



**KSIT BANGALORE**

**DEPARTMENT OF ELECTRONICS & COMMUNICATION  
ENGINEERING**

**COURSE FILE**

**NAME OF THE STAFF : V.SANGEETHA**

**COURSE CODE/NAME : 21EC642-CRYPTOGRAPHY**

**SEMESTER/YEAR : VI/III**

**ACADEMIC YEAR : 2023 – 2024**

**BRANCH : ECE (B)**

  
**COURSE IN-CHARGE**

  
**HOD**



# K. S. INSTITUTE OF TECHNOLOGY

## VISION

“ To impart quality technical education with ethical values, employable skills and research to achieve excellence”.

## MISSION

- To attract and retain highly qualified, experienced & committed faculty.
- To create relevant infrastructure.
- Network with industry & premier institutions to encourage emergence of new ideas by providing research & development facilities to strive for academic excellence.
- To inculcate the professional & ethical values among young students with employable skills & knowledge acquired to transform the society.



## K.S. INSTITUTE OF TECHNOLOGY

### DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

#### VISION:

“To achieve excellence in academics and research in Electronics & Communication Engineering to meet societal need”.

#### MISSION:

- To impart quality technical education with the relevant technologies to produce industry ready engineers with ethical values.
- To enrich experiential learning through active involvement in professional clubs & societies.
- To promote industry-institute collaborations for research & development.



# K.S. INSTITUTE OF TECHNOLOGY



DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

## PROGRAM EDUCATIONAL OBJECTIVES (PEO'S)

**PEO1:** Excel in professional career by acquiring domain knowledge.

**PEO2:** To pursue higher Education & research by adopting technological innovations by continuous learning through professional bodies and clubs.

**PEO3:** To inculcate effective communication skills, team work, ethics , entrepreneurship skills and leadership qualities.

## PROGRAM SPECIFIC OUTCOMES (PSO'S)

**PSO1:** Graduate should be able to understand the fundamentals in the field of Electronics & Communication and apply the same to various areas like Signal processing, embedded systems, Communication & Semiconductor technology.

**PSO2:** Graduate will demonstrate the ability to design, develop solutions for Problems in Electronics & Communication Engineering using hardware and software tools with social concerns.



## K S INSTITUTE OF TECHNOLOGY

### PROGRAM OUTCOMES (PO'S)

#### Engineering Graduates will be able to:

- PO1 :Engineering knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
- PO2 : 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.
- PO3 : 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.
- PO4 : 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.
- PO5 : 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.
- PO6 : 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.
- PO7 : 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.
- PO8 : Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

**PO9 :Individual and team work:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

**PO10 :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.

**PO11 ;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.

**PO12: 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.



**K.S. INSTITUTE OF TECHNOLOGY, BANGALORE - 560109**  
**DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING**  
**ACADEMIC YEAR 2023-2024 EVEN SEMESTER**

**CO-PO MAPPING WITH JUSTIFICATION**

<b>Course:</b> <u>CRYPTOGRAPHY</u>		<b>Course Code:</b> 21EC642	<b>Type:</b> Elective	
<b>Course In charge:</b> Dr P N Sudha & Mrs. Sangeetha V			<b>Academic year:</b> 2023-24	
<b>No of Hours per week</b>				
Theory (Lecture Class)	Practical/Field Work/Allied Activities	Total/Week		Total teaching hours
4	1	5		50
<b>Marks</b>				
Internal Assessment	Examination		Total	Credits
50	50		100	3
<b><u>Aim/Objective of the Course:</u></b>				
This Course will enable students to:				
<ol style="list-style-type: none"> <li>1. Enable students to understand the basics of symmetric key and public key cryptography.</li> <li>2. Equip students with some basic mathematical concepts and pseudorandom number generators required for cryptography.</li> <li>3. Enable students to authenticate and protect the encrypted data.</li> <li>4. Enrich knowledge about Email, IP and Web security.</li> </ol>				
<b>Course Learning Outcomes:</b>				<b>Bloom's Level</b>
After completing the course, the students will be able to,				
21EC642.1	<b>Examine</b> the Fundamental concepts of number theory & finite field and <b>apply</b> the same for simplification.			K4[Analysing]
21EC642.2	<b>Inspect</b> the concepts of Symmetrical ciphers and <b>design</b> security system using symmetrical cipher algorithm			K4[Analysing]
21EC642.3	<b>Interpret</b> various concepts of number theory and <b>analyze</b> cryptographic algorithm using these concepts.			K4[Analysing]
21EC642.4	<b>Infer</b> the prominent techniques used for public-key cryptosystems and Asymmetric Cipher schemes and <b>evaluate</b> the same.			K5[Evaluating]
21EC642.5	<b>Study</b> Pseudo-Random-Sequence Generators and Stream Ciphers & <b>design</b> the same.			K4[Analysing]
<b>Syllabus Content:</b>				
<b>Module 1:</b> BASIC CONCEPTS OF NUMBER THEORY & FINITE FIELDS: Divisibility and 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(2 <sup>m</sup> )				<b>CO1</b> <b>8 hrs</b>
LO: At the end of this session the student will be able to,				PO1-3
1. Use division algorithm for various application				PO2-2
2. Use Euclidean algorithm to find GCD				PO3-2
3. Explain the various terminologies like Group, Ring and Field.				PO4-3
				PO9 -3
				PO11-2
				PO12-2

	PSO1-2 PSO2-2
<b>Module2</b> <b>Introduction: Computer Security Concepts, A model for Network Security.</b> <b>Classical Encryption Techniques: Symmetrical cipher model, Substitution techniques, Transposition techniques</b>  LO: At the end of this session the student will be able to <ol style="list-style-type: none"> <li>1. Understand the Computer Security Concepts</li> <li>2. Explain and use various classical encryption techniques</li> </ol>	<b>CO2</b> <b>8 hrs</b> PO1-3 PO2-3 PO3-2 PO4-3 PO9 -2 PO11-2 PO12-2 PSO1-2 PSO2-2
<b>Module 3</b> <b>Block Ciphers: Traditional Block cipher structure, Data Encryption standard, The AES cipher.</b> <b>More on number theory: Prime numbers, Fermat's and Euler's theorem, Discrete logarithm</b>  LO: At the end of this session the student will be able to, <ol style="list-style-type: none"> <li>1. Understand and analyze the working of DES and AES algorithm.</li> <li>2. Apply Fermat's &amp; Euler's theorem for finding inverse mod function.</li> </ol>	<b>CO3</b> <b>8 hrs</b> PO1-3 PO2-3 PO3-3 PO4-3 PO9 -2 PO11-2 PO12-2 PSO1-2 PSO2-2
<b>Module 4</b> <b>ASYMMETRIC CIPHER</b> Principle of public Key cryptosystem, Principles of Public-Key Cryptosystems: The RSA algorithm, Diffie - Hellman Key Exchange, Elliptic Curve Arithmetic, Elliptic Curve Cryptography  LO: At the end of this session the student will be able to, <ol style="list-style-type: none"> <li>1. Explain public key algorithms</li> <li>2. Analyze the RSA algorithm</li> <li>3. Analyze Diffie - Hellman Key Exchange</li> <li>4. Understand Elliptic Curve Arithmetic</li> </ol>	<b>CO4</b> <b>8 hrs</b> PO1-3 PO2-3 PO3-2 PO4-3 PO9 -2 PO11-2 PO12-2 PSO1-2 PSO2-2
<b>Module 5: PSEUDO-RANDOM-SEQUENCE GENERATORS AND STREAM CIPHERS:</b>  Linear congruential Generators, Linear Feedback Shift Registers, Design and analysis of stream ciphers, Design & analysis of Stream ciphers using LFSRs, A5 algorithm, Hughes XPD/KPD, Additive generators, Gifford generator, PKZIP LO: At the end of this session the student will be able to, <ol style="list-style-type: none"> <li>1. Explain Linear Feedback Shift Registers</li> <li>2. Design and analysis of stream ciphers</li> <li>3. Design &amp; analysis of Stream ciphers using LFSRs</li> <li>4. Explain A5 algorithm, Hughes XPD/KPD, Additive generators, Gifford generator, PKZIP</li> </ol>	<b>CO5</b> <b>8 hrs</b> PO1-3 PO2-3 PO3-3 PO4-3 PO9 -2 PO11-2 PO12-2 PSO1-2 PSO2-2



**PSO1:** Graduate should be able to understand the fundamentals in the field of Electronics & Communication and apply the same to various areas like Signal Processing embedded systems, Communication & Semiconductor technology.

**PSO2:** Graduate will demonstrate the ability to design, develop solutions for Problems in Electronics & Communication Engineering using hardware and software tools with social concerns

**CO PO mapping for the events conducted after gap identification**

Sl. No.	Gap Identification	Activity Planned to fill the gap	CO	Relevant PO Mapping
1	PO4- PO12	Mini Project & Presentation	CO1, CO2, CO3, CO4, CO5	PO4, PO9, PO10, PO11, PO12

**CO PO MAPPING DETAILS FOR CRYPTOGRAPHY**

CO	Bloom's	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO12	PSO1	PSO 2
21EC642															
21EC642.1	K3	3	2	2	-	-	-	-	-	-	-	-	-	2	2
21EC642.2	K3	3	3	2	-	-	-	-	-	-	-	-	-	2	2
21EC642.3	K5	3	3	3	-	-	-	-	-	-	-	-	-	2	2
21EC642.4	K3	3	3	2	-	-	-	-	-	-	-	-	-	2	2
21EC642.5	K5	3	3	3	-	-	-	-	-	-	-	-	-	2	2
21EC642		3	2.8	2.4	-	-	-	-	-	-	-	-	-	2	2

**CO PO MAPPING DETAILS FOR CRYPTOGRAPHY: WITH CONTENT BEYOND SYLLABUS**

CO	Bloom's Level	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO12	PSO1	PSO2
21EC642															
21EC642.1	K3	3	2	2	3	-	-	-	-	3	2	2	2	2	2
21EC642.2	K3	3	3	2	-	-	-	-	-	-	-	2	-	2	2
21EC642.3	K5	3	3	3	3	-	-	-	-	-	2	-	2	2	2
21EC642.4	K3	3	3	2	3	-	-	-	-	3	2	2	2	2	2
21EC642.5	K5	3	3	3	-	-	-	-	-	3	2	2	2	2	2
21EC642		3	2.8	2.4										2	2
Strength for Content Beyond Syllabus activity: miniproject					3	-	-	-	-	3	2	2	2	2	2
21EC642		3	2.8	2.4	3	-	-	-	-	3	2	2	2	2	2

<p><b>Text Books:</b></p> <ul style="list-style-type: none"> <li>• William Stallings, “Cryptography and Network Security Principles and Practice”, Pearson Education Inc., 6th Edition, 2014, ISBN: 978-93-325-1877-3</li> <li>• Bruce Schneier, “Applied Cryptography Protocols, Algorithms, and Source code in C”, Wiley Publications, 2nd Edition, ISBN: 9971-51-348-X.</li> </ul>			
<p><b>Reference Books:</b></p> <ul style="list-style-type: none"> <li>• Understanding Cryptography - A Textbook for Students and Practitioners, Paar, Christof, Pelzl, Jan, Springer (2010).</li> <li>• Cryptography Engineering: Design Principles and Practical Applications, Niels Ferguson, Bruce Schneier, Tadayoshi Kohno, Wiley (2010).</li> <li>• Cryptography: Theory and Practice, Third Edition, Douglas R. Stinson, CRC Press (2005).</li> <li>• 4. Cryptography: A Very Short Introduction, Fred C. Piper; Sean Murphy, Oxford University Press (2002)..</li> </ul>			
<p><b>Useful websites:</b></p> <ul style="list-style-type: none"> <li>• <a href="https://learncryptography.com/">https://learncryptography.com/</a></li> <li>• <a href="http://www.cryptolab.us/">www.cryptolab.us/</a></li> <li>• <a href="https://cryptopals.com">https://cryptopals.com</a></li> </ul>			
<p><b>Useful Journals</b></p> <ul style="list-style-type: none"> <li>• Journal of Cryptology</li> <li>• International Journal of Applied Cryptography</li> <li>• International Journal of Cryptography and Security</li> </ul>			
<p><b>Teaching and Learning Methods:</b></p> <ol style="list-style-type: none"> <li>1. Lecture class: 40 hrs.</li> <li>2. Self-study: 5hrs.</li> <li>3. Field visits/Group Discussions/Seminars: 5hrs.</li> </ol>			
<p><b>Type of test/examination: Written examination:</b>  <b>Continuous Internal Evaluation (CIE) : Total 100 marks from under mentioned components will be scaled down to 50 marks</b></p> <ul style="list-style-type: none"> <li>• 3 CIE for 20 marks each (Total three test marks for 60 will be considered)</li> <li>• 2 Assignments each of 10 marks</li> <li>• 1 activity of 10 marks</li> </ul> <p><b>Semester End Exam(SEE) : 100 marks</b> (students have to answer all main questions)  Test duration: 1 hr  Examination duration: 3 hrs</p>			
<p><b>CO - PO MAPPING</b></p> <table border="1" data-bbox="240 1628 1325 1908"> <tr> <td data-bbox="240 1628 776 1908"> <p><b>PO1:</b> Science and engineering Knowledge  <b>PO2:</b> Problem Analysis  <b>PO3:</b> Design &amp; Development  <b>PO4:</b> Investigations of Complex Problems  <b>PO5:</b> Modern Tool Usage</p> </td> <td data-bbox="776 1628 1325 1908"> <p><b>PO6:</b> Engineer &amp; Society  <b>PO7:</b> Environment and Sustainability  <b>PO8:</b> Ethics  <b>PO9:</b> Individual &amp; Team Work  <b>PO10:</b> Communication  <b>PO11:</b> Project Management &amp; Finance  <b>PO12:</b> Life long Learning</p> </td> </tr> </table>	<p><b>PO1:</b> Science and engineering Knowledge  <b>PO2:</b> Problem Analysis  <b>PO3:</b> Design &amp; Development  <b>PO4:</b> Investigations of Complex Problems  <b>PO5:</b> Modern Tool Usage</p>	<p><b>PO6:</b> Engineer &amp; Society  <b>PO7:</b> Environment and Sustainability  <b>PO8:</b> Ethics  <b>PO9:</b> Individual &amp; Team Work  <b>PO10:</b> Communication  <b>PO11:</b> Project Management &amp; Finance  <b>PO12:</b> Life long Learning</p>	
<p><b>PO1:</b> Science and engineering Knowledge  <b>PO2:</b> Problem Analysis  <b>PO3:</b> Design &amp; Development  <b>PO4:</b> Investigations of Complex Problems  <b>PO5:</b> Modern Tool Usage</p>	<p><b>PO6:</b> Engineer &amp; Society  <b>PO7:</b> Environment and Sustainability  <b>PO8:</b> Ethics  <b>PO9:</b> Individual &amp; Team Work  <b>PO10:</b> Communication  <b>PO11:</b> Project Management &amp; Finance  <b>PO12:</b> Life long Learning</p>		

