COEP Tech

T1 - EXAM

Cryptography and Network Security

Program: B.Tech. (Computer Engineering/Information Technology)
Year: 2023-24
Duration: 1 hr.
Semester: VII
Max. Marks: 20

Student MIS No.:

1	1	2	0	0	3	0	1	2

Instructions:

1. **Mobile phones and programmable calculators are strictly prohibited.**
2. **Writing anything on question paper is not allowed.**
3. **Exchange/Sharing of stationery, calculator etc. not allowed.**
4. **Write your MIS Number on Question Paper.**
5. **Make appropriate assumptions wherever necessary.**
6. **Give examples and draw neat diagrams wherever necessary.**

Q.1. A. Fill in the blanks and **Re-write** the complete sentence with correct answer: **(5)**

1. Find the primitive roots of G=<Z11*, x>?
   a) {2, 6, 8}
   b) {2, 5, 8}
   c) {3, 4, 7, 8}
   d) {2, 6, 7, 8}
2. On Encrypting "cryptography" using Vignere Cipher System using the keyword "LUCKY" we get cipher text
   a) nlazeiibljji
   b) nlazrzatknss
   c) olaaeiibljkiij
   d) mlaaeiibljki
3. Calculate the GCD of 102947526 and 239821932 using Euclidean algorithm (show your calculations).
   a) 11 b) 12 c) 8 d) 6

4. If we want to ensure the principle of _____, the contents of a message must not change while in transit.
   a. Confidentiality
   b. Authentication
   c. Integrity
   d. Non–repudiation

5. The statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext the scheme is known as _____.
   a) Confusion
   b) Diffusion
   c) Error Propagation
   d) Avalanche Effect

B. Use Hill cipher and decrypt the following message. **(5)**

Message: "ZSHLFGLKTVDUWAQBCG"

Encryption key: "CDPFIMBNE".

Q.2. A. Solve the simultaneous congruence's **(5)**
$x \equiv 6 \pmod{11}$, $x \equiv 13 \pmod{16}$, $x \equiv 9 \pmod{21}$,
$x \equiv 19 \pmod{25}$ using Chinese Remainder Theorem (CRT).

B. Encrypt the plaintext " She is funny a girl" using Playfair cipher. The key used as 'SWIMMING' **(3)**

C. Solve the following **(2)**
   a) Using Fermat's little theorem find $13^{2010} \bmod 71$
   b) Find the multiplicative inverse of 27 (mod 392)

COEP Technological University

(COEP Tech)

A Unitary Public University of Government of Maharashtra

w.e.f 21st June 2022

(Formerly College of Engineering Pune)

T2 - EXAM

Cryptography and Network Security

Program: B.Tech. (Computer Engineering)

Year: 2023-24 Semester: VII

Duration: 1 hr. Max. Marks: 20

Student MIS No.:

1	1	2	0	0	3	0	1	2

Instructions:

1. **Mobile phones and programmable calculators are strictly prohibited.**
2. **Writing anything on question paper is not allowed.**
3. **Exchange/Sharing of stationery, calculator etc. not allowed.**
4. **Write your MIS Number on Question Paper.**
5. **Make appropriate assumptions wherever necessary.**
6. **Give examples and draw neat diagrams wherever necessary.**

Q.1. A.

1. i) Which cryptanalytic attack is possible against Electronic code book mode? **(2)**

   ii) The key space for DES algorithm is ----------.

2. State the name of mode of operation used in block ciphers where bit error may occur. During the transmission of C4 (the fourth cipher block) using the above mode of operation, an error in the 3rd bit had occurred. How many and which plaintext blocks will be affected, if we are using 16-bit mode for DES? Justify your answer? **(3)**

B.

1. Draw the block diagram for the key generation process for DES algorithm. **(2)**
2. What are weak keys? How many weak keys are there in DES algorithm? List the weak keys in DES. **(3)**

Q.2. A. In asymmetric encryption using RSA, the cipher text is $C = 4$ and the public key is $e = 89$, $p=11$, $q=47$. Find **(5)**

(i) The key for decryption (private key)?

(ii) The plaintext M?

B. Users A and B use the Diffie-Hellman Key exchange technique a common prime q=71 and a positive root α= 7. **(3)**

i. If user A has private key $X_A = 5$, what is A's public key Y_A?

ii. If user B has private key $X_B=12$, what is B's public key Y_B?

iii. What is the shared secret key?

C. Describe Man-in-the-middle attack with suitable example. **(2)**

COLLEGE OF ENGINEERING PUNE

(An Autonomous Institute of Govt. of Maharashtra)

END-SEMESTER EXAMINATION

Cryptography and Network Security

Program: **B.Tech. (Computer Engineering)**
Year: 2023-24
Duration: 3 hr.

