

TA-1 Semester Examination

Program	Name: CS,	/ DFIS Sem - III	Date- 16/9/2023
Subject N	lame- Blo	ockchain and Cryptocurrency Subject Code- CTMSCS SIII P1 / C	TMSDFIS SIII P3
Time- 45			Max. Marks- 25
Instructio	ns - 1) An	swer all questions. 2) Assume suitable data.	
Q.1	Multip	le Choice Questions (1 mark each)	10 marks
	1.	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 g) 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	1 mark
	X.	A symmetric-key cipher uses a)1 Key b) 2 Key c) 3 Key d) 4 Key	1 mark
Q.2	Answ	er any 3 questions (3x5 marks each)	15 Marks
		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)	IL	25A Plain text is Philaded	With

Sender's Princite Key Pheselvess & -- ...

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

DCm7= 160
2
3
4
5
6
1

mr 2027 (: re wad 1 = 2023 hoo 114 = (2023) (153) hod 184 = (1533) . 153 hod 184 = (3h) . 157 hod 184 (= 153

(202)²)³-2023 hos 182 - (7427023 hos 182 - 153

~ = (3 ko) h = 157 ko) 184 = (153) 10.153 ko) 18 = (343) 3.34.153 ko) 18 (743) 3.34.153 ko) 14 -39.32.153 hos 1+2



2034

्या अमृत		(0)
	Sem -III	Date- 30/10/2023
ranch - N	I.Sc.DFIS / MSC CS	& CTMSDFIS SIII P3
ubject Nan	ne-Blockchain and Cryptocurrency Subject Code- CTMSCS SITE I	
		Max. Marks- 50
ime- 1.5 H	ours - 1) Answer all questions. 2) Assume suitable data.	100
		20 marks
2.1	Solve any four	CIV
	a. Compare blockchain and distributed databases.	5 marks
FILE	a. Compare blockchain and distributed databases.	
	b./ Explain bitcoin transaction flow.	5 marks
	b. Explain bitcoin transaction flow.	
	c./ Draw and explain merkle tree.	5 marks
	c. Draw and explain merkle tree.	
	d/ How bitcoin handles temporary fork?	5 marks
	d. How bitcoin handles temporary lorks	
-	e. Explain bitcoin crypto economy.	5 marks
	C. Explain bicoom of per	
Q.2	Attempt all	15 marks
	a. Explain bitcoin cryptopuzzle?	5 marks
	6. Is Following statement is true. Justify your answer.	5 marks
	Miners should propose nonempty blocks	
		E marks
1	c. What are the different types of blockchains? Explain any two.	₫ marks
		15 marks
Q.3	Attempt a and b	151111111111111111111111111111111111111
Q.3 a	Attempt any one	
1	Write short note on i) Eclipse attack ii) Selfish mining attack	8 marks
1	OR	
1	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.	D marks
	OR	
	2) Compare PoW and PoS consensus mechanisms.	7 marks

Date: 01/01/2024

Seat No .: 2074

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Cyber Security Semester – III – January - 2024

Subject Code: CTMSCS SIII P1

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.

Q.1 Attempt any three.

(a) Explain Encryption & Hash Function.

(b) Explain Two General Problem & Byzantine General Problem.

(c) Explain Hash Pointers & Merkle Tree.

(d) Explain Blockchain and How is it different from Conventional databases.

Q.2 Attempt any three.

(a) Explain the advantage and disadvantage of Blockchain.

(b) Explain Private Blockchain and Why to use it.

(c) Explain Public Blockchain and Why to use it.

(d) Explain the following term: Soft Fork, Hard Fork, Gas Limit, Decentralized Autonomous Organization

Q.3 Attempt any three.

(a) Explain Proof of Work.

(b) Explain Proof of Stake

(c) Explain Proof of Burn and Proof of Space.

(d) Write short notes on the following: Difficulty level, Nakamoto Consensus Protocol.

Q.4 Attempt any two.

(a) Explain sybil attack and 51% attack and how they are different

(b) Explain RAFT Protocol and PAXOS Algorithm

(c) What are smart contract constructions. Explain its working with the benefits.

Q.5 Attempt any two.

(a) Explain the following: Double spending, and Selfish mining attack, Eclipse attack.

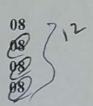
(b) Discuss one practical application of Blockchain in real life such as the medical industry, domain name service, Internet of Things, etc. You are free to choose any practical application of your choice.

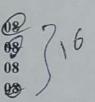
(c) Discuss Ethereum and What are the features of Ethereum.

