ವಿಶ್ವೇಶ್ವರಯ್ಯ ತಾಂತ್ರಿಕ ವಿಶ್ವವಿದ್ಯಾಲಯ

(ವಿ ಟಿ ಯು ಅಧಿನಿಯಮ ೧೯೯೪ ರ ಅಡಿಯಲ್ಲಿ, ಕರ್ನಾಟಕ ಸರ್ಕಾರದಿಂದ ಸ್ಥಾಪಿತವಾದ ರಾಜ್ಯ ವಿಶ್ವವಿದ್ಯಾಲಯ)

Visvesvaraya Technological University

(State University of Government of Karnataka Established as per the VTU Act, 1994)
"Jnana Sangama" Belagavi-590018, Karnataka, India

Dr. T.N. Sreenivasa
BE.,ME.,PhD.,FIE,CEng.
Registrar (Evaluation)

Phone : (0831) 2498131
Fax : (0831) 2498184

Ref.No/VTU/Exam/QPDS/CW(2)/2023-2024/ 662

Date: 25 AUG 20

CIRCULAR

Sub: Time Table of UG/PG (2022 Scheme), July/August 2023 Examination.

The time table of the University examination for I/II Semester of B.E. / B.Tech. / MBA/ MCA/ M.Tech. / M.Plan. / M.Arch. (2022 Scheme) courses is published on the VTU Website **https://vtu.ac.in**

The Principals of all the affiliated engineering colleges and constituent engineering college are requested to go through the time table and bring the contents of the same to the notice of all the concerned.

Sd/-
Registrar (Evaluation)

To,
The Principals of all the affiliated engineering colleges and constituent engineering college.

C.W.C. :

1. The Hon'ble Vice Chancellor, through the Secretary to VC, VTU, Belagavi, for kind information.
2. The Registrar, VTU, Belagavi, for kind information.
3. The Regional Directors, R.O. Bengaluru /Belagavi /Kalaburagi /Mysuru, for kind information.
4. The Director, ITISMU, VTU Belagavi, for information and needful.

25.8.23

Registrar (Evaluation)

VISVESVARAYA TECHNOLOGICAL UNIVERSITY

State University of Government of Karnataka Established as per the VTU Act, 1994 "JnanaSangama" Belagavi-590018, Karnataka, India

Prof. B. E. Rangaswamy, Ph.D
REGISTRAR

Phone: (0831) 2498100
Fax: (0831) 2405467

REF: VTU/MYS/VTU-COE/2023-24/ 2692

Date: 26 AUG 2023

Notification

Sub: Fee Structure for Online Degree Programmes for UG, PG and PG Diploma Online Programmes - reg

Ref: Hon'ble Vice Chancellor Approval dated: 24.08.2023

With reference to the subject cited above, the fee structure for Online Degree Programme of VTU is as defined below:

Undergraduate: BBA / BCA				
#	Particulars	I Year	II Year	III Year
01	Registration Fee	450/-	---	---
02	Application Fee	300/-	---	---
03	Convocation Fee	1500/-	---	---
04	Academic fee	22,500/-	22,500/-	22,500/-
05	Exam Fee	1500/-	1500/-	1500/-
06	Marks Card Fee	1000/-	1000/-	1000/-
Total fee Payable (Indian Students)		Rs. 27,250/-	Rs. 25,000/-	Rs. 25,000/-

Postgraduate : MBA / MCA			
#	Particulars	I Year	II Year
01	Registration Fee	450/-	----
02	Application Fee	300/-	----
03	Convocation Fee	1500/-	----
04	Academic fee	57,750/-	57,750/-
05	Exam Fee	1500/-	1500/-
06	Marks Card Fee	750/-	750/-
Total fee Payable (Indian Students)		Rs. 62,250/-	Rs. 60,000/-

Postgraduate Diploma: Management / Computer Applications			
#	Particulars	I Year	II Year
01	Registration Fee	450/-	----
02	Application Fee	300/-	—
03	Convocation Fee	1500/-	----
04	Academic fee	47,750/-	47,750/-
05	Exam Fee	1500/-	1500/-
06	Marks Card Fee	750/-	750/-
Total fee Payable (Indian Students)		Rs. 52,250/-	Rs. 50,000/-

By order

26/08/23

Registrar

To,

1. The principals of all affiliated/constituent/autonomous engineering colleges and school of Architecture of VTU- for kind information and needful.
2. The Chairpersons of all the Departments, Centers for PG Studies in Muddenahalli, Belagavi, Kalaburgi and Mysuru – for kind information and needful.

Copy to:

1. The Secretary to VC, VTU, Belagavi- for kind information.
2. The Director, VTU Centre for Online Education, Mysuru - for information and needful.

ವಿಶ್ವೇಶ್ವರಯ್ಯ ತಾಂತ್ರಿಕ ವಿಶ್ವವಿದ್ಯಾಲಯ

("ವಿ ಟಿ ಯು ಅಧಿನಿಯಮ ೧೯೯೪" ರ ಅಡಿಯಲ್ಲಿ ಕರ್ನಾಟಕ ಸರ್ಕಾರದಿಂದ ಸ್ಥಾಪಿತವಾದ ರಾಜ್ಯ ವಿಶ್ವವಿದ್ಯಾಲಯ)

VISVESVARAYA TECHNOLOGICAL UNIVERSITY

(State University of Government of Karnataka Established as per the VTU Act, 1994)
"JnanaSangama" Belagavi-590018, Karnataka, India

Prof. Dr. B. E. Rangaswamy, Ph.D.
REGISTRAR

Phone: (0831) 2498100
Fax : (0831) 2405467

REF: VTU/BGM/ACA/2023-24/ 2668

DATE: 2 5 AUG 2023

NOTIFICATION

Subject: Tentative Academic Calendar of 1st semesters of B.E./B.Tech./B.Arch./B.Plan., and VII semester of B.E./B.Tech., programs of University regarding...

Reference: Dean faculty of Engineering, VTU Belagavi approval dated 24.08.2023
Hon'ble Vice-Chancellor's approval dated: 24.08.2023

The tentative academic calendar concerned to 1st semesters of B.E./B.Tech./B.Arch./B.Plan., and VII semester of B.E./B.Tech., programs of University for academic year 2023-24 are hereby notified as mentioned below;

	I semester B.E./B.Tech (2022 scheme)	**I semester B.Plan/B.Arch** (2022 scheme)	**VII semester B.E./B.Tech** (2018 scheme)
Commencement of the Semester	04.09.2023	04.09.2023	14.08.2023
# Internship/Students Induction Program	04.09.2023 To 14.09.2023	04.09.2023 To 14.09.2023	14.08.2023 To 09.09.2023
Commencement of Classes	15.09.2023	15.09.2023	11.09.2023
Last Working day of the Semester	06.01.2024	06.01.2024	06.01.2024
Practical Examination	08.01.2024 To 19.01.2024	08.01.2024 To 19.01.2024	08.01.2024 To 19.01.2024
Theory Examinations	22.01.2024 To 17.02.2024	22.01.2024 To 17.02.2024	22.01.2024 To 09.02.2024
Commencement of NEXT Semester	19.02.2024	19.02.2024	13.02.2024

# Internship for VI semester completed students and Students Induction Program for 1st semester Students

Please Note:

- The academic sessions for ODD semesters should commence on the date mentioned above.

** **Induction Program** shall be conducted for 11 days at the beginning of 1st semester and 10 days at the beginning of the 2nd semester. During the induction program, college has to brief about the new curriculum that implemented from the academic year 2022-23.

- If required, the college can plan to have extra classes on 1st and 3rd Saturday and Sundays to complete academic activities within the duration mentioned.
- The faculty/staff shall be available to undertake any work assigned by the university.
- Notification regarding the Calendar of Events relating to the conduct of University **Examinations** will be issued by the Registrar (Evaluation) from time to time.
- Academic Calendar **may be modified** based on guidelines/directions issued in the future by UGC/AICTE/State Government.
- Academic Calendar is also applicable for **Autonomous Colleges.** If any changes are to be effected by Autonomous Colleges in the academic terms and examination schedule, they could do so with the approval of the University.
- The circular related to AICTE Activity point will be issued by the Registrar's office separately.
- If any suggestions/clarification/correction, please email to -sbhvtuso@yahoo.com

The Principals of Affiliated, Constituent and Autonomous Engineering Colleges, Chairpersons of the University departments are hereby informed to bring the academic calendar to the notice of all concerned.

Sd/-

REGISTRAR

To,

1. The Principals of all affiliated/ constituent /Autonomous Engineering Colleges under the ambit of VTU Belagavi.
2. The chairperson, of the Department of Mechanical Engineering /Civil Engineering /Computer Science and Engineering& Communication Electronics Engineering of the University.

Copy to.

1. To the Hon'ble Vice-Chancellor through the secretary to VC, VTU Belagavi for information
2. The Registrar (Evaluation), VTU Belagavi for information.
3. The Regional Directors (I/c) of all the regional offices of VTU for circulation.
4. The Director I/c. ITI SMU, VTU Belagavi for information and to make arrangements to upload Academic Calendar on the VTU web portal.
5. The Director of Physical Education, VTU Belagavi for information
6. The Director, Central Placement Cell, VTU Belagavi for information
7. The Special Officer Library, VTU Belagavi for information
8. OS for information and make arrangements to send the circular regarding AICTE Activity Points
9. All the concerned Special Officer/s and Caseworker/s of the academic section, VTU, Belagavi

25/08/23

REGISTRAR

ವಿಶ್ವೇಶ್ವರಯ್ಯ ತಾಂತ್ರಿಕ ವಿಶ್ವವಿದ್ಯಾಲಯ

("ವಿ ಟಿ ಯು ಅಧಿನಿಯಮ ೧೯೯೪" ರ ಅಡಿಯಲ್ಲಿ ಕರ್ನಾಟಕ ಸರ್ಕಾರದಿಂದ ಸ್ಥಾಪಿತವಾದ ರಾಜ್ಯ ವಿಶ್ವವಿದ್ಯಾಲಯ)

VISVESVARAYA TECHNOLOGICAL UNIVERSITY

(State University of Government of Karnataka Established as per the VTU Act, 1994)
"JnanaSangama" Belagavi-590018, Karnataka, India

Prof. Dr. B. E. Rangaswamy, Ph.D.
REGISTRAR

Phone: (0831) 2498100
Fax : (0831) 2405467

REF: VTU/BGM/ACA/2023-24/ 2668

DATE: 25 AUG 2023

NOTIFICATION

Subject: Tentative Academic Calendar of 1st semesters of B.E./B.Tech./B.Arch./B.Plan., and VII semester of B.E./B.Tech., programs of University regarding...

Reference: Dean faculty of Engineering, VTU Belagavi approval dated 24.08.2023
Hon'ble Vice-Chancellor's approval dated: 24.08.2023

The tentative academic calendar concerned to 1st semesters of B.E./B.Tech./B.Arch./B.Plan., and VII semester of B.E./B.Tech., programs of University for academic year 2023-24 are hereby notified as mentioned below;

	I semester B.E./B.Tech (2022 scheme)	**I semester B.Plan/B.Arch** (2022 scheme)	**VII semester B.E./B.Tech** (2018 scheme)
Commencement of the Semester	04.09.2023	04.09.2023	14.08.2023
# Internship/Students Induction Program	04.09.2023 To 14.09.2023	04.09.2023 To 14.09.2023	14.08.2023 To 09.09.2023
Commencement of Classes	15.09.2023	15.09.2023	11.09.2023
Last Working day of the Semester	06.01.2024	06.01.2024	06.01.2024
Practical Examination	08.01.2024 To 19.01.2024	08.01.2024 To 19.01.2024	08.01.2024 To 19.01.2024
Theory Examinations	22.01.2024 To 17.02.2024	22.01.2024 To 17.02.2024	22.01.2024 To 09.02.2024
Commencement of NEXT Semester	19.02.2024	19.02.2024	13.02.2024

# Internship for VI semester completed students and Students Induction Program for 1st semester Students

Please Note:

- The academic sessions for ODD semesters should commence on the **date mentioned** above.

** **Induction Program** shall be conducted for 11 days at the beginning of 1st semester and 10 days at the beginning of the 2nd semester. During the induction program, college has to brief about the new curriculum that implemented from the academic year 2022-23.

- If required, the college can plan to have extra classes on 1st and 3rd Saturday and Sundays to complete academic activities within the duration mentioned.
- The faculty/staff shall be available to undertake any work assigned by the university.
- Notification regarding the Calendar of Events relating to the conduct of University **Examinations** will be issued by the Registrar (Evaluation) from time to time.
- Academic Calendar **may be modified** based on guidelines/directions issued in the future by UGC/AICTE/State Government.
- Academic Calendar is also applicable for **Autonomous Colleges.** If any changes are to be effected by Autonomous Colleges in the academic terms and examination schedule, they could do so with the approval of the University.
- The circular related to AICTE Activity point will be issued by the Registrar's office separately.
- If any suggestions/clarification/correction, please email to -sbhvtuso@yahoo.com

The Principals of Affiliated, Constituent and Autonomous Engineering Colleges, Chairpersons of the University departments are hereby informed to bring the academic calendar to the notice of all concerned.

Sd/-
REGISTRAR

To,

1. The Principals of all affiliated/ constituent /Autonomous Engineering Colleges under the ambit of VTU Belagavi.
2. The chairperson, of the Department of Mechanical Engineering /Civil Engineering /Computer Science and Engineering& Communication Electronics Engineering of the University.

Copy to.

1. To the Hon'ble Vice-Chancellor through the secretary to VC, VTU Belagavi for information
2. The Registrar (Evaluation), VTU Belagavi for information.
3. The Regional Directors (I/c) of all the regional offices of VTU for circulation.
4. The Director I/c. ITI SMU, VTU Belagavi for information and to make arrangements to upload Academic Calendar on the VTU web portal.
5. The Director of Physical Education, VTU Belagavi for information
6. The Director, Central Placement Cell, VTU Belagavi for information
7. The Special Officer Library, VTU Belagavi for information
8. OS for information and make arrangements to send the circular regarding AICTE Activity Points
9. All the concerned Special Officer/s and Caseworker/s of the academic section, VTU, Belagavi

BE
25/08/23
REGISTRAR

ವಿಶ್ವೇಶ್ವರಯ್ಯ ತಾಂತ್ರಿಕ ವಿಶ್ವವಿದ್ಯಾಲಯ

ವಿ ಟಿ ಯು ಅಧಿನಿಯಮ ೧೯೯೪ ರ ಅಡಿಯಲ್ಲಿ, ಕರ್ನಾಟಕ ಸರ್ಕಾರದಿಂದ ಸ್ಥಾಪಿತವಾದ ರಾಜ್ಯ ವಿಶ್ವವಿದ್ಯಾಲಯ

Visvesvaraya Technological University

(State University of Government of Karnataka Established as per the VTU Act, 1994)
"Jnana Sangama" Belagavi-590018, Karnataka, India

Dr. T.N. Sreenivasa
BE.,ME.,PhD.,FIE,CEng.
Registrar (Evaluation)

Phone : (0831) 2498131
Fax : (0831) 2498184

Ref.No/VTU/Exam/QPDS/CW(2)/2023-2024/ 1463 Date: 27 JAN 2024

CIRCULAR

Sub : Rescheduling of I/II-Semester, BE. / B.Tech. Examinations, Dec. 2023/Jan. 2024 ,

The examinations for I / II Semester, B.E. / B.Tech. [CBCS, 2022 Scheme] are rescheduled. The rescheduled time table is published here with and is available on VTU Website **https://vtu.ac.in**

The contents of this circular may kindly be brought to the notice of all the concerned.

Sd/-
Registrar (Evaluation)

To,
The Principals of all the affiliated engineering colleges and constituent engineering college.

C.W.C. :

1. The Hon'ble Vice Chancellor, through the Secretary to VC, VTU, Belagavi, for kind information.
2. The Registrar, VTU, Belagavi, for kind information.
3. The Regional Directors, R.O. Bengaluru / Belagavi / Kalaburagi /Mysuru, for kind information.
4. The Director, ITISMU, VTU Belagavi, for information and needful.