Semester: VII
Max. Marks: 60

Student MIS No.:

1	1	2	0	0	3	0	1	2

Instructions:

1. **Mobile phones and programmable calculators are strictly prohibited.**
2. **Writing anything on question paper is not allowed.**
3. **Exchange/Sharing of stationery, calculator etc. not allowed.**
4. **Write your MIS Number on Question Paper.**
5. **Make appropriate assumptions wherever necessary.**
6. **Give examples and draw neat diagrams wherever necessary.**

			COs	POs
Q.1.	**A.**	Answer the following and show your calculations clearly. 1. The multiplicative Inverse of 24140 mod 40902 is 2. Calculate the GCD of 102947526 and 239821932 using Euclidean algorithm. 3. Find the remainder when 3^{100} is divided by 7 using Euler's Theorem. 4. Solve 7^{2001} (modulo 5) using Fermat's Little Theorem 5. Find the last two digits of 91^{246}	**(5)**	**CO-1, CO-3, CO-4, CO-5**	**a, b, h**
	B.	Use Hill cipher technique and decrypt the following message. Message: "ZSHLFGLKTVDUWAQBCG" where Encryption key is: "CDPFIMBNE".	**(5)**		
Q.2.	**A.**	Consider $\Phi(n) = 180$. Find minimum **FIVE** possible numbers for n which should be more than 200.	**(5)**	**CO-1, CO-3,**	**a,b, c,e,**
	B.	Explain the various fields of X.509 Certificates. Why Certificate Hierarchy is required?	**(5)**	**CO-4**	
Q.3.	**A.**	Perform AES mix column transformation for following and show your calculations	**(5)**	**CO-3 CO-4, CO-5**	**c, d, e, h**

$$\text{Rcon} = \begin{matrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{matrix} \qquad \text{State column} = \begin{matrix} 04 \\ 66 \\ 81 \\ E5 \end{matrix}$$

B. For the following questions, assume the use of the field F_{2^3}. The field is described here using polynomial representation with the irreducible polynomial $x^3 + x + 1$. A generator for the field is g = (010), and the powers of g are: (5)

$g^1 = (010)$ $g^2 = (100)$ $g^3 = (011)$ $g^4 = (110)$ $g^5 = (111)$
$g^6 = (101)$ $g^7 = (001) = 1$

1) Does the elliptic curve equation y2 + xy = x3 + g5x2 + g6 define a group over F23?
2) Do the points P(g3, g6) and Q(g5, g2) lie on the elliptic curve y2 + xy = x3 + g2x2 + g6 over F23?
3) What are the negatives of the following elliptic curve points over F23? P(g3,g6) Q(g,0) R(0,g3)
4) In the elliptic curve group defined by y2 + xy = x3 + g2x2 + g6 over F23, what is P + Q if P = (g2, g6) and Q = (g5, g5)?
5) In the elliptic curve group defined by y2 + xy = x3 + g2x2 + g6 over F23, what is 2P if P = (g3, g4)?

OR

B. User A chooses simplified IDEA encryption technique with key 1100 0110 0011 0101 1111 0111 0101 1010. Generate the subkeys for decryption. In Simplified IDEA algorithm if the plaintext is 0000 0100 0000 0101 and the first four sub keys are 0011 0000 0011 0000. What is the output after first four steps of round 1? (Show all the calculations) (5)

Q.4. A. State the purpose of hash functions. What is the size of hash/ message digest and the block for MD5? How many numbers of rounds are there in MD5? If the message of size is 514 bits, how many numbers of bits are required for padding this message? Justify your answer. (5)

B. In Secure Socket Layer (SSL) protocol there are different protocols. One of these protocols Handshake protocol. In this protocol a logical connection is initiated between the client and server. What are the fields of client_hello message? Discuss the content/importance of each field. (5)

Q.5. A. Write the steps for following algorithms for digital signature schemes: (5) CO-1, a, e

i. A key generation algorithm CO-5, f, l
ii. A signing algorithm CO-6
iii. A verification algorithm

B. What is DMZ? What is the importance of DMZ? Where is it located? What are the different devices located in DMZ? Explain packet filtering firewall with its advantages and disadvantages. (5)

Q.6. A. Comment on Man-in-the-middle-Attack. In a Diffie-Hellman Key exchange algorithm, user A want to share key K_{AB} with the user B. The public parameters are q =19, a primitive root α = 3 and A's private key is X_A =10, B's private key is X_B= 11 and two private keys as of user C are X_{CA} = 7 & X_{CB} = 11. Using these parameters demonstrate the Man-in-the-middle-Attack for Diffie-Hellman Key exchange algorithm. (5) CO-2, a, CO-3, b, d,

B. Draw a neat architecture diagram of Kerberos. List down the various steps involved during the authentication of users with respect to Kerberos, use proper conventions for the same. (5)

COLLEGE OF ENGINEERING, PUNE

(An Autonomous Institute of Government of Maharashtra.)

Test-1 Examination

(CT(DE)-22009) **Internet of Things**

Course: B.Tech , Semester VII

Branch: Computer Engineering (Div-1 & Div- 2)

Academic Year: 2023-2024

Max.Marks:20

Duration: 1 Hours

Date: 17/09/2023

Instructions:

Student MIS No. | 1 | 1 | 2 | 0 | 0 | 3 | 0 | 1 | 2 |

1. Figures to the right indicate the full marks.
2. Mobile phones and programmable calculators are strictly prohibited.
3. Writing anything on question paper is not allowed.
4. Exchange/Sharing of stationery, calculator etc. not allowed.
5. Write your MIS Number on Question Paper