## JUSTIFICATION FOR CO - PO & PSO MAPPING

Sl No.	CO	PO	Number Of Key Elements of PO Mapped To CO	Justification
<b>CO1: Examine the Fundamental Concepts, Principles of Classical Encryption Techniques and Design the same.</b>				
1.	CO1	1	<b>The students will able to gain</b> <ul style="list-style-type: none"> <li>• Knowledge Of Mathematics</li> <li>• Knowledge In Specific Engg. Problem &amp; To Find Solution</li> </ul>	3 Keywords Are Mapped Hence Strength Is 3
2.		2	<b>The students will able to</b> <ul style="list-style-type: none"> <li>• Identify</li> <li>• Formulate</li> <li>• Analyse Complex Engineering Problems</li> </ul>	2
3.		3	<b>The students will able to</b> <ul style="list-style-type: none"> <li>• Design Solutions for Public Health &amp; Safety</li> <li>• Design Solutions for Cultural &amp; Societal Issues.</li> <li>• Design Solutions for Environmental Considerations</li> </ul>	3
4.		4	<b>The students will able to</b> <ul style="list-style-type: none"> <li>• Design,Of Solution for Complex Problems</li> <li>• Analysis Of Problems.</li> </ul>	3
5		9	<b>The students will able to work effectively in multidisciplinary as</b> <ul style="list-style-type: none"> <li>• Individual</li> <li>• In a Team</li> </ul>	3
6		10.	<b>The students will able to Communicate effectively by</b> <ul style="list-style-type: none"> <li>• Write Effective Reports</li> <li>• Effective Presentations</li> </ul>	2
7		11	<b>The students will able to gain the knowledge and understand</b> <ul style="list-style-type: none"> <li>• Engineering principles</li> <li>• Management of projects in a team</li> </ul>	2
8		12	<b>The students will able to engage in knowledge upgradation through</b> <ul style="list-style-type: none"> <li>• Independent learning</li> <li>• Lifelong learning</li> </ul>	2
9		PSO1	<b>The students will able to understand the fundamentals of ECE in</b> <ul style="list-style-type: none"> <li>• Signal Processing</li> <li>• Embedded systems</li> <li>• Communication</li> <li>• Semiconductor Technology</li> </ul>	2
10		PSO2	<b>The students will able to gain the knowledge to</b> <ul style="list-style-type: none"> <li>• Design a tool for societal concern</li> <li>• Develop solutions for hardware/software tools</li> </ul>	2
<b>CO2: Examine the concepts of Symmetrical ciphers and determine is working function</b>				
11	CO2	1	<b>The students will able to gain the</b> <ul style="list-style-type: none"> <li>• Knowledge Of Mathematics</li> <li>• Knowledge Of Science,</li> <li>• Knowledge In Specific Engg. Problem &amp; To Find Solution</li> </ul>	3
12		2	<b>The students will able to</b> <ul style="list-style-type: none"> <li>• Identify</li> <li>• Formulate</li> <li>• Analyse Complex Engineering Problems</li> </ul>	3

13		3	<b>The students will able to</b> <ul style="list-style-type: none"> <li>• <b>Design</b> solutions for public health &amp; safety</li> <li>• <b>Design</b> solutions for environmental considerations</li> </ul>	2
14		4	<b>The students will able to</b> <ul style="list-style-type: none"> <li>• Design of solution for complex problems</li> <li>• Analysis of problems</li> <li>• Synthesis of solution for complex problems</li> </ul>	3
15		9	<b>The students will able to work effectively in multidisciplinary as</b> <ul style="list-style-type: none"> <li>• Individual</li> <li>• In a Team</li> </ul>	2
16		10.	<b>The students will able to Communicate effectively by</b> <ul style="list-style-type: none"> <li>• <b>Write Effective Reports</b></li> <li>• <b>Effective Presentations</b></li> </ul>	2
17		11	<b>The students will able to gain the knowledge and understand</b> <ul style="list-style-type: none"> <li>• Engineering principles</li> <li>• Management of projects in a team</li> </ul>	2
18		12	<b>The students will able to engage in knowledge upgradation through</b> <ul style="list-style-type: none"> <li>• Independent learning</li> <li>• Lifelong learning</li> </ul>	2
19		PSO1	<b>The students will able to gain the knowledge in the fundamentals of ECE in</b> <ul style="list-style-type: none"> <li>• Signal Processing</li> <li>• Embedded systems</li> <li>• Communication</li> <li>• Semiconductor Technology</li> </ul>	2
20		PSO2	<b>The students will have the ability to</b> <ul style="list-style-type: none"> <li>• Design a tool for societal concern</li> <li>• Develop solutions for hardware/software tools</li> </ul>	2
<b>CO3: Interpret various concepts of number theory and design cryptographic algorithm using these concepts.</b>				
21	<b>CO3</b>	1	The students will able to gain the <ul style="list-style-type: none"> <li>• Knowledge Of Mathematics</li> <li>• Knowledge Of Science,</li> <li>• Knowledge In Specific Engg. Problem &amp; To Find Solution</li> </ul>	3
22		2	The students will able to <ul style="list-style-type: none"> <li>• Identify</li> <li>• Formulate</li> <li>• Analyse Complex Engineering Problems</li> </ul>	3
23		3	The students will able to gain <ul style="list-style-type: none"> <li>• <b>Design</b> solutions for public health &amp; safety</li> <li>• <b>Design</b> solutions for environmental considerations</li> </ul>	3
24		4	The students will able to <ul style="list-style-type: none"> <li>• Design of solution for complex problems</li> <li>• Analysis of problems</li> <li>• Synthesis of solution for complex problems</li> </ul>	3
25		9	<b>The students will able to work effectively in multidisciplinary as</b> <ul style="list-style-type: none"> <li>• Individual</li> <li>• In a Team</li> </ul>	2
26		10.	<b>The students will able to Communicate effectively by</b> <ul style="list-style-type: none"> <li>• <b>Write Effective Reports</b></li> <li>• <b>Effective Presentations</b></li> </ul>	2

27		11	<p><b>The students will able to gain the knowledge and understand</b></p> <ul style="list-style-type: none"> <li>• Engineering principles</li> <li>• Management of projects in a team</li> </ul>	2
28		12	<p><b>The students will able to engage in knowledge upgradation through</b></p> <ul style="list-style-type: none"> <li>• Independent learning</li> <li>• Lifelong learning</li> </ul>	2
29		PSO1	<p>The students will able to gain the fundamentals of ECE in</p> <ul style="list-style-type: none"> <li>• Signal Processing</li> <li>• Embedded systems</li> <li>• Communication</li> <li>• Semiconductor Technology</li> </ul>	2
30		PSO2	<p>The students will able to gain the ability to</p> <ul style="list-style-type: none"> <li>• Design a tool for societal concern</li> </ul>	2
<b>CO4: Examine the prominent techniques used for public-key cryptosystems and Asymmetric Cipher schemes and evaluate the same.</b>				
31	CO4	1	<p>The students will able to gain the</p> <ul style="list-style-type: none"> <li>• Knowledge Of Mathematics</li> <li>• Knowledge Of Science,</li> <li>• Knowledge In Specific Engg. Problem &amp; To Find Solution</li> </ul>	3
32		2	<p>The students will able to</p> <ul style="list-style-type: none"> <li>• Identify</li> <li>• Formulate</li> <li>• Analyse Complex Engineering Problems</li> </ul>	3
33		3	<p>The students will able to</p> <ul style="list-style-type: none"> <li>• <b>Design</b> solutions for public health &amp; safety</li> <li>• <b>Design</b> solutions for environmental considerations</li> </ul>	2
34		4	<p>The students will able to gain</p> <ul style="list-style-type: none"> <li>• Design of solution for complex problems</li> <li>• Analysis of problems</li> <li>• Synthesis of solution for complex problems</li> </ul>	3
35		9	<p>The students will able to work effectively in multidisciplinary as</p> <ul style="list-style-type: none"> <li>• Individual</li> <li>• In a Team</li> </ul>	2
36		10.	<p>The students will able to Communicate effectively by</p> <ul style="list-style-type: none"> <li>• Write Effective Reports</li> <li>• Effective Presentations</li> </ul>	2
37		11	<p>The students will able to gain knowledge and understanding</p> <ul style="list-style-type: none"> <li>• Engineering principles</li> <li>• Management of projects in a team</li> </ul>	2
38		12	<p>The students will gain the ability to engage in knowledge upgradation through</p> <ul style="list-style-type: none"> <li>• Independent learning</li> <li>• Lifelong learning</li> </ul>	2
39		PSO1	<p>The students will able to gain the knowledge in the fundamentals of ECE in</p> <ul style="list-style-type: none"> <li>• Signal Processing</li> <li>• Embedded systems</li> <li>• Communication</li> <li>• Semiconductor Technology</li> </ul>	2
40		PSO2	<p>The students will able to gain the ability to</p> <ul style="list-style-type: none"> <li>• Design a tool for societal concern</li> <li>• Develop solutions for hardware/software tools</li> </ul>	2

**CO5: Examine Pseudo-Random-Sequence Generators and Stream Ciphers & Design the same.**

41	CO5	1	The students will able to gain <ul style="list-style-type: none"><li>• Knowledge Of Mathematics</li><li>• Knowledge In Specific Engg. Problem &amp; To Find Solution</li></ul>	2 Keywords Are Mapped Hence Strength Is 3
42		2	The students will able to <ul style="list-style-type: none"><li>• Identify</li><li>• Formulate</li><li>• Analyse Complex Engineering Problems</li></ul>	3
43		3	The students will able to <ul style="list-style-type: none"><li>• Design Solutions for Public Health &amp; Safety</li><li>• Design Solutions for Cultural &amp; Societal Issues.</li><li>• Design Solutions for Environmental Considerations</li></ul>	3
44		4	The students will able to <ul style="list-style-type: none"><li>• Design Of Solution for Complex Problems</li><li>• Analysis Of Problems.</li></ul>	3
45		9	The students will able to work effectively in multidisciplinary as <ul style="list-style-type: none"><li>• Individual</li><li>• In a Team</li></ul>	2
46		11	The students will able to gain the knowledge and understanding in <ul style="list-style-type: none"><li>• Engineering principles</li><li>• Management of projects in a team</li></ul>	2
47		12	The students will have the ability to engage in knowledge upgradation through <ul style="list-style-type: none"><li>• Independent learning</li><li>• Lifelong learning</li></ul>	2
48		PSO1	The students will able to gain the knowledge in the fundamentals of ECE in <ul style="list-style-type: none"><li>• Signal Processing</li><li>• Embedded systems</li><li>• Communication</li><li>• Semiconductor Technology</li></ul>	3
49		PSO2	The students will able to gain the ability to <ul style="list-style-type: none"><li>• Design a tool for societal concern</li><li>• Develop solutions for hardware/software tools</li></ul>	3



Signature of Course In-charge



Signature of Module Coordinator



Signature of HOD ECE



**K. S INSTITUTE OF TECHNOLOGY, BENGALURU-560109**  
**DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING**  
**TENTATIVE CALENDAR OF EVENTS: VI EVEN SEMESTER (2023-2024)**  
**SESSION: APRIL TO JULY 2024**

Week No.	Month	Day						Days	Activities	Department Activities Tentative Dates
		Mon	Tue	Wed	Thu	Fri	Sat			
1	APR/ MAY	29*	30		2	3		4	29* -Commencement of VI sem 1- May Day	
2	MAY	6	7	8	9		11	5	10 - Basava Jayanthi 11- Friday Time Table	
3	MAY	13	14	15	16	17 TA		5		
4	MAY	20	21	22	23	24	25 TA	6	25- Monday Time Table	24th May Technical Talk on Logical Thinking and Problem solving Under IETE, IEEE, IEI, ISTE
5	MAY/ JUNE	27 T1	28 T1	29 T1	30	31		5	29 - First Faculty Feed Back	
	JUNE	3 BV	4 ASD	5* FFB1	6	7	8	6	8- Monday Time Table	
7	JUNE	10	11	12	13	14		5		14th June Industrial Visit Under IETE, IEEE, IEI, ISTE 15th June Marathan Under IEEE
8	JUNE		18	19	20	21	22	5	17- Bakrid 22- Wednesday Time Table	22nd June Workshop on Baise knowledge on Drone Mechanism Under Garut Aurobotics Club
9	JUNE	24	25	26 TA	27 T2	28 T2	29 T2	6		24th June Technical Talk on Microstrip Antenna under IETE
10	JULY	1 BV	2 ASD	3* FFB2	4	5		5	3* - First Faculty Feed Back	
11	JULY	8	9	10	11	12	13	6	13- Friday Time Table	13th July Alumini Talk Under IEEE
12	JULY	15	16		18	19 TA		4	17- Last Day of Moharam	
13	JULY	22 T3	23 T3	24 T3	25 LT	26 LT	27 LT	6		
14	JULY	28 LT	30	31*				3	31* - Last Working day	

Total No of Working Days : 71

Total Number of working days ( Excluding holidays and Tests)=58

H	Holiday
BV	Blue Book
T1, T2, T3	Tests 1,2,3
ASD	Attendance & Sessional Display
DH	Declared Holiday
LT	Lab Test
TA	Test attendance

Monday	12
Tuesday	12
Wednesday	11
Thursday	11
Friday	12
Total	58

*[Signature]*  
**HEAD OF THE DEPARTMENT**  
 ept. of Electronics & Communication Engg.  
 K. S. Institute of Technology  
 Bengaluru - 560 109.

*[Signature]*  
**PRINCIPAL**  
 K.S. INSTITUTE OF TECHNOLOGY  
 BENGALURU - 560 109.



**K. S. INSTITUTE OF TECHNOLOGY, BENGALURU-560109**

TENTATIVE CALENDAR OF EVENTS: VI EVEN SEMESTER (2023-2024)

SESSION: APRIL TO JULY 2024



Week No.	Month	Day						Days	Activities
		Mon	Tue	Wed	Thu	Fri	Sat		
1	APR/ MAY	29*	30	1 H	2	3	4 DH	4	29* -Commencement of VI sem 1- May Day
2	MAY	6	7	8	9	10 H	11	5	10 - Basava Jayanthi 11- Friday Time Table
3	MAY	13	14	15	16	17 TA	18 DH	5	
4	MAY	20	21	22	23	24	25TA	6	25- Monday Time Table
5	MAY/ JUNE	27 T1	28 T1	29 T1	30	31	1 DH	5	29 - First Faculty Feed Back
6	JUNE	3 BV	4 ASD	5* FFB1	6	7	8	6	8- Monday Time Table
7	JUNE	10	11	12	13	14	15 DH	5	
8	JUNE	17 H	18	19	20	21	22	5	17- Bakrid 22- Wednesday Time Table
9	JUNE	24	25	26TA	27T2	28T2	29T2	6	
10	JULY	1BV	2ASD	3* FFB2	4	5	6 DH	5	3* - First Faculty Feed Back
11	JULY	8	9	10	11	12	13	6	13- Friday Time Table
12	JULY	15	16	17 H	18	19TA	20 DH	4	17- Last Day of Moharam
13	JULY	22T3	23T3	24T3	25LT	26LT	27LT	6	
14	JULY	29LT	30	31*				3	31* - Last Working day

Total No of Working Days : 71

Total Number of working days ( Excluding holidays and Tests)=58

H	Holiday
BV	Blue Book Verification
T1,T2,T3	Tests 1,2,3
ASD	Attendance & Sessional Display
DH	Declared Holiday
LT	Lab Test
TA	Test attendance

Monday	12
Tuesday	12
Wednesday	11
Thursday	11
Friday	12
<b>Total</b>	<b>58</b>

*[Signature]*  
24/4/24

PRINCIPAL  
K.S. INSTITUTE OF TECHNOLOGY  
BENGALURU - 560 109.