27.1.24
Registrar (Evaluation)

Visvesvaraya Technological University, Belagavi

Rescheduled - Time Table for I/II - Semester, 2022 Scheme [CBCS]

B.E./B.TECH. Examinations, Dec.2023 / Jan.2024

Sr.No.	Subject Code	Subject Tittle	Date	Time
I	BMATM201	Mathematics-II for ME Stream	30/01/2024	2.00 pm to 5.00 pm
	BMATE201	Mathematics-II for EEE Stream		
	BMATC201	Mathematics-II for Civil Engg stream		
	BMATS201	Mathematics-II for CSE Stream		
II	BMATM101	Mathematics-I for ME Stream	02/02/2024	2.00 pm to 5.00 pm
	BMATE101	Mathematics-I for EEE Stream		
	BMATC101	Mathematics-I for Civil Engg stream		
	BMATS101	Mathematics-I for CSE Stream		
III	BPHYM102/202	Applied Physics for ME Stream	04/02/2024	2.00 pm to 5.00 pm
	BPHYE102/202	Applied Physics for EEE Stream		
	BPHYC102/202	Applied Physics for Civil Engg Stream		
	BPHYS102/202	Applied Physics for CSE Stream		
IV	BCHEM102/202	Applied Chemistry for ME Stream	05/02/2024	2.00 pm to 5.00 pm
	BCHEE102/202	Chemistry for EEE Stream		
	BCHEC102/202	Applied Chemistry for Civil Engg Stream		
	BCHES102/202	Applied Chemistry for CSE Stream		
V	BEMEM103/203	Elements of Mechanical Engineering	06/02/2024	2.00 pm to 5.00 pm
	BEEE103/203	Elements of Electrical Engineering		
	BBEE103/203	Basic Electronics for EEE Stream		
	BCIVC103/203	Engineering Mechanics		
	BPOPS103/203	Principles of Programming Using C		
VI	BESCK204A	Introduction to Civil Engineering	07/02/2024	2.00 pm to 5.00 pm
	BESCK204B	Introduction to Electrical Engineering		
	BESCK204C	Introduction to Electronics & Communication		
	BESCK204D	Introduction to Mechanical Engineering		
	BESCK204E	Introduction to C Programming		
VII	BESCK104A	Introduction to Civil Engineering	08/02/2024	2.00 pm to 5.00 pm
	BESCK104B	Introduction to Electrical Engineering		
	BESCK104C	Introduction to Electronics & Communication		
	BESCK104D	Introduction to Mechanical Engineering		
	BESCK104E	Introduction to C Programming		
VIII	BETCK205A	Smart Materials and Systems	09/02/2024	2.00 pm to 5.00 pm
	BETCK205B	Green Buildings		
	BETCK205C	Introduction to Nano Technology		
	BETCK205D	Introduction to Sustainable Engineering		
	BETCK205E	Renewable Energy Sources		
	BETCK205F	Waste Management		
	BETCK205G	Emerging Applications of Biosensors		
	BETCK205H	Introduction to Internet of Things (IoT)		
	BETCK205I	Introduction to Cyber Security		
	BETCK205J	Introduction to Embedded Systems		

27·1·24

Sr.No.	Subject Code	Subject Tittle	Date	Time
IX	BETCK105A	Smart Materials and Systems	*10/02/2024*	2.00 pm to 5.00 pm
	BETCK105B	Green Buildings		
	BETCK105C	Introduction to Nano Technology		
	BETCK105D	Introduction to Sustainable Engineering		
	BETCK105E	Renewable Energy Sources		
	BETCK105F	Waste Management		
	BETCK105G	Emerging Applications of Biosensors		
	BETCK105H	Introduction to Internet of Things (IoT)		
	BETCK105I	Introduction to Cyber Security		
	BETCK105J	Introduction to Embedded Systems		
X	BPLCK105A	Introduction to Web Programming	*12/02/2024*	2.00 pm to 5.00 pm
	BPLCK105B	Introduction to Python Programming		
	BPLCK105C	Basics of JAVA Programming		
	BPLCK105D	Introduction to C++ Programming		
XI	BPLCK205A	Introduction to Web Programming	*13/02/2024*	2.00 pm to 5.00 pm
	BPLCK205B	Introduction to Python Programming		
	BPLCK205C	Basics of JAVA Programming		
	BPLCK205D	Introduction to C++ Programming		
XII	BENGK106/206	Communicative English	*14/02/2024*	2.00 pm to 3.00 pm
XIII	BPWSK106/206	Professional Writing Skills in English	*15/02/2024*	2.00 pm to 3.00 pm
XIV	BKSKK107/207	Samskrutika Kannada	*16/02/2024*	2.00 pm to 3.00 pm
	BKBKK107/207	Balake Kannada		
XV	BICOK107/207	Indian Constitution	*17/02/2024*	2.00 pm to 3.00 pm
XVI	BIDTK158/258	Innovation and Design Thinking	*19/02/2024*	2.00 pm to 3.00 pm
XVII	BSFHK158/258	Scientific Foundations of Health	*20/02/2024*	2.00 pm to 3.00 pm

27·1·24

Registrar (Evaluation)

ವಿಶ್ವೇಶ್ವರಯ್ಯ ತಾಂತ್ರಿಕ ವಿಶ್ವವಿದ್ಯಾಲಯ

("ವಿ ಟಿ ಯು ಅಧಿನಿಯಮ ೧೯೯೪" ರ ಅಡಿಯಲ್ಲಿ ಕರ್ನಾಟಕ ಸರ್ಕಾರದಿಂದ ಸ್ಥಾಪಿತವಾದ ರಾಜ್ಯ ವಿಶ್ವವಿದ್ಯಾಲಯ)

Visvesvaraya Technological University

(State University of Government of Karnataka Established as per the VTU Act, 1994)

"Jnana Sangama" Belagavi-590018, Karnataka, India.

Dr. T.N. Sreenivasa
BE.,ME., PhD.,FIE,CEng.
Registrar (Evaluation)

Phone : (0831) 2498131
Fax : (0831) 2498184

Ref. No. VTU/BGM/Reg(E)/PS/2023-2024/1482

Date: 30 JAN 2024

CIRCULAR

Sub: Conduct of UG Practical Examinations of Dec.2023/Jan 2024.
Ref: 1. VTU/BGM/Reg.(E)/PS/2023-2024/1198, date 29 NOV 2023.
2. VTU/Exam/QPDS/CW(2)/2023-2024/1447, date 23 JAN 2024.
3. VTU/BOS/AC2023-2024(ODD)/5858, date 24 JAN 2024.

The Principals of Constituent and Affiliated Engineering Colleges are requested to note the following in respect of Conduct of Odd Semester B.Plan VII semester practical examinations of Eligible Students as per below.

- **B.Plan VII sem.**

SCHEDULES

Events	Dates
Uploading Batch lists through web interface and approval of batches by the Principals of respective institutions.	**31.01.2024**
Approval by the Incharge Regional Directors	**01.02.2024**
Allocation of Examiners by the BoE Coordinators	**01.02.2024**
Practical Examinations; VII Sem. B.Plan	**05.02.2024** **To** **10.02.2024**

For other instructions please refer to the circulars under reference above.

For Conduction of Question Paper related practical subjects please refer to the circular under reference no. 2 above.

The contents of this circular must be brought to the notice of all the concerned.

Sd/-
REGISTRAR (EVALUATION)

To,
1. The Principals of Constituent and Affiliated engineering colleges.
2. Chairpersons and Program Coordinators of VTU PG Centers.

Copy FWC's to:
1. Hon'ble Vice-Chancellor through the Sec. to VC, VTU, Belagavi for information.
2. The Registrar, VTU, Belagavi for information.
3. The Incharge Regional Directors of VTU Regional Offices, for information & needful.
4. The I/c Director, ITISMU, VTU, Belagavi for information & needful.

30-1

REGISTRAR (EVALUATION)

ವಿಶ್ವೇಶ್ವರಯ್ಯ ತಾಂತ್ರಿಕ ವಿಶ್ವವಿದ್ಯಾಲಯ

("ವಿ ಟಿ ಯು ಅಧಿನಿಯಮ ೧೯೯೪" ರ ಅಡಿಯಲ್ಲಿ ಕರ್ನಾಟಕ ಸರ್ಕಾರದಿಂದ ಸ್ಥಾಪಿತವಾದ ರಾಜ್ಯ ವಿಶ್ವವಿದ್ಯಾಲಯ)

Visvesvaraya Technological University

(State University of Government of Karnataka Established as per the VTU Act, 1994)

"Jnana Sangama" Belagavi-590018, Karnataka, India.

Dr. T.N. Sreenivasa
BE.,ME., PhD.,FIE,CEng.
Registrar (Evaluation)

Phone : (0831) 2498131
Fax : (0831) 2498184

Ref. No. VTU/BGM/Reg(E)/PS/2023-2024/1482

Date: 30 JAN 2024

CIRCULAR

Sub: Conduct of UG Practical Examinations of Dec.2023/Jan 2024.
Ref: 1. VTU/BGM/Reg.(E)/PS/2023-2024/1198, date 29 NOV 2023.
2. VTU/Exam/QPDS/CW(2)/2023-2024/1447, date 23 JAN 2024.
3. VTU/BOS/AC2023-2024(ODD)/5858, date 24 JAN 2024.

The Principals of Constituent and Affiliated Engineering Colleges are requested to note the following in respect of Conduct of Odd Semester B.Plan VII semester practical examinations of Eligible Students as per below.

- **B.Plan VII sem.**

SCHEDULES

Events	Dates
Uploading Batch lists through web interface and approval of batches by the Principals of respective institutions.	**31.01.2024**
Approval by the Incharge Regional Directors	**01.02.2024**
Allocation of Examiners by the BoE Coordinators	**01.02.2024**
Practical Examinations; VII Sem. B.Plan	**05.02.2024** **To** **10.02.2024**

For other instructions please refer to the circulars under reference above.

For Conduction of Question Paper related practical subjects please refer to the circular under reference no. 2 above.

The contents of this circular must be brought to the notice of all the concerned.

Sd/-
REGISTRAR (EVALUATION)

To,
1. The Principals of Constituent and Affiliated engineering colleges.
2. Chairpersons and Program Coordinators of VTU PG Centers.

Copy FWC's to:
1. Hon'ble Vice-Chancellor through the Sec. to VC, VTU, Belagavi for information.
2. The Registrar, VTU, Belagavi for information.
3. The Incharge Regional Directors of VTU Regional Offices, for information & needful.
4. The I/c Director, ITISMU, VTU, Belagavi for information & needful.

30-1-24

REGISTRAR (EVALUATION)

ವಿಶ್ವೇಶ್ವರಯ್ಯ ತಾಂತ್ರಿಕ ವಿಶ್ವವಿದ್ಯಾಲಯ

[illegible]

Visvesvaraya Technological University

(State University of Government of Karnataka Established as per the VTU Act, 1994)
"Jnana Sangama" Belagavi-590018, Karnataka, India

Prof. B. E. Rangaswamy Ph.D
REGISTRAR

Phone: (0831) 2498100
Fax : (0831) 2405467

VTU/BGM/Aca/Ph.D./2022-23/ 1190

Date: 30 JAN 2024

CIRCULAR

Sub: The Provisional Ph.D. / M. S. (Research) Registration reg...

Ref: 1. VTU/BGM/Aca./Ph.D./2022-23/227 dated 06-06-2023.

2. VTU/BGM/Aca./Ph.D./2022-23/1109 dated 17-01-2024.

The Candidates who submit all necessary documents and attested copies to the allotted Research center, and the Principals of the Colleges under VTU, Chairpersons / Director of University Departments, Principals or Dean (Architecture)/ Heads of the Research centers are to be verified all the necessary documents and Approved candidates are required to pay the following University fees

Registration fee	Rs.7,000/-
University Development fee	Rs.3,000/-
E-consortium fees	Rs.3,000/-
Total	**Rs.13,000/-**

This amount has to be paid to VTU, directly by using online mode through the gateway by using their respective login credentials: https: jnanashodha.vtu.ac.in

The provisional Ph.D./M.S (Research) Registration order copy is available on,https: jnanashodha.vtu.ac.in. The Head of Research center / Research Supervisor / Candidate may download the same using their login credentials and same would be available from 04:00 pm onwards on 01st February 2024.

The candidates, who have not completed the document verification for any reasons, can do so on or before 07-02-2024 with a penal fee of Rs.1000/- payable to University through online mode, failing which no further opportunity will be given for the current ETR.

All other conditions and details remain unchanged as per the notification as referred above.

30/01/24
REGISTRAR
30/1/24.

To,

1. The Principal of all Affiliated, Autonomous, and Constituent Colleges under the ambit of VTU, Belagavi.
2. All Chairpersons of Department VTU Belagavi.
3. The Heads of Recognized Research Centers of VTU
4. The Regional Director (I/c), of VTU's Regional Office at Bengaluru, Belagavi, Kalaburagi, and Mysuru.
5. The Director, R&D, VTU, Belagavi for information.
6. The Director (I/c), ITISMU VTU, Belagavi for information and uploading on a website.

Copy to:

1. The Hon'ble Vice-Chancellor, through the Secretary to VC, VTU, Belagavi
2. The Registrar Officer, VTU, Belagavi for information.
3. The Registrar (Evaluation) Officer, VTU, Belagavi for information
4. The Finance Officer, VTU, Belagavi for information.
5. Office Copy.

ವಿಶ್ವೇಶ್ವರಯ್ಯ ತಾಂತ್ರಿಕ ವಿಶ್ವವಿದ್ಯಾಲಯ

("ವಿ ಟಿ ಯು ಅಧಿನಿಯಮ 1994"ರ ಅಡಿಯಲ್ಲಿ ಕರ್ನಾಟಕ ಸರ್ಕಾರದಿಂದ ಸ್ಥಾಪಿತವಾದ ರಾಜ್ಯ ವಿಶ್ವವಿದ್ಯಾಲಯ)

VISVESVARAYA TECHNOLOGICAL UNIVERSITY

(State University of Government of Karnataka Established as per the VTU Act, 1994)

Phone :0
Fax : 0
Email : re
Web : h

P

Prof. B. E. Rangaswamy, Ph.D
REGISTRAR

REF: VTU/BGM/BoS/598/2024-25/ 1813 DATE: 23 JUL 2024

CIRCULAR

Dear Sir/ Madam

Subject: 2021 scheme **Industry Internship /Research Internship (21INT82)**: Regarding

Reference:

1. Joint Board of Studies recommendation vide proceeding no. 01(g) meetin 21.06.2024
2. Proceeding number 2.2.1 of 178th EC meeting dated 17.07.2024
3. VTU/BGM/Aca/BoS/2023/257, Dated: 10.04.2023
4. Dean Faculty of Engineering approval dated: 22.07.2024
5. Hon'ble Vice-Chancellor's approval Dated: 23.07.2024

This refers to the subject mentioned earlier, based on the recommendation of tl Board of Studies and approval by the EC of VTU, Belagavi, the duration of the Ir Internship/Research Internship (21INT82) under the 2021 scheme has been fixe weeks. The institute has the flexibility to interchange(swap) the internship betw and 8th semesters based on the total number of students, and the availab internships (the colleges shall assist in getting internships to the students). This 1 semester duration will help students to complete their academic requirements o The students have to follow the rules and guidelines for the Ir Internship/Research Internship which is made available https://vtu.ac.in/pdf/regulations2021/anex4.pdf (Annexure-IV Activities Internship).

1. An industry or research internship should be conducted under the superv a faculty mentor or guide (refer to clause 1.3 of Annexure IV: Activities Internship, page 06). The mentor or guide is responsible for assisting stuc securing appropriate industry internships and ensuring that they acqu necessary skills to benefit their future careers.
2. Students undertaking internships must maintain a daily diary (internship as specified in Annexure IV (Activities under Internship).
3. The faculty mentor or guide must adhere to the guidelines provided conduct of CIE and SEE. Additionally, they are responsible for guiding the

"ಜ್ಞಾನ ಸಂಗಮ" ಬೆಳಗಾವಿ – 590 018. ಕರ್ನಾಟಕ "Jnana Sangama" Belagavi - 590 018 |

to ensure the smooth execution of the internship and the preparation of the internship report (daily diary).

4. The mentor/guide/college shall submit all related documents to the University whenever requested.
5. For an industry internship, the intern must adhere to all the safety regulations of the internship provider. Any deviation from these safety norms and the resulting consequences are solely the responsibility of the intern (student).
6. With the consent of the internal guide and Principal of the Institution, students shall be allowed to carry out the internship within or outside the state or abroad, provided favorable facilities are available for the internship and the student remains regularly in contact with the internal guide.
7. University shall not bear any cost involved in carrying out the internship by students. However, students can receive any financial assistance extended by any organization.
8. As in the reference point number 03, students who are unable to secure an internship must take SKILL ENHANCEMENT COURSES, with credits totaling the same as those of the internship. Students are required to enroll in and complete the Skill Enhancement Courses available at (https://online.vtu.ac.in/category/courses/Skill-Enhancement-Course).

All the principals of autonomous/affiliated/constituent engineering colleges are hereby informed to bring the content of the circular to the notice of the Mentor/Guide for internship and the concerned students.

Sd/-
Registrar

To,

1. Principals of all A Engineering Colleges of the University
2. The Chairpersons of the University departments of VTU at Kalaburgi, Mysuru, Bengaluru and Belagavi

Copy to

1. To the Hon'ble Vice-Chancellor through the secretary to VC, VTU Belagavi for information
2. The Registrar (Evaluation), VTU Belagavi for information and needful.
3. The Regional Directors (I/c) of all the regional offices of VTU for circulation.
4. The Director ITI SMU, VTU Belagavi for information and to make arrangements to upload the Academic Calendar on the VTU web portal.
5. The Director, Central Placement Cell, VTU Belagavi for information
6. Office copy

23/07/24
REGISTRAR

ವಿಶ್ವೇಶ್ವರಯ್ಯ ತಾಂತ್ರಿಕ ವಿಶ್ವವಿದ್ಯಾಲಯ

(ವಿ ಟಿ ಯು ಅಧಿನಿಯಮ ೧೯೯೪ ರ ಅಡಿಯಲ್ಲಿ, ಕರ್ನಾಟಕ ಸರ್ಕಾರದಿಂದ ಸ್ಥಾಪಿತವಾದ ರಾಜ್ಯ ವಿಶ್ವವಿದ್ಯಾಲಯ)

Visvesvaraya Technological University

(State University of Government of Karnataka Established as per the VTU Act, 1994)

"Jnana Sangama" Belagavi-590018, Karnataka, India

Dr. T.N. Sreenivasa
BE.,ME.,PhD.,FIE.,CEng
Registrar (Evaluation)

Phone : (0831) 2498131
Fax : (0831) 2498184

Ref.No/VTU/Exam/QPDS/CW(2)/2024-2025/ 587 Date: 25 JUL 2024

CIRCULAR

Sub: Time Table for 2021 Scheme, III/IV Semester, B.E./B.Tech. Examination, June/July 2024.

The Time Table for eligible students of III and IV Semester, B.E. / B.Tech. 2021 Scheme (CBCS), June/July 2024 Examination is published herewith and is also available on the VTU Website **https://vtu.ac.in**.

The Principals of all the constituent and affiliated Engineering Colleges are requested to go through the time table and bring the contents of the same to the notice of all the concerned.