Q 1 A] Choose the correct answer from the given options. [5]

a) Which of the following can not be considered an IoT device?
a) Smartwatch b) Andriod Phone c) Laptop d) Tubelight

b) In IoT, does the _____ layer help in end-to-end communication?
a) security b) transport c) data communication d) logical

c) Which of the following is not an application of IoT?
a) Wearables b) Smart Grid c) Arduino d) Smart City

d) What is the full form of the LPWAN?
a) Low Protocol Wide Area Network b) Low Power Wide Area Network
c) Long Protocol Wide Area Network d) Long Power Wide Area Network

e) An IoT network is a collection of _____ devices.
a) Signal b) Machine to Machine c) Interconnected d) Network to Network

f) What is the full form of the MQTT?
a) Multi-Queue Telemetry Things b) Multiple Queue Telemetry Things
c) Message Queue Telemetry Things d) Message Queue Telemetry Transport

g) A _____ IoT system has multiples nodes that perform local analysis.
a)Level 1 b) Level 2 c) Level 3 d) Level 4

h) In M2M more emphasis is on _____
a)Software b) Hardware c) Middleware d) Layered Architecture

i) Which type of wireless network is used to connect devices within a city to create a metropolitan-area network (MAN)?
a) WiMAX b) LTE c) ZigBee d) Bluetooth

j) Which attribute of big data involves an exponential data growth rate?
a) variety b) value c) volume d) velocity

Q 2 A] Illustrate the generic block diagram of an IoT device and explain it briefly. [5]

OR

B] With the help of neat diagrams, explain the M2M system architecture. [5]

Q 3 A] With a neat sketch, explain the Publish–Subscribe communication model of IoT. [5]

Q4 A] Explain the differences between Machines in M2M and Things in IOT? [5]

Test-2 Examination

(CT(DE)-22009) Internet of Things

Course: B.Tech , Semester VII

Branch: Computer Engineering (Div-1 & Div- 2)

Academic Year: 2023-2024

Max.Marks:20

Duration: 1 Hours

Date: 18/10/2023

Instructions:

Student MIS No. 1 1 2 0 0 3 0 1 2

1. Figures to the right indicate the full marks.
2. Mobile phones and programmable calculators are strictly prohibited.
3. Writing anything on question paper is not allowed.
4. Exchange/Sharing of stationery, calculator etc. not allowed.
5. Write your MIS Number on Question Paper

Q 1 A] Choose the correct answer from the given options. [5]

a) The following is one of the ETSI high Level architecture domains
   a) Transport Domain
   b) Application and Network Domain
   c) Services Domain
   d) Security Domain

b) Gateway is a functional unit of which domain of ETSI high Level architecture:
   a) Network & Gateway Domain
   b) Transport & Gateway Domain
   c) Device & Gateway Domain
   d) Application & Gateway Domain

c) M2M Area Network is a functional unit of which domain of ETSI high Level architecture:
   a) Network & Device Domain
   b) Transport & Device Domain
   c) Device & Gateway Domain
   d) Application & Gateway Domain

d) M2M Management functions comes under which domain of ETSI high Level architecture:
   a) Network Domain
   b) Transport Domain
   c) Device Domain
   d) Application Domain

e) Which of the following layer provides the main functional capabilities of sensing, actuation, and embedded identities?
   a) Asset Layer
   b) Communication Layer
   c) Service Support Layer
   d) Resource Layer

f) In _____, data acquired is checked for correctness and meaningfulness within the specific operating context.
   a) Data verification
   b) Data acquisition
   c) Data validation
   d) Data generation

g) _____ is the act of securely establishing the identity of the device to ensure that it can be trusted.
   a) Device Addition
   b) Device authentication
   c) Device activation.
   d) Device deletion.

h) _____ is a process where only devices that present the proper credentials are registered.
a) Authorization. b) Authentication. c) Adjunt. d) Addition.

i) _____ is the process of enrolling a device into the system.
a) Provisioning. b) Authentication. c) Authorization. d) Wireless Standard.

j) The _____ provides the functionalities for interacting with instances of concepts defined in the Domain model.
a) Functional View b) Functional Group c) Function IoT d) Device Group

Q 2 A] Design a neat sketch; discuss the M2M high-level ETSI architecture. [5]

Q 3 A] Describe the functional view of Internet of Things? [5]

Q4 A] Describe the challenges and opportunities of data management in Internet of Things with example. [5]

END Semester Examination

(CT(DE)-22009) Internet of Things

Course: B Tech , Semester VII

Branch: Computer Engineering (Div-1 & Div- 2)

Academic Year: 2023-2024

Max.Marks:60

Duration: 03 Hours

Date: 7/12/23

Instructions:

Student MIS No. 1 1 2 0 0 3 0 1 2

1. Figures to the right indicate the full marks.
2. Mobile phones and programmable calculators are strictly prohibited.
3. Writing anything on question paper is not allowed.
4. Exchange/Sharing of stationery, calculator etc. not allowed.
5. Write your MIS Number on Question Paper

			Mark	CO	PO
Q.1	A]	Describe the physical and logical design of Internet of Things.	[5]	1	1
	B]	Consider a Health issues as the real world use case example and explain the potential and benefits of an IoT oriented approach over M2M. Compare the Main characteristics of M2M and IoT.	[5]	1	3
Q.2	A]	Describe the characteristics and levels of IoT with proper examples.	[5]	1	1,2
	B]	Discuss the design objectives of IoT architecture needed to target a horizontal system of real-world services.	[5]	1	1,2
Q.3	A]	Explain Functional View, Information View, Deployment and Operational View, Other Relevant architectural views of IOT reference architecture.	[5]	2	2,3
	B]	Identify the key characteristics of M2M data. Also, explain the data generation, data acquisition, data validation steps in M2M data management.	[5]	2	2,3
		OR			
	C]	Describe M2M high level architecture with their device, gateway & network domain entities.	[5]	2	2,3
Q.4	A]	Determine the types of data generated by a forest fire detection system? Describe alternative approaches for storing the data. What type of analysis is required for forest fire detection from the data collected?	[5]	2	2,4
	B]	What is Data Analytics? Explain the different phases of Analytics.	[5]	3	3,4
		OR			
	C]	List various M2M/IoT device types, their characteristics and the deployment scenarios.	[5]	3	3,4

