THAMIRABHARANI ENGINEERING COLLEGE

(Approved by AICTE, New Delhi and Affiliated to Anna University, Chennai)
Chathirampudukulam, Chidambaranagar - Vepemkulam Road
Thatchanallur, Tirunelveli 627 358, Tamil Nadu.

6.5.1 *Internal Quality Assurance Cell (IQAC) has contributed significantly for institutionalizing the quality assurance strategies and processes*

EXAM CELL CIRCULAR

All II and III year students and staff members are informed that **Internal Assessment Test (IAT) – 1** will be conducted on **02, 04, 05, 06, 07 and 08 February 2019**. Two units will be considered for test. Time table and Hall allotment will be displayed on department notice board.

Test Timings   :   **9.05 AM to 10.35 AM**

To be read in all class rooms.

Department	II year	III Year
CIVIL		
CSE		
EEE		
ECE		
MECH		

Department	HOD Signature
CIVIL	
CSE	
EEE	
ECE	
MECH	
S&H	

Exam Coordinator

PRINCIPAL
THAMIRABHARANI ENGINEERING COLLEGE
Chethirampudukulam Village,
Chidambaranagar - Vepemkulam Road,
Thatchanallur, Tirunelveli - 627 358.

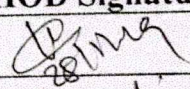Principal

DATE: 28.01.2019
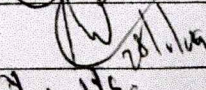
EXAM CELL CIRCULAR

HODs are informed to arrange the following for the conduct of IAT.

- ➤ They are informed to submit format 1, 2 and 3 (attached with this circular) to college exam cell before **10.30 pm 29.01.19.**

- ➤ Requirements like graph sheets, tables, data books, drawing sheets etc.., for the subjects handled by their department staff shall be submitted in written format before **10.30 pm 29.01.19.**

- ➤ They are informed to provide **two separate question paper for every subject** to exam cell before **10.30 pm 29.01.19.**

- ➤ HODs should make sure all their department students are present in their respective halls 5 minutes prior to the commencement of examination.

- ➤ The invigilators have to be present at exam cell to get question paper and answer sheets 10 minutes prior to the commencement of examination; also they have to be present in their allotted halls 5 minutes prior to the commencement of examination.

- ➤ HODs have to make arrangements to receive the written answer sheets from exam cell in the next session of the IAT being conducted.

Department	HOD Signature
CIVIL	
CSE	
EEE	
ECE	
MECH	
S&H	

Exam Coordinator

PRINCIPAL
THAMIRABHARANI ENGINEERING COLLEGE
Chathirampudukulam Village,
Chidambaranagar - Vepemkulam Road.
Thatchanallur, Tirunelveli - 627 353.
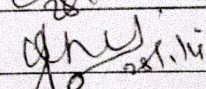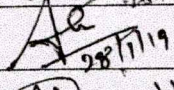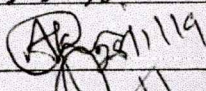
Principal

THAMIRABHARANI ENGINEERING COLLEGE
EXAM CELL
IAT I AUG 2018 – Time table

Department: CIVIL   **Format – I**

Date	Year	Subject Code – Subject Name
16/8/18	II	MA8353 – Transforms and Partial Differential Equations
	III	CE 6701 – Structural Analysis – II ✓
	IV	CE 6701 – Structural Dynamics and Earth quake Engineering
18/8/18	II	CE 8351 – Surveying
	III	CE 6504 – Highway Engineering
	IV	CE 6702 – Prestressed concrete
20/8/18	II	CE 8351 – Construction materials
	III	CE 6703 – Environmental Engineering – II
	IV	CE 6703 – Water Resources and Irrigation Engineering
21/8/18	II	CE 8301 – Strength of Materials – I
	III	CE 6506 – Construction Techniques Equipment and Practice
	IV	CE 6704 – Estimation and quantity Surveying
23/8/18	II	CE 8352 – Engineering Geology
	III	CE 6505 – Design of RC Elements
	IV	CE 6006 – Traffic Engineering and Management
24/8/18	II	CE 8302 – Fluid mechanics
	III	CE 6502 – Foundation Engineering
	IV	EN 6001 – Municipal solid waste management

10/8/18
HOD

THAMIRABHARANI ENGINEERING COLLEGE
EXAM CELL
IAT I AUG 2018 – Time table
Format – 3

