National Forensics Sciences University, Goa Campus
TA-1 Semester Examination

2023

Program Name: CS/ DFIS **Sem – III** **Date- 16/9/2023**

Subject Name- Blockchain and Cryptocurrency Subject Code- CTMSCS SIII P1 / CTMSDFIS SIII P3

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
	I. Transposition cipher ____ a) Substitutes letter b) Rearranges letter c) both a and b d) None of the these	1 mark
	II. Encryption does not protect data from modification by another party. a) True b) False	1 mark
	III. Key space for ceaser cipher can be ____ >25 b) 0< keysize >25 c) Any positive integer d) Any integer	1 mark
	IV. Y = EK(X). Here y is______. a) plain text b) Cipher text c) Key d) Encipher	1 mark
	V. Which is not active attack? a)Modification b) Fabrication b) Replay attack d) none of the these	1 mark
	VI. Amongst which of the following is /are good use for Hash function, a) Password protection b) Data integrity / file verification c) Digital signatures and virus signatures d) All of the mentioned above	1 mark
	VII. When a hash function is used to provide message authentication, the hash function value is called to as: a) Message Field b) Message Digest c) Message Score d) Message Leap	1 mark
	VIII. When a hash function is used to provide message authentication, the hash function value is called to as: a) Message Field b) Message Digest c) Message Score d) Message Leap	1 mark
	IX. Encryption algorithm is used to transforms plaintext into.......................... a)Simple Text b) Cipher Text c) Empty Text d) None of the above	1 mark
	X. A symmetric-key cipher uses a)1 Key b) 2 Key c) 3 Key d) 4 Key	1 mark
Q.2	Answer any 3 questions (3x5 marks each)	15 Marks
	I. If p = 17, q = 11 are two prime numbers then find out suitable public key pair and private key using RSA encryption.	5 marks

(8) In RSA plain text is encrypted with sender's private key preserves ____

a) Integrity b) confidentiality

	II.	Using the key generation in Que 2 (i), find ciphertext for 2023. For the same plaintext How RSA can preserve sender side no repudiation?	5 marks
	III.	List the types of cryptanalytic attacks?	5 marks
	IV.	How hash functions provide password protection?	5 marks
	V.	What are the properties of good hash function?	5 marks

$\phi(n) = 160$

160×1
2
3
4
5
6
7
8
9
10

$m = 2023$

$C = m^e \bmod n$

$= 2023^7 \bmod 187$

$= (\cancel{2023})(153)^7 \bmod 187$

$= (153^2)^3 \cdot 153 \bmod 187$

$= (34)^3 \cdot 157 \bmod 187$

$C = \underline{153}$

$((2023^2)^3 \cdot 2023 \bmod 187$

$= (34)^3 2023 \bmod 187$

$= \underline{\underline{153}}$

$m = C^d \bmod n$

$= 153^{23} \bmod 187$

$= (153^2)^{10} \cdot 153^3 \bmod 187$

$= (34)^{10} \cdot 153 \bmod 187$

$(34^3)^3 \cdot 34 \cdot 153 \bmod 187$

$= 34 \cdot 34 \cdot 153 \bmod 187$

$= \underline{153}$

National Forensics Sciences University, Goa Campus
Mid- semester Examination

2034

Branch – M.Sc.DFIS / MSc CS	Sem –III	Date- 30/10/2023
Subject Name-Blockchain and Cryptocurrency	Subject Code- CTMSCS SIII P1 & CTMSDFIS SIII P3	
Time- 1.5 Hours		Max. Marks- 50

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

Q.1	Solve any four	20 marks /20 (12)
	a. Compare blockchain and distributed databases.	5 marks
	b. Explain bitcoin transaction flow.	5 marks
	c. Draw and explain merkle tree.	5 marks
	d. How bitcoin handles temporary fork?	5 marks
	e. Explain bitcoin crypto economy.	5 marks
Q.2	**Attempt all**	**15 marks** /15
	a. Explain bitcoin cryptopuzzle?	5 marks
	b. Is Following statement is true. Justify your answer. **Miners should propose nonempty blocks**	5 marks
	c. What are the different types of blockchains? Explain any two.	5 marks
Q. 3	**Attempt a and b**	15 marks /15
Q.3 a	**Attempt any one**	
	1) Write short note on i) Eclipse attack ii) Selfish mining attack	8 marks
	OR	
	2) How attacker can perform Sybil attack? Explain severity of the Sybil attack.	8 marks
Q.3 b	**Attempt any one**	
	1) Explain steps of the PoB and list advantages and disadvantages of PoB.	7 marks
	OR	
	2) Compare PoW and PoS consensus mechanisms.	7 marks