Q.5	A]	Why security required in IoT? Explain in detail various security model in Internet of things.	[5]	3	3,4
	B]	Describe the following steps involved in IoT system design methodology: (i) Purpose & Requirements Specification (ii) Process Specification	[5]	3	3,4
Q.6	A]	Explain the flow of information through a context enrichment process in IoT.	[5]	4	4,6
	B]	What are the requirements that IoT application for industrial application should meet?	[5]	4	4,6

COLLEGE OF ENGINEERING PUNE
(An Autonomous Institute of Government of Maharashtra)

END Semester Examination

Programme: B.Tech | Semester: VII

Course Code: CT (DE)-22003 | Course Name: Information Retrieval

Branch: Computer Engineering | Academic Year: 2023-24

Duration: 3 hours | Max Marks: 60

Student PRN No. | 1 | 1 | 2 | 0 | 0 | 3 | 0 | 1 | 2 |

Instructions:

1. Figures to the right indicate the full marks.
2. Mobile phones and programmable calculators are strictly prohibited.
3. Writing anything on question paper is not allowed.
4. Exchange/Sharing of stationery, calculator etc. not allowed.
5. Write your PRN Number on Question Paper.
6. Use log to base 10 for all calculations in paper.

			Marks	CO	PO
Q1	A	Differentiate between Information Retrieval System and Data Retrieval System (atleast 3 points).	3	1	1
	B	Draw a neat diagram to show taxonomy of IR model.	3		
Q2	A	Consider the corpus given below (remove punctuations and consider both lower case and uppercase words as same): Doc1: Sachin Ramesh Tendulkar, is an Indian former international cricketer who captained the Indian national team. He is widely regarded as one of the greatest batsmen in the history of cricket. Doc2: Sourav Chandra Ganguly, also known as Dada, is an Indian cricket commentator and former cricketer who captained the Indian national cricket team and known as one of the most successful cricket captains. Doc3: Rahul Sharad Dravid is an Indian cricket coach and former captain of the Indian national team, currently serving as its head coach.	4	2	1, 3
	a	Create positional index for word: Indian, former, cricket			
	b	Write proximity query to retrieve documents where words Indian and cricket are occurring at distance of 3 from each other.			
	c	Evaluate the corpus for inverse document frequency of word 'commentator'.			
	B	Consider the Document: car insurance auto insurance and query: best car insurance. Apply SMART notation lnc.ltc scheme to score the document for the given query. Document frequency for words auto, best, car and insurance are 5000, 50000, 10000 and 1000 respectively.	3		
	C	Words present in corpus are: abundance, cargo, diamond, filibuster, fishmonger, fishmonster, presume, pregame, secure, train.	6		
	a	What key would one lookup if using permuterm index to search the documents containing the words matching the wild card query 'fi*mo*er'.			
	b	Identify the words listed after execution of the key answered in (a) on the permuterm index of the above corpus.			
	c	List the issue in the result obtained in (b).			
	d	Provide solution for the issue listed in (c).			
	e	For the given wild card query 'fi*mo*er' give equivalent Boolean query which can be used over bi-gram index for retrieving required result.			

PTO

f Compare and comment on the result obtained in (a) and (e). 2 3 1, 2

Q3 A Recommend a query processing strategy for:
a (tangerine OR trees) AND (marmalade OR skies) AND (kaleidoscope OR eyes) with respect to the following postings list sizes:

Term	Postings list size
eyes	213312
kaleidoscope	87009
marmalade	107913
skies	271658
tangerine	46653
trees	316812

B Summarize Soundex algorithm and their use in IR system. Derive soundex code for the word 'Wilkins' and 'Walakynowski' and comment on its result. 6 7 4 1, 2

Q4 A Consider the corpus with 1000 documents. Only 3 documents Doc1, Doc2 and Doc3 are relevant to the query 'modern information retrieval' and their length is 26, 39 and 32 respectively. Average length of document in corpus is 75, while other statistics for corpus and relevant documents is given below:

Term	Document Frequency	Term Frequency		
		Doc1	Doc2	Doc3
Modern	15	3	4	5
Information	90	2	2	4
Retrieval	60	1	1	3

a Apply BM25 model to obtain RSV score for each document. (Do not consider query weight, use k=1.2 and b=0.75)
b Rank given 3 documents using score obtained in (a)

B Corpus contains 1000120 documents in all. When a query is thrown to system, out of 80 relevant documents for the given query only $1/4^{th}$ of relevant documents in the system are retrieved. Retrieved but not relevant documents are twice that of relevant retrieved documents. Evaluate the corpus for given statistics and answer the following: 4

a Provide matrix:

	Relevant	Non-relevant	Total
Retrieved			
Not retrieved			
Total			

b Precision
c Recall
d F1-score

C Answer the following:
a Suppose the vocabulary for inverted index consists of the following terms: presumed, pregames, prename, preflame. Design the dictionary data structure for this index which will be able to store the actual terms using dictionary as a string storage with front coding, show the resulting storage of the above vocabulary. 6 2 1, 3
b What is Gamma code and its use? Give gamma code if number 24 is to be coded.