**K.S.INSTITUTE OF TECHNOLOGY**  
**DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGG.**  
**LIST OF STUDENTS STUDYING IN VI SEMESTER ( B SECTION)**  
**FOR THE ACADEMIC YEAR 2023-24 (EVEN SEMESTER)**

SL. NO	USN	NAME OF THE STUDENT	Gender	Date of Birth	EMAIL_ID	Student Phone No	NAME OF THE FATHER	Father Phone No	Mother	Mother Phone No	Address
1	1KS21EC062	PRAJWAL D	Male	12-05-2003	prajwalrock9019@gmail.com	9019104400	DAKSHINA MURTHY	9008332873	CHANDRAKAL A	6362532232	#8/16 j g jayakumar h nagalakshmi 11 th main pipe line road shakambarinagar jp nagar 1st phase
2	1KS21EC063	PRAJWAL G V	Male	21-1-2004	prajjuprajwalgv@gmail.com	6363264894	VFFRABHADRA E GOWDA	9740756633	SUMITHRA	8296330594	Guttalahunase village and post maralavadi hobli kanakapura taluk ramanagara district
3	1KS21EC064	PRAJWAL H S	Male	06 03 2003	prajjuakir@gmail.com	8197043039	SIDDALINGAI AH	9742829320	PUSHPA LATHA	8310444025	#D-14 keb quartres N R colony Tyagaraj nagar basvangudi Banglore
4	1KS21EC065	PRAJWAL R	Male	03-07-2003	prajwalrece2021@ksit.edu.in	9148190655	RAMACHANDRA	9965401153	VARALAKSHMI	9535067746	#72,Ramakrishnappa building,rajivi Gandhi road,naidu layout,jaraganahalli,JP nagar post ,Bangalore 560078
5	1KS21EC066	PRATHAM R SHANBHAG	Male	03-03-2003	prathamshanbhag333@gmail.com	8431092728	RAMANATH D SHANBHAG	9945639066	ROOPA R SHANBHAG	9740141715	#13 1st cross 1st main sudham nagar blore 27
6	1KS21EC067	PRAYAG SINGH S	Male	07-12-2003	prayagsingh2003@gmail.com	7676106160	SANDEEP NARAYAN SINGH	9880102048	MEENA KUMARI	9448032636	Kuppareddy kere opposite to BWSSB quarters kanakapura road Bangalore-62
7	1KS21EC068	PREETHAM M	Male	30-08-2003	Preethamgowda3008@gmail.com	6364607169	MAHESHA P	9901335547	SHAILAJA	9880509326	Anjeneya temple , rice mill road , ambedkar nagar , kanakapura

8	1KS21EC069	PREKSHA S	Female	03-08-2003	preksha03082003@gmail.com	9036423382	V H SWAMY	9845541165	SARITHA D R	9611620504	#13, 2nd Cross, Govindappa layout, Jaraganahalli, J P Nagar, Bangalore-78
9	1KS21EC070	PUNITH M	Male	04-07-2004	Pruthvipuni35@gmail.com	7337854558	MANJUNATH. P	9880425406	SUNITHA	9741214275	#51, 9th main road, chandra nagar, kumarswamy layout, bengaluru 560078
10	1KS21EC071	RAGHAVENDRA NARAYAN PUJAR	Male	15-04-2003	raghavendrapujar04@gmail.com	8904150960	NARAYANA	9739270399	SUNANDA	8970492778	R K Nagar bellatti
11	1KS21EC072	RAKSHITH S	Male	17-06-2003	rakshith1317@gmail.com	9632461925	SHASHIDHAR GS	9845704449	REKHA R	9740785586	Block 16 001 janabharathi residential enclave mylasandra kengeri
12	1KS21EC073	RAKSHITHA M R	Female	04-01-2004	rakshitharudramuni@gmail.com	7795896828	RUDRAMUNI	9731932381	LINGARAJAMMA	9380697864	Marale (v) kanakapura (t) ramanagara (d)
13	1KS21EC074	RAYADURG JOISH SHRIYA	Female	27-05-2004	rjshriya499@gmail.com	6305219266	R.J JAYATHEERTHA	7013808016	R.J VASUNDHARA	7013859945	#29, Near Gopalan Sanskriti, Krishna County Bangalore
14	1KS21EC075	REHAMAN SHARIFF	Male	30-09-2004	rehamanshariff45@gmail.com	8310255473	SHAFIULLA	9008036141	RAFIYA BANU	6362511679	#60, Billvaradhalli, Next to New winners School, BG Road, Banglore-560083
15	1KS21EC076	RITESH KUMAR SINHA	Male	24-09-2002	ritheshkumarsinha123@gmail.com	8618038332	MANOJ KUMAR SINHA	+919472231377	RINA SINHA	9731830382	#124Vinayaka street near tiles factory kanakapura
16	1KS21EC077	RITHIKA M	Female	24-10-2002	rithika1560@gmail.com	7899004683	MANJUNATH S	8197392110	SUBHASHINI V	7619672110	#18 sarakki jp nagar 1st phase behind anjaneya temple 3rd main 12th cross Bangalore 78
17	1KS21EC078	S HARI DHANUSH	Male	03-03-2004	haridhanush337@gmail.com	8618922395	SARAVANAN	8884558418	SHANTHI	7411546683	#03, manjunath colony chenanamkere Bangalore

18	1KS21EC080	S SHAJITH ALI	Male	15-07-2003	shajithali04@gmail.com	7975376909	SIRAJUDEEN	9900029602	A.SHAMEEM	9632390399	Nitesh Ceasas Palace , B1104, Bangaalore Municipal Corporation Layout , Kanakapura Main Road, Vajarahalli, Bangalore -560062
19	1KS21EC081	SAGAR G S	Male	22-06-2003	Sagargs203@gmail.com	7204647563	SATHYA MADEVA. G. K	9972811616	GEETHA	7204647563	Guttalahunase village and post maralavadi hobli kanakapura taluk ramanagara district
20	1KS21EC082	SAI RAHUL N	Male	02-10-2003	sairahuln461@gmail.com	6363375378	N VENKATARAM ANA	6363375378	N MADHAVI	7026651613	6th ward sriramnagar, taluk:Gangavathi, district:Koppal - 583282
21	1KS21EC083	SAMHITHA PRAKASH	Female	05-09-2003	samhithaprakash0515@gmail.com	9353381280	PRAKASH G M	9481037085	MANJULA M.S	9900277671	No 144 allamaprabhu road hanumantanagar gavipuram Bangalore- 19
22	1KS21EC084	SANJANA V	Female	14-08-2003	sanjanagowdav46@gmail.com	7892240241	C K VENKATESH	9845049516	S BHAGYA	9066779915	#46, 4th A cross, M.S Layout, near Royal Enfield Garage, Yelachenahalli
23	1KS21EC085	SANJAY G	Male	26-04-2003	sanjaygowdagm62@gmail.com	8296649992	GOPAL S	9740077041	MALA G	9980782032	#10,13th cross bendre nagar, kadeircnahalli circle , Banashankari 2nd stage, banglore 70
24	1KS21EC086	SANJAY N	Male	13-11-2002	sanjaynsanju002@gmail.com	8147203868	NAGARAJAIAH H	9448660777	KUSUMA H S	9141410149	SREE BASAVESHWARA NILAYA GADDE BAYALU CM EXTENTION KYATHASANDRA TUMAKURU
25	1KS21EC087	SANJAY P	Male	10-1-2004	sanjayperumal8582@gmail.com	9008112369	PERUMAL G	9036248582	SUMATHI P	9740320106	#54,11th cross,ittamadu,bsk 3rd stage Bengaluru 560085

26	1KS21EC088	SATHYAM KUMAR MANDAL S	Male	30-11-2002	sathyamkumar333mandal@gmail.com	8618306717	SANJAY KUMAR MANDAL	9448509333	PREMALATHA	9353573935	#473, 4th A cross, gururaja layout, behind Vidyapeeta circle, Bengaluru 5600 28
27	1KS21EC089	SHAIK ARFATH	Male	9-5-2003	Shaikarfath.2003@gmail.com	8951842434	NASEER PASHA	9945215029	FARZANA BANU	8971537909	Devegowda badavane turuvekere town
28	1KS21EC090	SHASHANK C U	Male	24-04-2003	shashankcu2003@gmail.com	8088764423	UMESH CP	9964016895	SAROJA	9964016895	Chikkapura, muttugadahalli (post), Turuvekere, tumkur
29	1KS21EC091	SHREYAS RAGHAVENDRA V	Male	28-09-2003	Shreeraghu01@gmail.com	9945341036	VIJAY KUMAR BR	9901095133	SUJATHA KR	9945349686	20/a panchamukki nilaya Uttarahalli Bangalore 61
30	1KS21EC092	SHWETHA V	Female	27-05-2003	shwethashwe276@gmail.com	9945815416	N VEDIAPPAN	9844185416	R RAJESWARI	9606555416	Door No,302, #378/1, SIRI ENCLAVE APARTMENT, 2ND CROSS, NANJUNDAIAH LAYOUT, BEGUR, BANGALORE 560068
31	1KS21EC093	SINDHU M NIMBAL	Female	11-11-2003	sindhumn2155@gmail.com	9663783040	MALLIKARJUN NIMBAL	9008821416	BHARATHI	9900415762	S4 S & S platinum apartment kalegowda garden layout RR Nagar Bangalore 560098
32	1KS21EC095	SPOORTHY M U	Female	06-04-2003	www.spoorthym.ugowda@gmail.com	7204973489	UMESH.M	9448854371	BHAGYA K.K	9686201489	15th cross ,near bright way school, gowdanapalya, banglore 61
33	1KS21EC096	SRILAKSHMI G	Female	04-02-2003	srilakshmiq229@gmail.com	6366011255	GANESH R	9448513599	VIDYA G	9606226340	#16, 6th cross, 5th Main, Srinidhi Layout, Konanakunte, Bangalore -62
34	1KS21EC097	SRIPRIYA H G	Female	01-01-2003	sripriyagopal1@gmail.com	7760685298	GOPAL HS	9916754622	KAMAKSHI VG	9886411954	954, "anugraha", 12th cross, 35th main jp Nagar 1st phase Bangalore 560078

35	1KS21EC098	SUMUKH P	Male	29-12-2002	sumukh560060@gmail.com	9844052673	PRAKASH Y G	9741525571	ROOPA B N	9844744761	#41/1sal brindavan enclave channasandra Bangalore
36	1KS21EC099	SUNEETHA	Female	16-04-2003	suneetha2002g@gmail.com	8792320048	GAVIDIDDEGO WDA	9731172310	LAKSHMI	9731265040	H kothanuru village &post ,kanakapura (t) ramanagara (d)
37	1KS21EC100	SUNEHA S	Female	13-08-2003	sunehas5678@gmail.com	9880812429	BL SURESH	9845001549	GN SUNITHA	9880812429	#1652/E, JP nagar, 2nd phase , 16th B main, banglore 560078
38	1KS21EC101	SUPREETH A	Male	07-09-2003	asupreeth17@gmail.com	7338319307	ASHOK KUMAR.G	7760608544	SHILPA	9008229833	#569,69th cross, Kumar Swamy Layout, Banglore 560078
39	1KS21EC102	SURABHI K R	Female	19-04-2003	Suhasking007@gmail.com	7676003022	RAMU K K	9620045158	SUDHA M S	7676003022	Jp nagar 6th phase 8th cross Bangalore 78
40	1KS21EC103	SUSHEN KRISHNAPUR	Male	10-02-2003	sushenkrishnapur@gmail.com	9591560186	ARAVIND P KRISHNAPUR	9741381172	VEENA R HERKAL	9535187566	67/2 (45/2),Shri Krishna dhama Rajashekar tent road subramanya pura post brindavan layout Bengaluru-61
41	1KS21EC104	TARUN M	Male	09-07-2003	tarunmgowda007@gmail.com	7619538524	MANJUNATH.B	9740023125	SHOBHAMANI	9538982319	#101, Srushti Swara apartment, Durga nagar layout, Krishna garden Road, RV College Post, Mylasandra, Bangalore - 59.
42	1KS21EC105	TEJASHREE N	Female	05-11-2002	tejashreenagaraja5@gmail.com	9148489567	V S NAGARAJA	973127492	NALINA K	9845200199	No 90 , 1st main, Kanaka layout , Banashankari 2nd stage , Bangalore -560070
43	1KS21EC106	THARUN K V	Male	17-01-2004	tharunkvteju@gmail.com	8217664453	VENKATESH KA	9845199408	CHANDRAKAL A SG	6362469735	Pipeline road kuvempunagara 3rd cross Kanakapura ( 562117)

44	1KS21EC107	THEJAS H V	Male	13-02-2004	thejashv57552@gmail.com	9380959092	VENKATEGOW DA HC	9008627720	SUNDRAMMA UK	9380959092	hukunda(v) Kodihalli hobli, kanakapura (t) ramanagara(d)
45	1KS21EC108	THUSHAR CHERIAN	Male	09-12-2002	thusharcherian06@gmail.com	7619641273	O.M.CHERIAN	7760670186	SUJATHA CHERIAN	7022009033	No. 10/30 Chaithra nilaya , 9th A main Srinivasnagar, Banashankari 3rd stage , Bangalore-560085.
46	1KS21EC109	UDAYA KUMAR S R	Male	5-12-2002	udaykumar29290@gmail.com	9353829290	SRINIVAS R	9448172142	GEETHA.S	8904789606	Near siddhivinayak temple compounder lane hospet
47	1KS21EC110	VAISHNAVI B A	Female	10-10-2003	vaishnaviba374@gmail.com	8861203655	B V ANANTHAPAD MANABHA	9663879058	SHUBHA B V	9110807592	#42, "Shri Rama Samartha", 3rd Cross, Sharadha nagar, Vasanthapura Main Road Bangalore-560061
48	1KS21EC111	VARSHA JAYAKUMAR	Female	06-04-2003	varshajayakumar6@gmail.com	8431849840	JAYAKUMAR K M	8762436626	DEVIKA M L	7975642784	#gf3, manyatha apartment, pattabhiraiah street, mavalli, banglore- 560004
49	1KS21EC112	VARSHA S DAVASKAR	Female	02- 01- 2004	varshadavaskar@gmail.com	6362840290	SRINIVAS P	8971987422	VEENA	8861889619	Mirza Badavane Bandamma Temple Hiriyur 577598
50	1KS21EC113	VARSHITH S	Male	19-12-2002	varshithshu@gmail.com	6360930497	SRIKANTH.S	9845894540	SHUBHA.S	9008149706	Malleshwaram md block bengaluru
51	1KS21EC114	VEERESH K N	Male	06-10-2003	veereshkn03@gmail.com	8970065970	NAGARAJA K E	9164023212	RAJESHWARI R S	9880323422	Mukthenahalli, Honnalli tq, Davangere dist, Karnataka
52	1KS21EC115	VIDYA I	Female	06-12-2003	vvidya385@gmail.com	7019048952	IYYAPPAN.K	9535336076	VIJAYA.I	7411572070	#28, chennamanakere,m anjunatha colony, bsk 3rd stage, banglore-85
53	1KS21EC116	VIDYA RAWAL D	Female	17- 01- 2004	vidyarawal0975@gmail.com	8971846158	P DEEPAK RAWAL	9060670621	RADHA RAWAL	9535400463	No 52 Sri ramchandrapura near reliance fresh ittamadu bglore 61

54	1KS21EC117	VIDYASHREE R	Female	8-12-2003	vidyashreer812@gmail.com	6360986997	RAMAKRISHNA GOWDA.C	8762413564	PRABHAVATHI	9845564565	19/25, Raghavendra industrial area , rajiv gandhi road, jaraganahalli , jp Nagar, banglore-560078
55	1KS21EC118	VIJAY YADAV R	Male	21-02-2003	vy21230452@gmail.com	9741810452	RAMU M	9845902563	MAMATHA.S	7760565623	Dharma raj workshop road near vani theater kanakapura
56	1KS21EC120	VYSHAK G R	Male	4 -6-2003	Vyshakgr40@gmail.com	9019443648	RAMU G K	9148133804	GOWRAMMA	7022905325	Thummalapalli, srinivasapura tq, Kolar Dt.
57	1KS21EC121	YASHWANATH.M	Male	25-11-2003	yashwanth0078147@gmail.com	+918073899452	M BALI NAIDU	9663077149	M BHANUMATHI	+918073899452	502 4th Floor Sri Sai Residency, 7th Main Nanda Kumar Layout, Arehalli, Bangalore South, Bengaluru,
58	1KS22EC407	PRAJWAL PATIL B S	Male	1/3/2002	patilprajwal2141@gmail.com	8861976073	SIDDAPPA B V	9741746264	NIRMALA	9900595327	# 95, MEDIKERENALLI, MEDIKERENALLI POST, JAGALUR TQ, DAVANAGERE DT-577553
59	1KS22EC408	SANGEETHA H M	Female	10/3/2002	sangeethajaanu000@gmail.com	8050268549	MUNINAGAPPA	9740536191	MANGALA	890406791	# 33, HOSADODDI, BOLARE POST, KANAKAPURA MAIN RAOD, BANGALORE -82
60	1KS22EC409	SOUNDARYA S	Female	22/9/2000	soundukrish979@gmail.com	7676173324	SHIVA PERUMAL N	9901963194	VENBU S	8867617207	# 40/1/1, 7TH MAIN, 7TH CROSS, DEVANTHA CHAR STREET, CHAMARAJ PET, BANGALORE -18
61	1KS22EC410	SOWMYA A M	Female	20/3/2001	sowmyamohan2032001@gmail.com	9448717667	MOHAN A H	9972448001 9448437982	SATHYABHAM A S R	9902033092	# 1, T GOPA GONDANAHALLI, MADIKE CHILUR POST, NAYMATHI TQ, DAVANAGERE DT,
62	1KS22EC411	SUDEEP P	Male	10/7/2001	acchusudeep6@gmail.com	9945138286	PARAMESWAR A	8277013538	HEMAVATHI C N	8277013528 8618713945	# THOTADA MANE, BEHIND CONER CHRCH, UJJINIPURA, BHADRAVATHI -577302