Department: CSE

Date	Year	Subject Code – Subject Name
16/8/18	II	MA8351 – Discrete Mathematics
	III	MA6566 – Discrete Mathematics
	IV	CS6701 – Cryptography and Network Security
18/8/18	II	CS8351 – Digital Principles and System Design
	III	CS6503 – Theory of Computation
	IV	CS6702 – Graph Theory and Applications
20/8/18	II	CS8392 – Object Oriented Programming
	III	CS6501 – Internet Programming
	IV	CS6004 – Cyber Forensics
21/8/18	II	CS8391 – Data Structures
	III	CS6504 – Computer Graphics
	IV	CS6703 – Grid and Cloud Computing
23/8/18	II	EC8395 – Communication Engineering
	III	CS6502 – Object Oriented Analysis and Design
	IV	CS6704 – Resource Management Techniques
24/8/18	II	–
	III	–
	IV	IT6005 – Digital Image Processing

PRINCIPAL
THAMIRABHARANI ENGINEERING COLLEGE
Chathirampudukulam Village,
Chidambaranagar - Vepemkulam Road,
Thatchanallur, Tirunelveli - 627 358.

HOD 9/8/18

THAMIRABHARANI ENGINEERING COLLEGE
EXAM CELL
IAT I AUG 2018 – Time table
Format – 3

Department: E.E.E.

Date	Year	Subject Code – Subject Name
16/8/2018	II	MA 8353 - Transforms and Partial Differential Equations (TPDE) ✓
	III	IC 6501 - Control Systems (CS) ✓
	IV	EE 6701 - High Voltage Engineering (HVE) ✓
18/8/2018	II	EC 8353 - Electronic Devices and Circuits (EDC)
	III	ME 6701 - Power Plant Engineering (PPE)
	IV	EE 6008 - Micro Controller Based System Design (MBSD)
20/8/2018	II	ME 8792 Power Plant Engineering (PPE)
	III	EE 6502 - Microprocessors and Microcontrollers (MP & MI)
	IV	EE 6702 - Protection and Switchgear (PSG)
21/8/2018	II	EE 8391 - Electromagnetic Theory (EMT)
	III	EE 6503 - Power Electronics (PE)
	IV	EE 6703 - Special Electrical Machines (SEM)
23/8/2018	II	EE 8301 - Electrical Machines - 1 (EM-1)
	III	EE 6501 - Power System Analysis - (PSA)
	IV	EE 6004 - Flexible Ac Transmission System (FACTS)
24/8/2018	II	EE 8351 - Digital logic circuits (DLC)
	III	EE 6504 - Electrical Machines - II (EM-II)
	IV	MG 6851 - Principles of Management (PoM)

PRINCIPAL
THAMIRABHARANI ENGINEERING COLLEGE
Chathirampudukulam Village,
Chidambaranagar - Vepemkulam Road.
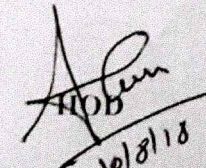Thatchanallur, Tirunelveli - 627 358.
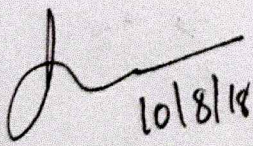
10/8/18

(A. Arun Mutharasu)

THAMIRABHARANI ENGINEERING COLLEGE
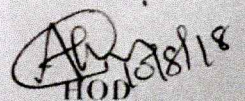## EXAM CELL
IAT I AUG 2018 – Time table
Format – 3

Department:

Date	Year	Subject Code – Subject Name
16.8.18	II	MA8352 Linear Algebra & Partial Differential Equations.
	III	EC6502 Principles of Digital Signal Process
	IV	IT6005 Digital image Processing.
18.8.18	II	Fundamentals of data Structures in C EC8394
	III	EC6501 Digital Communication
	IV	EC6703 Embedded & Realtime Systems.
20.8.18	II	EC8352. Signals & Systems.
	III	GE6351 Environmental Sciences & engineering.
	IV	EC6701 RF&Microwave Engineering.
21.8.18	II	EC8303 Electronic Circuits-II
	III	EC6503 Transmission Lines & Wave Guides.
	IV	EC6702. Optical Communications networks.
23.8.18	II	EC8395 Digital Electronics.
	III	EC6504 Micro Processor & Micro Controller.
	IV	EC6016 OPTo Electronic Devices.
24.8.18	II	EC8393 Control System Engineering.
	III	EC6
	IV	EC6007 Speech Processing.