Seat No.: 7074

Enrolment No. 03770037074

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.** 20

3

- (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.** 12

3

- (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.** 16

3

- (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.** 8

2

- (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.** 12

2

- (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---

2034

National Forensics Sciences University, Goa Campus
TA1 Examination

23/25

Program – M.Sc. Cyber Security/Digital forensic and information security

Sem – III

Date - 18-09-2023

Subject Name – IoT Security and Forensics

Subject Code – CTMSCS SIII P2/ CTMSDFIS SIII P2

Time- 11:00 A.M. to 11:45 A.M.

Max. Marks- 25

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

Q.1	Multiple Choice Questions (1 mark each)	10 marks
✓	i. “Internet of things” term first coined in: a. 1998 [✓ b.] 1999 c. 2000 d. 2001	1 mark
✓	ii. Who coined the term “Internet of Things”? [✓ a.] Kevin Aston b. John wright c. Edward jameson d. None	1 mark
✓	iii. Which of the following is not an application of IoT [✓ a.] sensors b. self-driven car c. smart city d. smart home	1 mark
✓	iv. Which layer is used for wireless connection in IoT devices? a. Application layer [✓ b.] Network layer c. Data link layer d. None	1 mark
✓	v. Which of the following is used to capture data from the physical world in IoT devices? [✓ a.] Sensors b. Actuators c. Microcontrollers d. all	1 mark
✓	vi. Which of the following protocol is used to link all the devices in the IoT? a. HTTP b. UDP c. Network	1 mark

		[✓ d.] TCP/IP	
✓	vii.	IoT systems can be categorized in: a. 4 Levels b. 5 Levels [✓ c.] 6 Levels d. 7 Levels	1 mark
	viii.	Cloud storage is not used in which level of IoT systems a. Level 2 b. Level 3 c. Level 4 [✓ d.] None	1 mark
✓	ix.	Which of the following is not a fundamental component of an IoT system? a. Sensors b. Connectivity and data processing c. User interface [✓ d.] Transformers	1 mark
✓	x.	Which of the following is false about IoT devices? a. IoT devices use the internet for collecting and sharing data b. IoT devices need microcontrollers c. IoT devices use wireless technology [✓ d.] IoT devices are completely safe	1 mark
Q.2	Answer any 3 questions (3x5 marks each)		15 Marks
✓	i.	Write the history, current status and future prospect of IoT?	5 marks
	ii.	Explain about the major components of IoT.	5 marks
✓	iii.	Illustrate the characteristics of IoT.	5 Marks
✓	iv.	Explain physical and logical design of IoT.	5 marks

National Forensics Sciences University, Goa Campus
Mid- semester Examination

Programme – M.Sc. Cyber Security / M.Sc. DFIS

Sem – III **Date- 01/11/2023**

Subject Name: IoT Security and Forensics **Subject Code- CTMSCS SIII P2/ CTMSDFIS SIII P2**

Duration- 1.5 Hours **Max. Marks- 50**

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

Q.1	Answer any four questions.	20 marks /20 → 13
	a. Explain the publish subscribe communication model.	5 marks
	b. Give classifications of sensors and actuator. Give two examples of each category.	5 marks
	c. What are the M2M enabling technologies. Briefly explain two of them.	5 marks
	d. Explain node behaviour in wireless sensor network.	5 marks
	e. What are the Challenges and Need for standards in M2M	5 marks
Q.2	Attempt all	15 marks /15 →
	a. Which are the different components of IoT? Explain it with respect to any one IoT application	5 marks 8
	b. Draw IoT protocol stack and explain each layer in brief.	5 marks
	c. Write characteristics of M2M technology and differentiate between M2M & IoT	5 marks
Q.3	Attempt a and b	15 marks /15 → 12
Q.3 a	Attempt any one	
Q.3 a	I Differentiate between MQTT & COAP	8 marks
	OR	
	II. What are the major components of MQTT protocol? Explain its working in detail.	8 marks
Q.3 a	Attempt any one	7 marks
Q3 b	I. Discuss the XMPP protocol and its architecture	7 marks
	OR	
	II. Write importance of IoT security with respect to any one IoT application.	7 marks