D Design the suffix tree for the string 'abaaba'. Find the longest repeated substring using the drawn suffix tree. Also explain node depth and label depth for the node where longest repeated substring is consumed in the drawn suffix tree. Also give suffix array for the given string. 6
NOTE: label drawn suffix tree properly

Q5 A Give True or False. Correct the statement if it is false. 4 5 1, 2

a A Markov chain is ergodic if it is irreducible and aperiodic.
b A good hub page is one that points to many authorities.
c A good authority page is one that is pointed to by many hub pages.
d Pagerank of everypage is at least α/N, where the number of pages in N and teleporting probability is α.

B A user of a browser can: 2
(i) click a hyperlink on the page 'x' he is currently browsing
(ii) use the back button to go back to the page from which he arrived at 'x'.
Can such a user of back buttons be modelled as a Markov chain

C Explain use of relevance feedback in IR system? List different types of relevance feedback techniques and also rank them according to their decreasing reliability. 4

END Semester Examination

Programme: B. Tech./B. Plan

Course Code: IOC-22008

Semester: VII

Branch:

Course Name: Principles of Marketing for Engineers

Duration: 3 hrs

Academic Year: 2023-24

Student PRN No.

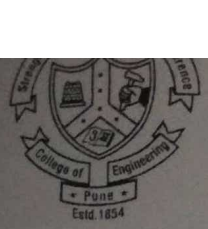
Max Marks: 60

1	1	2	0	0	3	0	1	2

1. Figures to the right indicate the full marks.
2. Mobile phones and programmable calculators are strictly prohibited.
3. Writing anything on question paper is not allowed.
4. Exchange/Sharing of stationery, calculator etc. not allowed.
5. Write your PRN Number on Question Paper.
6. All questions are compulsory.

Q 1			Marks	CO	PO
	a	Identify a product (online/offline/hybrid) that could be **launched in INDIA**. The selection of the product shall be done on the basis of: 1. Market Potential 2. Market Acceptance 3. Market size 4. Gap Analysis 5. Competitive Benchmarking	5	CO3	
	b	**In context with selected product in above question**, Prepare the strategy/plan to disrupt the market based on the 1. Customer value (value proposition statement) 2. STP 3. Market Research as per your knowledge 4. Marketing mix elements 5. Go-to market strategy. 6. Any other relevant framework(s)	10	CO3	
Q2		Give recommendations to the Apple CEO whether the **expansion shall be made or not** in the Indian Market by taking into consideration the following marketing concepts. 1. Competitive landscape 2. New Product Development 3. Positioning map 4. Buyer Behaviour & Psychology of selling 5. Branding decision 6. Integrating Marketing Communication 7. Global marketing: opportunities and challenges	7.5	CO4	

Q3		What is marketing? Why marketing is important along with functions of marketing?	7.5	CO1	
Q4		Explain Concepts & Approach in marketing along with difference between Selling Vs Marketing?	10	CO1	
Q5		What are 4P's, 4C's & 4A's of Marketing? Explain using example of McDonald's.	10	CO4	
Q 6	a	What is Consumer's Buying behaviour? What are factors & Steps Involved?	5	CO2	
	b	What are types of buying behaviour with various conditions in decision of Buying? Explain examples?	5	CO2	



ENGINEERING, PUNE
(An Autonomous Institute of Govt. of Maharashtra)

Test T1 Examination

Malware Analysis

Programme : B. Tech.	**Branch: Computer Engineering**
Duration: 1 Hr	**Course Name: Malware Analysis**
Max Marks: 20	**Academic Year: 2023-24**

Instructions:

1. *Figures to the right indicate the full marks.*
2. *Mobile phones and programmable calculators are strictly prohibited.*
3. *Writing anything on question paper is not allowed.*
4. *Exchange/Sharing of stationery, calculator etc. not allowed.*
5. *Write your MIS Number on Question Paper*

Marks

Q.1. What do you understand by "Threat", "Vulnerability" and "Risk"? Explain with an example. **[04]**

Q.2. Compare and contrast between following types of security attacks with examples **[04]**

a. Active attacks
b. Passive attacks

Q. 3. In reference to the Information Security, explain the following with examples. **[04]**

a. NVD
b. CVE
c. CVSS
d. CPE

Q. 4. What is a compiler and a linker? What are their functions and what are their inputs and outputs? **[04]**

Q. 5. What is a symbol table and how is it used by linker to resolve symbols? **[04]**

Test T2 Examination

Malware Analysis

Programme : B. Tech.	**Branch: Computer Engineering**
Duration: 1 Hr	**Course Name: Malware Analysis**
Max Marks: 20	**Academic Year: 2023-24**

Instructions:

1. *Figures to the right indicate the full marks.*
2. *Mobile phones and programmable calculators are strictly prohibited.*
3. *Writing anything on question paper is not allowed.*
4. *Exchange/Sharing of stationery, calculator etc. not allowed.*
5. *Write your MIS Number on Question Paper*