10/8/18

HOD 8/18

THAMIRABHARANI ENGINEERING COLLEGE
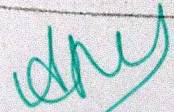
EXAM CELL

IAT I AUG 2018 – Time table

Format – 3

Department: MECHANICAL

Date	Year	Subject Code – Subject Name
16 – 8 – 18	II	EE 8353 – ELECTRICAL DRIVES AND CONTROLS
	III	ME 6505 – DYNAMICS OF MACHINERY
	IV	ME 6701 – POWER PLANT ENGINEERING
18 – 8 – 18	II	MA 8353 – TRANSFORM AND PARTIAL DIFFERENTIAL EQUATION
	III	ME 6501 – COMPUTER AIDED DESIGN
	IV	GE 6757 – TOTAL QUALITY OF MANAGEMENT
20 – 8 – 18	II	CE 8394 – FLUID MECHANICS AND MACHINERY
	III	ME 6502 – HEAT AND MASS TRANSFER
	IV	ME 6702 – MECHATRONICS
21 – 8 – 18	II	ME 8351 – MANUFACTURING TECHNOLOGY – I
	III	ME 6504 – METROLOGY AND MEASUREMENTS
	IV	ME 6703 – COMPUTER INTEGRATED MANUFACTURING SYSTEMS
23 – 8 – 18	II	ME 8391 – ENGINEERING THERMODYNAMICS
	III	GE 6075 – PROFESSIONAL ETHICS ENGINEERING
	IV	ME 6005 – PROCESS PLANNING AND COST ESTIMATION
24 – 8 – 18	II	—
	III	ME 6503 – DESIGN OF MACHINE ELEMENTS
	IV	ME 6012 – MAINTENANCE ENGINEERING

PRINCIPAL
THAMIRABHARANI ENGINEERING COLLEGE
Chathiramputhukulam Vill.
Chidambaranagar . V . . .
Thatchanallur, Tirunelveli

HOD

THAMIRABHARANI ENGINEERING COLLEGE

(Approved by AICTE, New Delhi and Affiliated to Anna University, Chennai)

Chathirampudukulam, Chidambaranagar - Vepemkulam Road

Thatchanallur, Tirunelveli - 627 358.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

INTERNAL ASSESSMENT TEST-I

Date of Exam: 26.08.2019 **Total Marks :** 50 Marks

Subject Code: CS6792 **Subject Name:** CRYPTOGRAPHY AND NETWORK SECURITY

Dept. / Year : CSE / IV year

Prepared By: Mr. R. Raja Sekar, AP/CSE **Approved By:** HOD/CSE

Q. No.	Part A	8x 2=16
1.	Define data integrity.	R, CO1
2.	"Internet security is very challenging"-justify.	U, CO1
3.	What is the need for traffic padding?	R, CO1
4.	List out the active attacks.	R, CO1
5.	What are the types of cryptanalysis?	R, CO1
6.	What are the known attacks in ciphertext?	A, CO1
7.	Differentiate block cipher and stream cipher.	R, CO2
8.	Perform polynomial multiplication $x^4 + 3x^2 + 1$ and $2x^2 + x$ over GF (2).	U, CO2

	Part B	2 x 13=26
9. A	Explain OSI Security Architecture model with neat diagram.	U, CO1
	(OR)	
9. B	What is Monoalphabetic cipher? Examine how it differs from Caesar cipher.	U, CO1
10. A	How counter mode has been stronger than other modes in block cipher?	U, CO2
	(OR)	
10. B	How the strength of DES algorithm has been determined?	U, CO2

	Part C	1 x 8=8
11	Encrypt the message "this is an exercise" using Caesar cipher with key = 20. Ignore the space between words. Decrypt the message to get the original plaintext.	U, CO1

Mapping between COs and Questions:

Question Numbers	COs	Total Marks	% Distribution of marks.
1,2,3,4,5,6,9,11	CO1: To understand the basics of network security with threats and classical encryption techniques.	33	66
7,8,10	CO2: To understand the different cryptographic operations of symmetric cryptographic algorithms.	17	34

PRINCIPAL
THAMIRABHARANI ENGINEERING COLLEGE
Chathirampudukulam Village,
Chidambaranagar - Vepemkulam Road,
Thatchanallur, Tirunelveli - 627 358.