--- End of Paper---

Marks













National Forensics Sciences University, Goa Campus **TA1 Examination**

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

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? 3. 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	1 mark
`/	G 6 Levels d. 7 Levels	
	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 IoT devices are completely safe	1 mark
Q.2	Answer any 3 questions (3x5 marks each)	15 Marks
٠	i. Write the history, current status and future prospect of IoT?	5 marks
	ii. Explain about the major components of IoT.	5 marks
V	iii. Illustrate the characteristics of IoT.	5 Marks
	iv. Explain physical and logical design of IoT.	5 marks



Programme	- M.Sc. Cyber Security / M.Sc. DFIS	
Sem - III	Date- 01/11/2023	
Subject Nar	ne: IoT Security and Forensics Subject Code- CTMSCS SIII P2/ CTMSD	FIS SIII P2
Duration- 1	.5 Hours	Max. Marks- 50
Instructions	s - 1) Answer all questions. 2) Assume suitable data.	1,
Q.1	Answer any four questions.	20 marks / (2 - (13)
	a. Explain the publish subscribe communication model.	(5)marks
	b. Give classifications of sensors and actuator. Give two examples of each category.	S 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
	a. Which are the different components of loT? Explain it with respect to any one loT application	@marks Ø
	b. Draw loT protocol stack and explain each layer in brief.	5 marks
	Write characteristics of M2M technology and differentiate between M2M & IoT	₿ marks
9.3	Attempt a and b	15 marks / 15 00
Q.3 a	Attempt any one	1130
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	Discuss the XMPP protocol and its architecture	7 marks
	OR	
	II. Write importance of IoT security with respect to any one IoT application.	@marks

End of Paper

M.Sc. Cyber Security Semester – III – January - 2024

Subject Code: CTMSCS SIII P2

CS SIII P2

Subject Name: IoT Security and Forensics

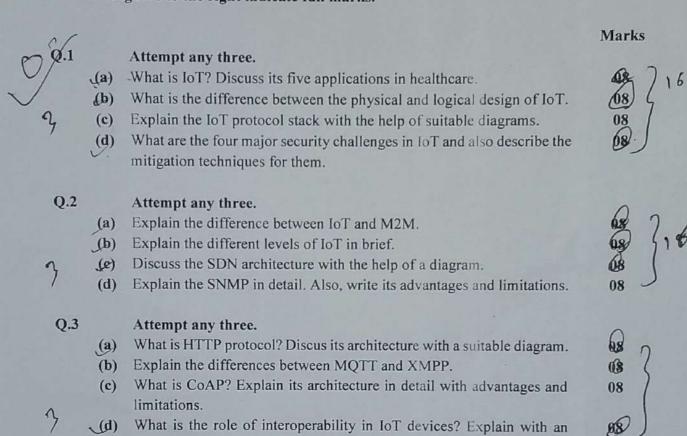
Time: 11:00 AM to 2:00 PM

Date: 02/01/2024

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.



Q.4 Attempt any two.

example.

- (a) Explain the security, privacy, and trust in IoT systems. What are the ways to achieve them?
- What is pen testing? Explain the steps of pen testing in detail.
 - (c) What is threat modeling? What are the benefits of threat modeling?

Q.5 Attempt any two.

- (a) What are OWASP top 10 vulnerabilities? Explain five of them. TUTP
- (b) Discuss the different IoT attack vectors. Also, Explain the different attack surfaces





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



--- End of Paper---



National Forensics Sciences University, Goa Campus TA-1 Examination

Program Name - M.Sc. CS/DFJS 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.	10 marks
Q.1 Multiple Choice Questions (1 mark each)	10 marks
	1 mark
1a) Which of the following provides the least security	I mark
a. IaaS	
b. PaaS	
c. SaaS d. None	
1b) Among the following, which attack can be performed at the	1 mark
application layer?	
a. Rootkit	
b. Buffer overflow	
· c. Trojans	
.d/ TOCTTOU	
1c) While indexing the data content to enhance the search	1 mark
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
a. Lack of access to data	I mark
Storage of data without control over the location of where the	
data is stored	
c. Lack of ability to back up data	
d. None	
1e) Policy ranking is the:	1 mark
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:	Tillaik
a. To protect data To execute the data	
c. To avoid virtualization threat	
d. None	
1g) The risk associated with Infrastructure as a Service can be	1 mark
minimised by using:	
a. PALM	
b. HyperSafe	
c. Closed box execution environment	MERITA STATE
Access control	
1h) CSP need not to decrypt the data while performing the search	h 1 mark
operation by using:	

