber Security)
Semester – I – January – 2024

Subject Code: CTMTAIDS SI P2
Subject Name: Network Security And Forensics **Date: 12/01/2024**
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. **Scientific Calculator is allowed.**
5. **Figures to the right indicate full marks.**
6. **Parts of the question should be attempted at the same place.**

			Marks
Q.1		**Attempt any three.**	
	(a)	You are the network administrator of a large organization. Justify the selection of specific internetworking devices to optimize network performance, considering scalability and security concerns.	08
	(b)	Differentiate between TCP and UDP. Explore potential vulnerabilities and attack scenarios for each protocol.	08
	(c)	Construct a Playfair cipher for following: ***Key: MTECH AIDS*** ***Plaintext: MTECH AI DS is future of NFSU.***	08
	(d)	Provide an overview of SSL/TLS and its role in securing communication over the internet.	08
Q.2		**Attempt any three.**	
	(a)	During live network enumeration, unexpected challenges arise. Describe a specific scenario and outline how you would adapt your live forensics approach to overcome these challenges.	08
	(b)	Name and briefly describe some tools used for packet sniffing in network security and monitoring.	08
	(c)	Consider the use of RSA encryption with two distinct prime numbers, where $p=101$ and $q=97$. Additionally, the public exponent is $e=11$. Perform the following operations: (i) Calculate the RSA public key (e,n) for encryption and determine the corresponding private key (d) for decryption. (ii) Encrypt the message $M=3$ using the computed public key.	08
	(d)	Discuss various applications of hash functions in network security and cryptography. Explain any one Hash algorithm.	08

	Attempt any three.	
(b)	Elaborate on the concept of Penetration Testing. Define the Network Pen Testing Life-Cycle and its key phases.	08
(c)	In an e-commerce platform, a customer purchases an expensive item and later denies making the transaction, attempting to get a refund while keeping the product. How can non-repudiation mechanisms be employed to ensure that the customer cannot falsely repudiate the transaction?	08
(d)	Describe the role of Public Key Infrastructure (PKI) in the context of digital signatures.	08
	Alice and Bob decide to use the Diffie-Hellman key exchange algorithm to establish a shared secret key. They agree on the prime modulus $p=31$ and the base or generator $g=11$. a. Calculate the secret key for both Alice and Bob if Alice's private key is $a=7$ and Bob's private key is $b=9$. b. Determine the shared session key that Alice and Bob will use for secure communication. c. Illustrate the step-by-step process of the Diffie-Hellman key exchange algorithm.	08
	Attempt any two.	
(a)	Describe the OSCAR Methodology in penetration testing. Provide examples of scenarios where the OSCAR Methodology is particularly effective.	07
(b)	Assume you are implementing a SIEM tool in a large organization. Describe the steps involved in the implementation process and how the tool enhances the organization's overall security posture.	07
(c)	Investigate the concept of Evil Twin in wireless networks. Discuss potential threats and countermeasures against such attacks.	07
	Attempt any two.	
(a)	During a confidential corporate board meeting conducted over a video conferencing platform, sensitive financial information is discussed. Unbeknownst to the board members, an employee is eavesdropping on the meeting. Discuss the potential consequences of such eavesdropping and propose measures to prevent it.	07
(b)	Provide an in-depth overview of IEEE 802.11 protocols. Discuss the vulnerabilities associated with WEP and propose alternative security measures.	07
(c)	Explain following terms: (i) HTTPS (ii) IPv6	07

--- End of Paper---

Seat No.: _____ Enrolment No._____

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Digital Forensics and Information Security
Semester – III – January - 2024

Subject Code: CTMSDFIS SIII P1
Subject Name: Network Security & Forensic
Time: 11:00 AM to 2:00 PM

Date: 03/01/2024

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		**Attempt any three.**	
	(a)	List all types of internetworking devices. Also explain any two application layer devices.	**08**
	(b)	Compare and contrast between DNS and DHCP server with example.	**08**
	(c)	Use the Vigenere cipher with keyword "NFSU" to encipher the message "SEMESTER EXAM".	**08**
	(d)	Discuss the merits and demerits of firewall with example.	**08**
Q.2		**Attempt any three.**	
	(a)	Discuss all the phases of penetration testing with suitable example.	**08**
	(b)	Explain dumpster diving and war driving.	**08**
	(c)	What would you do if ***nmap*** port scans are blocked by network security administrator? How would you gather host information in such case?	**08**
	(d)	Explain in details tools used for packet sniffing in network security and monitoring.	**08**
Q.3		**Attempt any three.**	
	(a)	Given the two prime 5 and 7, the value of **e** is 5. Encrypt the message **M = 2**, calculate the public key, private key, and the corresponding cipher text. (Hint: use **RSA**)	**08**
	(b)	Encrypt the plain text "DFIS" with the key "MONARCHY" using Playfair cipher. Also, verify the plain text from the generated cipher text.	**08**
	(c)	List and briefly explain the three security goals.	**08**
	(d)	Explain virtual private network (VPN) with suitable example. How does it provide the end-to-end security?	**08**
Q.4		**Attempt any two.**	
	(a)	Discuss in detail WEP and WPA protocol with suitable diagram.	**07**
	(b)	Explain in detail security flaws in WLAN.	**07**
	(c)	During a routine antivirus scan, a government system administrator	**07**