**K.S. INSTITUTE OF TECHNOLOGY, BANGALORE -109**  
**DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING**  
**INDIVIDUAL TIME TABLE FOR THE YEAR - 2024 ( EVEN SEMESTER)**

W.E.F. : 29/4/2024

NAME OF THE FACULTY : SANGEETHA .V

DESIGNATION: ASSISTANT PROFESSOR

PERIOD	1	2	10.20 AM 10.35 AM	3	4	12.25 PM 1.15 PM	5	6	7
TIME DAY	8.30 AM 9.25 AM	9.25 AM 10.20 AM		10.35 AM 11.30 AM	11.30 AM 12.25 PM		1.15 PM 2.10 PM	2.10 PM 3.05 PM	3.05 PM 4.00 PM
MON		CRYPTO (21EC642)	T E A B R E A K			L U N C H  B R E A K	← MWA LAB (21EC62)-A2 →		
TUE		CRYPTO (21EC642)					← MWA LAB (21EC62)-B2 →		
WED	CRYPTO (21EC642)						← MWA LAB (21EC62)-A3 →		
THU	CRYPTO (21EC642)						← MWA LAB (21EC62)-B3 →		
FRI	← MWA LAB (21EC62)-A1 →				← MWA LAB (21EC62)-B1 →				

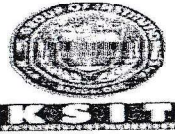
	Subject Code	Subject Name	Sem	Section	Work Load
Subject 1	21EC642	Cryptography (Professional Elective Course-I)	VI	B	4
Lab-1	21EC62	Microwave Theory and Antennas (Theory Lab )	VI	A&B	18
Mini project	21ECMP67	Mini Project (Guide )	VI		2
Project	18ECP83	Project Work Phase -2(Guide)	VIII		2
Internship	18ECI85	Internship (Guide )	VIII		2
ADDITIONAL WORK: MENTORING AND OTHERS					
TOTAL LOAD= 28 Hrs/Week					

*Sangeetha V*  
Time Table Co-ordinator

*Sangeetha V*  
**HEAD OF THE DEPARTMENT**  
Dept. of Electronics & Communication Engg  
K.S. Institute of Technology  
Bangalore - 560 109

*Shree Kumar*  
**PRINCIPAL**  
K.S. INSTITUTE OF TECHNOLOGY  
BENGALURU - 560 109.





# K.S. INSTITUTE OF TECHNOLOGY, BANGALORE -109

## DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

### VI SEMESTER TIME TABLE FOR THE YEAR 2024 (EVEN SEMESTER)

W.E.F. : 29/4/2024

CLASS TEACHER : Dr. Dinesh Kumar D S

SEC : 'B'

CLASS ROOM : OB LH 311

PERIOD	1	2	10.20 AM 10.35 AM	3	4	12.25 PM 1.15 PM	5	6	7
TIME DAY	8.30 AM 9.25 AM	9.25 AM 10.20 AM		10.35 AM 11.30 AM	11.30 AM 12.25 PM		1.15 PM 2.10 PM	2.10 PM 3.05 PM	3.05 PM 4.00 PM
MON	DS (21CS651)	CRYPTO(21EC642) /PYTHON (21EC643)	T E A  B R E A K	MWA (21EC62)	VLSI (21EC63)	L U N C H  B R E A K	← INTERNSHIP (21INT68) →		
TUE	VLSI (21EC63)	CRYPTO(21EC642) /PYTHON (21EC643)		M&E (21EC61)	MWA (21EC62)		← VLSI LAB (21ECL66)-B1 / MWA LAB (21EC62)-B2 →		
WED	CRYPTO(21EC642) /PYTHON (21EC643)	MWA (21EC62)		DS (21CS651)	M&E (21EC61)		← Mini Project (21ECMP67) →		
THU	CRYPTO(21EC642) /PYTHON (21EC643)	M&E (21EC61)		VLSI (21EC63)	DS (21CS651)		← VLSI LAB (21ECL66)-B2 / MWA LAB (21EC62)-B3 →		
FRI	M&E (21EC61)	VLSI (21EC63)		MWA (21EC62)	DS (21CS651)		← VLSI LAB (21ECL66)-B3 / MWA LAB (21EC62)-B1 →		

Sub-Code	Subject Name	Faculty Name
21EC61	Technological Innovation Management and Entrepreneurship	Dr. B.Sudharshan
21EC62	Microwave Theory and Antennas	Dr. Dinesh Kumar D S
21EC63	VLSI Design & Testing	Mr. Praveen.A
21EC642	Cryptography (Professional Elective Course-I)	Mrs.Sangeetha.V
21EC643	Python Programming (Professional Elective Course-I) + (Theory Lab )	Mr. Christo Jain
21CS651	Introduction to Data Structures (Open Elective Course-I)	Mrs. Bhargavi Ananth
21ECL66	VLSI Laboratory	Mr. Praveen.A (B1,B2,B3), Mrs. Bhanumathi A(B1,B2,B3)
21ECMP67	Mini Project	Dr. Devika B, Dr. B. Sudharshan
21INT68	Innovation/Entrepreneurship /Societal Internship	Mr. Santhosh Kumar B R , Mrs.Suma Santosh
21EC62	Microwave Theory and Antennas (Theory Lab )	Dr. Electa Alice Jayarani A(B1,B2,B3) , Mrs.Sangeetha.V(B1,B2,B3)

Time Table Co-ordinator

**HEAD OF THE DEPARTMENT**  
Dept. of Electronics & Communication Engg  
K.S. Institute of Technology

Principal  
**PRINCIPAL**  
K.S. INSTITUTE OF TECHNOLOGY  
BANGALORE - 560 109

## VI Semester

<b>Cryptography</b>			
Course Code	<b>21EC642</b>	CIE Marks	50
Teaching Hours/Week (L:T:P:S)	2:2:0:0	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	3	Exam Hours	3
<b>Course objectives:</b>			
This course will enable students to:			
<ul style="list-style-type: none"> <li>• Preparation: To prepare students with fundamental knowledge/ overview in the field of Information Security with knowledge of mathematical concepts required for cryptography.</li> <li>• 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</li> </ul>			
<b>Teaching-Learning Process (General Instructions)</b>			
The sample strategies, which the teacher can use to accelerate the attainment of the various course outcomes are listed in the following:			
<ol style="list-style-type: none"> <li>1. Lecture method (L) does not mean only the traditional lecture method, but a different type of teaching method may be adopted to develop the outcomes.</li> <li>2. Show Video/animation films to explain the different Cryptographic Techniques / Algorithms</li> <li>3. Encourage collaborative (Group) Learning in the class</li> <li>4. Ask at least three HOTS (Higher order Thinking) questions in the class, which promotes critical thinking</li> <li>5. Adopt Problem Based Learning (PBL), which fosters students' Analytical skills, develop thinking skills such as the ability to evaluate, generalize, and analyze information rather than simply recall it.</li> <li>6. Topics will be introduced in a multiple representation.</li> <li>7. Show the different ways to solve the same problem and encourage the students to come up with their own creative ways to solve them.</li> <li>8. Discuss how every concept can be applied to the real world - and when that's possible, it helps improve the students' understanding.</li> <li>9. Adopt Flipped class technique by sharing the materials / Sample Videos prior to the class and have discussions on the that topic in the succeeding classes</li> <li>10. Give Programming Assignments</li> </ol>			
<b>Module-1</b>			
<b>Basic Concepts of Number Theory and Finite Fields:</b> 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 $GF(2^m)$ (Text 1: Chapter 3)			
<b>Teaching-Learning Process</b>	Chalk and Talk, YouTube videos, Flipped Class Technique Programming on implementation of Euclidean algorithm, multiplicative inverse, Finite fields of the form $GF(p)$ , construction of finite field over $GF(2^m)$ . <b>RBT Level: L1, L2, L3</b>		
<b>Module-2</b>			
<b>Introduction:</b> Computer Security Concepts, A Model for Network Security (Text 1: Chapter 1) <b>Classical Encryption Techniques:</b> Symmetric cipher model, Substitution techniques, Transposition techniques (Text 1: Chapter 1)			
<b>Teaching-Learning Process</b>	Chalk and Talk, YouTube videos, Flipped Class Technique and PPTs. Programming on Substitution and Transposition techniques. Self-study topics: Security Mechanisms, Services and Attacks. <b>RBT Level: L1, L2, L3</b>		
<b>Module-3</b>			

<p><b>Block Ciphers:</b> Traditional Block Cipher structure, Data encryption standard (DES) (Text 1: Chapter 2: Section 1, 2) The AES Cipher. (Text 1: Chapter 4: Section 2, 3, 4)</p> <p><b>More on Number Theory:</b> Prime Numbers, Fermat's and Euler's theorem, discrete logarithm. (Text 1: Chapter 7: Section 1, 2, 5)</p>	
<b>Teaching-Learning Process</b>	<p>Chalk and Talk, YouTube videos, Flipped Class Technique and PPTs.</p> <p>Implementation of SDES using programming languages like C++/Python/Java/Scilab.</p> <p>Self-study topics: DES S-Box- Linear and differential attacks</p> <p><b>RBT Level: L1, L2, L3</b></p>
<b>Module-4</b>	
<p><b>ASYMMETRIC CIPHERS:</b> Principles of Public-Key Cryptosystems, The RSA algorithm, Diffie - Hellman Key Exchange, Elliptic Curve Arithmetic, Elliptic Curve Cryptography (Text 1: Chapter 8, Chapter 9: Section 1, 3, 4)</p>	
<b>Teaching-Learning Process</b>	<p>Chalk and Talk, YouTube videos, Flipped Class Technique and PPTs.</p> <p>Implementation of Asymmetric key algorithms using programming languages like C++/Python/Java/Scilab</p> <p>Numerical examples on Elliptic Curve Cryptography</p> <p><b>RBT Level: L1, L2, L3</b></p>
<b>Module-5</b>	
<p><b>Pseudo-Random-Sequence Generators and Stream Ciphers:</b></p> <p>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 (Text 2: Chapter 16)</p>	
<b>Teaching-Learning Process</b>	<p>Chalk and Talk, YouTube videos, Flipped Class Technique and PPTs.</p> <p>Implementation of simple stream ciphers using programming languages like C++/Python/Java/Scilab.</p> <p><b>RBT Level: L1, L2, L3</b></p>
<p><b>Course outcomes (Course Skill Set)</b></p> <p>At the end of the course the student will be able to:</p> <ol style="list-style-type: none"> <li>1. Explain traditional cryptographic algorithms of encryption and decryption process.</li> <li>2. Use symmetric and asymmetric cryptography algorithms to encrypt and decrypt the data.</li> <li>3. Apply concepts of modern algebra in cryptography algorithms.</li> <li>4. Design pseudo random sequence generation algorithms for stream cipher systems.</li> </ol>	
<p><b>Assessment Details (both CIE and SEE)</b></p> <p>The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 35% (18 Marks out of 50) in the semester-end examination (SEE), and a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.</p>	
<p><b>Continuous Internal Evaluation:</b></p> <p>Three Unit Tests each of <b>20 Marks (duration 01 hour)</b></p> <ol style="list-style-type: none"> <li>1. First test at the end of 5<sup>th</sup> week of the semester</li> <li>2. Second test at the end of the 10<sup>th</sup> week of the semester</li> <li>3. Third test at the end of the 15<sup>th</sup> week of the semester</li> </ol> <p>Two assignments each of <b>10 Marks</b></p> <ol style="list-style-type: none"> <li>4. First assignment at the end of 4<sup>th</sup> week of the semester</li> <li>5. Second assignment at the end of 9<sup>th</sup> week of the semester</li> </ol> <p>Group discussion/Seminar/quiz any one of three suitably planned to attain the COs and POs for <b>20 Marks (duration 01 hours)</b></p> <ol style="list-style-type: none"> <li>6. At the end of the 13<sup>th</sup> week of the semester</li> </ol>	

The sum of three tests, two assignments, and quiz/seminar/group discussion will be out of 100 marks and will be **scaled down to 50 marks**

(to have less stressed CIE, the portion of the syllabus should not be common /repeated for any of the methods of the CIE. Each method of CIE should have a different syllabus portion of the course).

**CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.**

**Semester End Examination:**

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the subject (**duration 03 hours**)

1. The question paper will have ten questions. Each question is set for 20 marks.
2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), **should have a mix of topics** under that module.

The students have to answer 5 full questions, selecting one full question from each module. Marks scored out of 100 shall be reduced proportionally to 50 marks

**Suggested Learning Resources:**

**Text Books:**

1. William Stallings , "Cryptography and Network Security Principles and Practice", Pearson Education Inc., 6<sup>th</sup> Edition, 2014, ISBN: 978-93-325-1877-3
2. Bruce Schneier, "Applied Cryptography Protocols, Algorithms, and Source code in C", Wiley Publications, 2<sup>nd</sup> 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.

**Web links and Video Lectures (e-Resources)**

- <https://nptel.ac.in/courses/106105031>

**Activity Based Learning (Suggested Activities in Class)/ Practical Based learning**

- Programming Assignments / Mini Projects can be given to improve programming skills



**KSIT**  
K. S. INSTITUTE OF TECHNOLOGY

# K.S. INSTITUTE OF TECHNOLOGY BANGALORE

## DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

**COURSE IN CHARGE** : Mrs.V.SANGEETHA

**COURSE CODE/NAME** : 21EC642/CRYPTOGRAPHY

**SEMESTER/YEAR** : VI/ III/B

**ACADEMIC YEAR** : 2023-2024

Sl. No.	Topic to be covered	Mode of Delivery	Teaching Aid	No. of Periods	Cumulative No. of Periods	Proposed Date
<b>MODULE 1: BASIC CONCEPTS OF NUMBER THEORY &amp; FINITE FIELDS:</b>						
1	Divisibility and division algorithm	L+D	BB	1	1	29 <sup>th</sup> April 2024
2	Modular arithmetic	L+D, PS	BB	1	2	30 <sup>th</sup> April 2024
3	Euclidean algorithm & problems	L+ D, PS	BB	1	3	2 <sup>nd</sup> May 2024
4	Extended Euclidean algorithm & problems	L+D	BB	1	4	13 <sup>th</sup> May 2024
5	Groups, Rings and Fields, Finite fields of the form GF(p), Polynomial arithmetic	L+D	BB	1	5	14 <sup>th</sup> May 2024
6	Finite fields of the form GF(2 <sup>m</sup> )	L+D	BB	1	6	15 <sup>th</sup> May 2024
7	QP problems	L+D,PS	BB	1	7	16 <sup>th</sup> May 2024
<b>MODULE 2: SYMMETRICAL CIPHERS</b>						
8	Computer Security Concepts & A model for Network Security	L+D	LCD	1	8	20 <sup>th</sup> May 2024
9	Classical Encryption Techniques: Symmetrical cipher model	L+D	BB	1	9	21 <sup>st</sup> May 2024
10	Substitution techniques	L+D	BB	1	10	22 <sup>nd</sup> May 2024