End of Paper

Seat No.: 234　　　　　　　　　　Enrolment No. 23

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Cyber Security

Semester – III – January - 2024

Subject Code: CTMSCS SIII P2 **Date: 02/01/2024**
Subject Name: IoT Security and Forensics
Time: 11:00 AM to 2:00 PM **Total Marks: 100**

Instructions:

1. **Write down each question on a 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.** 　16

3

(a) What is IoT? Discuss its five applications in healthcare. **08**

(b) What is the difference between the physical and logical design of IoT. **08**

(c) Explain the IoT protocol stack with the help of suitable diagrams. **08**

(d) What are the four major security challenges in IoT and also describe the mitigation techniques for them. **08**

Q.2 **Attempt any three.** 　16

3

(a) Explain the difference between IoT and M2M. **08**

(b) Explain the different levels of IoT in brief. **08**

(c) Discuss the SDN architecture with the help of a diagram. **08**

(d) Explain the SNMP in detail. Also, write its advantages and limitations. **08**

Q.3 **Attempt any three.**

3

(a) What is HTTP protocol? Discus its architecture with a suitable diagram. **08**

(b) Explain the differences between MQTT and XMPP. **08**

(c) What is CoAP? Explain its architecture in detail with advantages and limitations. **08**

(d) What is the role of interoperability in IoT devices? Explain with an example. **08**

Q.4 **Attempt any two.** 　12

2

(a) Explain the security, privacy, and trust in IoT systems. What are the ways to achieve them? **07**

(b) What is pen testing? Explain the steps of pen testing in detail. **07**

(c) What is threat modeling? What are the benefits of threat modeling? **07**

Q.5 **Attempt any two.** 　12

2

(a) What are OWASP top 10 vulnerabilities? Explain five of them. IUTP **07**

(b) Discuss the different IoT attack vectors. Also, Explain the different attack surfaces **07**

(c) What are the different IoT forensic tools? What kind of information can be collected from these tools? 07

--- End of Paper---

National Forensics Sciences University, Goa Campus
TA-1 Examination

Program Name – M.Sc. CS/DFIS Sem – III Date- 16.09.23

Subject Name- Cloud Security & Forensics Subject Code- CTMSCS S3-P3

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) Which of the following provides the least security** [✓ **a.** IaaS] **b.** PaaS **c.** SaaS **d.** None	1 mark
✓	**1b) Among the following, which attack can be performed at the application layer?** a. Rootkit b. Buffer overflow c. Trojans [✓ d. TOCTTOU]	1 mark
✓	**1c) While indexing the data content to enhance the search performance we can avoid the inclusion of sensitive data by using:** [✓ a. Low protection] b. Medium protection c. Strong Protection d. None of these	1 mark
✓	**1d) What is a possible risk of cloud computing** **a.** Lack of access to data [✓ **b.** Storage of data without control over the location of where the data is stored] **c.** Lack of ability to back up data **d.** None	1 mark
✓	**1e) Policy ranking is the:** [✓ **a.** Ranking of different policies] **b.** Indexing of data **c.** Tool to help the user to select CSP **d.** None	1 mark
✓	1f) In **cloud computing JAR files are used to:** **a.** To protect data [✓ **b.** To execute the data] **c.** To avoid virtualization threat **d.** None	1 mark
✓	**1g) The risk associated with Infrastructure as a Service can be minimised by using:** a. PALM b. HyperSafe c. Closed box execution environment [✓ d. Access control]	1 mark
✓	**1h) CSP need not to decrypt the data while performing the search operation by using:**	1 mark

	a. ECC b. RSA [✓ c. Searchable encryption technique] [✓ d. All are correct]	
	1i) Among the following which not a public cloud: a. AWS b. Azure [✓ c. nextCloud] d. All are correct	1 mark
	1j) Among the following which hypervisor is a bare metal hypervisor. a. Oracle VB [✓ b. KVM] c. Vmware workstation d. None of these	1 mark
Q.2	Answer any 3 questions (3x5 marks each)	15 Marks
	i. Discuss the possible vulnerabilities with respect to layers in cloud environment.	5 marks
	[✓ ii.] Discuss and draw the NIST cloud security architecture model.	5 marks
	[✓ iii.] What is indexing in cloud environment? Why do we need it, discuss in detail?	5 marks
	[✓ iv.] What is multi cloud explain with suitable example and also discuss the security risk associated with it?	5 marks