Marks

Q. 1. Describe the structure of a Portable Executable (PE) file? What is the difference between a section and a segment? **[05]**

Q. 2. Define is a Codecave? Explain following attributes of a codecave. **[05]**

i) Location
ii) Entry and Exit
iii) Stack and register modification

Q. 3. Explain the meaning of the following addresses with example. **[05]**

i) Translation-time address
ii) Linked address
iii) Load-time address

Q. 4. Illustrate the function of the following elements, their requirements and which subsystem(s) process them. **[05]**

i) Relocation loader
ii) Symbol Table linker
iii) Position Independent Code (PIC)
iv) Global Offset Table (GOT)
v) Procedure Linkage Table (PLT)

COLLEGE OF ENGINEERING, PUNE
(An Autonomous Institute of Govt. of Maharashtra)

End Semester Examination

(CT(HO)-22002) Malware Analysis

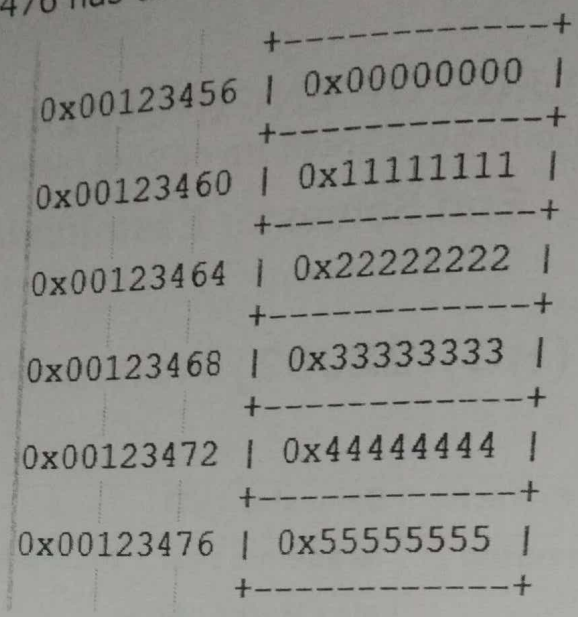
Programme : Final Year B. Tech.	**Semester : VII**
Branch : Computer Engineering	**Academic Year : 2023-24**
Duration : 3 Hrs	**Max Marks : 60**

Instructions:

1. *Figures to the right indicate the full marks.*
2. *Mobile phones and programmable calculators are strictly prohibited.*
3. *Writing anything on question paper is not allowed.*
4. *Exchange/Sharing of stationery, calculator etc. not allowed.*
5. *Write your MIS Number on Question Paper*

			Marks	CO	PO
Q.1	**A)**	What is the difference between big endian and little endian? Where is big endian used typically? Where is little endian used typically?	**[10]**	**1,3**	**1,4**
	B)	What is a Promiscuous Mode of a network interface? Draw and explain the sequence diagram of packet flow when TCP connection is established (TCP three-way handshake) and when TCP connection is terminated (TCP four-way handshake).			
Q.2	**A)**	What is the difference between the instructions "mov" and "lea"?	**[10]**	**1,2**	**2,3**
	B)	Suppose registers "eax" and "ebx" contain the following data eax = 0x00000000 ebx = 0x00123456 Suppose the memory from address 0x00123456 to			

0x00123476 has the content as shown below.



What will be the data after execution of the following instruction?

mov eax, [ebx+8]

what will be the data after execution of the following instruction?

lea eax, [ebx+8]

Q. 3 **A)** Describe Von Neumann Architecture. What are the major elements of a Von Neumann Architecture? **[10]** **1,3** **4,5**

B) Compare and contrast among the following with example

1. Instruction
2. Mnemonic
3. Opcode

C) Compare and contrast between the assembly language and the machine code.

Q.4 A) What is the difference between EAX, AX, AH and AL registers? **[10]** **2,4**

B) Which register is exploited by the malware authors in buffer overflow attack?

C) What is a NOP sled? How is it used by malware authors?

Q.5 A) How do you understand by malware mutation? Why is evolved? **[10]** **1,4** **3,**

B) Explain and contrast three types of mutations.

Q.6 Explain the following malwares. Compare and contrast among them. **[10]** **2,4** **1,4**

1. Boot Sector Infectors
2. File Infectors
3. Data File Infectors (Macro Viruses)
4. Memory Resident Virus
5. Fileless Virus

COLLEGE OF ENGINEERING PUNE

(An Autonomous Institute of Government of Maharashtra.)

END Semester Examination

Programme: B.Tech

Semester: VIII

Course Code: CT(DE)-22032

Course Name: Geographical Information Systems

Branch: Computer Engineering

Academic Year: 2023-24

Duration: 3hr

Max Marks: 60

Student PRN No.