11	Problems on Substitution techniques	L+D,PS	BB	1	11	23 <sup>rd</sup> May 2024
12	Substitution techniques types	L+D	BB	1	12	25 <sup>th</sup> May 2024
13	Problems on Substitution techniques	L+D,PS	BB	1	13	30 <sup>th</sup> May 2024
14	Transposition techniques	L+D	BB	1	14	3 <sup>rd</sup> June 2024
15	Problems Transposition techniques	L+D,PS	BB	1	15	4 <sup>th</sup> June 2024
<b>MODULE 3: Block Ciphers</b>						
16	Traditional Block cipher structure	L+D	BB	1	16	5 <sup>th</sup> June 2024
17	Data Encryption standard	L+D	BB	1	17	8 <sup>th</sup> June 2024
18	The AES cipher	L+D	BB	1	18	10 <sup>th</sup> June 2024
19	More on number theory: Prime numbers, Fermat's	L+D	BB	1	19	11 <sup>th</sup> June 2024
20	Euler's theorem	L+D	BB	1	20	12 <sup>th</sup> June 2024
21	Euler's theorem problems	L+D,PS	BB	1	21	13 <sup>th</sup> June 2024
22	Discrete logarithm	L+D	BB	1	22	18 <sup>th</sup> June 2024
23	Euler's theorem problems	L+D,PS	BB	1	23	19 <sup>th</sup> June 2024
24	Fermat's theorem problems	L+D,PS	BB	1	24	20 <sup>th</sup> June 2024
<b>MODULE 4: ASYMMETRIC CIPHER</b>						
25	Principle of public Key cryptosystem	L+D, PS	BB,LCD	1	25	22 <sup>nd</sup> June 2024
26	Principles of Public-Key Cryptosystems: The RSA algorithm	L+D	BB	1	26	23 <sup>rd</sup> June 2024
27	RSA algorithm problems	L+D, PS	BB	1	27	24 <sup>th</sup> June 2024
28	RSA algorithm problems	L+D, PS	BB	1	28	25 <sup>th</sup> June 2024
29	Diffie - Hellman Key Exchange	L+D	BB	1	29	26 <sup>th</sup> June 2024
30	Elliptic Curve Arithmetic,	L+D	BB	1	30	1 <sup>st</sup> July 2024
31	Elliptic Curve Cryptography	L+D	BB	1	31	2 <sup>nd</sup> July 2024
32	problems Elliptic Curve Cryptography	L+D, PS	BB	1	32	3 <sup>rd</sup> July 2024
33	Diffie - Hellman Key Exchange problems	L+D, PS	BB	1	33	4 <sup>th</sup> July 2024
34	Diffie - Hellman Key Exchange problems	L+D, PS	BB	1	34	8 <sup>th</sup> July 2024
35	Elliptic Curve problems	L+D, PS	BB	1	35	9 <sup>th</sup> July 2024
<b>MODULE 5: Pseudo Random : Sequence Generators and Stream Ciphers:</b>						
36	Linear Feedback Shift Registers	L+D	BB	1	36	10 <sup>th</sup> July 2024
37	Linear Feedback Shift Registers Problems	L+D, PS	BB	1	37	11 <sup>th</sup> July 2024

38	Design and analysis of stream ciphers	L+D	BB	1	38	15 <sup>th</sup> July 2024
39	Design & analysis of Stream ciphers using LFSRs	L+D	BB,LCD	1	39	16 <sup>th</sup> July 2024
40	A5 algorithm	L+D	BB	1	40	18 <sup>th</sup> July 2024
41	Hughes XPD/KPD	L+D	BB	1	41	22 <sup>nd</sup> July 2024
42	Nanoteq, Additive generators	L+D	BB	1	42	23 <sup>rd</sup> July 2024
43	Gifford generator, PKZIP	L+D	BB	1	43	24 <sup>th</sup> July 2024
44	Revision	L+D	BB	1	44	25 <sup>th</sup> July 2024
45	Revision	L+D	BB	1	45	26 <sup>th</sup> July 2024
46	Revision	L+D	BB	1	46	30 <sup>th</sup> July 2024

### Text Books:

- William Stallings, "Cryptography and Network Security Principles and Practice", Pearson Education Inc., 6th Edition, 2014, ISBN: 978-93-325-1877-3
- Bruce Schneier, "Applied Cryptography Protocols, Algorithms, and Source code in C", Wiley Publications, 2nd Edition, ISBN: 9971-51-348-X

### Reference Books:

- Understanding Cryptography - A Textbook for Students and Practitioners, Paar, Christof, Pelzl, Jan, Springer (2010).
- Cryptography Engineering: Design Principles and Practical Applications, Niels Ferguson, Bruce Schneier, Tadayoshi Kohno, Wiley (2010).
- Cryptography: Theory and Practice, Third Edition, Douglas R. Stinson, CRC Press (2005).
- Cryptography: A Very Short Introduction, Fred C. Piper; Sean Murphy, Oxford University Press (2002)..

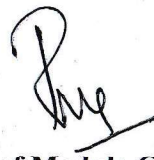
### WEB MATERIALS:


- <https://learncryptography.com/>
- [www.cryptolab.us/](http://www.cryptolab.us/)
- <https://cryptopals.com>

### Details for the teaching Aids

1. BB
2. LCD

  
Signature of Course In charge

  
Signature of Module Coordinator

  
Signature of HOD

K.S. INSTITUTE OF TECHNOLOGY, BANGALORE - 560109



DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

FIRST ASSIGNMENT QUESTIONS 2023-24 EVEN SEMESTERS

Batch	2021- 2025		
Year/Semester/section	III/VI / A		
Course Code-Title	21EC642 - CRYPTOGRAPHY		
Name of the Course in charge	Dr P N Sudha Mrs.V.Sangeetha	Dept	ECE

Note: K-Levels: K1-Remembering, K2-Understanding, K3-Applying, K4-Analyzing, K5-Evaluating, K6-Creating

Assignment No: 1		Total marks:10		
Date of Issue:22 <sup>nd</sup> May 2024		Date of Submission: 30 <sup>th</sup> May 2024		
Sl.No	Assignment Questions	K Level	CO	Marks
1.	List all the properties of modular arithmetic	K3	1	1
2.	Solve & find GCD for (1960,1066)	K3	1	1
3.	Solve & find inverse of $1234 \pmod{4321}$	K3	1	1
4.	Solve & find GCD for the polynomial $x^6+x^5+x^4+x^3+x^2+x+1$ and $x^4+x^2+x+1$	K3	1	1
5.	Solve & find inverse of $(x^8+x^4+x^3+x+1) \pmod{(x^7+x+1)}$	K3	1	1
6.	Construct mod 7 additive and multiplicative table and solve inverse for all the set values	K3	1	1
7.	Construct mod 11 additive and multiplicative table and Solve inverse for all the set values. Also Solve & find GCD(USN,67)	K3	2	2
8.	Solve & find inverse for the given problems 1] $23^{-1} \pmod{11}$ 2] $6^{-1} \pmod{23}$ 3] $4^{-1} \pmod{7}$ 4] $9^{-1} \pmod{13}$	K3	2	2

  
COURSE IN-CHARGE

  
HOD-ECE





DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING  
ASSIGNMENT 1-QUESTIONS

Academic Year	2023-2024		
Batch	2021-2025		
Year/Semester/section	III/VI/ B		
Subject Code-Title	21EC642-CRYPTOGRAPHY		
Name of the Instructor	Mrs. SANGEETHA.V	Dept	ECE

- Commutative laws  $(a + b) \bmod n = (b + a) \bmod n$   
 $(a \times b) \bmod n = (b \times a) \bmod n$
- Associative laws  $[(a + b) + c] \bmod n = [a + (b + c)] \bmod n$   
 $[(a \times b) \times c] \bmod n = [a \times (b \times c)] \bmod n$
- Distributive laws  $[a \times (b + c)] \bmod n = [(a \times b) + (a \times c)] \bmod n$
- Identities  $(a + 0) \bmod n = a \bmod n$   
 $(a \times 1) \bmod n = a \bmod n$
- Additive inverse (-a)  $\forall a \in \mathbb{Z}_n \exists b \text{ s.t. } a + b = 0 \bmod n$
- Multiplicative inverse ( $a^{-1}$ )  $\forall a (\neq 0) \in \mathbb{Z}_n$ , if a is relative prime to n,  
 $\exists b \text{ s.t. } a \times b = 1 \bmod n$

1) (2M)

q	a	b	r
1	1960	1066	894
1	1066	894	172
5	894	175	34
5	172	34	2
17	34	2	0
X	2	0	X

2)  $\text{GCD}(1960,1066)=2$  (2M)

3) The Multiplicative inverse of 1234 and 4321= $4321-1032=3239$

q	a	b	r	T <sub>1</sub>	T <sub>2</sub>	T
3	4321	1234	619	0	1	-3
1	1234	619	615	1	-3	4
1	619	615	4	-3	4	-7
153	615	4	3	4	-7	1075
1	4	3	1	-7	1075	-1032
3	3	1	0	1075	-108	4321
x	1	0	X	-1032	4321	0

(2M)

4)

q	a	b	r
$x^2+x$	$x^6+x^5+x^4+x^3+x^2+x+1$	$x^4+x^2+x+1$	$x^3+x^2+1$
$x+1$	$x^4+x^2+x+1$	$x^3+x^2+1$	0
$x$	$x^3+x^2+1$	0	$x$

(2M)

5)

q	a	b	r
x	$x^8+x^4+x^3+x+1$	$x^7+x+1$	$x^4+x^3+x^2+1$
$x^3+x^2+1$	$x^7+x+1$	$x^4+x^3+x^2+1$	x
$x^3+x^2+x$	$x^4+x^2+x+1$	x	1
1	x	1	0
X	1	0	x

6)

+	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

a	-a
0	0
1	6
2	5
3	4
4	3
5	2
6	1

x	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

a	$a^{-1}$
1	1
2	4
3	5
4	2
5	3
6	6

	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1


7)

8) Solve & find inverse for the given problems

1]  $23^{-1} \pmod{11} = 2$  2]  $6^{-1} \pmod{23} = 4$  3]  $4^{-1} \pmod{7} = 2$  4]  $9^{-1} \pmod{13} = 3$

(2M)

  
Course In-charge

  
HOD-ECE



KSIT Bangalore

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING  
ASSIGNMENT 1A-QUESTIONS

Academic Year	2023-2024		
Batch	2021-2025		
Year/Semester/section	III/VI/ B		
Subject Code-Title	21EC642-Cryptography		
Name of the Instructor	Mrs. SANGEETHA.V	Dept	ECE

Assignment No: 1A  
Date of Issue: 25.6.24

Total marks:10  
Date of Submission: 2.7.24

Sl.No	Assignment Questions	K Level	CO	Marks
1.	Encrypt the plain text 'PAY' using Hill cipher algorithm and Solve the cipher text. Given Key K=	Applying K3	CO2	2
2.	Make use of Feistel structure with neat diagram and explain Feistel encryption and decryption model .	Applying K3	CO3	2
3.	Solve the following by using Fermats theorem (i) $\phi(169)$ (ii) $\phi(35)$ (iii) $\phi(1000)$	Applying K3	CO3	2
4.	Solve the following by using Eulers theorem (i) mod7 (ii) mod 6	Applying K3	CO3	2
5.	Make use of the model of symmetric cryptosystems and explain in detail with diagram	Applying K3	CO4	2

  
Course In-charge

  
HOD-ECE



KSIT Bangalore

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING  
ASSIGNMENT/2-QUESTIONS

Academic Year	2023-2024		
Batch	2021-2025		
Year/Semester/section	III/VI/ B		
Subject Code-Title	21EC642-CRYPTOGRAPHY		
Name of the Instructor	Mrs. SANGEETHA.V	Dept	ECE

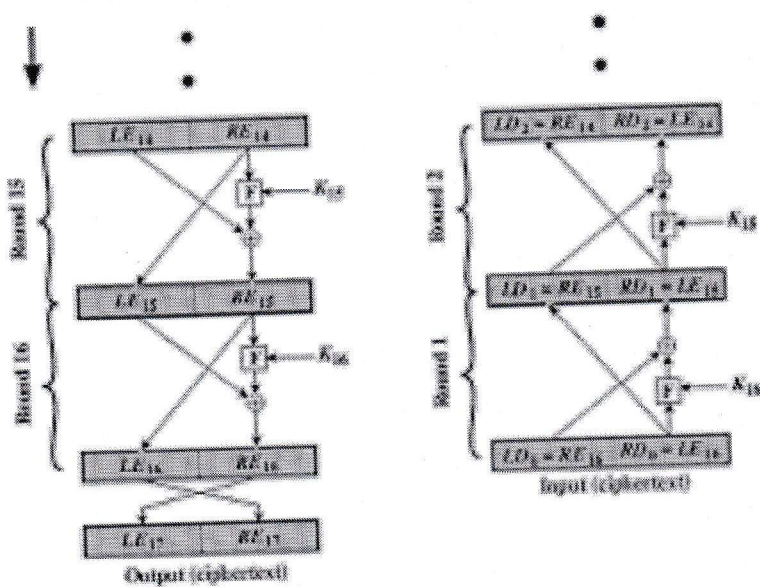
1)  $K = \begin{bmatrix} 17 & 17 & 15 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$

$P = [15 \ 0 \ 24], c = [17 \ 17 \ 5], K^{-1} = K = \begin{bmatrix} 8 & 3 & 7 \\ 17 & 23 & 2 \\ 22 & 0 & 21 \end{bmatrix}$

(2M)

2) Feistel Encryption and Decryption Model:

(2M)



3) (i)  $\Phi(169) = 156$  (ii)  $\Phi(35) = 24$  (iii)  $\Phi(1000) = 400$

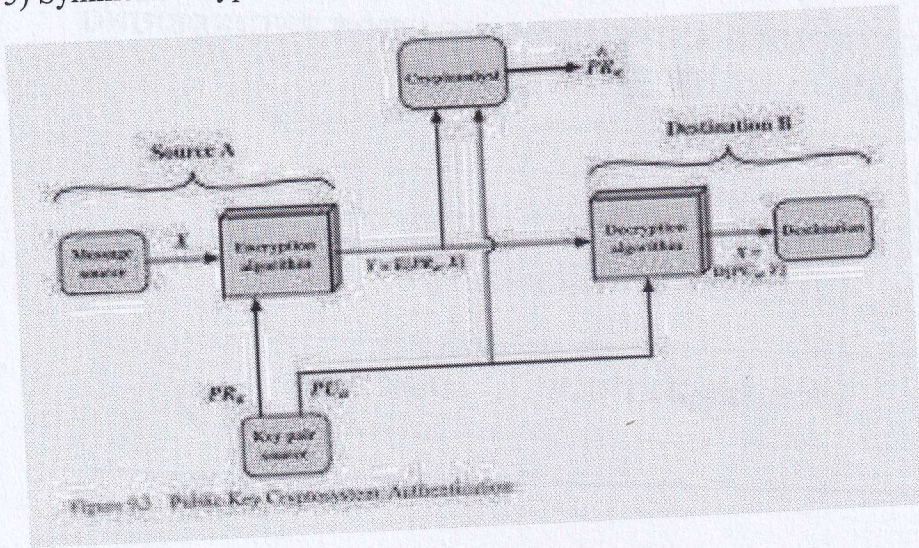
(2M)

4) (i)  $125^{127} \bmod 7 = 125 \bmod 7 = 6$  (ii)  $75^{750} \bmod 6 = 75 \bmod 6 = 1$

(2M)

(2M)

5) Symmetric Cryptosystem :



*V. S. S.*  
Course In-charge

*[Signature]*  
HOD-ECE



**K.S. INSTITUTE OF TECHNOLOGY, BANGALORE - 560109**  
**FIRST INTERNAL TEST QUESTION PAPER-2023-24 EVEN SEMESTER**  
**SET A**

USN									
-----	--	--	--	--	--	--	--	--	--


Degree : B.E Semester : VI A& B  
 Branch : Electronics & Communication Engg. Course Code : 21EC642  
 Course Title : Cryptography Date : 29<sup>th</sup> MAY 2024  
 Duration : 60 Minutes Max Marks : 20

**Note: Answer ONE full question from each part.**

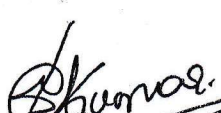
K-Levels: K1-Remembering, K2-Understanding, K3-Applying, K4-Analyzing, K5-Evaluating, K6-Creating

Q No.	Question	Marks	CO mapping	K-Level
<b>PART-A</b>				
1(a)	Explain the extended Euclid's algorithm for determining the multiplicative inverse of two positive integers. Solve the GCD of (24140,16762)	4	C01	K3
(b)	State the axioms of Field and Solve additive & multiplicative table for GF(2 <sup>2</sup> ) give primitive polynomial as (x <sup>2</sup> +x+1)	4	C01	K3
(c)	Construct additive and multiplicative table for Z <sub>7</sub> and Solve all additive and multiplicative inverse elements	4	C01	K3
<b>OR</b>				
2(a)	Explain the Euclid's algorithm & find GCD of a number and Solve the multiplicative inverse of 1234 mod 4321	4	C01	K3
(b)	Check whether (X <sup>3</sup> +X <sup>2</sup> +1) is irreducible and Solve multiplicative inverse for (X <sup>3</sup> +X <sup>2</sup> +1) mod (X <sup>2</sup> +X+1)	4	C01	K3
(c)	Construct mod8 additive and multiplicative table and Solve all additive and multiplicative inverse elements.	4	C01	K3
<b>PART-B</b>				
3(a)	Make use of Symmetrical encryption model and explain it with a neat diagram and define Substitution Technique and Transposition technique.	4	C02	K3
(b)	Make use of Playfair algorithm and solve cipher text for "TECHNOLOGY" with keyword "ATTACK"	4	C02	K3
<b>OR</b>				
4(a)	Encrypt the plain text MONDAY using Hill cipher with key [J E F H] and Solve inverse of the Key matrix.	4	C02	K3
(b)	Make use of Playfair algorithm and Explain it with an example.	4	C02	K3

  
 Name & Signature of  
 Course In charge:

  
 Name & Signature of  
 Module Coordinator

  
 HOD ECE

  
 Principal

*Selected*



**K.S. INSTITUTE OF TECHNOLOGY, BANGALORE - 560109**  
**I SESSIONAL TEST QUESTION PAPER 2023-24 ODD SEMESTER**  
**SCHEME AND SOLUTION for SET A**

**Degree: B.E**  
**Branch: E&CE**  
**Course Title : Cryptography**

**Semester: VI A & B**  
**Course Code: 21EC642**  
**Max Marks: 20**

**1 a**

The Euclidean Algorithm for finding GCD(A,B) is as follows:  
 If  $A = 0$  then  $GCD(A,B)=B$ , since the  $GCD(0,B)=B$ , and we can stop.  
 If  $B = 0$  then  $GCD(A,B)=A$ , since the  $GCD(A,0)=A$ , and we can stop.  
 Write A in quotient remainder form ( $A = B \cdot Q + R$ )  
 Find GCD(B,R) using the Euclidean Algorithm since  $GCD(A,B) = GCD(B,R)$

2M

$GCD(24140, 16762) = GCD(16762, 7378) = GCD(7378, 2006) =$   
 $GCD(2006, 1360) = GCD(1360, 646) = GCD(646, 68) = GCD(68, 34) =$   
 $GCD(34, 0) = 34$

2M

4M

**1b**

**Properties of Field**  
 Satisfies all the properties of group like closure, associative, Identity, Inverse and commutative property and also satisfies properties of Ring like closure, associative, Identity, distributive and also satisfies Inverse property.