		was alerted to suspicious files on a server. The files appeared to be part of a well-known root kit. The server did not host any confidential data other than password hashes, but there were several other systems on the local subnet that contained Social Security numbers and financial information of thousands of state residents who had filed for unemployment assistance. The administrative account usernames and passwords were the same for all servers on the local subnet. Answer the following question on the above scenario: **i.** Was the server truly compromised? **ii.** If so, how was the system exploited?	
Q.5		**Attempt any two.**	
	(a)	Discuss in detail network traffic capture analysis for Linux operating system.	07
	(b)	What is network forensic? What are various network forensics instigation methods?	07
	(c)	Differentiate the ARP poising and MAC flooding.	07

--- End of Paper---

Seat No.: _____ Enrolment No._____

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Cyber Security

Semester – III – January - 2024

Subject Code: CTMSCS SIII P1 **Date: 01/01/2024**

Subject Name: Blockchain and Cryptocurrencies

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		**Attempt any three.**	
	(a)	Explain Encryption & Hash Function.	**08**
	(b)	Explain Two General Problem & Byzantine General Problem.	**08**
	(c)	Explain Hash Pointers & Merkle Tree.	**08**
	(d)	Explain Blockchain and How is it different from Conventional databases.	**08**
Q.2		**Attempt any three.**	
	(a)	Explain the advantage and disadvantage of Blockchain.	**08**
	(b)	Explain Private Blockchain and Why to use it.	**08**
	(c)	Explain Public Blockchain and Why to use it.	**08**
	(d)	Explain the following term : Soft Fork, Hard Fork, Gas Limit, Decentralized Autonomous Organization	**08**
Q.3		**Attempt any three.**	
	(a)	Explain Proof of Work.	**08**
	(b)	Explain Proof of Stake	**08**
	(c)	Explain Proof of Burn and Proof of Space.	**08**
	(d)	Write short notes on the following: Difficulty level, Nakamoto Consensus Protocol..	**08**
Q.4		**Attempt any two.**	
	(a)	Explain sybil attack and 51% attack and how they are different	**07**
	(b)	Explain RAFT Protocol and PAXOS Algorithm	**07**
	(c)	What are smart contract constructions. Explain its working with the benefits.	**07**
Q.5		**Attempt any two.**	
	(a)	Explain the following: Double spending, and Selfish mining attack, Eclipse attack.	**07**
	(b)	Discuss one practical application of Blockchain in real life such as the medical industry, domain name service, Internet of Things, etc. You are free to choose any practical application of your choice.	**07**
	(c)	Discuss Ethereum and What are the features of Ethereum.	**07**

--- End of Paper---

Seat No.: _____ Enrolment No._____

NATIONAL FORENSIC SCIENCES UNIVERSITY

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

Subject Code: CTMSCS SIII P1 **Date: 23/11/2023**

Subject Name: Blockchain and Cryptocurrencies

Time: 11:00am-2:00pm **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 cryptography and explain its significance in modern computing.	**10**
	(b)	Differentiate between symmetric and asymmetric encryption algorithms.	**10**
Q.2	**(a)**	Elaborate on the concept of hash functions and their role in ensuring data integrity.	**05**
	(b)	Discuss the use of hash pointers in data structures for maintaining security.	**05**
Q.3	**(a)**	Explain the working of Digital Signatures with a focus on the ECDSA algorithm.	**10**
	(b)	What is a Zero Knowledge Proof? Provide an example to illustrate its application.	**10**
Q.4	(a)	Define blockchain and outline its key features. Enumerate the advantages of blockchain over conventional distributed databases.	**10**
	(b)	Describe the mining mechanism in a blockchain and its role in maintaining consensus.	**10**
	(c)	Differentiate between soft and hard forks in blockchain.	10
Q.5	**(a)**	Explain the Nakamoto Consensus and its role in blockchain networks.	**10**
	(b)	Discuss the concept of Proof of Work and Proof of Stake and its advantages and disadvantages.	**10**

END OF PAPER

Enrolment No._____

NATIONAL FORENSIC SCIENCES UNIVERSITY
GOA CAMPUS
M.Tech. (AI&DS) and M.Sc. DFIS - Semester -III Term Assessment-I