Sd/-
Registrar (Evaluation)

To,
The Principals of all the affiliated Engineering Colleges and constituent Engineering College.

C.W.C. :

1. The Hon'ble Vice Chancellor, through the Secretary to VC, VTU, Belagavi, for kind information.
2. The Registrar, VTU, Belagavi, for kind information.
3. The Regional Directors, R.O. Bengaluru / Belagavi / Kalaburagi / Mysuru, for kind information.
4. The Director, ITISMU, VTU Belagavi, for information and needful.

25.7.24

Registrar (Evaluation)

Visvesvaraya Technological University, Belagavi

Time Table for Eligible Students of B.E./B.TECH, III/IV Semester, 2021 Scheme [CBCS] Examinations, June/July 2024

Date, Day	B.E./B.Tech.	
	III - Semester	IV - Semester
	2.00pm to 5.00pm	2.00pm to 5.00pm
26-08-2024, Monday	--	21MAT41/21MAT*41
28-08-2024, Wednesday	21 * * 31 (includes 21MAT31)	--
29-08-2024, Thursday	--	21 * * 42
30-08-2024, Friday	21 * * 32	--
02-09-2024, Monday	--	21 * * 43
03-09-2024, Tuesday	21 * * 33	--
04-09-2024, Wednesday	--	21 * * 44
05-09-2024, Thursday	21 * * 34	--
06-09-2024, Friday	--	21BE45
09-09-2024, Monday	21KSK37 / 21KBK37 (2.00pm to 3.00pm)	21KSK47 / 21KBK47 (2.00pm to 3.00pm)
10-09-2024, Tuesday	21CIP37 (2.00pm to 3.00pm)	21CIP47 (2.00pm to 3.00pm)
11-09-2024, Wednesday	--	21UH49 (2.00pm to 3.00pm)
12-09-2024, Thursday	21 * * 38 *	--
13-09-2024, Friday	--	21 * * 48 *

25.7.24

Registrar (Evaluation)

ವಿಶ್ವೇಶ್ವರಯ್ಯತಾಂತ್ರಿಕವಿಶ್ವವಿದ್ಯಾಲಯ
ವಿಟಿಯುಅಧಿನಿಯಮ೧೯೯೪ರಅಡಿಯಲ್ಲಿಕರ್ನಾಟಕಸರ್ಕಾರದಿಂದಸ್ಥಾಪಿತವಾದರಾಜ್ಯವಿಶ್ವವಿದ್ಯಾಲಯ
VISVESVARAYA TECHNOLOGICAL UNIVERSITY
State University of Government of Karnataka Established as per the VTU Act, 1994"JnanaSangama" Belagavi-590018,
Karnataka, India

Prof. B. E. Rangaswamy, Ph.D
REGISTRAR

Phone: (0831) 2498100
Fax: (0831) 2405467

REF: VTU/BGM/BoS/Conf/2023-24/ 1966

DATE: 31 JUL 2024

CIRCULAR

Sir/ Madam,

Subject: Clarification of 2021 scheme Industry/Research Internship (21INT82) regarding

Reference: VTU/BGM/BoS/598/2024-25/1813, Dated 23.07.2024

Based on the queries received, the following points are clarified for the (21INT82) Industry/Research Internship:

1. According to the teaching and examination scheme, the Technical Seminar (21SEM81) and Industry/Research Internship (21INT82) are scheduled for the eighth semester, while the Project Work (21PROJ76) and other theory courses (21xx71 to 21xx75X) are in the seventh semester.
2. Industry /Research Internship duration is **15 weeks** as per 178th EC proceedings
3. According to the scheme, the seventh and eighth semesters are **interchangeable** (Swappable). In the ODD semester, 50% of the final-year students can choose to take eighth-semester courses (technical seminar and internship), while the remaining students can take project work along with the theory courses of the seventh-semester. In the EVEN semester, the roles are reversed.
4. This swapping arrangement is designed to ensure that all students have the opportunity to participate in an internship. However, students who do not secure an internship can instead take Skill Enhancement Courses (SEC), which have credits totalling to those of the internship. The SECsare available @ online.vtu.ac.in.
5. Guidelines for Internship are mentioned in Annexure-IV (Activities under Internship) which is made available @ https://vtu.ac.in/pdf/regulations2021/anex4.pdf

Please note that the college must inform the Registrar (Evaluation) about the details of the students who are taking seventh-semester courses, those taking eighth-semester courses, and those opting for Skill Enhancement Courses (SEC) in the upcoming semester. These details must reach the Registrar (Evaluation) office within 10 days of the start of the odd semester.

All principals of affiliated or constituent engineering colleges and chairpersons of university departments are hereby informed to update these details for all concerned faculty and students..

Sd/-
REGISTRAR

To,
All the Principals of Engineering Colleges under the ambit of the University
All the Chairpersons/Program Coordinators of University Departments at Kalburgi, Mysuru, Bengaluru, and Belagavi

Copy to

- The Hon'ble Vice-Chancellor through the secretary to VC for information
- The Registrar (Evaluation) for information and needful
- The Director, ITI,SMU,VTU Belagavi for information and needful also request to upload the circular onthe University website
- The Special Officer QPDS section of VTU Belagavi for information and needful
- Special Officer, COEMysuru for information and upload the circular onthe website online.vtu.ac.in
- Office copy

30/07/24
REGISTRAR

VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI
B.E. in name of the Program
Scheme of Teaching and Examinations 2021
Outcome Based Education(OBE) and Choice Based Credit System (CBCS)
(Effective from the academic year 2021 - 22)

Swappable VII and VIII SEMESTER

VII SEMESTER

Sl. No	Course and Course Code	Course Title	Teaching Department (TD) and Question Paper Setting Board (PSB)	Teaching Hours /Week				Examination				Credits
				Theory Lecture	Tutorial	Practical/ Drawing	Self -Study	Duration in hours	CIE Marks	SEE Marks	Total Marks	
				L	T	P	S					
1	PCC 21XX71	Professional Core Course						3	50	50	100	3
2	PCC 21XX72	Professional Core Course						3	50	50	100	2
3	PEC 21XX73X	Professional elective Course-II						3	50	50	100	3
4	PEC 21XX74X	Professional elective Course-III						3	50	50	100	3
5	OEC 21XX75X	Open elective Course-II	Concerned Department					3	50	50	100	3
6	Project 21XXP76	Project work		Two contact hours /week for interaction between the faculty and students.				3	100	100	200	10
								Total	350	350	700	24

VIII SEMESTER

Sl. No	Course and Course Code		Course Title	Teaching Department	Teaching Hours /Week				Examination				Credits
					Theory Lecture	Tutorial	Practical/ Drawing	Self -Study	Duration in hours	CIE Marks	SEE Marks	Total Marks	
					L	T	P	S					
1	Seminar 21XX81		Technical Seminar		One contact hour /week for interaction between the faculty and students.				--	100	--	100	01
2	INT 21INT82		Research Internship/ Industry Internship		Two contact hours /week for interaction between the faculty and students.				03 (Batch wise)	100	100	200	15
3	NCMC	21NS83	National Service Scheme (NSS)	NSS	Completed during the intervening period of III semester toVIII semester.				--	50	50	100	0
		21PE83	Physical Education (PE) (Sports and Athletics)	PE									
		21YO83	Yoga	Yoga									
									Total	250	150	400	16

Professional Elective - II

21XX731		21XX734	
21XX732		21XX735	
21XX733			

Professional Elective - III

21XX741		21XX744	
21XX742		21XX745	
21XX743			

Open Electives - II offered by the Department to other Department students			
21XX751		21XX754	
21XX752		21XX755	
21XX753			

Note: PCC: Professional Core Course, **PEC:** Professional Elective Courses, **OEC**–Open Elective Course, **AEC** –Ability Enhancement Courses. L –Lecture, T – Tutorial, P- Practical / Drawing, S – Self Study Component, CIE: Continuous Internal Evaluation, SEE: Semester End Examination.

Note: VII and VIII semesters of IV year of the programme

(1) Institutions can swap VII and VIII Semester Scheme of Teaching and Examinations to accommodate research internship/ industry internship after the VI semester.

(2) Credits earned for the courses of VII and VIII Semester Scheme of Teaching and Examinations shall be counted against the corresponding semesters whether VII or VIII semester is completed during the beginning of IV year or later part of IV year of the program.

PROJECT WORK (21XXP75): The objective of the Project work is

(i) To encourage independent learning and the innovative attitude of the students.
(ii) To develop interactive attitude, communication skills, organization, time management, and presentation skills.
(iii) To impart flexibility and adaptability.
(iv) To inspire team working.
(v) To expand intellectual capacity, credibility, judgment and intuition.
(vi) To adhere to punctuality, setting and meeting deadlines.
(vii) To install responsibilities to oneself and others.
(viii) To train students to present the topic of project work in a seminar without any fear, face the audience confidently, enhance communication skills, involve in group discussion to present and exchange ideas.

CIE procedure for Project Work:

(1) Single discipline: The CIE marks shall be awarded by a committee consisting of the Head of the concerned Department and two senior faculty members of the Department, one of whom shall be the Guide.

The CIE marks awarded for the project work, shall be based on the evaluation of the project work Report, project presentation skill, and question and answer session in the ratio 50:25:25. The marks awarded for the project report shall be the same for all the batch mates.

(2) Interdisciplinary: Continuous Internal Evaluation shall be group-wise at the college level with the participation of all guides of the college. Participation of external guide/s, if any, is desirable. The CIE marks awarded for the project work, shall be based on the evaluation of project work Report, project presentation skill, and question and answer session in the ratio 50:25:25. The marks awarded for the project report shall be the same for all the batch mates.

SEE procedure for Project Work: SEE for project work will be conducted by the two examiners appointed by the University. The SEE marks awarded for the project work shall be based on the evaluation of project work Report, project presentation skill, and question and answer session in the ratio 50:25:25.

TECHNICAL SEMINAR (21XXS81): The objective of the seminar is to inculcate self-learning, present the seminar topic confidently, enhance communication skill, involve in group discussion for the exchange of ideas. Each student, under the guidance of a Faculty, shall choose, preferably, a recent topic of his/her interest relevant to the program of Specialization.

(i) Carry out a literature survey, and systematically organize the content. **(ii)** Prepare the report with your own sentences, avoiding a cut and paste act. **(iii)**Type the matter to acquaint with the use of Micro-soft equation and drawing tools or any such facilities. **(iv)** Present the seminar topic orally and/or through PowerPoint slides. **(v)** Answer the queries and involve in debate/discussion. **(vi)** Submit a typed report with a list of references.

The participants shall take part in the discussion to foster a friendly and stimulating environment in which the students are motivated to reach high standards and become self-confident.

Evaluation Procedure:

The CIE marks for the seminar shall be awarded (based on the relevance of the topic, presentation skill, participation in the question and answer session, and quality of report) by the committee constituted for the purpose by the Head of the Department. The committee shall consist of three teachers from the department with the senior-most acting as the Chairman.

Marks distribution for CIE of the course:

Seminar Report:50 marks
Presentation skill:25 marks
Question and Answer: 25 marks.■No SEE component for Technical Seminar

Non–credit mandatory courses (NCMC):

National Service Scheme/Physical Education (Sport and Athletics)/ Yoga:

(1) Securing 40 % or more in CIE,35 % or more marks in SEE, and 40 % or more in the sum total of CIE + SEE leads to successful completion of the registered course.

(2) In case, students fail to secure 35 % marks in SEE, they have to appear for SEE during the subsequent examinations conducted by the University.

(3) In case, any student fails to register for NSS, PE or Yoga/fails to secure the minimum 40 % of the prescribed CIE marks, he/she shall be deemed to have not completed the requirements of the course. In such a case, the student has to fulfill the course requirements during subsequently to earn the qualifying CIE marks subject to the maximum program period.

(4) Successful completion of the course shall be indicated as satisfactory in the grade card. Non-completion of the course shall be indicated as Unsatisfactory.

(5) These courses shall not be considered for vertical progression as well as for the calculation of SGPA and CGPA, but completion of the courses shall be mandatory for the award of a degree.

ADICHUNCHANAGIRI INSTITUTE OF TECHNOLOGY

Electronics & Communication Engineering (EC)

Course Name : CRYPTOGRAPHY (21EC642)
Class : Semester 6 A

Professor & Head
Dept. of Electronics & Communication Eng
Adichunchanagiri Institute of Technology
Chikmagalur - 577 102

Ms Divya G S,
Assistant Professor,
2023-24

1 . Faculty Details

Name	: Ms Divya G S
Qualification	: -
Department	: EC
Permanent Address	: Housing Board, Near Sai Mandir, Jyothinagar, Chikkamagaluru, 577102, India
Phone Number	: 9980557726
Email ID	: divya.jchandra@gmail.com
Specimen Signature	: ____________________

HOD

2 . Course Allotted

Allotted Duty	Course Title	Course Code
THEORY 1	CRYPTOGRAPHY	21EC642

3 . Academic calendar 2023-24 (Semester 6)

Date	Day	Event
29 Apr 2024	MONDAY	Term Start Date
1 May 2024	WEDNESDAY	May Day
10 May 2024	FRIDAY	Basaveshwara Jayanthi
17 Jun 2024	MONDAY	BAKRID
17 Jul 2024	WEDNESDAY	\tLat day of Moharam
31 Jul 2024	WEDNESDAY	Term End Date

4 . Timetable

	1	2	3	4		5	6	7
	09:00 AM To 10:00 AM	10:00 AM To 11:00 AM	11:15 AM To 12:15 PM	12:15 PM To 01:15 PM	01:15 PM To 02:30 PM	02:30 PM To 03:20 PM	03:20 PM To 04:10 PM	04:10 PM To 05:00 PM
MON		BE BEC503 EC Semester 5 Section B			B R E A K	BE BECL504 EC Semester 5 Section B		
TUE				BE BEC503 EC Semester 5 Section B				
WED	BE BEC503 EC Semester 5 Section B					BE BECL504 EC Semester 5 Section B		
THU						BE BECL504 EC Semester 5 Section A		
FRI			BE BEC503 EC Semester 5 Section B			BE BECL504 EC Semester 5 Section B		
SAT								
SUN								

HOD

2. Department Details

2.1 Preliminary Information

PROGRAM OUTCOMES(POs)

1. **Engineering knowledge**: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

2. **Problem analysis**: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

3. **Design/development of solutions**: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

4. **Conduct investigations of complex problems**: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

5. **Modern tool usage**: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

6. **The engineer and society**: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

7. **Environment and sustainability**: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

8. **Ethics**: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

9. **Individual and team work**: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

10. **Communication**: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

11. **Project management and finance**: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

12. **Life-long learning**: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

6 . Course Information

6 . 1 Course Content

Title of the Course : CRYPTOGRAPHY
Semester : 6

Academic Year : 2023-24

Subject Code : 21EC642	IA Marks : 50
Hours/week : 4	Total Hours : 40
Exam Hours : 3	Exam Marks : 50
Course Plan Author : Divya	Planned Date : 2024-04-29
Approved by : Dr Goutham M A	Approved Date : 2024-04-29

Objectives:

1 . Preparation: To prepare students with fundamental knowledge/ overview in the field of Information Security with knowledge of mathematical concepts required for cryptography

2 . Core Competence: To equip students with a basic foundation of Cryptography by delivering the basics of symmetric key and public key cryptography and design of pseudo random sequence generation technique

Course Outcomes (COs) :

1 . Illustrate the concepts of number theory and finite fields applicable to cryptosystems.

2 . Describe traditional cryptographic algorithms of encryption and decryption process

3 . Describe the set of procedures and computations used in public key cryptosystems.

4 . Classify the different types of stream ciphers along with its functional characteristics.

PROGRAM SPECIFIC OUTCOMES(PSO's)

PSO 1 : Professional Skills: Graduates are able to analyze and design systems in the fields related to Digital signal processing, communication and networking, VLSI and embedded systems.

PSO 2 : Problem-Solving Skills: Graduates are able to identify problems in the areas of Signal processing, communication and embedded systems and provide efficient solutions using computational tools and algorithms individually or working in a team.

HOD

6 . Course Information

6 . 1 . 1 Course Syllabus

Objectives:
Title of the Course : CRYPTOGRAPHY
Subject Code : 21EC642

Module 1

Basic Concepts of Number Theory and Finite Fields :

Divisibility and The Division Algorithm Euclidean algorithm, Modular arithmetic, Groups, Rings and Fields, Finite fields of the form GF(p), Polynomial Arithmetic, Finite Fields of the Form GF

Module 2

Introduction :

Computer Security Concepts, A Model for Network Security

Module 3

Block Ciphers :

Traditional Block Cipher structure, Data encryption standard (DES) (Text 1: Chapter 2: Section1, 2) The AES Cipher

Module 4

ASYMMETRIC CIPHERS :

Principles of Public-Key Cryptosystems, The RSA algorithm, Diffie - Hellman Key Exchange, Elliptic Curve Arithmetic, Elliptic Curve Cryptography

Module 5

Pseudo-Random-Sequence Generators and Stream Ciphers :

Linear Congruential Generators, Linear Feedback Shift Registers, Design and analysis of stream ciphers, Stream ciphers using LFSRs, A5, Hughes XPD/KPD, Nanoteq, Rambutan, Additive generators, Gifford, Algorithm M, PKZIP

6 . Course Information

6 . 1 . 1 Course Syllabus

Objectives:
Title of the Course : CRYPTOGRAPHY
Subject Code : 21EC642

Module 1

Basic Concepts of Number Theory and Finite Fields :

Divisibility and The Division Algorithm Euclidean algorithm, Modular arithmetic, Groups, Rings and Fields, Finite fields of the form GF(p), Polynomial Arithmetic, Finite Fields of the Form GF

Module 2

Introduction :

Computer Security Concepts, A Model for Network Security

Module 3

Block Ciphers :

Traditional Block Cipher structure, Data encryption standard (DES) (Text 1: Chapter 2: Section1, 2) The AES Cipher

Module 4

ASYMMETRIC CIPHERS :

Principles of Public-Key Cryptosystems, The RSA algorithm, Diffie - Hellman Key Exchange, Elliptic Curve Arithmetic, Elliptic Curve Cryptography

Module 5

Pseudo-Random-Sequence Generators and Stream Ciphers :

Linear Congruential Generators, Linear Feedback Shift Registers, Design and analysis of stream ciphers, Stream ciphers using LFSRs, A5, Hughes XPD/KPD, Nanoteq, Rambutan, Additive generators, Gifford, Algorithm M, PKZIP

6 . Course Information

6 . 1 . 2 Text Books and Reference Books

TEXT BOOKS :

1 . William Stallings , "Cryptography and Network Security Principles and Practice", Pearson Education Inc., 6th Edition, 2014, ISBN: 978-93-325-1877-3

2 . Bruce Schneier, "Applied Cryptography Protocols, Algorithms, and Source code in C", Wiley Publications, 2nd Edition, ISBN: 9971-51-348-X.