Civil Engineering

No	Name	Designation/Department
1	A Rajesh	Assistant Professor /CIVIL
2	J S Johnson Daniel	Assistant Professor /CIVIL
3	P Shanmugapriya	Assistant Professor /CIVIL
4	L Nithya	Assistant Professor /CIVIL
5	P Senthilkumar	Assistant Professor /CIVIL
6	JP Dhanalakshmi	Assistant Professor /CIVIL
7	P Ramu	Assistant Professor /CIVIL
8	P SivaRaja	Assistant Professor /CIVIL
9	V Tamilarasi	Assistant Professor /CIVIL

Computer Science and Engineering

No	Name	Designation/Department
10	Selva Chithra P	Assistant Professor /CSE
11	Twinkle Gnojini	Assistant Professor /CSE
12	Solai Raja V	Assistant Professor /CSE
13	Jeeva R	Assistant Professor /CSE
14	Raja Sekar R	Assistant Professor /CSE
15	Kamarun Nisha H	Assistant Professor /CSE

THAMIRABHARANI ENGINEERING COLLEGE
Chettikulam
Chidambaranagar
Tirichendur

THAMIRABHARANI ENGINEERING COLLEGGE
EXAM CELL
ANNA UNIVERSITY INTERNAL EXAMINATION - I/FEB 2018
INTERNAL INVIGILATOR ALLOCATION LIST

No	Name	Designation/Department	Duties	Hall	09.02.2018 Hall	12.02.2018 Hall	13.02.2018 Hall	14.07.2018 Hall	15.02.2018 Hall	17.02.2018 Hall
		Civil Engineering								
1	A.Rajesh	Assistant Professor /CIVIL	1							
2	J S Jebastin Daniel	Assistant Professor /CIVIL	2		Duty				Duty	Duty
3	P Shanmugapriyan	Assistant Professor /CIVIL	2					Duty	Duty	
4	L Nithya	Assistant Professor /CIVIL	2		Duty		Duty			
5	P Senthilkumar	Assistant Professor /CIVIL	2				Duty		Duty	Duty
6	P Dhanalakshmi	Assistant Professor /CIVIL	1		Duty					
7	P Ramar	Assistant Professor /CIVIL	2			Duty			Duty	
8	P Sindhuja	Assistant Professor /CIVIL	2					Duty		
9	V Tamilarasi	Assistant Professor /CIVIL	1							
		Computer Science and Engineering								
10	Selva Chithra P	Assistant Professor /CSE	1						Duty	Duty
11	Twinkle Geojini	Assistant Professor /CSE	2		Duty		Duty			
12	Solai Raja V	Assistant Professor /CSE	1		Duty			Duty		
13	Jeeva R	Assistant Professor /CSE	2		Duty	Duty				
14	Raja Sekar R	Assistant Professor /CSE	2		Duty	Duty		Duty	Duty	
15	Kamarun Nisha H	Assistant Professor /CSE	2			Duty		Duty		

PRINCIPAL
THAMIRABHARANI ENGINEERING COLLEGGE
Chathiramputhukulam Village
Chidambaranagar, Vepamkulam Road
Thatchanallur, Tirunelveli - 627 353

Electrical and Electronics Engineering

No	Name	Designation/Department	Duties	09.02.2018 Hall	12.02.2018 Hall	13.02.2018 Hall	14.02.2018 Hall	15.02.2018 Hall	17.02.2018 Hall	Signature
16	S Sudararajan	Assistant Professor /EEE	1			Duty				
17	S Anusha	Assistant Professor /EEE	1	Duty						
18	H Ragupathi	Assistant Professor /EEE	1						Duty	
19	Selva Prasath M	Assistant Professor /EEE	2	Duty	Duty					
20	T Ravi	Assistant Professor /EEE	2			Duty	Duty		Duty	
21	E Subramanian	Assistant Professor /EEE	1							
23	P Siva shanmuga sudar	Assistant Professor /EEE	2	Duty			Duty			
24	Kali Ponraj N	Assistant Professor /EEE	2		Duty				Duty	