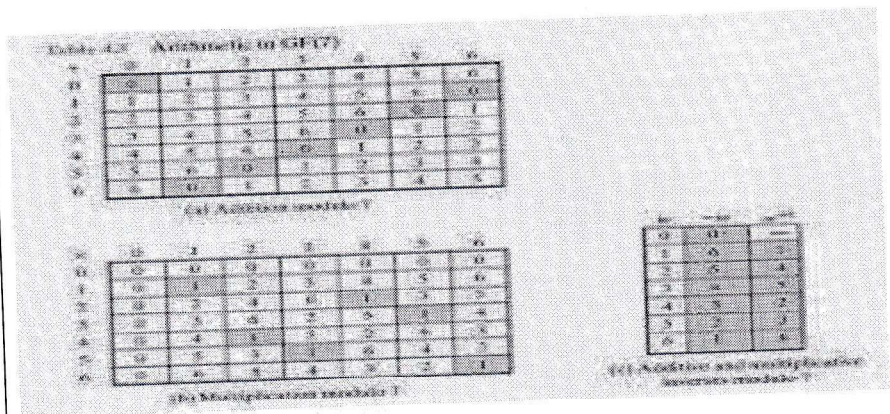
Additive & Multiplicative table for  $GF(2^2)$  give primitive polynomial as  $(x^2+x+1)$   
 Set elements are  $(0,1,X,X+1)$   
 Additive inverse of

4M

Elements	Additive Inverse	Multiplicative Inverse
0	0	0
1	1	1
X	X	X+1
X+1	X+1	X

Additive and multiplicative table for  $Z_7$

**1c**



4M

**2a.**

The explanation of Euclid's algorithm 1M

Multiplicative inverse of  $1234 \pmod{4321} = 3239 \pmod{4321}$  3M

4M

2b. Yes  $(X^3+X^2+1)$  is irreducible and  
 The multiplicative inverses for  $(X^3+X+1)^{-1} \pmod{(X^2+X+1)}$  is  $[x+1]$   
 $(X^2+X+1)^{-1} \pmod{(X^3+X+1)} = x^2$

2c. mod8 additive and multiplicative

(A) Addition modulo 8

	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

4M

(B) Multiplication modulo 8

	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	1	0	3	1
6	0	6	4	2	0	6	2	0
7	0	7	6	5	3	1	7	3

(C) Additive and multiplicative inverses modulo 8

a	a <sup>-1</sup>
1	1
3	3
5	5
7	7

3a. Symmetrical encryption model

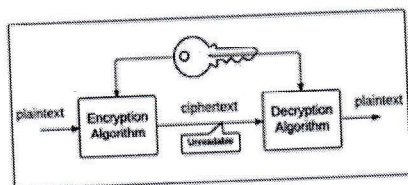


Diagram & Explanation 3M

4M

Define for Substitution & Transposition Techniques: 1M

4M

3b. PLAY FAIR cipher with the key **ATTACK** encrypt the message  
 "TECHNOLOGY" 4M

4a.  $K^{-1} = \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix}$

4M

4b. Explanation Playfair algorithm with an example

4M





**K.S. INSTITUTE OF TECHNOLOGY, BANGALORE - 560109**  
**FIRST INTERNAL TEST QUESTION PAPER 2023-24 EVEN SEMESTER**  
**SET B**

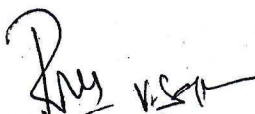
USN									
-----	--	--	--	--	--	--	--	--	--

Degree : B.E Semester : VI A& B  
 Branch : Electronics & Communication Engg. Course Code : 21EC642  
 Course Title : Cryptography Date : 29<sup>th</sup> MAY 2024  
 Duration : 60 Minutes Max Marks : 20

**Note: Answer ONE full question from each part.**

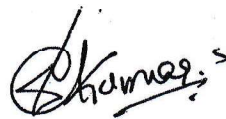
K-Levels: K1-Remembering, K2-Understanding, K3-Applying, K4-Analyzing, K5-Evaluating, K6-Creating

Q No.	Question	Marks	CO mapping	K-Level
<b>PART-A</b>				
1(a)	Mention all modular arithmetic properties & obtain additive & multiplicative table for Mod5 and Solve all additive & multiplicative inverse for the same	4	CO1	K3
(b)	Solve GCD [a(x),b(x)] for a(x) = x <sup>6</sup> +x <sup>5</sup> +x <sup>4</sup> +x <sup>3</sup> +x <sup>2</sup> +x+1 and b(x) = x <sup>4</sup> +x <sup>2</sup> +x+1 and write all modular arithmetic properties	4	CO1	K3
(c)	Construct additive and multiplicative table for GF(7) and Solve all additive and multiplicative inverse elements	4	CO1	K3
<b>OR</b>				
2(a)	Solve the multiplicative inverse of a(x) = x <sup>8</sup> +x <sup>4</sup> +x <sup>3</sup> +x+1 and b(x) = x <sup>7</sup> +x+1	4	CO1	K3
(b)	Check whether (X <sup>4</sup> +X <sup>3</sup> +X <sup>2</sup> +1) is irreducible and Solve multiplicative invers for (X <sup>3</sup> +X+1) mod (X <sup>2</sup> +X+1)	4	CO1	K3
(c)	Construct Z <sub>8</sub> additive and multiplicative table and Solve all additive and multiplicative inverse elements.	4	CO1	K3
<b>PART-B</b>				
3(a)	Make use of Symmetric Crypto system and explain it with a neat diagram and define reducible and irreducible polynomial.	4	CO2	K3
(c)	Make use of playfair cipher ,Encrypt the plain text "ELECTRONICS" with a key INDIA also mention all the rules for encryption.	4	CO2	K3
<b>OR</b>				
4(a)	Encrypt the plain text MONDAY using Hill cipher with key $K = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$ and Solve inverse of the Key matrix	4	CO2	K3
(b)	Make use of Playfair cipher with the key largest encrypt the message "Must see you today"	4	CO2	K3

  
 Name & Signature of Course In charge:

  
 Name & Signature of Module Coordinator

  
 HOD ECE

  
 Principal



**K.S. INSTITUTE OF TECHNOLOGY, BANGALORE - 560109**  
**I SESSIONAL TEST QUESTION PAPER 2023-24 ODD SEMESTER**  
**SCHEME AND SOLUTION for SET B**

**Degree: B.E**  
**Branch: E&CE**  
**Course Title : Cryptography**

**Semester: VI A & B**  
**Course Code: 21EC642**  
**Max Marks: 20**

**1 a**

Mod 5

Additive modulo 5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

multiplication modulo 5

X	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

4M

**1b**

GCD a

$a(x) = x^6+x^5+x^4+x^3+x^2+x+1$  and 3M

$b(x) = x^4+x^2+x+1$

is  $x^3+x^2+1$

Modular Properties :

$(a+b) \text{ mod } n = a \text{ mod } n + b \text{ mod } n$  1M

$(a-b) \text{ mod } n = a \text{ mod } n - b \text{ mod } n$

$(a*b) \text{ mod } n = a \text{ mod } n * b \text{ mod } n$

4M

**1c**

Additive and multiplicative table for  $x^3+x+1$

		000	001	010	011	100	101	110	111
	*	0	1	x	x+1	x <sup>2</sup>	x <sup>2</sup> +1	x <sup>2</sup> +x	x <sup>2</sup> +x+1
000	0	0	0	0	0	0	0	0	0
001	1	0	1	x	x+1	x <sup>2</sup>	x <sup>2</sup> +1	x <sup>2</sup> +x	x <sup>2</sup> +x+1
010	x	0	x	x <sup>2</sup>	x <sup>2</sup> +x	x+1	1	x <sup>2</sup> +x+1	x <sup>2</sup> +1
011	x+1	0	x+1	x <sup>2</sup> +x	x <sup>2</sup> +1	x <sup>2</sup> +x+1	x <sup>2</sup>	1	x
100	x <sup>2</sup>	0	x <sup>2</sup>	x+1	x <sup>2</sup> +x+1	x <sup>2</sup> +x	x	x <sup>2</sup> +1	1
101	x <sup>2</sup> +1	0	x <sup>2</sup> +1	1	x <sup>2</sup>	x	x <sup>2</sup> +x+1	x+1	x <sup>2</sup> +x
110	x <sup>2</sup> +x	0	x <sup>2</sup> +x	x <sup>2</sup> +x+1	1	x <sup>2</sup> +1	x+1	x	x <sup>2</sup>
111	x <sup>2</sup> +x+1	0	x <sup>2</sup> +x+1	x <sup>2</sup> +1	x	1	x <sup>2</sup> +x	x <sup>2</sup>	x+1

4M

**2a.**

Multiplicative Inverse for  $a(x) = x^8+x^4+x^3+x+1$  is and

$b(x) = x^7+x+1$  is  $x^7$

**2b**

No  $(X^4+X^3+X^2+1)$  is not irreducible and

The multiplicative invers for  $(X^3+X+1) \text{ mod } (X^2+X+1)$

X and X+1

2c.

$Z_8$  additive and multiplicative table

Table 4.2 Arithmetic Modulo 8

(a) Addition modulo 8

x \ y	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

(b) Multiplication modulo 8

x \ y	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	5	4	7	2
4	0	4	0	5	4	0	7	3
5	0	5	4	1	4	0	2	7
6	0	6	4	7	0	2	4	6
7	0	7	2	3	7	3	6	1

(c) Additive and multiplicative inverse modulo 8

x	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	5	4	7	2
4	0	4	0	5	4	0	7	3
5	0	5	4	1	4	0	2	7
6	0	6	4	7	0	2	4	6
7	0	7	2	3	7	3	6	1

4M

4M

3a.

model of Symmetric Crypto system

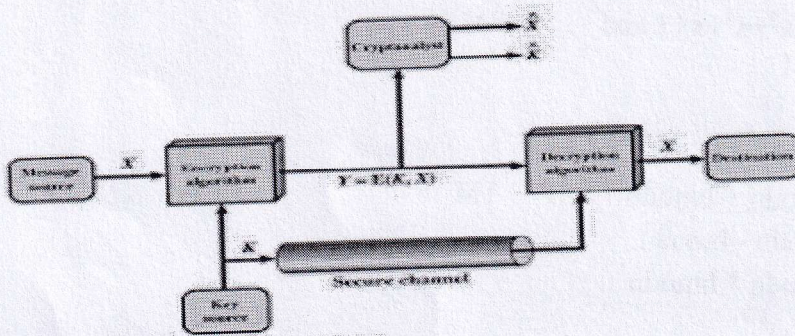


Figure 2.2 Model of Symmetric Cryptosystem

4M

3b.

INDIA  
EL EC TR ON IC SX  
LR FE US LA CK XD

4M

4a

plain text MONDAY using Hill cipher with key

$K = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$   
 $k^{-1} = \begin{pmatrix} 24 & 5 \\ 19 & 14 \end{pmatrix}$

PlayFair cipher with the key **largest** encryt the message "Must see you today"

MU ST SE EY OU TO DA YX

4M

4b.

UZ TB DL GZ PN AW TE ZY

4M

*V. S. K.*  
Signature of Course in-charge

*P. S.*  
Signature of Module Coordinator

*P. S.*  
Signature of HOD ECE



**K.S. INSTITUTE OF TECHNOLOGY, BANGALORE - 560109**  
**SECOND INTERNAL TEST QUESTION PAPER 2023-24 EVEN SEMESTER**  
**SET A**

USN										
-----	--	--	--	--	--	--	--	--	--	--

Degree : B.E  
 Branch : Electronics & Communication Engg.  
 Course Title : Cryptography  
 Duration : 60 Minutes

Semester : VI A& B  
 Course Code : 21EC642  
 Date : 29<sup>th</sup> June 2024  
 Max Marks : 20

**Note: Answer ONE full question from each part.**

K-Levels: K1-Remembering, K2-Understanding, K3-Applying, K4-Analyzing, K5-Evaluating, K6-Creating

Q No.	Question	Marks	CO mapping	K-Level
<b>PART-A</b>				
1(a)	Explain with a neat diagram the operation performed in 1 <sup>st</sup> & 10 <sup>th</sup> round of AES algorithm.	4	CO3	K2
(b)	State & prove Fermat's theorem and Solve $3^{990} \pmod{91}$ & $3^{999} \pmod{10}$ using it	4	CO3	K3
(c)	With a neat diagram explain round operation in DES encryption	4	CO3	K2
<b>OR</b>				
2(a)	With a neat diagram of DES encryption & decryption process and explain the working principle for the same.	4	CO3	K2
(b)	Explain Key expansion technique in AES algorithm & Define Euler's theorem and Solve Totient function for 37 & 600	4	CO3	K3
(c)	Explain the parameters of Feistel structure and design Feistel network for encryption & decryption.	4	CO3	K2
<b>PART-B</b>				
(a)	Encrypt the plain text 'PAYMOREMONEY' using Hill cipher algorithm and Solve the cipher text. Given Key $K = \begin{bmatrix} 17 & 17 & 15 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$	4	CO2	K3
(b)	With a neat block diagram explain the Principles of Public-Key Cryptosystems with authentication & Solve cipher text and plain text using the RSA algorithm given $P=5, Q=11, e=3$ and encrypt the message $M=EC$ and decrypt the same.	4	CO4	K3
<b>OR</b>				
(a)	Make use of Substitution and Transposition technique definition with an example also define Diffusion and Confusion technique. solve the Encrypt the plain text AUTHENTICATION using Rail fence method & Key technique given KEY as 4132	4	CO2	K3
b)	Make use of the concepts of Public key explain Principles of Public-Key Cryptosystems with authentication and secrecy with a neat diagram. & Explain RSA algorithm	4	CO4	K3

*[Signature]*  
 Name & Signature of  
 Course In charge:

*[Signature]*  
 Name & Signature of  
 Module Coordinator

*[Signature]*  
 HOD ECE

*[Signature]*  
 Principal  
*[Signature]*



**K.S. INSTITUTE OF TECHNOLOGY, BANGALORE - 560109**  
**SECOND INTERNAL TEST 2023-24 EVEN SEMESTER**  
**SCHEME AND SOLUTION for SET A**

Degree : B. E  
 Branch : E&CE  
 Course Title : Cryptography

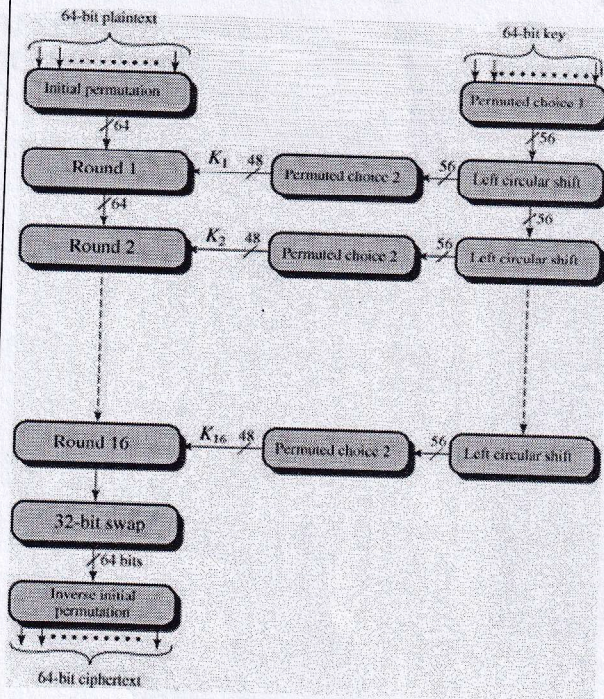
Semester: VI A & B  
 Course Code: 21EC642  
 Max Marks: 30

Q No.	Points	Marks
1 a	<div style="text-align: center;"> </div> <p>Fig 1 M and explanation 3M</p>	4M
1 b	<p>State Fermat's theorem: 1 M          Proof: 2M  <math>3^{990} \bmod 91 = 1</math>                      ½ marks each          &amp;  <math>3^{999} \bmod 10 = 1</math></p>	4M
1 c		4M

2M for diagram & 2M for explanation.