REFERENCE BOOKS :

1 . Cryptography and Network Security, Behrouz A Forouzan, TMH, 2007

2 . Cryptography and Network Security, Atul Kahate, TMH, 2003

HOD

6 . Course Information

6 . 2

Semester : 6 **Section :** A **Course :** CRYPTOGRAPHY

Period	Plan/ Execution	Date	Topic	Source material to be referred	Course Outcome	Bloom's Level	Execution Methods	Learning Validation Method
Module 1								
1	P	29 Apr 2024	Divisibility and The Division Algorithm Euclidean algorithm	Text 1, Ref 1	CO 1	Understand	Lecture	
1	E	29 Apr 2024	Divisibility and The Division Algorithm Euclidean algorithm	Text 1, Ref 1	CO 1	Understand	Lecture	
2	P	30 Apr 2024	Modular arithmetic	Text 1, Ref 1	CO 1	Understand	Lecture	
2	E	30 Apr 2024	Modular arithmetic	Text 1, Ref 1	CO 1	Understand	Lecture	
3	P	2 May 2024	Modular arithmetic	Ref 1	CO 1	Understand	Lecture	
3	E	2 May 2024	Modular arithmetic	Ref 1	CO 1	Understand	Lecture	
4	P	6 May 2024	Groups, Rings and Fields	Text 1, Ref 1	CO 1	Understand	Lecture	
4	E	6 May 2024	Groups, Rings and Fields	Text 1, Ref 1	CO 1	Understand	Lecture	
5	P	7 May 2024	Finite fields of the form GF(p)	Text 1, Ref 1	CO 1	Understand	Lecture	
5	E	7 May 2024	Finite fields of the form GF(p)	Text 1, Ref 1	CO 1	Understand	Lecture	
6	P	9 May 2024	Polynomial Arithmetic	Text 1, Ref 1	CO 1	Understand	Lecture	
6	E	9 May 2024	Polynomial Arithmetic	Text 1, Ref 1	CO 1	Understand	Lecture	
7	P	13 May 2024	Polynomial Arithmetic	Text 1, Ref 1	CO 1	Understand	Lecture	
7	E	13 May 2024	Polynomial Arithmetic	Text 1, Ref 1	CO 1	Understand	Lecture	
8	P	14 May 2024	Finite Fields of the Form GF	Text 1, Ref 1	CO 1	Understand	Lecture	
8	E	14 May 2024	Finite Fields of the Form GF	Text 1, Ref 1	CO 1	Understand	Lecture	
Module 2								
9	P	16 May 2024	Computer Security Concepts	Text 1	CO 2	Understand	Lecture	
9	E	16 May 2024	Computer Security Concepts	Text 1	CO 2	Understand	Lecture	
10	P	20 May 2024	A Model for Network Security	Text 1	CO 2	Understand	Lecture	
10	E	20 May 2024	A Model for Network Security	Text 1	CO 2	Understand	Lecture	

Period	Plan/ Execution	Date	Topic	Source material to be referred	Course Outcome	Bloom's Level	Execution Methods	Learning Validation Method
11	P	21 May 2024	Classical Encryption Techniques: Symmetric Cipher Model	Text 1	CO 2	Understand	Lecture	
11	E	21 May 2024	Classical Encryption Techniques: Symmetric Cipher Model	Text 1	CO 2	Understand	Lecture	
12	P	23 May 2024	Classical Encryption Techniques: Symmetric cipher model	Text 1	CO 2	Understand	Lecture	
12	E	23 May 2024	Classical Encryption Techniques: Symmetric cipher model	Text 1	CO 2	Understand	Lecture	
13	P	27 May 2024	Substitution techniques	Text 1	CO 2	Understand	Lecture	
13	E	27 May 2024	Substitution techniques	Text 1	CO 2	Understand	Lecture	
14	P	28 May 2024	Substitution techniques	Text 1	CO 2	Understand	Lecture	
14	E	28 May 2024	Substitution techniques	Text 1	CO 2	Understand	Lecture	
15	P	30 May 2024	Substitution techniques	Text 1	CO 2	Understand	Lecture	
15	E	30 May 2024	Transposition techniques	Text 1	CO 2	Understand	Lecture	
16	P	3 Jun 2024	Transposition techniques	Text 1	CO 2	Understand	Lecture	
16	E	3 Jun 2024	Transposition techniques	Text 1	CO 2	Understand	Lecture	
Module 3								
17	P	4 Jun 2024	Traditional Block Cipher structure	Text 1	CO 2	Understand	Lecture	
17	E	4 Jun 2024	Traditional Block Cipher structure	Text 1	CO 2	Understand	Lecture	
18	P	6 Jun 2024	Data Encryption Standard	Text 1	CO 2	Understand	Lecture	
18	E	6 Jun 2024	Data Encryption Standard	Text 1	CO 2	Understand	Lecture	
19	P	10 Jun 2024	Data encryption standard (DES)	Text 1	CO 2	Understand	Lecture	
19	E	10 Jun 2024	Data encryption standard (DES)	Text 1	CO 2	Understand	Lecture	
20	P	11 Jun 2024	The AES Cipher	Text 1	CO 2	Understand	Lecture	
20	E	11 Jun 2024	The AES Cipher	Text 1	CO 2	Understand	Lecture	
21	P	13 Jun 2024	The AES Cipher	Text 1	CO 2	Understand	Lecture	
21	E	13 Jun 2024	The AES Cipher	Text 1	CO 2	Understand	Lecture	
22	P	17 Jun 2024	More on Number Theory: Prime Numbers	Text 1, Ref 1	CO 1	Understand	Lecture	
22	E	17 Jun 2024	More on Number Theory: Prime Numbers	Text 1, Ref 1	CO 1	Understand	Lecture	
23	P	20 Jun 2024	Fermat's and Euler's theor	Text 1, Ref 1	CO 1	Understand	Lecture	
23	E	20 Jun 2024	Fermat's and Euler's theor	Text 1, Ref 1	CO 1	Understand	Lecture	
24	P	24 Jun 2024	Discrete logarithm	Text 1, Ref 1	CO 1	Understand	Lecture	

Period	Plan/ Execution	Date	Topic	Source material to be referred	Course Outcome	Bloom's Level	Execution Methods	Learning Validation Method
24	E	24 Jun 2024	Discrete logarithm	Text 1, Ref 1	CO 1	Understand	Lecture	
Module 4								
25	P	25 Jun 2024	Principles of Public-Key Cryptosystems	Text 1	CO 3	Understand	Lecture	
25	E	25 Jun 2024	Principles of Public-Key Cryptosystems	Text 1	CO 3	Understand	Lecture	
26	P	27 Jun 2024	Principles of Public-Key Cryptosystems	Text 1	CO 3	Understand	Lecture	
26	E	27 Jun 2024	Principles of Public-Key Cryptosystems	Text 1	CO 3	Understand	Lecture	
27	P	1 Jul 2024	The RSA algorithm	Text 1	CO 3	Understand	Lecture	
27	E	1 Jul 2024	The RSA algorithm	Text 1	CO 3	Understand	Lecture	
28	P	2 Jul 2024	The RSA algorithm	Text 1	CO 3	Understand	Lecture	
28	E	2 Jul 2024	The RSA algorithm	Text 1	CO 3	Understand	Lecture	
29	P	4 Jul 2024	Diffie - Hellman Key Exchange	Text 1	CO 3	Understand	Lecture	
29	E	4 Jul 2024	Diffie - Hellman Key Exchange	Text 1	CO 3	Understand	Lecture	
30	P	8 Jul 2024	Diffie - Hellman Key Exchange	Text 1	CO 3	Understand	Lecture	
30	E	8 Jul 2024	Diffie - Hellman Key Exchange	Text 1	CO 3	Understand	Lecture	
31	P	9 Jul 2024	Elliptic Curve Arithmetic	Text 1	CO 3	Understand	Lecture	
31	E	9 Jul 2024	Elliptic Curve Arithmetic	Text 1	CO 3	Understand	Lecture	
32	P	11 Jul 2024	Elliptic Curve Cryptography	Text 1	CO 3	Understand	Lecture	
32	E	11 Jul 2024	Elliptic Curve Cryptography	Text 1	CO 3	Understand	Lecture	
Module 5								
33	P	15 Jul 2024	Linear Congruential Generators, Linear Feedback Shift Registers	Text 2	CO 4	Understand	Lecture	
33	E	15 Jul 2024	Linear Congruential Generators, Linear Feedback Shift Registers	Text 2	CO 4	Understand	Lecture	
34	P	16 Jul 2024	Design and analysis of stream ciphers, Stream ciphers using LFSRs	Text 2	CO 4	Understand	Lecture	
34	E	16 Jul 2024	Design and analysis of stream ciphers, Stream ciphers using LFSRs	Text 2	CO 4	Understand	Lecture	
35	P	18 Jul 2024	Hughes XPD/KPD, A5	Text 2	CO 4	Understand	Lecture	
35	E	18 Jul 2024	Hughes XPD/KPD, A5	Text 2	CO 4	Understand	Lecture	
36	P	22 Jul 2024	Nanoteq, Rambutan	Text 2	CO 4	Understand	Lecture	
36	E	22 Jul 2024	Nanoteq, Rambutan	Text 2	CO 4	Understand	Lecture	
37	P	23 Jul 2024	Additive generators	Text 2	CO 4	Understand	Lecture	
37	E	23 Jul 2024	Additive generators	Text 2	CO 4	Understand	Lecture	
38	P	25 Jul 2024	Gifford	Text 2	CO 4	Understand	Lecture	
38	E	25 Jul 2024	Gifford	Text 2	CO 4	Understand	Lecture	

Period	Plan/ Execution	Date	Topic	Source material to be referred	Course Outcome	Bloom's Level	Execution Methods	Learning Validation Method
39	P	29 Jul 2024	Algorithm M	Text 2	CO 4	Understand	Lecture	
39	E	29 Jul 2024	Algorithm M	Text 2	CO 4	Understand	Lecture	
40	P	30 Jul 2024	PKZIP	Text 2	CO 4	Understand	Lecture	
40	E	30 Jul 2024	PKZIP	Text 2	CO 4	Understand	Lecture	

6 . Course Information

6 . 2 . 1 Compliance Report

Semester : 6 **Section :** A **Course :** CRYPTOGRAPHY

Module No.	# of Classes Planned(till date)	Planned Effort(till date)	# of Classes Executed(till date)	Actual Efforts(till date)	% Coverage
1	8	8hrs 0min	8	8hrs 0min	100.0
2	8	8hrs 0min	8	8hrs 0min	100.0
3	8	8hrs 0min	8	8hrs 0min	100.0
4	8	8hrs 0min	8	8hrs 0min	100.0
5	8	8hrs 0min	8	8hrs 0min	100.0

HOD

6 . Course Information

6 . 2 . 2 CO PO Mapping

No CO PO mapping available

HOD

6 . Course Information

6 . 2 . 3 CO-PSO Mapping

No CO PSO mapping available

HOD

6 . Course Information

6 . 3 Other Assessment

SEMINAR/QUIZ : 1

Semester:6-CBCS 2021

Subject : CRYPTOGRAPHY (21EC642)

Faculty : Divya

Max Marks: 20

Answer All Questions		
Q.No		Max Marks
1	1. Which of the following is the meaning of crypt? a. Hidden b. Writing c. Copied d. Both a and b 2. Jim has encrypted his company's confidential files using a secret key. Attacker John tries to decipher those files without knowing the key. what is this process called? a. Cryptography b. Cryptanalysis c. Decryption d. None of the above 3. Which of the following are the components of crypto system? a. Plain text b. Cipher text c. Keys d.All of the above 4. Which of the following is the other name of symmetric key cryptography? a. Private key b. Secret key c. ideal key d. Both a and b 5. Find an integer 5. x 5. that satisfies the equation 5x 5. 5. ≡ 1 mod 7 b: a. 2 b. 3 c. 5 d. 7 6. Determine 11 mod 5 a. 4 b. -1 c. 1 d. 4 7. Given integers a and b, multiplicative inverse exists if and only if gcd(a,b) = a. a b. 1 c. b d. None 8. Which of the following cipher techniques involves matrix operations in their algorithms of encryption and decryption? a. Hill Cipher b.Playfair Cipher c. Both a &b d. None of the above 9. With symmetric key algorithms, the ____ key is used for the encryption and decryption of data. a.Different b. Same c. Both a & b d. None of the above	20

Evaluation

USN	Name	Present (P) / Absent (Ab)	IA Total
4AI21EC001	Abhishek K M	P	8
4AI21EC002	Akanksha C	P	8
4AI21EC003	Ananya M	P	16
4AI21EC004	Ankith P	P	10
4AI21EC005	Ankush D D	P	4
4AI21EC006	Anusha A	P	12
4AI21EC007	Anushree J K	P	16

USN	Name	Present (P) / Absent (Ab)	IA Total
4AI21EC008	Ashwin Gowda S J	P	18
4AI21EC010	Benakesh S N	P	12
4AI21EC011	Bhavana H P	P	10
4AI21EC012	Bhoomika B C	P	10
4AI21EC013	Bhumika D M	P	16
4AI21EC014	Bibi Swagra	P	20
4AI21EC015	Chaithanya J	P	12
4AI21EC016	Chaithra L P	P	16
4AI21EC017	Chandana K	P	14
4AI21EC018	Chandana Patil C S	P	16
4AI21EC019	Chandrakanth S M	P	12
4AI21EC020	Chethan N M	P	18
4AI21EC021	Darshan S	P	8
4AI21EC022	Darshini B	P	8
4AI21EC023	Deeksha K B	P	10
4AI21EC024	Deeksha K R	P	14
4AI21EC025	Deepak M S	P	8
4AI21EC027	Deepakraj R B	P	10
4AI21EC028	Dhanush Gowda H	P	6
4AI21EC031	Gowtham B G	P	8
4AI21EC033	Jeevan R M	P	10
4AI21EC034	Karthikeyan J	P	6
4AI21EC035	Kavana K S	P	10
4AI21EC036	Keerthana L S	P	10
4AI21EC037	Likhith S V	P	14
4AI21EC038	Likitha C M	P	8
4AI21EC040	Manjushree K S	P	8
4AI21EC042	Manupatel S P	P	10

USN	Name	Present (P) / Absent (Ab)	IA Total
4AI21EC043	Manya U	P	12
4AI21EC044	Meghana R	P	10
4AI21EC045	Mohammed Wasib	P	6
4AI21EC046	Nakul P M	P	16
4AI21EC047	Neha G M	P	12
4AI21EC048	Nidhi K M	P	12
4AI21EC049	Niranjan G M	P	20
4AI21EC050	Nishanth Gowda V S	P	10
4AI21EC051	Nishchitha M	P	16
4AI21EC052	Pavan Kumar	P	10
4AI21EC053	Pooja H H	P	12
4AI22EC400	Arpitha C S	P	12
4AI22EC402	Avinash H R	P	10
4AI22EC406	Chethan V	P	10
4AI22EC407	Dayananda H L	P	4
4AI22EC408	Deepu P	P	8
4AI22EC413	Indika G	P	10
4AI22EC414	Kanakraj H R	P	10
4AI22EC415	Karanraj Hr	P	8
4AI22EC418	Naveen H L	P	9
4AI22EC419	Pavan Kumar C N	P	14
4AI22EC420	Punith R	P	6
4AI22EC423	Sandya M	P	12
4AI22EC424	Shashank K G	P	10
4AI22EC425	Shashikiran M	P	10
4AI22EC426	Sneha S V	P	10