Electronics and Communication Engineering

No	Name	Designation/Department	Duties	09.02.2018 Hall	12.02.2018 Hall	13.02.2018 Hall	14.02.2018 Hall	15.02.2018 Hall	17.02.2018 Hall	Signature
25	Saravana Selvi	Assistant Professor /ECE	1						Duty	
26	Girija .S	Assistant Professor /ECE	2			Duty			Duty	
27	Niyas Ahamed A	Assistant Professor /ECE	1			Duty				
29	Sam Kingsly	Assistant Professor /ECE	2		Duty		Duty			
30	V Arunachalam	Assistant Professor /ECE	2		Duty		Duty			
31	Wisey Gifta	Assistant Professor /ECE	1		Duty					

PRINCIPAL
THAMIRABHARANI ENGINEERING COLLEGE
Chathiampudukulam Village,
Chidambaranagar - Vepankulam Post,
Thatchanallur, Tirunelveli - 627 358.

THAMIRABHARANI ENGINEERING COLLEGE

THATCHANALLUR - 627 358.

DEPARTMENT OF ELECTRICAL AND ELECTRONICS ENGINEERING

INTERNAL ASSESSMENT TEST - III

SEATING ARRANGEMENT

HALL NO. - EE107

Sl. No.	Column 1		Column 2		Column 3	
1	953118105001	953119105304	953118105013	953120105023	953119105501	953120105301
2	953118105005	953119105305	953118105302	953120105026		953120105302
3	953118105011	953119105306	953118105304	953120105030		953120105303

L.B. Manif 20/1/2021
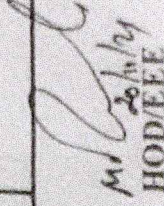ASSESSMENT COORDINATOR

HOD/EEE

PRINCIPAL
THAMIRABHARANI ENGINEERING COLLEGE
Chathirampudukulam Village,
Chidambaranagar - Vepemkulam Road,
Thatchanallur, Tirunelveli - 627 358.

THAMIRABHARANI ENGINEERING COLLEGE

THATCHANALLUR - 627 358.

DEPARTMENT OF ELECTRICAL AND ELECTRONICS ENGINEERING

INTERNAL ASSESSMENT TEST - III

SEATING ARRANGEMENT

HALL NO. - EE016

Sl. No.	Column 1	Column 2		Column 3	
1	95311810516	953119105002	953120105003	953119105012	953120105008
2	95311810518	953119105003	953120105004	953119105017	953120105012
3	95311810519	953119105006	953120105006	953119105302	953120105017

R. g. Hari 30/11/2021
ASSESSMENT COORDINATOR

20/11/21
HOD/EEE

PRINCIPAL
THAMRABHARANI ENGINEERING COLLEGE
Ch-thirampudukulam Village,
Chi nagar - Vepemkulam Road.
Th..... inunelveli - 627 358.

THAMIRABHARANI ENGINEERING COLLEGE
THATCHANALLUR - 627 358.
DEPARTMENT OF ELECTRICAL AND ELECTRONICS ENGINEERING
INTERNAL ASSESSMENT TEST - III
SEATING ARRANGEMENT

S.No	Column 1		Column 2		Column 3		Column 4	
1	953120105001	953119105005	953120105011	953119105013	953120105020	953118105003	953120105027	953118105009
2	953120105002	953119105007	953120105014	953119105015	953120105021	953118105004	953120105028	953118105010
3	953120105005	953119105008	953120105015	953119105016	953120105022	953118105006	953120105031	953118105014
4	953120105007	953119105010	953120105016	953119105018	953120105024	953118105007	953119105001	953118105015
5	953120105009	953119105011	953120105018	953118105002	953120105025	953118105008		

E.g Manif 20/11/2021
ASSESSMENT COORDINATOR

HOD/EEE

THAMIRABHARANI ENGINEERING COLLEGE
EXAMCELL
APPLICATION FOR EXAM GRIEVANCE
Internal Assessment Test – 2

Academic Year	2018-19	Year & Semester	III CSE & v.	Date	26.9.18

Requirement (Write Yes on the required fields):

Revaluation		Retotaling	✓	Question Grievance	

Particulars:
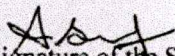
Name	Srinivasa Perumal. A.
Register Number	95311 6104 035
Date of Exam		Degree & Branch	
Subject Code	CS6501	Subject Name	Internet programming
Comments (If any)	

Fill below only for Exam Question Grievance:

Question Number	Grievance
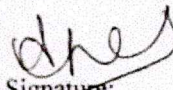
Reference Number (To be filled by Department Exam coordinator)& Remarks (if any):