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



	e – M. Sc. Cyber Security / DFIS Sem – III Dat me- Cloud Security & Forensic Subject Code- CTMSCS S3-P3	te- 31.10.23
ime- 1.5 l	Hours Max.	Marks- 50
nstruction	ns - 1) Answer all questions. 2) Assume suitable data.	1
2.1	Solve any four	20 marks 20 112
	a. What is Object-based storage in cloud computing?	narks
P. A. S. L.	b, How does a Kernel-based virtual machine work? Explain.	& marks
	c. Write a note on containerization.	(8 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.	Symarks /
Q.2	Attempt all	15 marks /\ 0 ¬(5
	a. How block-based storage is different from file-based storage.	(3/marks
	b. What is a SOC-2 certification?	5 marks
	What is Para virtualization? List out at least three hypervisors based on it.	& marks
Q. 3	Attempt a and b	15 marks / 15 → C12,
Q.3 a	Attempt any one	
Q.3 a	I. Differentiate between KVM, VMware ESXI, Hyper V, and Xen hypervisor.	& 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	What is scaling? How horizontal scaling is different from vertical scaling.	Q marks
	OR	
	II. What is a Docker? How containers are different from images, explain with a suitable example.	7 marks

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

Subject Code: CTMSCS SIII P3

Subject Name: Cloud Security and Forensics

Time: 11 AM TO 2 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.



Attempt any three.

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



Attempt any three.

Explain the importance of Logs in the cloud computing? Which are the different sources of Logs in Cloud Computing Environment?

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?

Explain the process in which Google App Engine architecture works

(d) Answer the following for RSA cryptosystem:

Briefly explain the idea behind the RSA cryptosystem

b. What is the one-way function in this system?

What is the trapdoor in this system?

d/ Define the public and private keys in this system

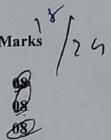
e./Describe the security of this system



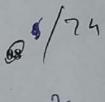
(a)

Attempt any three.

What is Cloud Accountability? Discuss possible solutions to achieve accountability in the cloud



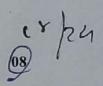


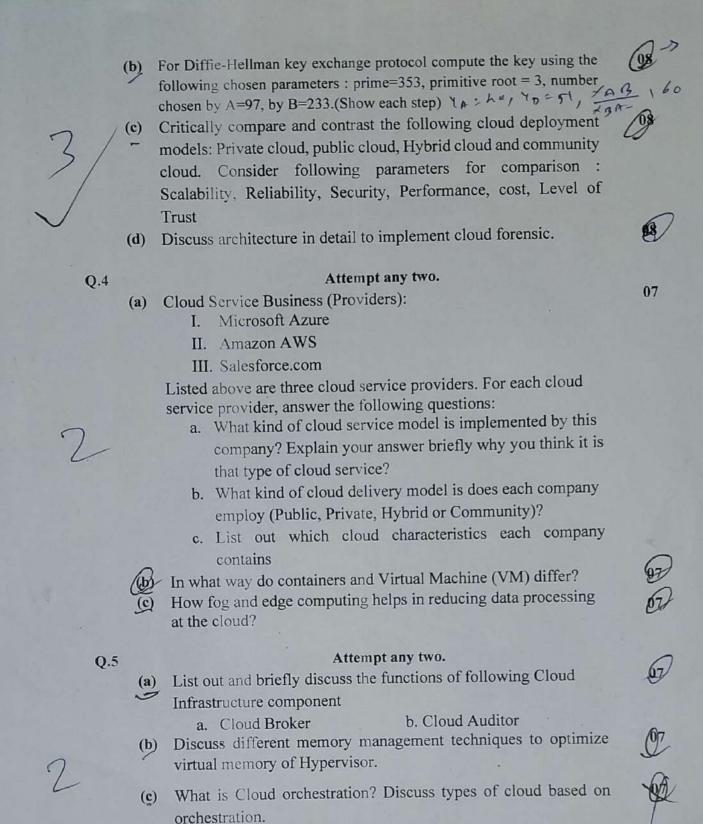












END OF PAPER



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.

	Multiple Choice Questions (1 mark each)	10 marks
		1 mark
	i. DCS stands for:	Tillaik
	a. Distributed central system	
	b. Design control system	
1	c. Distributed control systems	
	d. None	
	ii. RTU is a:	1 mark
	a. Master control unit.	
	b. Human machine interface	
//		
()	ç, None	
	jii. One of PLC functionalities is:	1 mark
	, , , , , , , , , , , , , , , , , , ,	
	a. managing the sensors and actuatorsb. displays the data to the user	
	c. None	
	C. None	
	iv. Data historian in SCADA:	1 mark
	a. is a human being.	
	(b) is a software.	
	c, Both	
	d. None	4 mode
	v. The risks involved in OT systems is/are:	1 mark
	a. Human Safety.	
	b. Environmental Safety.	
	c. Material damage	
	d. all	1 mark
	/vi. Sensors are the part of which level of PURDUE model:	Tillaik
	a. Level 0	
	b. Level 1	2
	c. Level 2	
	d. None	1 mark
	vii. Data historian is a part of which level of PURDUE model?	Z man
	a. Level 0	
	b. Level 1	