2 Scheme of Evaluation

QUIZ SOLUTIONS

1. Which of the following is the meaning of crypt?
   a. Hidden b. Writing c. Copied d. Both a and b
2. Jim has encrypted his company's confidential files using a secret key. Attacker John tries to decipher those files without knowing the key, what is this process called?
   a. Cryptography b. Cryptanalysis c. Decryption d. None of the above
3. Which of the following are the components of crypto system?
   a. Plain text b. Cipher text c. Keys d. All of the above
4. Which of the following is the other name of symmentric key cryptography?
   a. Private key b. Secret key c. Ideal key d. Both a and b
5. Find an integer x that satisfies the equation 5x ≡ 3 (mod 11).
   a. 2 b. 3 c. 5 d. 1
6. Determine : 11 mod -5.
   a. -4 b. -1 c. 1 d. 4
7. Given integers a and b, multiplicative inverse exists if and only if gcd(a,b) =
   a. a b. 1 c. b d. None
8. Which of the following cipher techniques involves matrix operations in their algorithms of encryption and decryption?
   a. Hill Cipher b. Playfair Cipher c. Both a &b d. None of the above
9. With symmetric key algorithms, the ____ key is used for the encryption and decryption of data.
   a. Different b. Same c. Both a & b d. None of the above
10. Which of the following is a type of attack on encryption that tries every possible key combination?
    a. Brute force attack b. Dictionary attack c. Collision attack d. Rainbow table attack
11. The theorems that play important roles in public-key cryptography are
    a. Fermat's theorem b. Euler's theorem c. Euclidean theorem d. Both a &b
12. Using the Euler's totient function, determine ϕ(253)
    a. 200 b. 209 c. 220 d. 252
13. What are the two keys that are used in asymmetric key cryptography?
    a. Secret key and private key b. Private key and public key
    c. Public key and secured key d. Secured key and private key
14. Jim and Joe decide to use Diffie-Hellman method. If they are not authenticated to each other, what type of security attack can be expected?
    a. Man-in-the-middle attack b. Brute force attack c. Plain text attack d. Cipher-only attack
15. How many rounds does 128 bits in AES requires?
    a. 10 b. 12 c. 14 d. 15
16. 128 bits plain text form of AES has __ bytes.
    a. 12 b. 14 c. 16 d. 18
17. Amongst which of the following is / are true with reference to the rounds in AES –
    a. Byte Substitution b. Shift Row c. Mix Column and Key Addition d. All of the above
18. The full-form of RSA in the RSA encryption technique
    a. Round Security Algorithm b. Rivest, Shamir, Adleman
    c. Robert, Shamir, Addie d. None of the above

19. Data encryption standard is a block cipher and encrypts data in blocks of size of _____ each.
    a. 16 bits b. 64bits c.128 bits d.32 bits
20. The ___________ method provides a one-time session key for two parties.
    a. Diffie-Hellman b.RSA c. AES d. DES

ADICHUNCHANAGIRI INSTITUTE OF TECHNOLOGY

Department of Electronics & Communication Engineering (EC)

ASSIGNMENT : 1

Semester:6-CBCS 2021

Subject : CRYPTOGRAPHY (21EC642)

Faculty : Divya

Max Marks: 10

Answer All Questions			
Q.No		**Max Marks**	**CO**
1	1.Define Computer Security. Explain in brief the 3 key objectives of computer security. 2. List down the challenges of computer security. 3. Explain the essential network and computer security requirements. 4. With neat block diagram, explain the model of network security. Also, list the 4 basic tasks in designing security services.	10	1,2

Evaluation

USN	Name	Present (P) / Absent (Ab)	IA Total
4AI21EC001	Abhishek K M	P	7
4AI21EC002	Akanksha C	P	5
4AI21EC003	Ananya M	P	9
4AI21EC004	Ankith P	P	6
4AI21EC005	Ankush D D	P	4
4AI21EC006	Anusha A	P	10
4AI21EC007	Anushree J K	P	10
4AI21EC008	Ashwin Gowda S J	P	8
4AI21EC010	Benakesh S N	P	7
4AI21EC011	Bhavana H P	P	10
4AI21EC012	Bhoomika B C	P	10

USN	Name	Present (P) / Absent (Ab)	IA Total
4AI21EC013	Bhumika D M	P	10
4AI21EC014	Bibi Swagra	P	10
4AI21EC015	Chaithanya J	P	10
4AI21EC016	Chaithra L P	P	10
4AI21EC017	Chandana K	P	10
4AI21EC018	Chandana Patil C S	P	10
4AI21EC019	Chandrakanth S M	P	10
4AI21EC020	Chethan N M	P	9
4AI21EC021	Darshan S	P	8
4AI21EC022	Darshini B	P	8
4AI21EC023	Deeksha K B	P	10
4AI21EC024	Deeksha K R	P	10
4AI21EC025	Deepak M S	P	7
4AI21EC027	Deepakraj R B	P	10
4AI21EC028	Dhanush Gowda H	P	9
4AI21EC031	Gowtham B G	P	6
4AI21EC033	Jeevan R M	P	7
4AI21EC034	Karthikeyan J	P	8
4AI21EC035	Kavana K S	P	9
4AI21EC036	Keerthana L S	P	9
4AI21EC037	Likhith S V	P	10
4AI21EC038	Likitha C M	P	10
4AI21EC040	Manjushree K S	P	8
4AI21EC042	Manupatel S P	P	10
4AI21EC043	Manya U	P	10
4AI21EC044	Meghana R	P	8
4AI21EC045	Mohammed Wasib	P	8
4AI21EC046	Nakul P M	P	8

USN	Name	Present (P) / Absent (Ab)	IA Total
4AI21EC047	Neha G M	P	9
4AI21EC048	Nidhi K M	P	10
4AI21EC049	Niranjan G M	P	10
4AI21EC050	Nishanth Gowda V S	P	4
4AI21EC051	Nishchitha M	P	10
4AI21EC052	Pavan Kumar	P	8
4AI21EC053	Pooja H H	P	10
4AI22EC400	Arpitha C S	P	8
4AI22EC402	Avinash H R	P	5
4AI22EC406	Chethan V	P	5
4AI22EC407	Dayananda H L	P	8
4AI22EC408	Deepu P	P	6
4AI22EC413	Indika G	P	6
4AI22EC414	Kanakraj H R	P	6
4AI22EC415	Karanraj Hr	P	7
4AI22EC418	Naveen H L	P	9
4AI22EC419	Pavan Kumar C N	P	8
4AI22EC420	Punith R	P	6
4AI22EC423	Sandya M	P	6
4AI22EC424	Shashank K G	P	6
4AI22EC425	Shashikiran M	P	7
4AI22EC426	Sneha S V	P	6

USN	Name	Present (P) / Absent (Ab)	IA Total
4AI21EC013	Bhumika D M	P	10
4AI21EC014	Bibi Swagra	P	10
4AI21EC015	Chaithanya J	P	10
4AI21EC016	Chaithra L P	P	10
4AI21EC017	Chandana K	P	10
4AI21EC018	Chandana Patil C S	P	10
4AI21EC019	Chandrakanth S M	P	10
4AI21EC020	Chethan N M	P	9
4AI21EC021	Darshan S	P	8
4AI21EC022	Darshini B	P	8
4AI21EC023	Deeksha K B	P	10
4AI21EC024	Deeksha K R	P	10
4AI21EC025	Deepak M S	P	7
4AI21EC027	Deepakraj R B	P	10
4AI21EC028	Dhanush Gowda H	P	9
4AI21EC031	Gowtham B G	P	6
4AI21EC033	Jeevan R M	P	7
4AI21EC034	Karthikeyan J	P	8
4AI21EC035	Kavana K S	P	9
4AI21EC036	Keerthana L S	P	9
4AI21EC037	Likhith S V	P	10
4AI21EC038	Likitha C M	P	10
4AI21EC040	Manjushree K S	P	8
4AI21EC042	Manupatel S P	P	10
4AI21EC043	Manya U	P	10
4AI21EC044	Meghana R	P	8
4AI21EC045	Mohammed Wasib	P	8
4AI21EC046	Nakul P M	P	8

USN	Name	Present (P) / Absent (Ab)	IA Total
4AI21EC047	Neha G M	P	9
4AI21EC048	Nidhi K M	P	10
4AI21EC049	Niranjan G M	P	10
4AI21EC050	Nishanth Gowda V S	P	4
4AI21EC051	Nishchitha M	P	10
4AI21EC052	Pavan Kumar	P	8
4AI21EC053	Pooja H H	P	10
4AI22EC400	Arpitha C S	P	8
4AI22EC402	Avinash H R	P	5
4AI22EC406	Chethan V	P	5
4AI22EC407	Dayananda H L	P	8
4AI22EC408	Deepu P	P	6
4AI22EC413	Indika G	P	6
4AI22EC414	Kanakraj H R	P	6
4AI22EC415	Karanraj Hr	P	7
4AI22EC418	Naveen H L	P	9
4AI22EC419	Pavan Kumar C N	P	8
4AI22EC420	Punith R	P	6
4AI22EC423	Sandya M	P	6
4AI22EC424	Shashank K G	P	6
4AI22EC425	Shashikiran M	P	7
4AI22EC426	Sneha S V	P	6

6 . Course Information

6 . 4 Internal Assessment

Internal : 1

Semester:6-CBCS 2021

Subject : CRYPTOGRAPHY (21EC642)

Faculty : Divya

Date : 14/06/2024

Time : 15:30 - 16:30

Max Marks: 40

Part A

Answer any 3 questions

Q.No		Max Marks	CO	BT/CL
1	Explain using flowchart, the Euclidean algorithm to determine the GCD of two numbers. Find the GCD of (i) (24140,16762).(ii)(2152,764).	10	1	L2
2a	(a) Explain the properties of modular arithmetic for Integers in Zn. (b) Construct additive and multiplicative tables for arithmetic modulo 7 and tabulate the additive and multiplicative inverses.	10	1	L2
3	Using Extended Euclidean Algorithm, find the multiplicative inverse of the following: (i) 17 mod 43 (ii) x^3 + x + 1 in GF(2^4) with m(x) = x^4 + x + 1	10	1	L2

4a		(a) Define Galois field. List all the axioms obeyed by GF. (b) Develop addition and multiplication tables based on polynomial arithmetic modulo for GF(4) with m(x) = x^2 + x + 1.	10	1	L2
5		Obtain the field elements of GF(2^4) using a generator polynomial x^4 + x + 1. Give the equivalent binary and hexadecimal representation.	10	1	L2

Part B				
Answer any 1 questions				
Q.No		**Max Marks**	**CO**	**BT/CL**
6	Define Computer Security. Explain in brief, the challenges of computer security.	10	2	L2
7	With neat block diagram, explain the model of network security. Also, list the 4 basic tasks in designing security services.	10	2	L2

Evaluation

USN	Name	Present (P) / Absent (Ab)	Q1	Q2	Q3	Q4	Q5	Q6	Q7	IA Total	BT/CL
				a		a					
4AI21EC001	Abhishek K M	P	6	0	0	0	0	0	6	12	Understand
4AI21EC002	Akanksha C	P	4	5	1	0	0	0	0	10	Understand
4AI21EC003	Ananya M	P	6.5	0	0	10	9.5	0	10	36	Understand
4AI21EC004	Ankith P	P	4	0	0	0	0	0	4	8	No Level
4AI21EC005	Ankush D D	P	0	2	0	0	0	0	0	2	No Level
4AI21EC006	Anusha A	P	4	4	7	0	9	0	8	28	Understand
4AI21EC007	Anushree J K	P	4	4	4	0	4	4	0	16	No Level
4AI21EC008	Ashwin Gowda S J	P	6	0	8	0	6	0	5	25	Understand
4AI21EC010	Benakesh S N	P	4	4	0	0	0	0	4	12	No Level
4AI21EC011	Bhavana H P	P	4	4	0	4	10	0	7	25	Understand
4AI21EC012	Bhoomika B C	P	4	5	0	5	0	0	7	21	Understand
4AI21EC013	Bhumika D M	P	4	0	0	9	10	0	10	33	Understand
4AI21EC014	Bibi Swagra	P	0	0	10	10	10	0	9	39	Understand
4AI21EC015	Chaithanya J	P	4	5	0	0	10	0	2	21	Understand
4AI21EC016	Chaithra L P	P	3	0	5	5	7	8	0	25	Understand
4AI21EC017	Chandana K	P	2	0	5	0	10	0	8	25	Understand
4AI21EC018	Chandana Patil C S	P	4	0	9	4	10	3	0	26	Understand
4AI21EC019	CHANDRAKANTH S M	P	0	4	10	0	10	0	4	28	Understand
4AI21EC020	Chethan N M	P	4	5	0	0	10	0	4	23	Understand
4AI21EC021	Darshan S	P	5	0	0	0	0	0	7	12	Understand
4AI21EC022	Darshini B	P	4	3	2	5	0	2	6	18	Understand

USN	Name	Present (P) / Absent (Ab)	Q1	Q2	Q3	Q4	Q5	Q6	Q7	IA Total	BT/CL
4AI21EC023	Deeksha K B	P	4	4	3	0	6	0	8	22	Understand
4AI21EC024	Deeksha K R	P	0	5	9	0	7	10	0	31	Understand
4AI21EC025	Deepak M S	P	4	5	4	0	0	0	6	19	Understand
4AI21EC027	Deepakraj R B	P	3	4	2	0	0	4	7	16	Understand
4AI21EC028	DHANUSH GOWDA H	P	3	5	0	2	0	0	5	15	Understand
4AI21EC031	Gowtham B G	P	4	4	0	2	0	0	0	10	No Level
4AI21EC033	Jeevan R M	P	5	3	7	0	0	0	5	20	Understand
4AI21EC034	Karthikeyan.j	P	4	5	0	0	0	2	5	14	Understand
4AI21EC035	Kavana K S	P	4	4	3	8	10	0	7	29	Understand
4AI21EC036	Keerthana L S	P	2	2	0	0	0	0	4	8	No Level
4AI21EC037	Likhith S V	P	8	5	6	0	0	0	7	26	Understand
4AI21EC038	Likitha C M	P	3	5	8	0	8	8	0	29	Understand
4AI21EC040	Manjushree K S	P	3	5	0	1	9	0	4	21	Understand
4AI21EC042	Manupatel S P	P	4	5	8	0	0	10	0	27	Understand
4AI21EC043	Manya U	P	4	5	9	3	0	0	6	24	Understand
4AI21EC044	Meghana R	P	3	0	2	5	6	0	3	17	Understand
4AI21EC045	Mohammed Wasib	P	0	4	6	0	0	0	9	19	Understand
4AI21EC046	Nakul P M	P	6	5	7	0	10	0	3	26	Understand
4AI21EC047	Neha G M	P	4	0	1	5	10	5	0	24	Understand
4AI21EC048	Nidhi K M	P	4	5	0	0	9	8	0	26	Understand
4AI21EC049	Niranjan G M	P	4	5	4	0	8	0	5	22	Understand
4AI21EC050	Nishanth Gowda V S	P	0	3	3	4	6	0	7	20	Understand
4AI21EC051	Nishchitha M	P	7	5	0	9	10	0	8	34	Understand
4AI21EC052	Pavan Kumar	P	4	0	6	3	10	0	0	20	Understand

USN	Name	Present (P) / Absent (Ab)	Q1	Q2	Q3	Q4	Q5	Q6	Q7	IA Total	BT/CL
4AI21EC053	Pooja H H	P	4	0	5	6	6	0	8	25	Understand
4AI22EC400	Arpitha C S	P	8	0	5	10	0	0	6	29	Understand
4AI22EC402	AVINASH.H.R	P	4	5	0	0	0	0	4	13	Understand
4AI22EC406	CHETHAN V	P	4	3	0	0	0	6	4	13	Understand
4AI22EC407	Dayananda H L	P	0	3	0	1	0	0	4	8	No Level
4AI22EC408	Deepu P	P	4	5	0	0	5	0	3	17	Understand
4AI22EC413	Indika. G	P	3	0	0	4	10	0	6	23	Understand
4AI22EC414	KANAKRAJ H R	P	0	4	0	0	0	0	4	8	No Level
4AI22EC415	KARANRAJ HR	P	4	5	0	0	0	6	7	16	Understand
4AI22EC418	Naveen H L	P	4	0	0	5	6	0	4	19	Understand
4AI22EC419	Pavan kumar C N	P	4	5	0	0	10	0	7	26	Understand
4AI22EC420	PUNITH R	P	4	0	0	0	5	0	7	16	Understand
4AI22EC423	Sandya M	P	4	5	0	0	6	6	7	22	Understand
4AI22EC424	Shashank K G	P	3	0	0	0	0	0	0	3	No Level
4AI22EC425	SHASHIKIRAN M	P	4	0	0	0	6	0	5	15	Understand
4AI22EC426	Sneha S V	P	3	5	0	0	0	7	0	15	Understand

2 Scheme of Evaluation

DEPT. OF ECE, AIT, Chikkamagaluru
I - INTERNAL ASSESSMENT
Subject: Cryptography (21EC642)
SCHEME & SOLUTIONS

Semester: 6
Max Marks: 40

Date: 14 Jun 2024

PART A
Answer any THREE full questions

Q. NO		MARKS	CO	BT/CL
1	**Explain using flowchart, the Euclidean algorithm to determine the GCD of two numbers. Find the GCD of (i) (24140,16762).(ii)(2152,764).**	10	CO1	L2

SOL :

Suppose we wish to determine the greatest common divisor d of the integers a and b; that is determine $d = \gcd(a, b)$. Because $\gcd(|a|, |b|) = \gcd(a, b)$, there is no harm in assuming $a \geq b > 0$.

Dividing a by b and applying the division algorithm, we can state

$$a = q_1 b + r_1 \qquad 0 \leq r_1 < b$$

First consider the case in which $r_1 = 0$. Therefore b divides a and clearly no larger number divides both b and a, because that number would be larger than b. So we have $d = \gcd(a, b) = b$.