TEC / CSE / 2018 -19/ ODD/ CSE 002

Signature of the Student   Signature of the Department Exam coordinator

Action Taken:	HOD Remarks
Retotaling done. No Changes in Marks	Verified

HOD Signature:

INSTRUCTION TO CANDIDATES
1. Application for Revaluation/Retotaling must be submitted to the Department Exam Coordinator within 24 hours of the publication of respective subject's result.
2. Application for Exam Question Grievance must be submitted to the Department Exam Coordinator within 1 hour of the completionrespective subject's exam.
3. No application will be accepted beyond the time.

PRINCIPAL
THAMIRABHARANI ENGINEERING COLLEGE
Chathirampudukulam Village,
Chidambaranagar - Vepemkulam Road.
Thatchanallur, Tirunelveli - 627 358.

THAMIRABHARANI ENGINEERING COLLEGE

(Approved by AICTE, New Delhi and Affiliated to Anna University, Chennai)
Chathirampudukulam, Chidambaranagar - Vepemkulam Road
Thatchanallur, Tirunelveli - 627 358.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

INTERNAL ASSESSMENT TEST-I- KEY

Date of Exam: 26.08.2019   **Total Marks :** 50 Marks

Subject Code: CS6792   **Subject Name:** CRYPTOGRAPHY AND NETWORK SECURITY

Dept. / Year : CSE / IV year

Prepared By: Mr. R. Raja Sekar, AP/CSE   **Approved By:** HOD/CSE

Q. No.	Part A	8x 2=16

1. Compare active and passive attack.   U, CO1
   Active and Passive Attacks are security attacks. In Active attack, an attacker tries to modify the content of the messages. Whereas in Passive attack, an attacker observes the messages, copy them and may use them for malicious purposes.

2. Encrypt the plaintext tobeornottobe using the Vigenere cipher for the key value Now.   U, CO1
   Ciphertext: gcxrcnacpgcxr

3. Calculate the ciphertext for the following one time pad.   U, CO1
   Plaintext: ROCK & Key: BOTS
   R = 17 B = 01 17+01 = 18 = S
   O = 14 O = 14 14+14 = 28=26 mod 28=2= C
   C = 02 T = 19 02+19 = 21 = V
   K = 10 S = 18 10+18 = 28=26 mod 28=2 = C

4. Specify the components of encryption algorithm.   R, CO1
   Plaintext - original message
   Ciphertext - coded message
   Cipher - algorithm for transforming plaintext to ciphertext
   Key - info used in cipher known only to sender/receiver
   Enciphering (encryption) - converting plaintext to ciphertext
   Deciphering (decryption) - recovering ciphertext from plaintext

5. Differentiate threat and attack.   U, CO1
   Threat: Possible danger that might exploit a vulnerability.
   Attacks: Deliberate attempt to evade security services and violate the security policy of a system.

6. List the techniques used in steganography.   R, CO1
   Character marking
   Invisible ink
   Pin punctures
   Typewriter correction ribbon

7. Perform polynomial multiplication $x^3 + x + 1$ and $x^2 + x + 1$ over GF (2).   U, CO2
   x^5+x^4+1

8. Find the GCD of (2740, 1760) using Euclid's Algorithm.   U, CO2
   20

Part B		2 x 13=26

9. A   Classify the security attacks and services in detail.   R, CO1

Attacks   **(OR)**

Passive attacks
- Release of message contents
- Traffic analysis

Active attacks
- Masquerade
- Replay
- Modification of messages
- Denial of service

Services
- Authentication
- Access control
- Data confidentiality
- Data integrity
- Non repudiation

9. B Explain the network security model and its important parameters with a neat block diagram.   R, CO1

A message is to be transferred from one party to another across some sort of Internet service. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place.

A logical information channel is established by defining a route through the Internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.

All the techniques for providing security have two components:
- A security-related transformation on the information to be sent.
- Secret information shared by the two parties.

10. A Illustrate the structure of DES and describe the steps in encryption process.   U, CO2
- Encryption   **(OR)**
- Round function
- S-Box

10. B Sketch the scenario for centralized and decentralized key distribution system   U, CO2
- With arbitrary entity
- Without arbitrary entity

<center>**Part C**   **1 x 8=8**</center>

11 Encrypt the following using play fair cipher using the keyword "MONARCHY".   U, CO1
"SWARAJ IS MY BIRTH RIGHT". Use X for blank spaces.