1	1	2	0	0	3	0	1	2

Instructions:

1. **Figures to the right indicate the full marks.**
2. **Mobile phones and programmable calculators are strictly prohibited.**
3. **Writing anything on question paper is not allowed.**
4. **Exchange/Sharing of stationery, calculator etc. not allowed.**
5. **Write your PRN Number on Question Paper.**

			Marks	CO	PO
Q 1	a	How GIS can be used as an effective tool in solving Intelligent Transportation System issues? Explain with help of examples any five issues and how GIS can solve them?	[06]	2	2,6
	b	What is Silver Polygon? Why it is important concept in GIS? Explain your answer with help of two examples.	[06]	3,5	2,3, 4 & 6
Q 2	a	Network analysis is very important component of GIS? Justify your answer with help of three real time applications.	[06]	2 & 6	2,3, 4,6 & 7
	b	What is overlay analysis? Explain the types of overlay analysis in detail with help of two examples for each type.	[06]	2 & 6	2,3, 4,6 & 7
Q 3	a	Reclassification is considered to be an essential and necessary process in GIS applications. Why? Justify your answer with help of three real time applications.	[06]	6	2,3, 4 & 7
	b	You are given the responsibility to head the flood monitoring and detection project. As a GIS expert what all things you will take into consderation from start of the project to its successful implementation. Justify your answer with suitable examples.	[06]	5 & 6	2,3, 4,6 & 7
Q 4	a	Vector data can represent details with high accuracy, still raster data is highly used. Why? Justify your answer with help of atleast two real time examples.	[06]	1,2, & 6	1,2, 3,4 & 7

COLLEGE OF ENGINEERING PUNE

(An Autonomous Institute of Government of Maharashtra.)

	b	Design a geodatabase for Precision Agriculture GIS application. Mention all the necesssary assumptions explicitly.	[06]	2	
Q 5	a	What is Site Suitability Analysis? Explain with help of three real time applications.	[06]	6	
	b	Write short notes on: a. Map Projections b. Coordinate Systems	[06]	2,5 & 6	

Test-1 Examination

CT(HO)- 22004 IOT Security

Course: B.Tech , Sem VIII

Academic Year:2023-2024

Branch: Computer Engineering

Duration: 1 Hour

Max.Marks:20

Date: 17/02/2024

Instructions:

Student MIS No. | 1 | 1 | 2 | 0 | 0 | 3 | 0 | 1 | 2 |

1. Figures to the right indicate the full marks.
2. Mobile phones and programmable calculators are strictly prohibited.
3. Writing anything on question paper is not allowed.
4. Exchange/Sharing of stationery, calculator etc. not allowed.
5. Write your MIS Number on Question Paper

Q. 1 A] Choose the correct answer from the given options. [3]

a) _____ are physical devices or software programs that route inbound or outbound data between controllers, sensors and devices and the cloud or servers and provide an additional layer of security for IoT data while in transit.
a) IoT actuators b) IoT portcullis c) IoT sensors d) IoT gateways

b) What is the difference between IoT authentication and authorization?
a) Authentication is the process of device identification, and authorization provides permissions.
b) Authentication provides an undisputed connection, and authorization is the process of writing identification.
c) Authentication gives permissions to human users, but authorization gives permissions to devices.
d) Authentication is when technology confirms you are not a robot, and authorization is when an OS confirms yours login information.

c) Which IoT security threat is defined as an attack where multiple compromised OSes target a server, website or network to overwhelm a network with traffic, causing it to slow down or crash and deny service to legitimate users or systems?
a) Ransomware b) Distributed denial of service (DDoS) c) Malware d) Man in the middle

d) Each IoT system should undergo a _____during the design stage.
a)service level agreement (SLA) b) privacy impact assessment (PIA)
c) privacy protected information (PPI) d) None of this

e) NERC (North American Electric Reliability Corporation) mandates the _____ standards for the protection of critical electrical generation and distribution systems.
a) Critical Infrastructure Protection (CIP) b) Data Security Standards (DSS)
c) PIN Transaction Services (PTS) d) Federal Information Protection Standards (FIPS)

f) Which of the following do Cyber attackers commonly target for fetching IP address of a target or victim user?
a) ip tracker b) emails c) websites d) web pages

B] What is cyber secûrity? Why is cyber security important?

C] Describe the Internet of things terminology with uses today in different fields.

Q. 2 A] Specify the common IoT attack types with ecosystem of attacks, vulnerabilities, and controls.

OR

B] Describe the types of Cyber Attacks with proper examples.

C] Explain threat modeling an IoT system with example.

Test-2 Examination

CT(HO)- 22004 IOT Security

Course: B.Tech , Sem VIII

Academic Year:2023-2024

Branch: Computer Engineering

Duration: 1 Hour

Max.Marks:20

Date: 18/03/2024

Instructions:

Student MIS No. | 1 | 1 | 2 | 0 | 8 | 3 | 0 | 1 | 2 |

1. Figures to the right indicate the full marks.
2. Mobile phones and programmable calculators are strictly prohibited.
3. Writing anything on question paper is not allowed.
4. Exchange/Sharing of stationery, calculator etc. not allowed.
5. Write your MIS Number on Question Paper

Q. 1 A] Choose the correct answer from the given options. [4]

a) Even with two-factor authentication, users may still be vulnerable to_____attacks.
a) Scripting b) Cross attack c) Man-in-the-middle d) Radiant

b) Example of a good password is
a) name of a partner or spouse b) word related to a job or hobby
c) words contains multiple random digits d) name of a child or pet

c) In asymmetric key cryptography, the private key is kept by
a) Receiver b) sender and receiver c) Sender d) all the connected devices to the network

d) In cryptography, what is cipher?
a) none of the mentioned b) encrypted message
c) both algorithm for performing encryption and decryption and encrypted message
d) algorithm for performing encryption and decryption

e) In dealing with the risk, which response is done by buying insurance
a) Risk acceptance b) Risk mitigation c) Risk transfer d) Risk avoidance

f) Secret words or numbers used for protection of devices is called
a) Biometrics data b) Private words c) Backup d) Passwords

g) What kind of electronic document contains a public key?
a) PIN b) Digital certificate c) PAN d) Biometrics

h) What type of authentication method identifies and recognises people based o physical traits such as finger prints?
a) WEP b) Digital certificates c) Biometrics d) RADIUS

[1]

B] Mention true or false. If false, write the correct statement

a) If the sender and receiver use different keys, the system is referred to as conventional cipher system.

b) An encryption scheme is unconditionally secure if the ciphertext generated does not contain enough information to determine uniquely the corresponding plaintext, no matter how much cipher text is available.

write any 3 .