	c. Level 2 Q 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
	Explain ICS and OT?	5 marks
	ii. What are the different applications of OT. Explain any two of them.	5 marks
~	Explain SCADA architecture with the help of diagram.	5 marks
	(iv) What is PURDUE model? Explain with the help of diagram.	5 marks



rogramm	e – M.Sc. Cyber Security / M.Sc. DFIS	
iem – 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
nstructio	ns - 1) Answer all questions. 2) Assume suitable data.	
Q.1	Answer any four questions.	20 marks 12
	a. Explain Critical infrastructure Security with example.	⊈ marks
	b. Explain RTU, PLC and IED in the context of SCADA.	& marks
	c. What is ICS-DMZ. Briefly describe its benefits.	5 marks
	d. Discuss about the evolution of SCADA Protocols.	₫ marks
FE PT	e. What are the major threats to the OT Systems?	⅓ marks
Q.2	Attempt all	15 marks
	a. What is PURDUE model? Explain with the help of diagram.	& marks
	b. What is SCADA? Explain its architecture.	3 marks
	_c. What are five best practices for OT security?	
Q. 3	Attempt a and b	15 marks (15)
Q.3 a	Attempt any one	
Q.3 a	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	What is Profibus protocol. Explain its variants.	7 marks
	OR	
	II. Explain Single firewall DMZ and dual firewall DMZ in SCADA in detail.	@marks

End of Paper

M.Sc. Cyber Security Semester – III – January - 2024

Subject Code: CTMSCS SIII P4 EL3

Subject Name: Critical Infrastructure Security

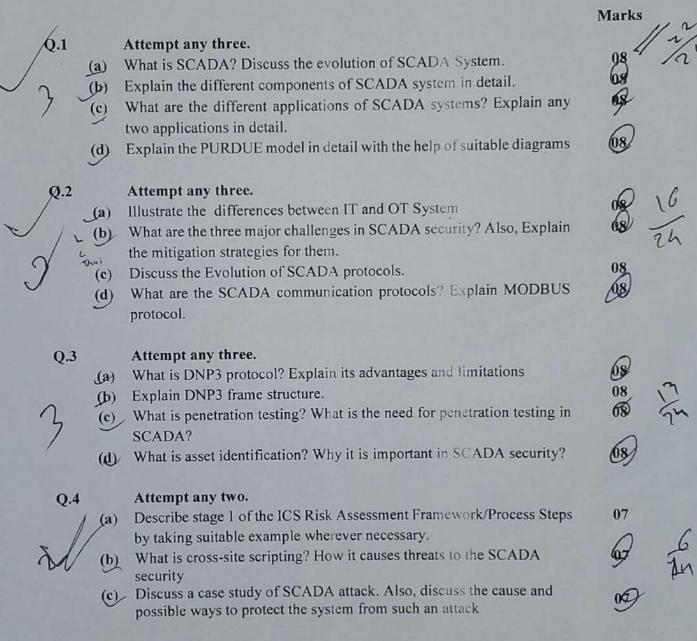
Time: 11:00 AM to 2:00 PM

Date: 04/01/2024

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.





Attempt any two.

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

8

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

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

--- End of Paper---

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

Subject Name: Social Network Analysis

Time: 11:00 AM to 2:00 PM

Date: 05/01/2024

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)	Define Social Media Forensics and explain its significance in digital investigations with appropriate example.	68
3	(b)	Discuss the ethical and legal considerations involved in conducting social media forensics.	08
	(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.	(8)
Q.2		Attempt any three.	
	(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
1	(b)	What is the difference between email tracing and email tracking?	68
>	(b) (c)	Discuss the terms in detail: Geographical Location Intelligence (GEOINT), Social Media Intelligence (SOCMINT), Financial Intelligence (FININT), Multimedia Intelligence (MULINT)	88
	(d)	Explain various platforms of social media and social network.	68
	-		
Q.3	(a)	Attempt any three. Discuss a real-world case where social media forensics played a crucial role in solving a crime or identifying a suspect.	08
	(b)	Write a note with appropriate example on API Integration to enhance the capabilities of Social Media Investigation.	08)
7	(c)	What do you mean by graph theory, explain nodes, edges concept in	(8)
	(d)	- al dete security? Explain various Operational	08
Q.4		Attempt any two.	

				#/
		(a)	Explore and discuss emerging trends in social media forensics and	
31 23	2000	<i>/</i>	OSINT.	6
2/		(b)	Explain emerging trends in social network forensics, considering technological advancements and changes in online communication.	
17	9	(6)	Explain these terms: Google dorks, Cyber Psychology, Fake News	10
// [
	Q.5		Attempt any two.	1
		(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?	© 3
2		(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?	<u> </u>
		E S		

--- End of Paper---

Outeto

9

a In

Su