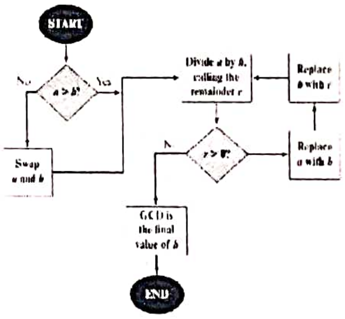
assume that $r_1 \neq 0$. Because $b > r_1$, we can divide b by r_1 and apply the division algorithm to obtain

$$b = q_2 r_1 + r_2 \qquad 0 \leq r_2 < r_1$$

As before, if $r_2 = 0$, then $d = r_1$ and if $r_2 \neq 0$, then $d = \gcd(r_1, r_2)$. Note that the remainders form a descending series of nonnegative values and so must terminate when the remainder is zero. This happens, say, at the $(n + 1)$th stage where r_{n-1} is divided by r_n. The result is the following system of equations:

$$\left.\begin{array}{ll} a = q_1 b + r_1 & 0 < r_1 < b \\ b = q_2 r_1 + r_2 & 0 < r_2 < r_1 \\ r_1 = q_3 r_2 + r_3 & 0 < r_3 < r_2 \\ \quad\vdots & \quad\vdots \\ r_{n-2} = q_n r_{n-1} + r_n & 0 < r_n < r_{n-1} \\ r_{n-1} = q_{n+1} r_n + 0 & \\ d = \gcd(a, b) = r_n & \end{array}\right\}$$

At each iteration, we have $d = \gcd(r_i, r_{i+1})$ until finally $d = \gcd(r_n, 0) = r_n$. Thus, we can find the greatest common divisor of two integers by repetitive application of the division algorithm. This scheme is known as the Euclidean algorithm.



(i) gcd(24140, 16762) = gcd(16762, 7378) = gcd(7378, 2006) = gcd(2006, 1360) = gcd(1360, 646) = gcd (646, 68) = gcd(68, 34) = gcd(34, 0) = 34

(ii) gcd(2152, 764) = gcd(764, 624) = gcd(624, 140) = gcd(140, 64) = gcd(64, 12) = gcd(12, 4) = gcd(4, 0) = 4

2	**a) Explain the properties of modular arithmetic for Integers in Z_n.** **b) Construct additive and multiplicative tables for arithmetic modulo 7 and tabulate the additive and multiplicative inverses.**	10	CO1	L2

(a) Define the set Z_n as the set of nonnegative integers less than n:

$$Z_n = \{0, 1, \ldots\ldots, (n - 1)\}$$

➢ If we perform modular arithmetic within Z_n, the properties shown in Table hold for integers in Z_n.

Property	Expression
Commutative Laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Associative Laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Distributive Law	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
Identities	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
Additive Inverse $(-w)$	For each $w \in Z_n$, there exists a z such that $w + z \equiv 0 \bmod n$

(b)

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Addition modulo 7

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Multiplication modulo 7

w	0	1	2	3	4	5	6
$-w$	0	6	5	4	3	2	1
w^{-1}	—	1	4	5	2	3	6

Additive and multiplicative inverses modulo 7

3	**Using Extended Euclidean Algorithm, find the multiplicative inverse of the following:** **(i) 17 mod 43** **(ii) $x^3 + x + 1$ in GF(2^4) with m(x) = $x^4 + x + 1$**	10	CO1	L2

Sol: (i) 17 mod 43

a mod b = 17 mod 43. Since a<b, swap a & b .Thus a = 43 & b = 17

i	r_i	q_i	$x_i = x_{i-2} - q_i x_{i-1}$	$y_i = y_{i-2} - q_i y_{i-1}$
-1	43		1	0
0	11		0	1
1	9	2	1	-2
2	8	1	-1	3
3	1	1	2	-5
4	0	8		

According to Extended Euclidean algorithm, ax+by = d=gcd(a,b) = 1

i.e. 43x + 17 y = 43*2 + 17*(-5) = 86 - 85 = 1

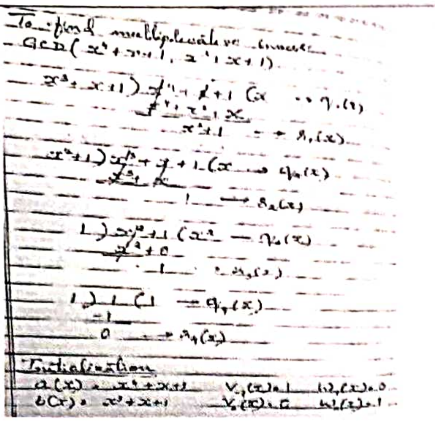
Therefore, b^{-1} = y implies $(17)^{-1}$ = -5

$(17)^{-1}$ mod 43 = -5 mod43 = -5+43 = 38.

(ii) $x^3 + x + 1$ in GF(2^4) with m(x) = $x^4 + x + 1$.

Given a(x) mod b(x) = ($x^3 + x + 1$) mod ($x^4 + x + 1$). Since b(x) is a higher degree polyno mial than a(x), swap a(x) with b(x).

Thus , a(x) = $x^4 + x + 1$ and b(x) = $x^3 + x + 1$



To find multiplicative inverse
GCD(x^4+x+1, x^3+x+1)

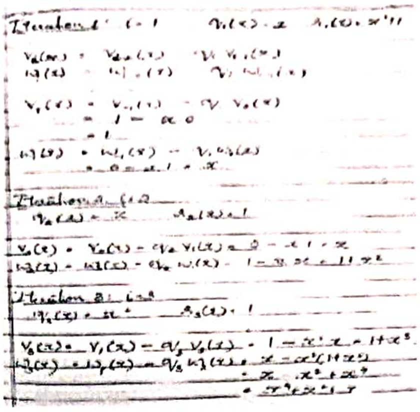
$x^3+x+1) \; x^4+x+1 \; (x \rightarrow q_1(x)$
x^4+x^2+x
$x^2+1 \rightarrow r_1(x)$

$x^2+1) \; x^3+x+1 \; (x \rightarrow q_2(x)$
x^3+x
$1 \rightarrow r_2(x)$

$1) \; x^2+1 \; (x^2 \rightarrow q_3(x)$
x^2+0
$1 \rightarrow r_3(x)$

$1) \; 1 \; (1 \rightarrow q_4(x)$
1
$0 \rightarrow r_4(x)$

Initialization
$a(x) = x^4+x+1$ $v_{-1}(x)=1$ $w_{-1}(x)=0$
$b(x) = x^3+x+1$ $v_0(x)=0$ $w_0(x)=1$



Iteration 1: $i=1$ $q_1(x)=x$ $r_1(x)=x^2+1$

$v_i(x) = v_{i-2}(x) - q_i v_{i-1}(x)$
$w_i(x) = w_{i-2}(x) - q_i w_{i-1}(x)$

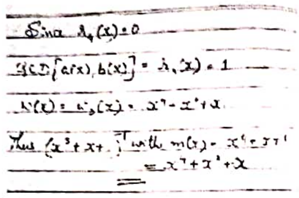
$v_1(x) = v_{-1}(x) - q_1 v_0(x)$
$= 1 - x \cdot 0$
$= 1$
$w_1(x) = w_{-1}(x) - q_1 w_0(x)$
$= 0 - x \cdot 1 = x$

Iteration 2: $i=2$
$q_2(x) = x$ $r_2(x)=1$

$v_2(x) = v_0(x) - q_2 v_1(x) = 0 - x \cdot 1 = x$
$w_2(x) = w_0(x) - q_2 w_1(x) = 1 - x \cdot x = 1+x^2$

Iteration 3: $i=3$
$q_3(x) = x^2$ $r_3(x) = 1$

$v_3(x) = v_1(x) - q_3 v_2(x) = 1 - x^2 \cdot x = 1+x^3$
$w_3(x) = w_1(x) - q_3 w_2(x) = x - x^2(1+x^2)$
$= x - x^2 + x^4$
$= x^4+x^2+x$



Since $r_4(x)=0$
$GCD[a(x), b(x)] = r_3(x) = 1$
$w(x) = w_3(x) = x^4-x^2+x$
Thus $(x^3+x+1)^{-1}$ with $m(x) = x^4+x+1$
$= x^4+x^2+x$

i	r_i	q_i	$v_i = v_{i-2} - q_i v_{i-1}$	$w_i = w_{i-2} - q_i w_{i-1}$
-1	$x^4 + x + 1$		1	0
0	$x^3 + x + 1$		0	1
1	x^2+1	x	1	x
2	1	x	x	x^2+1
3	1	x^2	x^3+1	$x^4 + x^2 + x$
4	0	1		

4.	(a) **Define Galois field. List all the axioms obeyed by GF.** (b) **Develop addition and multiplication tables based on polynomial arithmetic modulo for GF(4) with m(x) = $x^2 + x + 1$.**	10	CO1	L2

Sol: (a) The finite field of order p^n is Galois field, in honor of the mathematician who first studied finite fields. The order of a finite field must be **a power of a prime p^n**, where n is a positive integer.

For a given prime, p, we define the finite field of order p, GF(p), as the set Z_p of integers {0, 1,....,p - 1} together with the arithmetic operations modulo p.

For Z_p, it has to satisfy the following properties:

(A1) Closure under addition:	If a and b belong to S, then $a + b$ is also in S
(A2) Associativity of addition:	$a + (b + c) = (a + b) + c$ for all a, b, c in S
(A3) Additive identity:	There is an element 0 in R such that $a + 0 = 0 + a = a$ for all a in S
(A4) Additive inverse:	For each a in S there is an element $-a$ in S such that $a + (-a) = (-a) + a = 0$
(A5) Commutativity of addition:	$a + b = b + a$ for all a, b in S
(M1) Closure under multiplication:	If a and b belong to S, then ab is also in S
(M2) Associativity of multiplication:	$a(bc) = (ab)c$ for all a, b, c in S
(M3) Distributive laws:	$a(b + c) = ab + ac$ for all a, b, c in S $(a + b)c = ac + bc$ for all a, b, c in S
(M4) Commutativity of multiplication:	$ab = ba$ for all a, b in S
(M5) Multiplicative identity:	There is an element 1 in S such that $a1 = 1a = a$ for all a in S
(M6) No zero divisors:	If a, b in S and $ab = 0$, then either $a = 0$ or $b = 0$
(M7) Multiplicative inverse:	For each $w \in Z_p$, $w \neq 0$, there exists a $z \in Z_p$ such that $w \times z \equiv 1 \pmod p$

(b) Polynomial Arithmetic Modulo over GF(4) ¦ = GF(2²)¦ with m(x) $(x^2 + x + 1)$:

		000	001	010	011
	+	0	1	x	$x + 1$
000	0	0	1	x	$x + 1$
001	1	1	0	$x + 1$	x
010	x	x	$x + 1$	0	1
011	$x + 1$	$x + 1$	x	1	0

Addition

		000	001	010	011
	×	0	1	x	$x + 1$
000	0	0	0	0	0
001	1	0	1	x	$x + 1$
010	x	0	x	$x + 1$	1
011	$x + 1$	0	$x + 1$	1	x

Multiplication

5.	Obtain the field elements of GF(2⁴) using a generator polynomial x⁴ + x + 1. Give the equivalent binary and hexadecimal representation.	10	CO1	L2

GF(2⁴)

$f(x) = x^4 + x + 1$

$g^4 + g + 1 = 0$

Elements are $\{0, 1, g, g^2, g^3, g^4, g^5, g^6, g^7, g^8, g^9, g^{10}, g^{11}, g^{12}, g^{13}, g^{14}\}$

$g^4 = g + 1$

$g^5 = g(g+1) = g^2 + g$

$g^6 = g(g^2 + g) = g^3 + g^2$

$g^7 = g(g^3 + g^2) = g^4 + g^3 = g^3 + g + 1$

$g^8 = g(g^3 + g + 1) = g^4 + g^2 + g = g + 1 + g^2 + g = g^2 + 1$

$g^5 = g(g^2 + 1) = g^3 + g$

$g^{10} = g(g^3 + g) = g^4 + g^2 = g^2 + g + 1$

$g^{11} = g(g^2 + g + 1) = g^3 + g^2 + g$

$g^{12} = g(g^3 + g^2 + g) = g^4 + g^3 + g^2 = g + 1 + g^3 + g^2 = g^3 + g^2 + g + 1$

$g^{13} = g(g^3 + g^2 + g + 1) = g^4 + g^3 + g^2 + g = g + 1 + g^3 + g^2 + g$
$= g^3 + g^2 + 1$

$g^{14} = g(g^3 + g^2 + 1) = g^4 + g^3 + g = g + 1 + g^3 + g = g^3 + 1$

Power Representation	Polynomial Representation	Binary Representation	Decimal (Hex) Representation
0	0	0000	0
$g^0 (= g^{15})$	1	0001	1
g^1	g	0010	2
g^2	g^2	0100	4
g^3	g^3	1000	8

g^4	$g + 1$	0011	3
g^5	$g^2 + g$	0110	6
g^6	$g^3 + g^2$	1100	12
g^7	$g^3 + g + 1$	1011	11
g^8	$g^2 + 1$	0101	5
g^9	$g^3 + g$	1010	10
g^{10}	$g^2 + g + 1$	0111	7
g^{11}	$g^3 + g^2 + g$	1110	14
g^{12}	$g^3 + g^2 + g + 1$	1111	15
g^{13}	$g^3 + g^2 + 1$	1101	13
g^{14}	$g^3 + 1$	1001	9

PART B

Answer any ONE full question

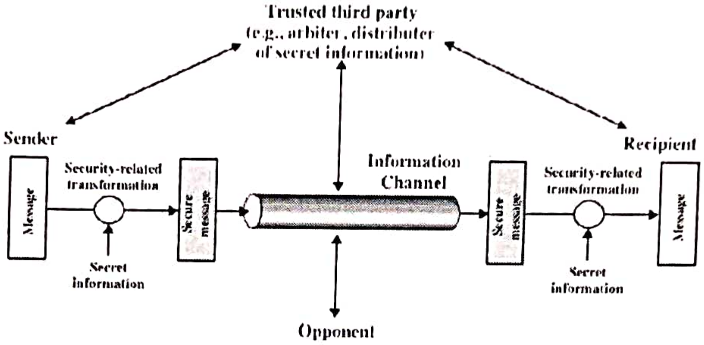
Q.NO		MARKS	CO	BT/CL
6	**Define Computer Security. Explain in brief, the challenges of computer security.**	10	CO2	L2
	The NIST *Computer Security Handbook* [NIST95] defines the term *computer security* as follows: • "The protection afforded to an automated information system to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)". • Computer Security Challenges 1. Security is not simple 2. Potential attacks on the security features need to be considered 3. Procedures used to provide particular services are often counter-intuitive. 4. It is necessary to decide where to use the various security mechanisms. 5. Requires constant monitoring 6. Is too often an afterthought 7. Security mechanisms typically involve more than a particular algorithm or protocol. 8. Security is essentially a battle of wits between a perpetrator and the designer 9. Little benefit from security investment is perceived until a security failure occurs. 10. Strong security is often viewed as an impediment to efficient and user-friendly operation			
7	**With neat block diagram, explain the model of network security. Also, list the 4 basic tasks in designing security services.**	10	CO2	L2
	A message is to be transferred from one party to another across some sort of Internet service. The two parties, called the principals, must cooperate for the exchange to take place. A logical information channel from source to destination and 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. EX : the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.			

- Some secret information shared by the two principals and, it is hoped, Unknown to the opponent.

EX : an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception

- A trusted third party may be needed to achieve secure transmission.

For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent. Or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.



This general model shows four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

Faculty :

Module Coordinator:

HOD :

ADICHUNCHANAGIRI INSTITUTE OF TECHNOLOGY

Department of Electronics & Communication Engineering (EC)

Internal : 2

Semester:6-CBCS 2021

Subject : CRYPTOGRAPHY (21EC642)

Faculty : Divya

Date : 05/07/2024

Time : 15:30 - 16:30

Max Marks: 40

Part A

Answer any 1 questions

Q.No		Max Marks	CO	BT/CL
1a	Explain with neat diagram the model of symmetric crypto system.	10	2	L2
1b	State the rules used for encryption in Playfair cipher. Construct a Playfair cipher for a key "AITCKM" and encrypt the message "ELECTRONICS AND COMMUNICATION".	10	2	L3
2a	Explain the Fiestel encryption and decryption process with its structure.	10	2	L2
2b	Explain the ShiftRows and Mixcolumns transformation techniques used in AES.	10	2	L2

Part B				
Answer all questions				
Q.No		Max Marks	CO	BT/CL
3a	Using Hill Cipher technique , encrypt and decrypt the plain text "ATTACK" using the key [2 3 ,3 6]	12	2	L3
3b	What is primitive root of a modulus? Given 3 as a primitive root of 19, construct a table of discrete logarithms. Or State and Prove Euler's theorem. Determine the Euler's totient function (i) (27), (ii) (231) and (iii) (440)	8	1	L2

Evaluation

USN	Name	Present (P) / Absent (Ab)	Q1		Q2		Q3		IA Total	BT/CL
			a	b	a	b	a	b		
4AI21EC001	Abhishek K M	P	4	0	0	0	11	0	15	Apply
4AI21EC002	Akanksha C	P	0	2	0	0	8	0	10	Apply
4AI21EC003	Ananya M	P	9	9	0	0	10	6	34	Apply
4AI21EC004	Ankith P	P	5	7	0	0	0	0	12	Apply
4AI21EC005	Ankush D D	P	0	0	0	0	0	0	0	No Level
4AI21EC006	Anusha A	P	8	9	0	0	12	3	32	Apply
4AI21EC007	Anushree J K	P	7	9	0	0	9	8	33	Apply
4AI21EC008	Ashwin Gowda S J	P	6	10	0	0	12	8	36	Apply
4AI21EC010	Benakesh S N	P	8	10	0	0	4	0	22	Apply
4AI21EC011	Bhavana H P	P	9	8	0	0	5	6	28	Apply
4AI21EC012	Bhoomika B C	P	0	0	6	6	9	7	28	Apply
4AI21EC013	Bhumika D M	P	10	10	0	0	12	6	38	Apply
4AI21EC014	Bibi Swagra	P	10	10	0	0	12	8	40	Apply
4AI21EC015	Chaitanya J	P	7	9	0	0	6	2	24	Apply
4AI21EC016	Chethan L P	P	8	10	0	0	10	7	35	Apply
4AI21EC017	Chandana K	P	8	7	0	0	9	7	31	Apply
4AI21EC018	Chandan Patil C S	P	7	7	0	0	12	7	33	Apply
4AI21EC019	CHANDRAKANTH S M	P	8	5	0	0	9	0	22	Apply
4AI21EC020	Chethan N M	P	9	6	0	0	10	4	29	Apply
4AI21EC021	Darshan S	P	7	2	0	0	4	0	13	Understand
4AI21EC022	Darshan B	P	7	9	0	0	9	4	29	Apply