4M

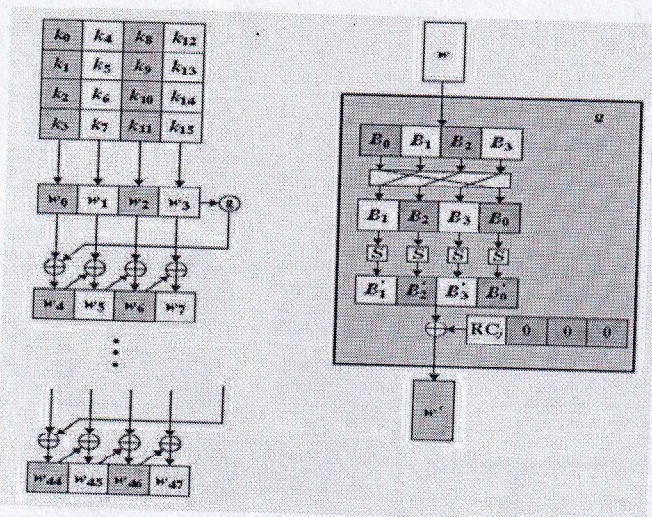
2a. DES encryption & decryption process



1M for diagram & 3M for explanation.

2b.

4M



1M for diagram & 2M for explanation.

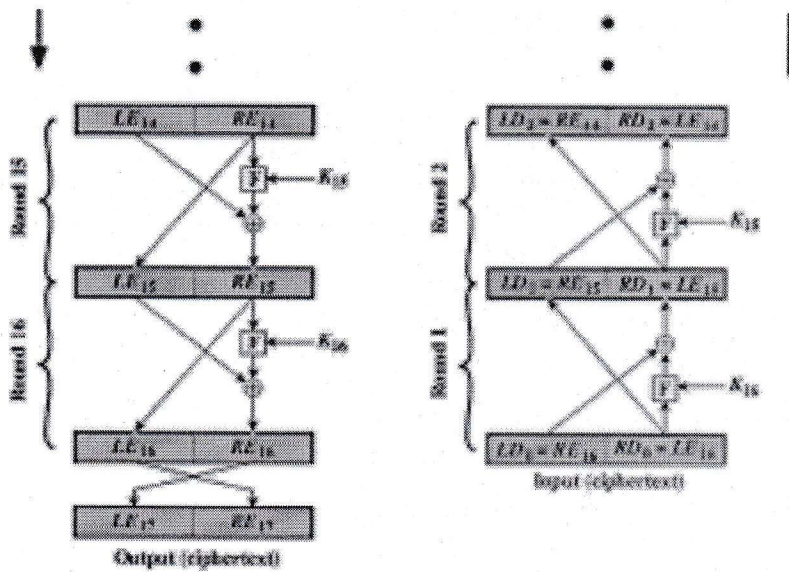
Definition of Euler's theorem

Totient function for  $37=36$

1M

$$600 = 2^3 \cdot 3 \cdot 5^2 = [8-4][3-1][25-5] = 160$$

2c.



4M

1M for diagram & 3M for explanation.

PAYMOREMONEY encrypt using Hill cipher

3a.

Key  $K = \begin{pmatrix} 17 & 17 & 15 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$

Plain text

$\begin{pmatrix} 15 & 0 & 24 \\ 12 & 14 & 17 \\ 4 & 12 & 14 \\ 13 & 4 & 24 \end{pmatrix}$

Cipher =  $\begin{pmatrix} 303 & 303 & 681 \\ 532 & 490 & 797 \\ 348 & 312 & 578 \\ 353 & 341 & 735 \end{pmatrix}$

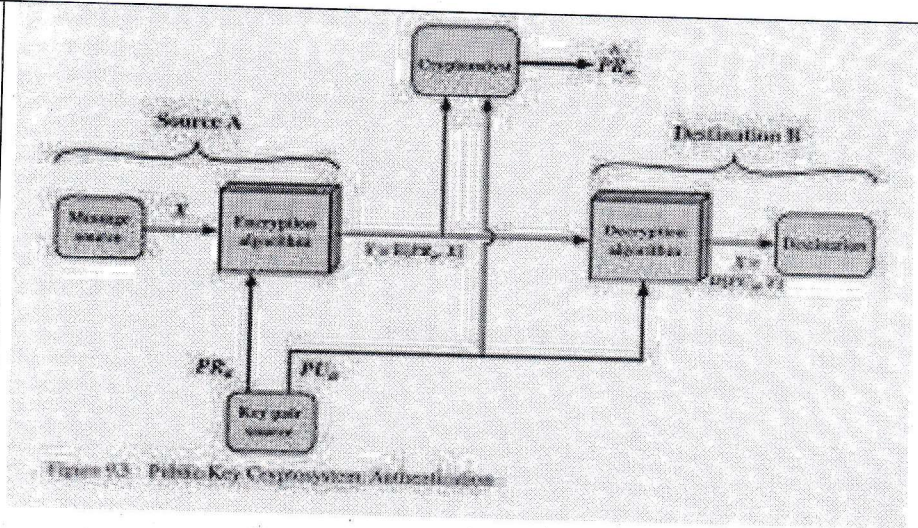
4M

Cipher =  $\begin{pmatrix} 17 & 17 & 5 \\ 12 & 22 & 17 \\ 10 & 0 & 6 \\ 15 & 3 & 7 \end{pmatrix}$

3b

The Principles of Public-Key Cryptosystems with authentication  
1M for diagram & 3M for explanation

4M



RSA algorithm given  $P=5, Q=11, e=3$  and encrypt the message  $M=EC$  and decrypt the same.

$P=5, Q=11, e=3$  and  $M=EC: 42$   
 $n=55, \Phi=40$   
 Given  $e=3$   
 $de \text{ mod } 40 = 1 \quad d=27$   
 Encryption  $C1 = M^e \text{ mod } n = 4^3 \text{ mod } 55 = 9$   
 $C2 = M^e \text{ mod } n = 2^3 \text{ mod } 55 = 8$   
 Decryption  $D = C1^d \text{ mod } n = 9^{27} \text{ mod } 55 = 4$   
 $C1^d \text{ mod } n = 4^{27} \text{ mod } 55 = 2$

4a. Def for Substitution and Transposition technique 1M  
 Diffusion and Confusion technique

AUTHENTICATION using Rail fence method & Key technique given KEY as 4132 4M

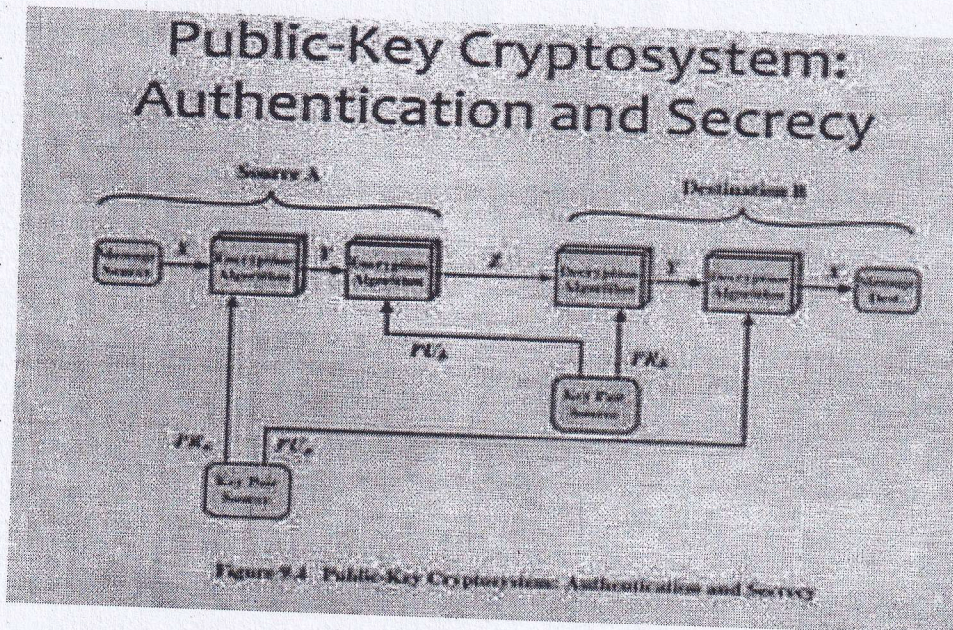
RAILFENCE: A T E T C T O  
           U H N I A I N  
 A T E T C T O U H N I A I N  
 4 1 3 2 O/P UNANHIIXTTTXXAECO  
 A U T H  
 E N T I  
 C A T I  
 O N X X



4b.

The Principles of Public-Key Cryptosystems with authentication and secrecy.

4M



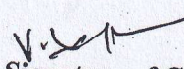
1M for diagram & 1M for explanation

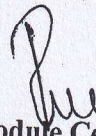
**RSA ALGORITHM**

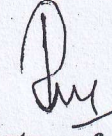
Key Generation	
Select $p, q$	$p$ and $q$ both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p - 1)(q - 1)$	
Select integer $e$	$\text{gcd}(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate $d$	$d = e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption	
Ciphertext:	$C$
Plaintext:	$M = C^d \pmod n$

  
Signature of Course In-charge

  
Signature of Module Coordinator

  
Signature of HOD



**K.S. INSTITUTE OF TECHNOLOGY, BANGALORE - 560109**  
**SECOND INTERNAL TEST QUESTION PAPER 2023-24 EVEN SEMESTER**  
**SET B**

egree : B.E  
 ranch : Electronics & Communication Engg.  
 ource Title : Cryptography  
 uration : 60 Minutes

USN									
-----	--	--	--	--	--	--	--	--	--

Semester : VI A & B  
 Course Code : 21EC642  
 Date : 29<sup>th</sup> June 2024  
 Max Marks : 20

**Note: Answer ONE full question from each part.**

K-Levels: K1-Remembering, K2-Understanding, K3-Applying, K4-Analyzing, K5-Evaluating, K6-Creating

Q No.	Question	Marks	CO mapping	K-Level
<b>PART-A</b>				
1(a)	State & prove Euler's theorem. Solve $\Phi(q)$ and $P^{\Phi(q)} \text{ mod } q$ given values 1) $P=3, q=7$ 2) $q=12, P=5$	4	CO3	K3
(b)	Explain the concept of Substitution byte, Mix column & Shift row operation with neat diagram in AES algorithm	4	CO3	K2
(C)	Illustrate the round operation in DES algorithm & compare DES and AES algorithm	4	CO3	K3
<b>OR</b>				
2(a)	Define a <b>WORD</b> in AES algorithm & illustrate the working of 'g' function in AES Key expansion algorithm with a neat diagram.	4	CO3	K3
(b)	Explain the Feistel encryption and decryption process with a neat diagram	4	CO3	K2
(C)	Define Fermat's little theorem and Solve the value of X given $X^{103} \equiv 4 \text{ mod } 11$ and find the remainder for $2^{35} \text{ mod } 7$ and $7^{20} \text{ mod } 21$	4	CO3	K3
<b>PART-B</b>				
3(a)	List and explain the process used in RSA algorithm for encrypting and decrypting the data & Define Authentication, Digital Signature, Confidentiality	4	CO2	K3
(b)	Encrypt the plain text 'CIPHER' using Hill cipher algorithm and Solve the cipher text. Given Key $K = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$	4	CO4	K3
<b>OR</b>				
4(a)	Solve the encrypted data given the plain text ELECTRONICS using Rail fence method & Key technique given KEY as 4132. & Define Monoalphabetic cipher & Polyalphabetic cipher	4	CO2	K3
(b)	With a neat block diagram explain the Principles of Public-Key Cryptosystems with confidentiality & Solve cipher text given plain text as KS using the RSA algorithm given $P=3, Q=11, e=7$	4	CO4	K3

Name & Signature of Course In charge:

Name & Signature of Module Coordinator

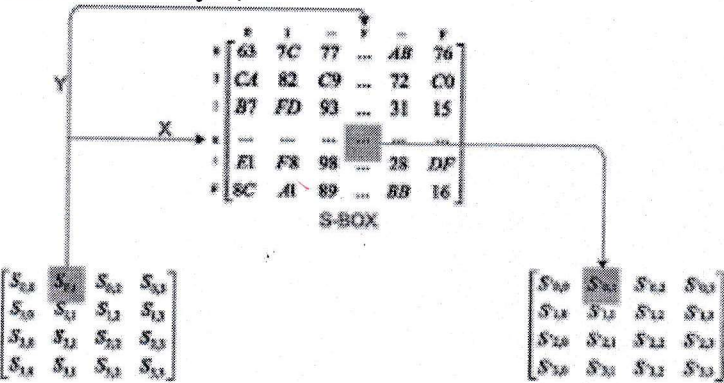
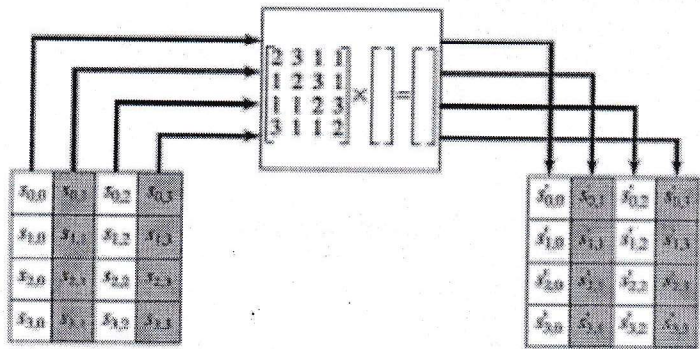
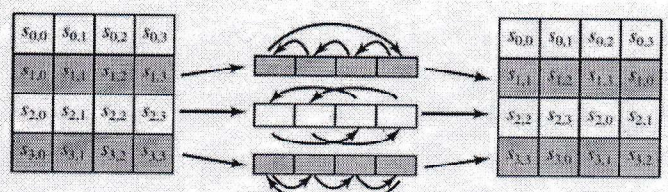
HOD ECE