National Forensics Sciences University, Goa Campus
Mid-semester Examination

Programme – M. Sc. Cyber Security / DFIS Sem – III		Date- 31.10.23
Subject Name- Cloud Security & Forensic Subject Code- CTMSCS S3-P3		
Time- 1.5 Hours		Max.Marks- 50
Instructions - 1) Answer all questions. 2) Assume suitable data.		
Q.1	Solve any four	20 marks /20 →12)
	a. What is Object-based storage in cloud computing?	5 marks
	b. How does a Kernel-based virtual machine work? Explain.	5 marks
	c. Write a note on containerization.	5 marks
	d. What is cloud logging? Explain.	5 marks
	e. How hardening helps to make our system secure. Explain by considering the use case of software application hardening.	5 marks
Q.2	Attempt all	15 marks /10 →15)
	a. How block-based storage is different from file-based storage.	5 marks
	b. What is a SOC-2 certification?	5 marks
	c. What is Para virtualization? List out at least three hypervisors based on it.	5 marks
Q. 3	Attempt a and b	15 marks /15 → (12,13)
Q.3 a	Attempt any one	
Q.3 a	I. Differentiate between KVM, VMware ESXi, Hyper V, and Xen hypervisor.	8 marks
	OR	
	II. What are some examples of metrics that service-level agreements cover?	8 marks
Q.3 b	Attempt any one	7 marks
Q3 b	I. What is scaling? How horizontal scaling is different from vertical scaling.	7 marks
	OR	
	II. What is a Docker? How containers are different from images, explain with a suitable example.	7 marks

Seat No.: 2034 Enrolment No. 2034

NATIONAL FORENSIC SCIENCES UNIVERSITY

Msc (Cyber Security) - Semester –III- January 2024

Subject Code: CTMSCS SIII P3 **Date: 03/01/2024**

Subject Name: Cloud Security and Forensics

Time: 11 AM TO 2 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 18/24

Q.1 **Attempt any three.** 3

- **(a)** Discuss different layers which define cloud architecture. **08**
- **(b)** Discuss different components of Docker Environment. **08**
- **(c)** Discuss THREE possible scenario in which Symmetric key cryptography is not suitable or efficient option for cloud environment. **08**
- **(d)** Compare the working of SaaS and PaaS based on following parameters : Services, Provider, Users, Limitation, Security, billing **08**

Q.2 **Attempt any three.** [illegible]/24 3

- **(a)** Explain the importance of Logs in the cloud computing? Which are the different sources of Logs in Cloud Computing Environment? **08**
- **(b)** What are the different challenges you face when you have been asked to investigate a case whose data lies over a cloud in some other country, discuss in detail considering all aspects? **08** 12
- **(c)** Explain the process in which Google App Engine architecture works **08**
- **(d)** Answer the following for RSA cryptosystem: **08**
  - a. Briefly explain the idea behind the RSA cryptosystem
  - b. What is the one-way function in this system?
  - c. What is the trapdoor in this system?
  - d. Define the public and private keys in this system
  - e. Describe the security of this system

Q.3 **Attempt any three.** 18/24 3

- **(a)** What is Cloud Accountability? Discuss possible solutions to achieve accountability in the cloud **08**

(b) For Diffie-Hellman key exchange protocol compute the key using the following chosen parameters : prime=353, primitive root = 3, number chosen by A=97, by B=233.(Show each step) $Y_A = 40$, $Y_B = 51$, $\frac{Y_{AB}}{K_{BA}}$ 160 08

3

(c) Critically compare and contrast the following cloud deployment models: Private cloud, public cloud, Hybrid cloud and community cloud. Consider following parameters for comparison : Scalability, Reliability, Security, Performance, cost, Level of Trust 08

(d) Discuss architecture in detail to implement cloud forensic. 08

Q.4 **Attempt any two.** 07

2

(a) Cloud Service Business (Providers):

I. Microsoft Azure

II. Amazon AWS

III. Salesforce.com

Listed above are three cloud service providers. For each cloud service provider, answer the following questions:

a. What kind of cloud service model is implemented by this company? Explain your answer briefly why you think it is that type of cloud service?

b. What kind of cloud delivery model is does each company employ (Public, Private, Hybrid or Community)?

c. List out which cloud characteristics each company contains

(b) In what way do containers and Virtual Machine (VM) differ? 07

(c) How fog and edge computing helps in reducing data processing at the cloud? 07