USN	Name	Present (P) / Absent (Ab)	Q1		Q2		Q3		IA Total	BT/CL
			a	b	a	b	a	b		
4AI21EC023	Deeksha K B	P	5	3	2	0	5	3	16	Understand
4AI21EC024	Deeksha K R	P	7	7	0	0	11	5	30	Apply
4AI21EC025	Deepak M S	P	6	5	0	0	5	5	21	Apply
4AI21EC027	Deepakraj R B	P	6	2	0	0	9	4	21	Apply
4AI21EC028	DHANUSH GOWDA H	P	7	8	0	0	4	5	24	Apply
4AI21EC031	Gowtham B G	P	6	8	0	0	6	0	20	Apply
4AI21EC033	Jeevan R M	P	7	5	0	0	9	4	25	Apply
4AI21EC034	Karthikeyan j	P	7	3	0	0	1	0	11	Understand
4AI21EC035	Kavana K S	P	8	9	0	0	9	5	31	Apply
4AI21EC036	Keerthana L S	P	0	0	6	0	4	5	15	Understand
4AI21EC037	Likhith S V	P	8	8	0	0	4	6	26	Apply
4AI21EC038	Likitha C M	P	0	0	6	7	5	4	22	Understand
4AI21EC040	Manjushree K S	P	4	3	5	7	5	0	17	Understand
4AI21EC042	Manupatel S P	P	9	10	0	0	4	0	23	Apply
4AI21EC043	Manya U	P	7	5	0	0	8	0	20	Apply
4AI21EC044	Meghana R	P	8	8	0	0	7	4	27	Apply
4AI21EC045	Mohammed Wasib	P	7	0	0	0	6	4	17	Apply
4AI21EC046	Nakul P M	P	8	7	0	0	10	8	33	Apply
4AI21EC047	Neha G M	P	4	7	0	0	6	3	20	Apply
4AI21EC048	Nidhi K M	P	8.5	8	0	0	4	3.5	24	Apply
4AI21EC049	Niranjan G M	P	9	10	0	0	8	0	27	Apply
4AI21EC050	Nishanth Gowda V S	P	6	2	0	0	4	3	15	Understand
4AI21EC051	Nishchitha M	P	7	10	0	0	4	8	29	Apply
4AI21EC052	Pavan Kumar	P	8	5	0	0	12	0	25	Apply

USN	Name	Present (P) / Absent (Ab)	Q1		Q2		Q3		IA Total	BT/CL
			a	b	a	b	a	b		
4AI21EC053	Pooja H H	P	6	8	0	0	4	7	25	Apply
4AI22EC400	Arpitha C S	P	8	4	0	0	9	4	25	Apply
4AI22EC402	AVINASH.H.R	P	6	7	0	0	7	0	20	Apply
4AI22EC406	CHETHAN V	P	7	8	0	0	6	0	21	Apply
4AI22EC407	Dayananda H L	P	6	0	0	0	6	0	12	Apply
4AI22EC408	Deepu P	P	6	8	0	0	0	4	18	Apply
4AI22EC413	Indika. G	P	0	0	6	8	4	4	22	Understand
4AI22EC414	KANAKRAJ H R	P	5	0	0	0	9	0	14	Apply
4AI22EC415	KARANRAJ HR	P	0	0	0	0	3	3	6	No Level
4AI22EC418	Naveen H L	P	4	4	0	0	11	0	19	Apply
4AI22EC419	Pavan kumar C N	P	8	10	0	0	12	6	36	Apply
4AI22EC420	PUNITH R	P	5	3	0	0	9	0	17	Apply
4AI22EC423	Sandya M	P	4	5	0	0	4	1	14	Apply
4AI22EC424	Shashank K G	P	6	7	0	0	0	0	13	Apply
4AI22EC425	SHASHIKIRAN M	P	6	7	0	0	0	0	13	Apply
4AI22EC426	Sneha S V	P	5	1	0	0	4	4	14	Understand

2 Scheme of Evaluation

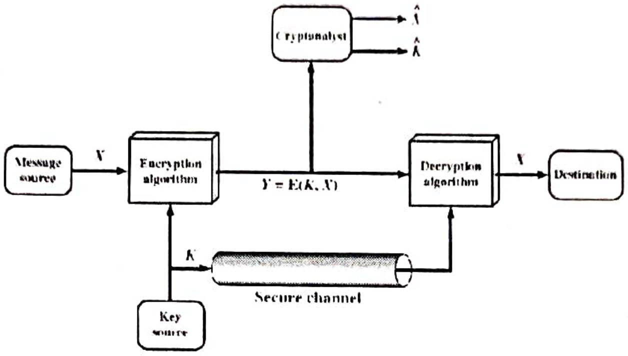
DEPT. OF ECE, AIT, Chikkamagaluru
Subject: Cryptography (21EC642)
II - INTERNAL ASSESSMENT SCHEME & SOLUTIONS

Semester: 6
Max Marks: 40

Date: 05 Jul 2024
Time: 3:30PM - 4:30 PM

PART A
Answer any one full question

Q.No			Marks	CO	BT/CL
1	a	Explain with neat diagram the model of symmetric crypto system.	10	CO2	L2



Model of Symmetric Cryptosystem

FIGURE - 4M
EXPLANATION - 6M

- A source produces a message in plain text, $X=\{X_1,X_2,...X_M\}$.
- The M elements of X are letters in some finite alphabet.
- Nowadays, X={0,1} is typically used.
- For encryption, a key of the form $K=[K_1, K_2, ...K_J]$ is generated.
- If the key is generated at the message source, then it must also be provided to the destination by means of some secure channel. Alternatively, a third party could generate the key and securely deliver it to both source and destination.
- With the message X and the encryption key K as input, the encryption algorithm forms the ciphertext $Y=[Y_1, Y_2, ...Y_N]$
- Y=E(K,X) indicates Y is produced by using encryption algorithm E as a function of the plaintext X with the specific function determined by the value of the key K.
- The intended receiver is able to invert the transformation, X=D(K,Y).
- An opponent, observing Y but not having access to K or X, may attempt to recover X or K or both X and K by generating estimate $\hat{X}$and $\hat{K}$.

			Marks	CO	BT/CL
1	b	State the rules used for encryption in Playfair cipher. Construct a Playfair cipher for a key "AITCKM" and encrypt the message "ELECTRONICS AND COMMUNICATION".	10	CO2	L2

Sol: **Playfair Cipher:** - 4M

- Based on the use of a 5 x 5 matrix of letters constructed using a keyword.
- Fill in letters of keyword (minus duplicates) from left to right and from top to bottom, then fill in the remainder of the matrix with the remaining letters in alphabetic order
- Plaintext is encrypted two letters at a time, according to the following rules:
  - If a pair is a repeated letter, insert filler like 'X'.
  - If both letters fall in the same row, replace each with the letter to its right (circularly).
  - If both letters fall in the same column, replace each with the letter below it (circularly).
  - Otherwise, each letter is replaced by the letter in the same row but in the column of the other letter of the pair.

Given Keyword : AITCKM Plaintext : ELECTRONICS AND COMMUNICATION

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

Matrix - 2M

Cipher text - 4M

Digrams	EL	EC	TR	ON	IC	SA	ND	CO	MX	MU	NI	CA TI	ON
Cipher text	DN	NE	DX	GO	TK	PC	LE	KN	DV	FP	HC	KI/J CT	GO

2	a	Explain the Fiestel encryption and decryption process with its structure.	10	CO2	L2

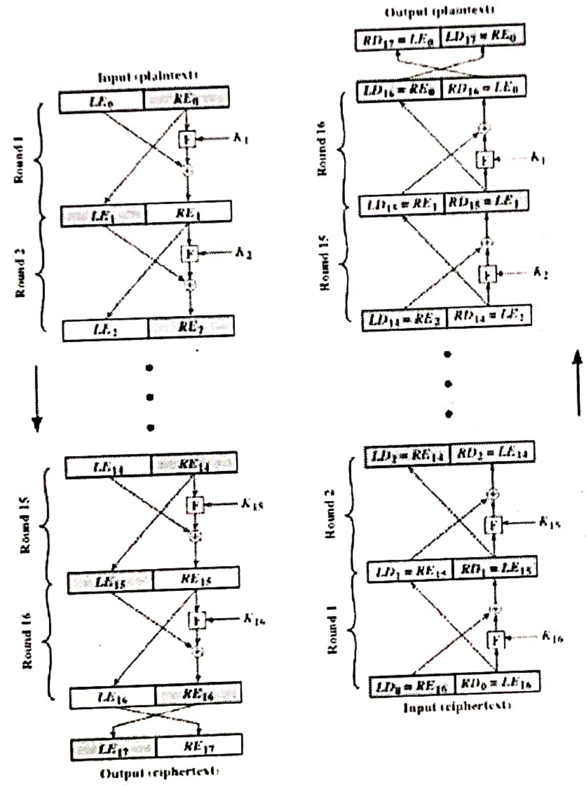


FIGURE - 5M
EXPLANATION - 5M

- The inputs to the encryption algorithm are a plaintext block of length 2w bits and a key K.
- The plaintext block is divided into two halves, LE_0 and RE_0
- The two halves of the data pass through n rounds of processing and then combine to produce the ciphertext block.
- Each round i has as inputs LE_{i-1} and RE_{i-1} derived from the previous round, as well as a subkey K_i derived from the overall K.
- All rounds have the same structure.

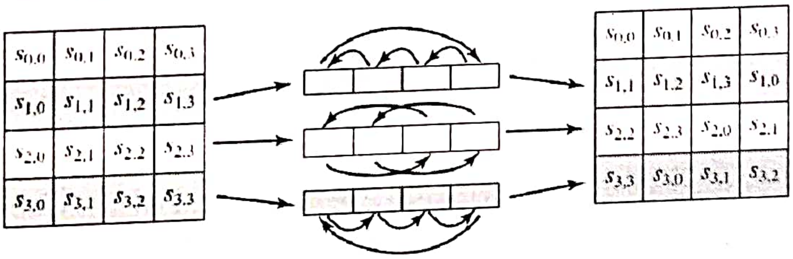
- A substitution is performed on the left half of the data
- This is done by applying a round function F to the right half of the data and then the output is exclusive-ORed with the left half of the data.
- F is a function of right-half block of w bits and a subkey of y bits, which produces an output value of length w bits: $F(RE_i, K_{i+1})$
- Then permutation is performed that consists of the interchange of the two halves of the data.
- This structure is a particular form of the substitution-permutation network (SPN) proposed by Shannon.
- The decryption process is same as the encryption process.
- Use the ciphertext as input to the algorithm, but use the subkeys K_i in reverse order. That is, use K_n in the first round, K_{n-1} in the second round, and so on, until K_1 is used in the last round.
- At every round, the intermediate value of the decryption process is equal to the corresponding value of the encryption process with the two halves of the value swapped.
- The output of the ith encryption round be $LE_i || RE_i$. Then the corresponding output of the $(16 - i)^{th}$ decryption round is $Re_i || LE_i$ or, equivalently, $LD_{16-i} || RD_{16-i}$.

2 B Explain the ShiftRows and Mixcolumns transformation techniques used in AES. 10 CO2 L2

Sol:

ShiftRows Transformation - 5M

- The forward shift row transformation called ShiftRows
  - The first row of State is not altered.
  - For the second row, a 1-byte circular left shift is performed.
  - For the third row, a 2-byte circular left shift is performed.
  - For the fourth row, a 3-byte circular left shift is performed.
- The inverse shift row transformation, called InvShiftRows, performs the circular shifts in the opposite direction for each of the last three rows.


$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,1}$ $s_{1,2}$ $s_{1,3}$ $s_{1,0}$
$s_{2,2}$ $s_{2,3}$ $s_{2,0}$ $s_{2,1}$
$s_{3,3}$ $s_{3,0}$ $s_{3,1}$ $s_{3,2}$

MixColumns Transformation - - 5M

- **The forward mix column transformation**, called MixColumns, operates on each column individually.
- Each byte of a column is mapped into a new value that is a function of all four bytes in that column.
- The transformation can be defined by the following matrix multiplication on State

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} = \begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix}$$

- The individual additions and multiplications are performed in $GF(2^8)$.

- The inverse mix column transformation, called InvMixColumns, is defined by the following matrix multiplication:

$$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} = \begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix}$$

PART B

Answer the question

Q.No			Marks	CO	BT/CL
3	a	Using Hill Cipher technique, encrypt and decrypt the plain text "ATTACK" using the key $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$	12	CO2	L2

Sol:

Encryption:

Plaintext	A	T	T	A	C	K
values	00	19	19	00	02	10

C = P K mod26

$[C_1 \quad C_2] = [00 \quad 19]\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} = [57 \quad 114]$ mod26 = $[05 \quad 10]$ =[F K]

$[C_3 \quad C_4] = [19 \quad 00]\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} = [38 \quad 57]$ mod26 = $[12 \quad 05]$ = [M F]

Encryption - 4M

$[C_5 \quad C_6] = [02 \quad 10]\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} = [34 \quad 66]$ mod26= $[08 \quad 14]$ = [I O]

Cipher text : FKMFIO

Decryption:

P = C K^{-1} mod26 $K^{-1} = (\det k)^{-1}\, adj\, K$ det K = (2X6)-(3X3) = 12-9= 3

$(\det k)^{-1}\, mod26$ = 3^{-1}mod26

Using Extended Euclidean algorithm to determine the multiplicative inverse of 3 mod26

i	r_i	q_i	$x_i = x_{i-2} - q_i\, x_{i-1}$	$y_i = y_{i-2} - q_i\, y_{i-1}$
-1	26		1	0
0	3		0	1
1	2	8	1	-8
2	1	1	-1	9

Inverse matrix calculation - 4M

$(\det k)^{-1}\, mod26$ = 3^{-1}mod26 = 9

$K^{-1} = (\det k)^{-1}\, adj\, K = 9\begin{bmatrix} 6 & -3 \\ -3 & 2 \end{bmatrix}$mod26 = $\begin{bmatrix} 54 & -27 \\ -27 & 18 \end{bmatrix}$ mod26 = $\begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix}$

$[P_1 \quad P_2] = [05 \quad 10]\begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} = [260 \quad 305]$ mod26 = $[00 \quad 19]$ =[A T]

Decryption - 4M

$[P_3 \quad P_4] = [12 \quad 05]\begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} = [149 \quad 390]$ mod26 = $[19 \quad 00]$ = [T A]

$[P_5 \quad P_6] = [08 \quad 14]\begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} = [366 \quad 452]$ mod26 = $[02 \quad 10]$ = [C K]

Decrypted or Diciphered text = ATTACK. Plaintext & decrypted text are the same.

3	b	**What is primitive root of a modulus? Given 3 as a primitive root of 19, construct a table of discrete logarithms.**	8	CO1	L2

Sol:

A primitive root of a prime number p is one whose powers modulo p generate all the integers from 1 to p - 1. That is, if a is a primitive root of the prime number p, then the numbers a mod p, a^2 mod p, ….. a^{p-1} mod p are distinct and consist of the integers from 1 through p - 1 in some permutation.

2M

For any integer a and a primitive root b of prime number p, we can find a unique exponent i such that $a \equiv b^i (\bmod p)$ where $0 \leq i \leq (p - 1)$.
This exponent i is referred to as the **discrete logarithm** of the number a for the base b (mod p) denoted as $dlog_{b,p}(a)$.
Thus, given b = 3 and p=19

i= (Log$_{a,p}$ (b))	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
a= 3^imod 19	3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1

6M

Discrete logarithms to the base 3, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$log_{3,19}(a)$	18	7	1	14	4	8	6	3	2	11	12	15	17	13	5	10	16	9

OR

3	b	**State and Prove Euler's theorem. Determine the Euler's totient function (i) Φ(27), (ii) Φ(231) and (iii) Φ(440)**	8	CO1	L2

Sol:

Euler's theorem
For every a and n that are relatively prime: $a^{\phi(n)} \equiv 1 (mod\ n)$
PROOF:
ϕ(n) is the number of positive integers less than n that are relatively prime to n.
Consider the set of such integers, labeled as
$R = \{x_1, x_2, ... , x_{\phi(n)}\}$
That is, each element x_i of R is a unique positive integer less than n with gcd(x_i,n) = 1.
Now multiply each element by a *modulo n*:
$S = \{(ax_1 \bmod n), (ax_2 \bmod n), ... , (ax_{\phi(n)} \bmod n)\}$
The set S *is a permutation of R* for the reasons:

1. Because a is relatively prime to n and x_i is relatively prime to n, ax_i must also be relatively prime to n. Thus, all the members of S are integers that are less than n and that are relatively prime to n.
2. There are no duplicates in S. If $ax_i \bmod n = ax_j \bmod n$, then $x_i = x_j$.