Q. 2 A] Specify the IoT security lifecycle management processes associated with IoT device implementation, integration, operation, and disposal.

B] Describe the types and uses of cryptographic primitives in the IoT.

C] Explain the key handling topics pertinent to the devices and the systems in cryptographic key management.

D] Describe a holistic identity and access management (IAM) program for the IoT.

END Semester Examination

Programme: B.Tech
Course Code: CT(HO)-22004
Branch: Computer Engineering
Duration: 3 Hours

Semester: VIII
Course Name: IOT Security
Academic Year: 2023-2024
Max Marks: 60

Student PRN No.

1	1	2	0	0	3	0	1	2

Instructions:

1. Figures to the right indicate the full marks.
2. Mobile phones and programmable calculators are strictly prohibited.
3. Writing anything on question paper is not allowed.
4. Exchange/Sharing of stationery, calculator etc. not allowed.
5. Write your PRN Number on Question Paper.

		Marks	CO	PO
Q 1	A) Explain cyber security and IoT security with proper examples.	[5]	1	1,2
	B) Describe the cyber physical systems with architecture and modules.	[5]	1	1,2
	OR			
	C) Describe the 7 layers of cyber security.	[5]	1	1,2
Q 2	A) Specify the common IoT attack types with ecosystem of attacks, vulnerabilities, and controls.	[5]	2	5,8
	B) Explain different categories of IoT devices with different real-time operating system (RTOS) solutions.	[5]	2	5,8
Q 3	A) Describe the threat modeling an IoT system with example.	[5]	2	5,8
	B) Describe the IoT security lifecycle management processes.	[5]	3	6,9
Q 4	A) Explain the key handling topics pertinent to the devices and the systems in cryptographic key management.	[5]	3	6,9
	B) Describe the issues and techniques related to securely engineering IoT systems.	[5]	3	6,9
Q 5	A) Describe the privacy design and engineering activities to the Internet of Things.	[5]	3	12
	B) Write short notes on (Any Two) 1. Security system integration 2. IoT security concept of operations (CONOPS) document 3. Identity and Access Management Solutions for the IoT	[5]	4	10,12
Q 6	A) Explain the types and uses of cryptographic primitives in the IoT	[5]	4	10,12
	B) Describe the future directions of the IoT and cryptography.			

COLLEGE OF ENGINEERING PUNE

(An Autonomous Institute of Government of Maharashtra.)

END Semester Examination

Programme: B.Tech

Course Code: CT(HO)-22004

Branch: Computer Engineering

Duration: 3 Hours

Semester: VIII

Course Name: IOT Security

Academic Year: 2022-2023

Max Marks: 60

Student PRN No.

Instructions:

1. Figures to the right indicate the full marks.
2. Mobile phones and programmable calculators are strictly prohibited.
3. Writing anything on question paper is not allowed.
4. Exchange/Sharing of stationery, calculator etc. not allowed.
5. Write your PRN Number on Question Paper.

			Marks	CO	PO
Q 1	A)	Describe the Internet of things terminology with uses today in different fields.	[4]	1	1,2
	B)	Explain different IoT lifecycle phases.	[4]	1	1,2
	C)	Describe the IoT in the enterprise.	[4]	1	1,2
Q 2	A)	Specify the common IoT attack types with ecosystem of attacks, vulnerabilities, and controls.	[4]	1	3,4
	B)	Describe the attack categories against enterprise IoT components.	[4]	1	3,4
	C)	Explain threat modeling an IoT system with example.	[4]	1	3,4
		OR			
	D)	Explain different categories of IoT devices with different real-time operating system (RTOS) solutions.	[4]	1	3,4
Q 3	A)	Describe the secure IoT system implementation lifecycle.	[4]	1	5,8
	B)	Explain the types and uses of cryptographic primitives in the IoT.	[4]	2	5,8
	C)	Explain the key handling topics pertinent to the devices and the systems in cryptographic key management.	[4]	2	5,8
Q 4	A)	Describe a holistic identity and access management (IAM) program for the IoT.	[4]	3	6,9
	B)	Explain the privacy challenges introduced by the IoT.	[4]	3	6,9
	C)	Specify the privacy engineering activities.	[4]	3	6,9
		OR			
	D)	Describe the privacy design and engineering activities to the Internet of Things.	[4]	3	12

Q 5 A) Explain the IoT threat area with targets/attacks from a cloud perspective. [4] 4

B) Describe the IoT cloud security architecture. [4] 4

C) Write notes on (Any Two) [4] 4

I) Future directions of the IoT and cryptography

II) Cloud services and the IoT

III) Cloud IoT security controls