Plaintext =swaraj is my birth right
             =sw ar aj xi sx my xb ir th xr ig ht

Key   =MONARCHY

Ciphertext=qx rm bs as xa nc ai ka pd za ki dp

Plaintext = sw ar ai/j xi/j sx my xb i/jr th xr i/jg ht
             =swarai/j is my birth right
             =swaraj is my birth right

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

Mapping between COs and Questions:

Question Numbers	COs	Total Marks	% Distribution of marks.
1,2,3,4,5,6,9,11	CO1: To understand the basics of network security with threats and classical encryption techniques.	33	66
7,8,10	CO2: To understand the different cryptographic operations of symmetric cryptographic algorithms.	17	34

THAMIRABHARANI ENGINEERING COLLEGE
(Approved by AICTE, New Delhi and Affiliated to Anna University, Chennai)
Chathirampudukulam, Chidambaranagar - Vepemkulam Road
Thatchanallur, Tirunelveli - 627 358.
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
INTERNAL ASSESSMENT TEST-I KEY

Date of Exam: 26.08.2019   **Total Marks :** 50 Marks

Subject Code: CS6792   **Subject Name:** CRYPTOGRAPHY AND NETWORK SECURITY

Dept. / Year : CSE / IV year

Prepared By: Mr. R. Raja Sekar, AP/CSE   **Approved By:** HOD/CSE

Q. No.	Part A	8x 2=16

1. Define data integrity.   R, CO1
   When sensitive information is exchanged, the receiver must have the assurance that the message has come intact from the intended sender and is not modified inadvertently or otherwise.

2. "Internet security is very challenging"-justify.   U, CO1
   Security weaknesses are exist in the operating systems of attached computers as well as vulnerabilities in Internet routers and other network devices. It is vulnerable to attacks like denial of service attacks; IP spoofing, in which intruders create packets with false IP addresses and exploit applications that use authentication based on IP.

3. What is the need for traffic padding?   R, CO1
   Traffic padding may be used to hide the traffic pattern, which means to insert dummy traffic into the network and present to the intruder a different traffic pattern. The apparent traffic pattern, which is observed by intruder, is referred to as a cover mode that hides the real operation mode of the system.

4. List out the active attacks.   R, CO1
   - Masquerade
   - Replay
   - Modification of messages
   - Denial of service

5. What are the types of cryptanalysis?   R, CO1
   - Differential cryptanalysis
   - Linear cryptanalysis

6. What are the known attacks in ciphertext?   A, CO1
   - Ciphertext Only Attacks (COA)
   - Brute Force Attack (BFA)
   - Birthday Attack
   - Man in Middle Attack (MIM)

7. Differentiate block cipher and stream cipher.   R, CO2
   Block cipher converts the plain text into cipher text by taking plain text's block at a time. While stream cipher Converts the plain text into cipher text by taking 1 byte of plain text at a time.

8. Perform polynomial multiplication $x^4 + 3x^2 + 1$ and $2x^2 + x$ over GF (2).   U, CO2
   $x^5+x^4+x^3+x$

<div align="center">

Part B   2 x 13=26

</div>

9. A   Explain OSI Security Architecture model with neat diagram.   U, CO1
- Security Attacks   **(OR)**
- Security Services
- Security Mechanisms

9. B   What is Monoalphabetic cipher? Examine how it differs from Caesar cipher.   U, CO1
The process of mapping from plain alphabet to cipher alphabet using permutation is called Monoalphabetic cipher. A permutation of a finite set of elements S is an ordered sequence of all the elements of S, with each element appearing exactly once.
Example with encryption and decryption.