Subject Code: CTMTSIDS SI P1 and CTMDFIS SIII P1
Date: 18/09/2023
Subject Name: Network Security & Forensics
Time: 45 Minutes **Total Marks: 25**

Instructions:

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

Q1 To Q10 Multiple Choice questions, each for 1 mark (10x1=10)
Select your appropriate answer:

Q 1 What layer of the OSI model is responsible for end-to-end communication between two devices? **01 Mark**

(i) Data Link Layer
(ii) Network Layer
(iii) Session Layer
(iv) Transport Layer
(v) Presentation Layer

Q 2 Which of the following statements could be valid with respect to the ICMP (Internet Control Message Protocol)? **01 Mark**

(i) It reports all errors which occur during transmission
(ii) A redirect message is used when a router notices that a packet seems to have been routed wrongly.
(iii) It informs routers when an incorrect path has been taken.
(iv) The "destination unreachable" type message is used when a router cannot locate the destination.
(v) All of the above !

Q 3 What is the primary purpose of a Network Operations Center (NOC)? **01 Mark**

(i) Monitor and manage network infrastructure
(ii) Block malicious traffic
(iii) Investigate security incidents
(iv) Assign IP addresses to devices on a network
(v) All of these.

Q 4 When you ping the loopback address, a packet is sent where? **01 Mark**

(i) On the network
(ii) Down through the layers of the IP architecture and then up the layers again
(iii) Across the wire
(iv) through the loopback dongle
(v) Not work.

Q 5 Transport layer aggregates data from different applications into a single stream before passing it to _____ **01 Mark**

(i) data link layer
(ii) application layer
(iii) network layer
(iv) physical layer
(v) both (i) and (ii)

Q 6 In Three-Way Handshaking process, the situation where both the TCP's issue an active open is _____ **01 Mark**

(i) Mutual open
(ii) Mutual Close
(iii) Simultaneous open
(iv) Simultaneous close
(v) Never Close.

Q 7 User datagram protocol is called connectionless because _____ **01 Mark**

(i) all UDP packets are treated independently by transport layer
(ii) it sends data as a stream of related packets

(iii) it is received in the same order as sent order
(iv) it sends data very quickly
(v) both (i) and (ii)

Q 8 What is the main function of a Firewall in a network? **01 Mark**

(i) To filter and control network traffic based on security rules
(ii) To route data packets between different networks
(iii) To provide dynamic IP addressing
(iv) To enhance network performance
(v) All of the above

Q 9 Which of the following is NOT a function of a router? **01 Mark**

Choose the appropriate answer:

(i) Packet forwarding
(ii) Logical addressing
(iii) Broadcast domain separation
(iv) Data frame switching
(v) All of these

Q 10 An assault on system security that derives from an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system is a(n) _____. **01 Mark**

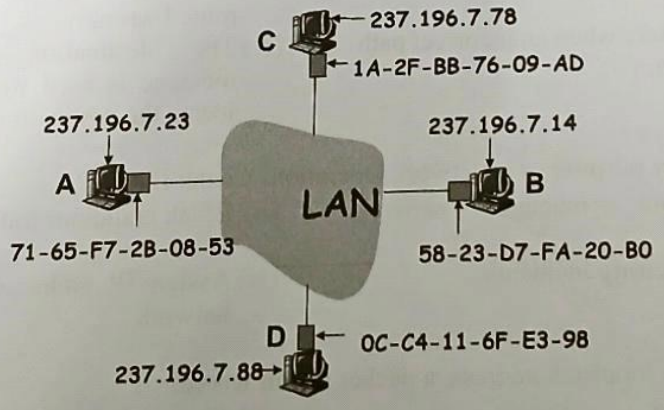
(i) risk
(ii) asset
(iii) attack
(iv) vulnerability
(v) countermeasure

Q11 to Q15 Descriptive 3 marks for each question (5x3=15)

Q11 Your organization has experienced an increase in phishing attacks recently. Describe what a phishing attack is, its common characteristics, and the countermeasures you can implement to mitigate this threat. **03 Marks**

Q 12 Differentiate the Non repudiation, Eavesdropping, and Masquerading. **03 Marks**

Consider the following Network: **(for Q 13-14)**



Q 13 Consider the above network topology, **User A** wants to communicate with **User B**. Explain the explain ARP protocol with respect to this scenario. Further consider **User C** as the attacker and explain the any ARP attack in the same topology. **03 Marks**

Q14 With respect to the same network topology, highlight the all-possible attack vectors and attack surfaces. **03 Marks**

Q 15 Explain following examples/terms: **03 Marks**

(i) VPN vs VLAN
(ii) Local DNS vs TLD
(iii) IDS vs IPS