Therefore,

$$\prod_{i=1}^{\phi(n)} (ax_i \bmod n) = \prod_{i=1}^{\phi(n)} x_i$$

$$\prod_{i=1}^{\phi(n)} ax_i \equiv \prod_{i=1}^{\phi(n)} x_i \pmod n$$

$$a^{\phi(n)} \times \left[\prod_{i=1}^{\phi(n)} x_i\right] \equiv \prod_{i=1}^{\phi(n)} x_i \pmod n$$

$$a^{\phi(n)} \equiv 1 \pmod n$$

Statement - 1M
Proof - 4M

- An alternative form of the theorem is also useful:
$a^{\phi(n)+1} \equiv a(mod\ n)$

	NOTE: The first form of Euler's theorem requires that *a* be relatively prime to n, but this form does not. i. $\phi(27) = \phi(3^3) = 3^3 - 3^2 = 27 - 9 = 18$ ii. $\phi(231) = \phi(3) \times \phi(7) \times \phi(11) = 2 \times 6 \times 10 = 120$ iii. $\phi(440) = \phi(2^3) \times \phi(5) \times \phi(11) = (2^3 - 2^2) \times 4 \times 10 = 160$	1M X 3 = 3M

Faculty : 6/7/24

Module Coordinator:

HOD : 6/8/24

Part B

Answer all questions

Q.No		Max Marks	CO	BT/CL
3a	Perform encryption and decryption using the RSA algorithm, given,p = 3; q = 11, e = 7; M = 5	5	3	L2
3b	Users A and B use the Diffie-Hellman key exchange technique with a common prime q = 71 and a primitive root a = 7. a. If A's private key is 5, what is A's public key ? b. If B's private key is 12, what is B's public key ?	5	3	L2
4	Explain the following algorithms : a) A5 b) Rambutan	10	4	L2
5	Explain the following additive generators : a)Fish b)Mush	10	4	L2

Evaluation

USN	Name	Present (P) / Absent (Ab)	Q1		Q2	Q3		Q4	Q5	IA Total	BT/CL
			a	b		a	b				
4AI21EC001	Abhishek K M	P	0	0	5	0	0	5	6	16	Understand
4AI21EC002	Akanksha C	P	0	0	0	2	0	1	0	3	No Level
4AI21EC003	Ananya M	P	0	0	10	3	3	10	10	36	Understand
4AI21EC004	Ankith P	P	0	0	8	1	4	10	0	23	Understand
4AI21EC005	Ankush D D	P	0	0	0	0	5	3	3	11	Understand
4AI21EC006	Anusha A	P	0	0	9	5	3	4	10	31	Understand
4AI21EC007	Anushree J K	P	3	4	0	5	2	8	9	31	Understand
4AI21EC008	Ashwin Gowda S J	P	0	0	7	5	5	0	0	17	Understand
4AI21EC010	Benakesh S N	P	0	0	10	5	4	9	9	37	Understand
4AI21EC011	Bhavana H P	P	0	0	10	5	5	7	5	32	Understand
4AI21EC012	Bhoomika B C	P	0	0	0	3	3	10	7	23	Understand
4AI21EC013	Bhumika D M	P	0	0	10	5	5	8	8	36	Understand
4AI21EC014	Bibi Swagra	P	0	0	10	5	5	10	10	40	Understand
4AI21EC015	Chaithanya J	P	0	0	8	5	3	8	0	24	Understand
4AI21EC016	Chaithra L P	P	0	0	10	5	3	10	9	37	Understand
4AI21EC017	Chandana K	P	5	0	10	5	3	10	10	38	Understand
4AI21EC018	Chandana Patil C S	P	0	0	10	2	5	6	6	29	Understand
4AI21EC019	CHANDRAKANTH S M	P	3	1	0	5	5	3	10	27	Understand
4AI21EC020	Chethan N M	P	5	0	9	5	5	10	5	34	Understand
4AI21EC021	Darshan S	P	0	0	7	4	0	9	7	27	Understand
4AI21EC022	Darshini B	P	0	0	8	5	4	9	10	36	Understand

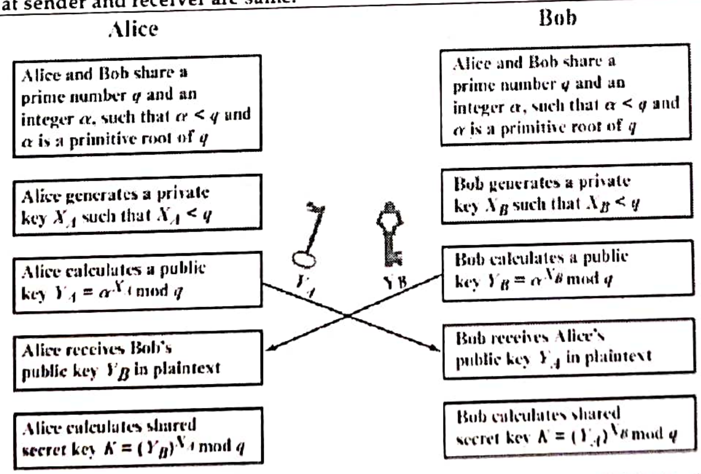
USN	Name	Present (P) / Absent (Ab)	Q1		Q2	Q3		Q4	Q5	IA Total	BT/CL
			a	b		a	b				
4AI21EC023	Deeksha K B	P	0	0	8	3.5	3	9.5	10	34	Understand
4AI21EC024	Deeksha K R	P	0	0	10	5	5	5	10	35	Understand
4AI21EC025	Deepak M S	P	0	0	0	5	2	7	8	22	Understand
4AI21EC027	Deepakraj R B	P	0	0	0	5	3	9	8	25	Understand
4AI21EC028	DHANUSH GOWDA H	P	0	4	0	0	0	10	10	24	Understand
4AI21EC031	Gowtham B G	P	4	0	7	5	0	7	9	28	Understand
4AI21EC033	Jeevan R M	P	0	0	7	0	2	10	7	26	Understand
4AI21EC034	Karthikeyan.j	P	3	0	0	4	0	4	8	19	Understand
4AI21EC035	Kavana K S	P	0	0	10	3	5	6	10	34	Understand
4AI21EC036	Keerthana L S	P	0	0	9	0	0	6	7	22	Understand
4AI21EC037	Likhith S V	P	3	0	0	5	2	10	8	28	Understand
4AI21EC038	Likitha C M	P	0	0	0	5	3	7	7	22	Understand
4AI21EC040	Manjushree K S	P	0	0	7	5	4	1	2	19	Understand
4AI21EC042	Manupatel S P	P	5	0	0	2	0	10	10	27	Understand
4AI21EC043	Manya U	P	0	0	10	3	5	8	9	35	Understand
4AI21EC044	Meghana R	P	0	0	6	3	5	4	8	26	Understand
4AI21EC045	Mohammed Wasib	P	0	0	0	5	4	10	10	29	Understand
4AI21EC046	Nakul P M	P	4	5	0	5	2	10	10	36	Understand
4AI21EC047	Neha G M	P	0	0	7	5	4	7	7	30	Understand
4AI21EC048	Nidhi K M	P	0	0	10	5	2	9	8	34	Understand
4AI21EC049	Niranjan G M	P	0	0	10	5	5	10	8	38	Understand
4AI21EC050	Nishanth Gowda V S	P	0	0	5	0	0	8	6	19	Understand
4AI21EC051	Nishchitha M	P	0	0	4	5	4	10	10	33	Understand
4AI21EC052	Pavan Kumar	P	5	0	0	5	3	8	6	27	Understand

USN	Name	Present (P) / Absent (Ab)	Q1		Q2	Q3		Q4	Q5	IA Total	BT/CL
·			a	b		a	b				
4AI21EC053	Pooja H H	P	0	0	10	5	4	10	10	39	Understand
4AI22EC400	Arpitha C S	P	0	0	8	5	5	9	10	37	Understand
4AI22EC402	AVINASH.H.R	P	0	0	7	2	0	7	7	23	Understand
4AI22EC406	CHETHAN V	P	0	0	5	1	0	10	10	26	Understand
4AI22EC407	Dayananda H L	P	0	0	9	1	0	8	8	26	Understand
4AI22EC408	Deepu P	P	0	0	9	0	0	6	6	21	Understand
4AI22EC413	Indika. G	P	0	0	4	1	4	7	2	18	Understand
4AI22EC414	KANAKRAJ H R	P	0	0	3	2	0	7	7	19	Understand
4AI22EC415	KARANRAJ HR	P	5	4	0	0	0	7	6	22	Understand
4AI22EC418	Naveen H L	P	0	0	8	1	0	7	7	23	Understand
4AI22EC419	Pavan kumar C N	P	0	0	8	5	5	8	10	36	Understand
4AI22EC420	PUNITH R	P	3	1	2	0	0	10	10	24	Understand
4AI22EC423	Sandya M	P	4	2	0	0	0	7	7	20	Understand
4AI22EC424	Shashank K G	P	0	0	2	4	3	9	7	25	Understand
4AI22EC425	SHASHIKIRAN M	P	0	0	7	5	5	8	0	25	Understand
4AI22EC426	Sneha S V	P	3	0	7	0	0	8	6	21	Understand

2 Scheme of Evaluation

DEPT. OF ECE, AIT, Chikkamagaluru
III - INTERNAL ASSESSMENT
Subject: Cryptography (21EC642)
SCHEME AND SOLUTIONS

PART A
Answer any one full question

Q.NO			MARKS	CO	BT/CL
1	a	List the requirements to be fulfilled for the Public key cryptography.	5	CO3	L2
SOL:		Requirements for Public-Key Cryptography 5M • It is computationally easy for a party B to generate a pair (public-key PU_b, private key PR_b) • It is computationally easy for a sender A, knowing the public key and the message to be encrypted, to generate the corresponding ciphertext. C = E(PU_b, M) • It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message. M = D(PR_b, C) = D[PR_b, E(PU_b, M)] • It is computationally infeasible for an adversary, knowing the public key, to determine the private key. • It is computationally infeasible for an adversary, knowing the public key and a ciphertext, to recover the original message, M. • The two keys can be applied in either order M = D[PU_b, E(PR_b, M)] = D[PR_b, E(PU_b, M)]			
1	b	Explain the five possible approaches to attack the RSA algorithm	5	CO3	L2
SOL:		Five possible approaches to attacking the RSA algorithm are 5M ■ **Brute force:** This involves trying all possible private keys. ■ **Mathematical attacks:** There are several approaches, all equivalent in effort to factoring the product of two primes. ■ **Timing attacks:** These depend on the running time of the decryption algorithm. ■ **Hardware fault-based attack:** This involves inducing hardware faults in the processor that is generating digital signatures. ■ **Chosen ciphertext attacks:** This type of attack exploits properties of the RSA algorithm.			
2		Explain Diffie-Hellman Key exchange algorithm. Show that the keys generated at sender and receiver are same.	10	CO3	L2
SOL:		 FIGURE -5M			

Alice
Bob
Alice and Bob share a prime number q and an integer α, such that $\alpha < q$ and α is a primitive root of q
Alice and Bob share a prime number q and an integer α, such that $\alpha < q$ and α is a primitive root of q
Alice generates a private key X_A such that $X_A < q$
Bob generates a private key X_B such that $X_B < q$
Y_A
YB
Alice calculates a public key $Y_A = \alpha^{X_A} \bmod q$
Bob calculates a public key $Y_B = \alpha^{X_B} \bmod q$
Alice receives Bob's public key Y_B in plaintext
Bob receives Alice's public key Y_A in plaintext
Alice calculates shared secret key $K = (Y_B)^{X_A} \bmod q$
Bob calculates shared secret key $K = (Y_A)^{X_B} \bmod q$

- There are two publicly known numbers: a prime number q and an integer a that is a primitive root of q
- User A selects a random integer $X_A < q$ and computes $Y_A = a^{X_A} \bmod q$
- Similarly, user B independently selects a random integer $X_B < q$ and computes $Y_B = a^{X_B} \bmod q$
- Each side keeps the X value private and makes the Y value available publicly to the other side. Thus, X_A is A's private key and Y_A is A's corresponding public key, and similarly for B
- User A computes the key as $K = (Y_B)^{X_A} \bmod q$ and user B computes the key as $K = (Y_A)^{X_B} \bmod q$
- These two calculations produce identical results:

$$\begin{aligned} K &= (Y_B)^{X_A} \bmod q \\ &= \left(a^{X_B} \bmod q\right)^{X_A} \bmod q \\ &= (a^{X_B})^{X_A} \bmod q \\ &= a^{X_B X_A} \bmod q \\ &= (a^{X_A})^{X_B} \bmod q \\ &= \left(a^{X_A} \bmod q\right)^{X_B} \bmod q \\ &= (Y_A)^{X_B} \bmod q \end{aligned}$$

EXPLANATION – 2M

DERIVATION – 3M

- The result is that the two sides have exchanged a secret value
- This secret value is used as shared symmetric secret key

PART B

Answer all the questions

Q.NO			MARKS	CO	BT/CL
3	a	**Perform encryption and decryption using the RSA algorithm, given ,** $p = 3; q = 11, e = 7; M = 5$	5	CO3	L2
SOL:		n=pxq = 3x11 = 33 ϕ(n) = ϕ(pq) = (p-1) x (q-1) = 2 x 10 =20 0.5 M d ≡ e⁻¹ mod(ϕ(n)) = 7⁻¹ mod(20) = 3 1.5 M C = Mᵉ mod(n) = 5⁷ mod 33 = 14 1.5M M = Cᵈ mod (n) = 14³ mod 33 = 5 1.5M			
3	b	**Users A and B use the Diffie-Hellman key exchange technique with a common prime q = 71 and a primitive root α = 7.** a. **If A's private key is 5, what is A's public key?** b. **If B's private key is 12, what is B's public key ?** c. **What is the shared secret key?**	5	CO3	L2
SOL:		Given $X_A = 5$, $X_B = 12$, $q = 71$,$a = 7$ a. $Y_A = a^{X_A} \bmod q = 7^5 \bmod 71 = 51$ - 1.5M b. $Y_B = a^{X_B} \bmod q = 7^{12} \bmod 71 = 4$ -1.5M c. $K = (Y_B)^{X_A} \bmod q = 4^5 \bmod 71 = 30$ or -2M $K = (Y_A)^{X_B} \bmod q = 51^{12} \bmod 71 = 30$			
4		**Explain the following algorithms : a)A5 b)Rambutan**	10	CO4	L2
SOL:		**a) A5** • The stream cipher used to encrypt GSM. • It is used to encrypt the link from the telephone to the base station. The rest of the link is unencrypted; the telephone company can easily eavesdrop on the conversations. • A5 consists of three LFSRs; the register lengths are 19, 22, and 23; all the feedback polynomials are sparse. • The output is the XOR of the three LFSRs. • A5 uses variable clock control. • Each register is clocked based on its own middle bit, XORed with the inverse threshold function of the middle bits of all three registers. Usually, two of the LFSRs clock in each round. • Its only known weakness is that its registers are short enough to make exhaustive search feasible	- 5M		

b) **Rambutan** - 5M

- A British algorithm, designed by the Communications Electronics Security Group
- It is only sold as a hardware module.
- The algorithm itself is secret, and the chip is not generally commercially available.
- Rambutan has a 112-bit key (plus parity bits) and can operate in three modes. ECB(Electronic CodeBook), CBC(Cipher Block Chain), and 8-bit CFB(Cipher FeedBack).
- It has five shift registers, each one of a different length around 80 bits.
- The feedback polynomials are fairly sparse, with only about 10 taps each.
- Each shift register provides four inputs to a very large and complex nonlinear function which eventually spits out a single bit.

5	**Explain the following additive generators : a)Fish b)Mush**	10	CO4	L2

SOL:

a)Fish - 5M

- Fish is an additive generator based on techniques used in the shrinking generator.
- It produces a stream of 32-bit words which can be XORed with a plaintext stream to produce ciphertext, or XORed with a ciphertext stream to produce plaintext.
- The algorithm is named as it is because it is a Fibonacci shrinking generator.
- Two additive generators are used. The key is the initial values of these generators.

$$A_i = (A_{i-55} + A_{i-21}) \bmod 2^{32}$$
$$B_i = (B_{i-52} + B_{i-19}) \bmod 2^{32}$$

- These sequences are shrunk, as a pair, depending on the least significant bit of B_i if it is 1, use the pair; if it is 0, ignore the pair.
- C_j is the sequence of used words from A_i, and D_j is the sequence of used words from B_i.
- These words are used in pairs—C_{2j}, C_{2j-1}, D_{2j}, and D_{2j+1}—to generate two 32-bit output words: K_{2j} and K_{2j+1}.

$$E_{2j} = C_{2j} \oplus (D_{2j} \quad D_{2j+1})$$
$$F_{2j} = D_{2j+1} \quad (E_{2j} \quad C_{2j-1})$$
$$K_{2j} = E_{2j} \oplus F_{2j}$$
$$K_{2j-1} \quad C_{2j+1} \oplus F_{2j}$$

- This algorithm is fast.
- On a 33 megahertz 486, a C implementation of Fish encrypts data at 15 megabits per second.
- Unfortunately, it is also insecure.

b)Mush - 5M

- Mush is a mutual shrinking generator.
- Take two additive generators: A and B.
- If the carry bit of A is set, clock B. If the carry bit of B is set, clock A.
- Clock A, and set the carry bit if there is a carry.
- Clock B, and set the carry bit if there is a carry.
- The final output is the XOR of the output of A and B.
- The easiest generators to use are the ones from Fish:

$$A_i = (A_{i-55} + A_{i-21}) \bmod 2^{32}$$
$$B_i = (B_{i-52} + B_{i-19}) \bmod 2^{32}$$

- On the average, three generator iterations are required to produce one output word.
- If the coefficients of the additive generators are chosen correctly and are relatively prime, the output sequence will be maximal length.

Faculty : 24/1/2024

Module Coordinator:

HOD :

Professor & Head
Dept. of Electronics & Communication Engg.
Adichunchanagiri Institute of Technology.
Chikmagalur - 577 102