Q.5 **Attempt any two.**

2

(a) List out and briefly discuss the functions of following Cloud Infrastructure component 07

a. Cloud Broker b. Cloud Auditor

(b) Discuss different memory management techniques to optimize virtual memory of Hypervisor. 07

(c) What is Cloud orchestration? Discuss types of cloud based on orchestration. 07

END OF PAPER

National Forensics Sciences University, Goa Campus
TA1 Examination

Program – M.Sc. Cyber Security/Digital forensic and information security

Sem – III

Date - 20-09-2023

Subject Name – Critical Infrastructure security

Subject Code – CTMSCS SIII P4 EL1/ CTMSDFIS SIII P4 EL1

Time- 11:00 A.M. to 11:45 A.M.

Max. Marks- 25

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

Q.1	Multiple Choice Questions (1 mark each)		10 marks
✓	i.	DCS stands for: a. Distributed central system b. Design control system [✓ c. Distributed control systems] d. None	1 mark
✓	ii.	RTU is a: a. Master control unit. b. Human machine interface [✓ c. None]	1 mark
✓	iii.	One of PLC functionalities is: [✓ a. managing the sensors and actuators] b. displays the data to the user c. None	1 mark
	iv.	Data historian in SCADA: a. is a human being. [✓ b. is a software.] [✓ c. Both] d. None	1 mark
✓	v.	The risks involved in OT systems is/are: a. Human Safety. b. Environmental Safety. c. Material damage [✓ d. all]	1 mark
✓	vi.	Sensors are the part of which level of PURDUE model: [✓ a. Level 0] b. Level 1 c. Level 2 d. None	1 mark
	vii.	Data historian is a part of which level of PURDUE model? a. Level 0 b. Level 1	1 mark

		c. Level 2 [✓ d.] Level 3	
✓	viii.	How many levels in the PURDUE model: a. 4 b. 5 c. 6 [✓ d.] 7	1 mark
✓	ix.	ICS-DMZ is the layer for sharing information: a. Between process control zone and operation zone [✓ b.] Business zone and operation zone c. IT and OT d. None	1 mark
	x.	IACS in the context of OT stands for: [✓ a.] Industrial automation and control system b. Industrial automated centre for security c. International authority of cyber security d. None	1 mark
Q.2	Answer any 3 questions (3x5 marks each)		15 Marks
	[✓ i]	Explain ICS and OT?	5 marks
	ii.	What are the different applications of OT. Explain any two of them.	5 marks
✓	[✓ iii]	Explain SCADA architecture with the help of diagram.	5 marks
✓	[✓ iv]	What is PURDUE model? Explain with the help of diagram.	5 marks

National Forensics Sciences University, Goa Campus
Mid- semester Examination

Programme – M.Sc. Cyber Security / M.Sc. DFIS		
Sem – III	**Date- 02/11/2023**	
Subject Name: Critical Infrastructure Security	**Subject Code- CTMSCS SIII P4 EL1/ CTMSDFIS SIII P4 EL1**	
Duration- 1.5 Hours		**Max. Marks- 50**
Instructions - 1) Answer all questions. 2) Assume suitable data.		

Q.1	Answer any four questions.	20 marks 12
	a. Explain Critical infrastructure Security with example.	5 marks
	b. Explain RTU, PLC and IED in the context of SCADA.	5 marks
	c. What is ICS-DMZ. Briefly describe its benefits.	5 marks
	d. Discuss about the evolution of SCADA Protocols.	5 marks
	e. What are the major threats to the OT Systems?	5 marks
Q.2	Attempt all	15 marks 15
	a. What is PURDUE model? Explain with the help of diagram.	5 marks
	b. What is SCADA? Explain its architecture.	5 marks
	c. What are five best practices for OT security?	5 marks
Q. 3	Attempt a and b	15 marks 15
Q.3 a	Attempt any one	
Q.3 a	I. What is MODBUS Protocol. Discuss in detail.	8 marks
	OR	
	II. Explain DNP3 Protocol in detail.	8 marks
Q.3 a	Attempt any one	7 marks
Q3 b	I. What is Profibus protocol. Explain its variants.	7 marks
	OR	
	II. Explain Single firewall DMZ and dual firewall DMZ in SCADA in detail.	7 marks

End of Paper

Seat No.: 2034 Enrolment No. 2034

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Cyber Security

Semester – III – January - 2024

Subject Code: CTMSCS SIII P4 EL3 **Date: 04/01/2024**

Subject Name: Critical Infrastructure Security

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

Instructions:

1. **Write down each question on a 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.**		22/24
3	(a)	What is SCADA? Discuss the evolution of SCADA System.	08	
	(b)	Explain the different components of SCADA system in detail.	08	
	(c)	What are the different applications of SCADA systems? Explain any two applications in detail.	08	
	(d)	Explain the PURDUE model in detail with the help of suitable diagrams	08	
Q.2		**Attempt any three.**		
	(a)	Illustrate the differences between IT and OT System	08	16/24
3	(b)	What are the three major challenges in SCADA security? Also, Explain the mitigation strategies for them.	08	
	(c)	Discuss the Evolution of SCADA protocols.	08	
	(d)	What are the SCADA communication protocols? Explain MODBUS protocol.	08	
Q.3		**Attempt any three.**		
	(a)	What is DNP3 protocol? Explain its advantages and limitations	08	
	(b)	Explain DNP3 frame structure.	08	17/24
3	(c)	What is penetration testing? What is the need for penetration testing in SCADA?	08	
	(d)	What is asset identification? Why it is important in SCADA security?	08	
Q.4		**Attempt any two.**		
	(a)	Describe stage 1 of the ICS Risk Assessment Framework/Process Steps by taking suitable example wherever necessary.	07	
2	(b)	What is cross-site scripting? How it causes threats to the SCADA security	07	6/14
	(c)	Discuss a case study of SCADA attack. Also, discuss the cause and possible ways to protect the system from such an attack	07	
Q.5		**Attempt any two.**		
2				8/14

(a) What is the CIA triad for SCADA? Which component of the triad is more important and why? 07

(b) How SCADA system is important to human life? What kind of loss can be caused due to disruption in the SCADA system? Explain with an example 07

(c) What are ICS cyber security standards? Discuss the NIST System Protection Profile for Industrial Control Systems (SPP ICS). 07

--- End of Paper---

Seat No.: 2024 Enrolment No. 2032

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Cyber Security and M.Sc. Digital Forensics and Information Security

Semester – III – January - 2024

Subject Code: CTMSCS SIII P5 EL1 / CTMSDFIS SIII P5 EL2 **Date: 05/01/2024**

Subject Name: Social Network Analysis

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.**		
3	(a) ✓	Define Social Media Forensics and explain its significance in digital investigations with appropriate example.	08	
	(b)	Discuss the ethical and legal considerations involved in conducting social media forensics.	08	15/24
	(c) ✓	Write a note on various privacy options in different social network platforms.	08	
	(d) ✓	Define Open-Source Intelligence (OSINT) and discuss its applications in the realm of social media / social network investigation.	08	
Q.2		**Attempt any three.**		
3	(a)	Write a note on URL/Domain and IP based OSINT Collection. Explain which parameters should be considered while collecting information pertaining to URL/Domain and IP.	08	
	(b)	What is the difference between email tracing and email tracking?	08	
	(c) ✓	Discuss the terms in detail: Geographical Location Intelligence (GEOINT), Social Media Intelligence (SOCMINT), Financial Intelligence (FININT), Multimedia Intelligence (MULINT)	08	18/24
	(d) ✓	Explain various platforms of social media and social network.	08	
Q.3		**Attempt any three.**		
	(a)	Discuss a real-world case where social media forensics played a crucial role in solving a crime or identifying a suspect.	08	
3	(b) ✓	Write a note with appropriate example on API Integration to enhance the capabilities of Social Media Investigation.	08	
	(c) ✓	What do you mean by graph theory, explain nodes, edges concept in graph theory.	08	15/24
	(d) ✓	What is the personal data security? Explain various Operational Security (OpSec) approaches in OSINT.	08	
Q.4		**Attempt any two.**		

	(a)	Explore and discuss emerging trends in social media forensics and OSINT.	07
	(b)	Explain emerging trends in social network forensics, considering technological advancements and changes in online communication.	07
	(c)	Explain these terms: Google dorks, Cyber Psychology, Fake News	07
Q.5		**Attempt any two.**	
	(a)	As an investigator tasked with examining an email ID related information available in cyber space, what approaches would you adopt during the intelligence gathering process?	07
	(b)	Present a case study where OSINT was instrumental in uncovering hidden information or activities.	07
	(c)	Explain the concept of image and document metadata in the context of social media forensics. How it can be useful in investigations?	07

9/14

5/14

--- End of Paper---