10. A   How counter mode has been stronger than other modes in block cipher?   U, CO2
- Electronic Codebook (ECB)   **(OR)**
- Cipher Block Chaining (CBC)
- Cipher Feedback (CFB)
- Output Feedback (OFB)
- Counter (CTR)

10. B   How the strength of DES algorithm has been determined?   U, CO2
- The Use of 56-Bit Keys
- The Nature of the DES Algorithm
- A timing attack

<div align="center">

Part C   1 x 8=8

</div>

11   Encrypt the message "this is an exercise" using Caesar cipher with key = 20. Ignore the   U, CO1
space between words. Decrypt the message to get the original plaintext.

$$T - 20 + 20 = 40 - 26 = 14 \; \mathbf{N}$$
$$H - 8 + 20 = 28 - 26 = 2 \; \mathbf{B}$$
$$I - 9 + 20 = 29 - 26 = 3 \; \mathbf{C}$$
$$S - 19 + 20 = 39 - 26 = 13 \; \mathbf{M}$$
$$I - 9 + 20 = 29 - 26 = 03 \; \mathbf{C}$$
$$S - 19 + 20 = 39 - 26 = 13 \; \mathbf{M}$$
$$A - 0 + 20 = 20 \; \mathbf{U}$$
$$N - 14 + 20 = 34 - 26 = 08 \; \mathbf{H}$$
$$E - 5 + 20 = 25 \; \mathbf{Y}$$
$$X - 24 + 20 = 44 - 26 = 18 \; \mathbf{R}$$
$$E - 5 + 20 = 25 \; \mathbf{Y}$$
$$R - 18 + 20 = 38 - 26 = 12 \; \mathbf{L}$$
$$C - 3 + 20 = 23 \; \mathbf{W}$$
$$I - 9 + 20 = 29 - 26 = 03 \; \mathbf{C}$$
$$S - 19 + 20 = 39 - 26 = 13 \; \mathbf{M}$$
$$E - 5 + 20 = 25 \; \mathbf{Y}$$

Therefore the encoded message is **NBCM CM UH YRYLWCMY**

Mapping between COs and Questions:

Question Numbers	COs	Total Marks	% Distribution of marks.
1,2,3,4,5,6,9,11	CO1: To understand the basics of network security with threats and classical encryption techniques.	33	66
7,8,10	CO2: To understand the different cryptographic operations of symmetric cryptographic algorithms.	17	34

PRINCIPAL
THAMIRABHARANI ENGINEERING COLLEGE
Chathirampudukulam
Chidambaranagar - Veper Road,
Thatchanallur, Tirunelveli -

THAMIRABHARANI ENGINEERING COLLEGE

COUNSELLING INFORMATION

(To be filled by the Mentor)

Name of the Student : Karthiga Devi K.

Year / Semester : III / V   Academic Year : 2018-19

Register Number : 95311610401A   Batch : 2016-20

Department : CSE

Date	Particulars	Student's Signature
1/8/18	As the University results are poor, asked to Concentrate on her Studies. Discussed whether she has any personal issues.	k. karthi
1/9/18	Regarding IAT-I, her Performance has been improved but below the average level. Asked to get Question bank from Concern staffs for all subjects.	k. karthi
27/9/18	Suggested her to attend Coaching class and write the questions & answers for practice.	k. karthi

Remarks:

She should attend the slow learner program. Instruct her to practice more, important questions can be given.
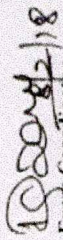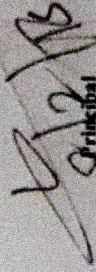
Signature of the Mentor   **Signature of the HoD/ Academic Head**

No	Name	Designation/Department	Duties	09.02.2018 Hall	12.02.2018 Hall	13.02.2018 Hall	14.02.2018 Hall	15.02.2018 Hall	17.02.2018 Hall	Signature
		Mechanical Engineering								
32	V Dhilip Kumar	Assistant Professor / Mechanical	1					Duty		
33	Subash T	Assistant Professor / Mechanical	1						Duty	
34	Saravana Kumar R	Assistant Professor / Mechanical	1			Duty				
35	A Suthan	Assistant Professor / Mechanical	2				Duty	Duty		
36	P Prabakaran	Assistant Professor / Mechanical	2					Duty	Duty	
37	S Ashok raj	Assistant Professor / Mechanical	1			Duty				
38	J Thomas Paul Dhanakaran	Assistant Professor / Mechanical	2		Duty		Duty			
39	P Arumugam	Assistant Professor / Mechanical	2		Duty	Duty				

No	Name	Designation/Department	Duties	09.02.2018 Hall	12.02.2018 Hall	13.02.2018 Hall	14.02.2018 Hall	15.02.2018 Hall	17.02.2018 Hall	Signature
40	John Augustin	Assistant Professor / Maths	1					Duty		
41	Kanagalakshmi	Assistant Professor / Maths	1					Duty		

Exam Coordinator

PRINCIPAL