Principal

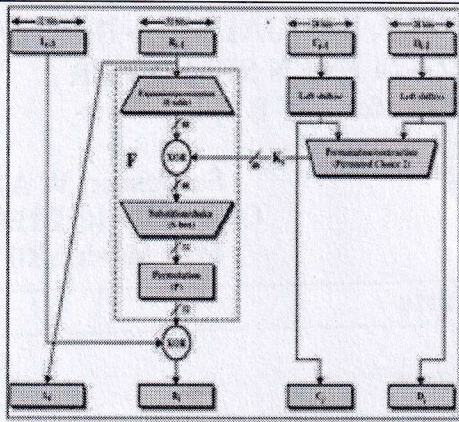
**K.S. INSTITUTE OF TECHNOLOGY, BANGALORE - 560109**  
**SECOND INTERNAL TEST 2023-24 EVEN SEMESTER**  
**SCHEME AND SOLUTION for SET B**

**Degree : B. E**  
**Branch : E&CE**  
**Course Title : Cryptography**

**Semester: VI A & B**  
**Course Code: 21EC642**  
**Max Marks: 30**

Q No.	Points	Marks
1 a	Def of Euler's theorem & proof . Find $\Phi(q)$ for $\Phi(7)=6$ , $\Phi(12)= 2^2*3 = 2*2= 4$ And $P^{\Phi(q)} \text{ mod } q$ given values $3^6 \text{ mod } 7=1$ $5^4 \text{ mod } 12 = 1$	4M
1b	<p><b>Substitution byte,</b></p>  <p><b>Mix column</b></p>  <p><b>Shift row operation in AES algorithm</b></p> <ul style="list-style-type: none"> <li>Rules of shifting rows,                             <ul style="list-style-type: none"> <li>Row 1 → No Shifting</li> <li>Row 2 → 1 byte left shift</li> <li>Row 3 → 2 byte left shift</li> <li>Row 4 → 3 byte left shift</li> </ul> </li> </ul> 	4M

1c



4M

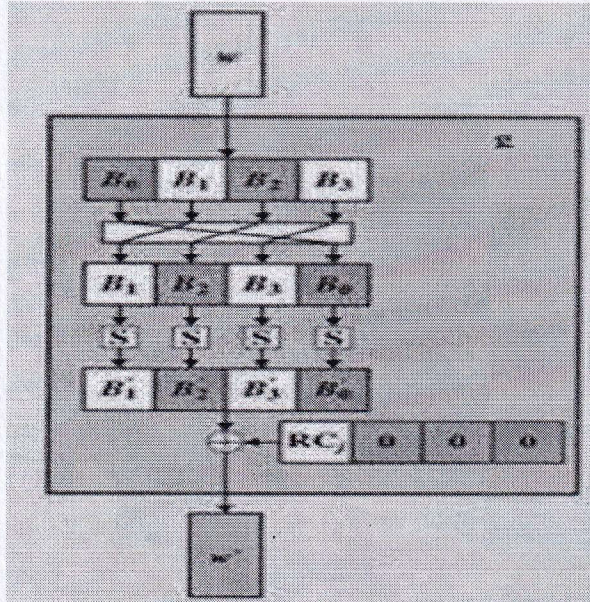
figure 1M & 2M for explanation

Comparison AES does not follow Feistel 1M

2a.

Def of WORD in AES algorithm 1M

The working of 'g' function in AES Key expansion

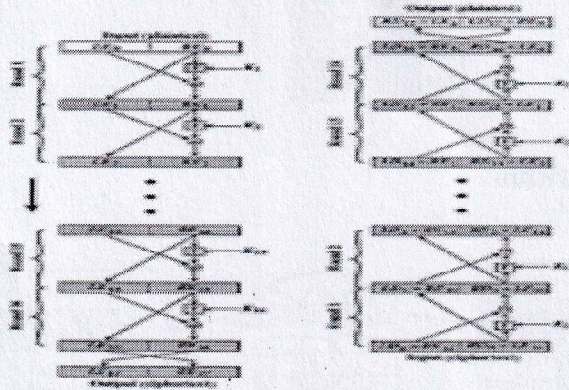


4M

1 M for figure and 2M for explanation

2b.

Feistel encryption and decryption process with a neat diagram



4M

1 M for figure and 3M for explanation

2c.

Definition Fermat's little theorem 1M

X given  $X^{103} \equiv 4 \pmod{11} = 5$  2M

The remainder for  $2^{35} \pmod{7} = 4$  2M  
and  $7^{20} \pmod{21} = 1$

4M

3a

Key Generation	
Select $p, q$	$p$ and $q$ both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer $e$	$\text{gcd}(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate $d$	$d = e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod{n}$

Decryption	
Ciphertext:	$C$
Plaintext:	$M = C^d \pmod{n}$

4M

3b

CIPHER' using Hill cipher algorithm and find the cipher text.

Given Key  $K = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$

Plain text  $\begin{pmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \end{pmatrix}$  cipher  $\begin{pmatrix} 416 & 431 & 307 \\ 434 & 521 & 302 \end{pmatrix} = \begin{pmatrix} 0 & 15 & 21 \\ 18 & 1 & 16 \end{pmatrix}$

4M

4a.

plain text **ELECTRONICS** using Rail fence method & Key technique given KEY as 4132

RAILFENCE: E E T O I S

1M

L C R N C

O/P= ETOISLCRNC

4M

Definition for Monoalphabetic cipher & Polyalphabetic cipher 1M EACH

4b. The Principles of Public-Key Cryptosystems with CONFIDENTIALITY.

4M

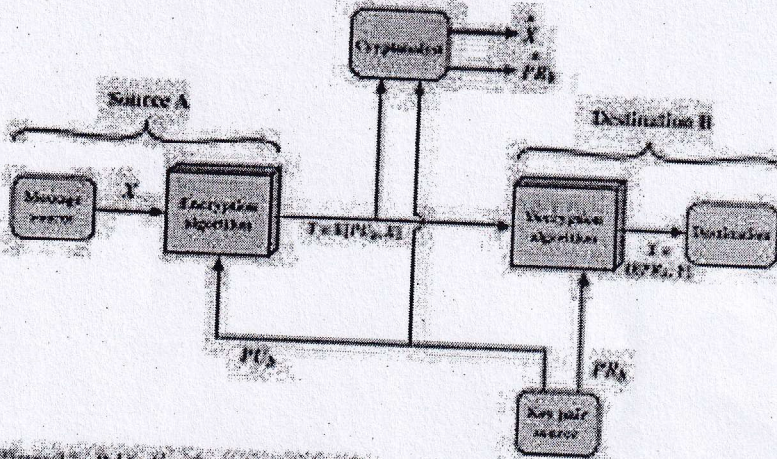


Figure 1.2 Public Key Cryptosystem: Security

2M

KS using the RSA algorithm given  $P=3, Q=11, e=7$   
 $P=3, Q=11, e=7$  and  $M=KS: 10\ 18$

$n=33, \Phi=20$

Given  $e=7$

$de \text{ mod } 20 = 1 \quad d=3$

Encryption  $C1 = M^e \text{ mod } n = 10^7 \text{ mod } 33 = 10$

$C2 = M^e \text{ mod } n = 18^7 \text{ mod } 33 = 6$

Decryption  $D = C1^d \text{ mod } n = 10^3 \text{ mod } 33 = 10$

$C1^d \text{ mod } n = 6^3 \text{ mod } 33 = 18$

2M

*[Signature]*  
 Signature of Course In charge

*[Signature]*  
 Signature of Module Coordinator

*[Signature]*  
 Signature of HOD



**K.S. INSTITUTE OF TECHNOLOGY, BENGALURU - 560109**  
**THIRD INTERNAL TEST QUESTION PAPER 2023-24 EVEN SEMESTER**

**KSIT**

**SET: A**

USN									
-----	--	--	--	--	--	--	--	--	--


Degree : B. E.,  
 Branch : E&CE  
 Course Title : Cryptography  
 Duration : 60 Minutes

Semester : VI  
 Course Code : 21EC642  
 Date : 31<sup>st</sup> July 2024  
 Max Marks : 20

Note: Answer **ONE** full question from each part.

K-Levels: K1-Remebering, K2-Understanding, K3-Appling, K4-Analyzing, K5-Evaluating, K6-Creating

Q No.	Questions	Marks	CO	K-Level
<b>PART-A</b>				
1(a)	<b>Explain</b> Generalized Geffe generator & Alternating Stop & Gogenerator with a neat diagram.	4	CO5	K2
(b)	<b>Explain</b> the application & working of A5 generator and Thresholdgenerator.	4	CO5	K2
(c)	<b>Explain</b> Linear feedback shift register with a neat diagram.	4	CO5	K2
<b>OR</b>				
2(a)	<b>Explain</b> Linear Congruential Generator with an example.	4	CO5	K2
(b)	<b>Explain</b> Gifford generator & Geffe generator.	4	CO5	K2
(c)	<b>Explain</b> Bilateral Stop and Go generator and Jennings Generator	4	CO5	K2
<b>PART -B</b>				
3(a)	<b>Solve</b> P+Q and 2P for the given $E_{11}(8,10)$ , $P=(3,7)$ and $Q=(5,9)$ and explain Elliptic Curve Arithmetic on the curve.	4	CO4	K3
(b)	Make use of Diffie Hellman's Key exchange algorithm and <b>solve</b> Public Key of user A & B for $E_{11}(1,6)$ , $G(1,3)$ and private Key of User A is 2 and B is 1 and explain ECC.	4	CO4	K3
<b>OR</b>				
4(a)	Make use of ECC algorithm encrypt the data given $E_{11}(1,1)$ , $G(1,3)$ , $n=20$ . Assume secret key between the user as 1. <b>Solve</b> all the private key and Public key.	4	CO4	K3
(b)	<b>Solve</b> Shared key if Public Key for $E_{11}(1,1)$ , $G(2,2)$ and private Key of User A is 1 and B is 2 and <b>Explain</b> ECC encryption algorithm.	4	CO4	K3

  
 Name & Signature of  
 Course In charge

  
 Name & Signature of  
 Module Coordinator

  
 HOD ECE

  
 Principal

*Selected*



**K.S. INSTITUTE OF TECHNOLOGY, BANGALORE - 560109**  
**THIRD INTERNAL TEST 2023-24 EVEN SEMESTER**  
**SCHEME AND SOLUTION for SET A**

Degree : B. E  
Branch : E&CE  
Course Title : Cryptography

Semester: VI A & B  
Course Code: 21EC642  
Max Marks: 20

Q No.	Points	Marks
1 a	<p><b>Generalized Geffe Generator:</b></p> <ul style="list-style-type: none"><li>• Instead of choosing between two LFSRs, this scheme chooses between <math>k</math> LFSRs, as long as <math>k</math> is a power of 2.</li><li>• More complex than Geffe generator and correlation attack is possible.</li><li>• Correlation attack is outputs of individual LFSRs can be combined keystream and attacked using linear algebra.</li></ul> <p><b>Alternate Stop and Go Generator</b></p> <ul style="list-style-type: none"><li>• It uses three LFSRs of different length. LFSR-2 is clocked when the output of LFSR-1 is 1;</li><li>• LFSR-3 is clocked when the output of LFSR-1 is 0. The output of the generator is the XOR of LFSR-2 and LFSR-3. This generator has a long period and large linear complexity.</li><li>• The correlation attack found against LFSR-1, but it does not substantially weaken the generator. There have been other attempts at keystream generators along these lines</li></ul>	4M
1b	<p><b>A5:</b></p> <ul style="list-style-type: none"><li>• A5 consist of 3 LFSRs; register lengths are 19, 22 and 23 ;</li><li>• All the feedback polynomials are sparse.</li><li>• The output is the XOR of the three LFSRs.</li><li>• A5 uses variable control clock. 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 LFS of clock in each round.</li><li>• The basic ideas behind A5 are good.</li><li>• It is very efficient. It passes all non statistical tests; it's only known weakness is that it's registers are short enough to make exhaustive search feasible. Variants of A5 with the longer shift registers and denser feedback polynomials should be secure.</li></ul>	4M



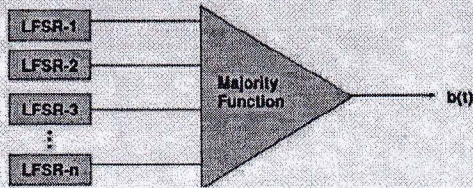
1c

Lets assume that we use three LFSRs, then the output generator can be written as:

$$b = (a_1 \wedge a_2) \oplus (a_1 \wedge a_3) \oplus (a_2 \wedge a_3) \text{ (similar to Geffe)}$$

Linear complexity:

$$n_1 n_2 + n_1 n_3 + n_2 n_3 \text{ (larger than Geffe)}$$



Threshold generator:

### Linear feedback shift registers (LFSRs)

• Characteristics:

- LFSRs are well-suited to hardware implementation
- Produce sequences of large period
- Produce sequences with good statistical properties
- Due to their structure, they can be readily analysed using algebraic techniques

• Definition:

A *linear feedback shift register* (LFSR) of length  $L$  consists of  $L$  stages (or delay elements) numbered  $0, 1, \dots, L-1$ , each capable of storing one bit and having one input and one output; and a clock which controls the movement of data. During each unit of time the following operations are performed:

- the content of stage  $0$  is output and forms part of the output sequence
- the content of stage  $i$  is moved to stage  $i-1$  for each  $i, 1 \leq i \leq L-1$
- the new content of stage  $L-1$  is the feedback bit  $s$ , which is calculated by adding together modulo  $2$  the previous contents of a fixed subset of stages  $0, 1, \dots, L-1$

2a.

2b.

A widely used technique for pseudorandom number generation is an algorithm first proposed by Lehmer [LEHM51], which is known as the linear congruential method. Linear congruential generators are pseudo random sequence generators of the form  $X_n = (aX_{n-1} + b) \text{ mod } m$  in which  $X_n$  is the  $n$ th number of the sequence, and  $X_{n-1}$  is the previous number of the sequence. The variables  $a, b$  and  $m$  are constants:  $a$  is the multiplier,  $b$  is the increment, and  $m$  is the modulus. The key or seed is the value of  $X_0$ .

The strength of the linear congruential algorithm is that if the multiplier and modulus are properly chosen, the resulting sequence of numbers will be statistically indistinguishable from a sequence drawn at random (but without replacement) from the set  $1, 2, \dots, m-1$ . But there is nothing random at all about the algorithm, apart from the choice of the initial value  $X_0$ . Once that value is chosen, the remaining numbers in the sequence follow deterministically. This has implications for cryptanalysis.

If an opponent knows that the linear congruential algorithm is being used and if the parameters are known (e.g.,  $a = 75, c = 0, m = 231 - 1$ ), then once a single number is discovered, all subsequent numbers are known. Even if the opponent knows only that a linear congruential algorithm is being used, knowledge of a small part of the sequence is sufficient to determine the parameters of the algorithm.

Suppose that the opponent is able to determine values for  $X_0, X_1, X_2$ , and  $X_3$ . Then

$$X_1 = (aX_0 + c) \text{ mod } m$$

$$X_2 = (aX_1 + c) \text{ mod } m$$

$$X_3 = (aX_2 + c) \text{ mod } m$$

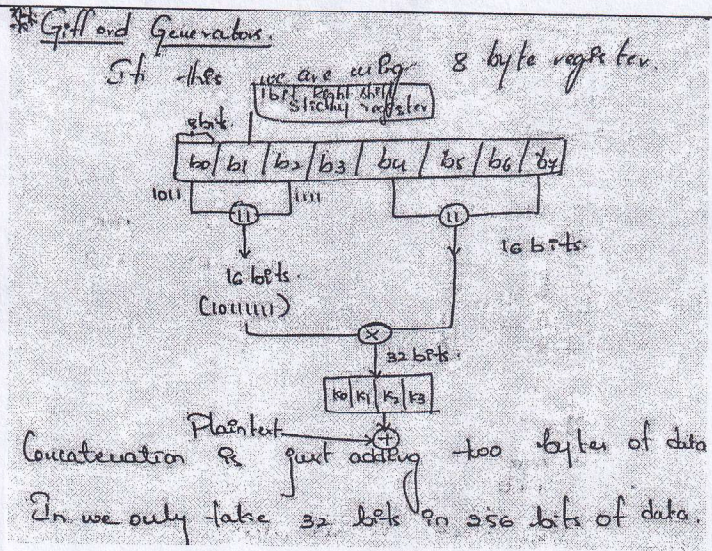
These equations can be solved for  $a, c$ , and  $m$ .

4M

4M

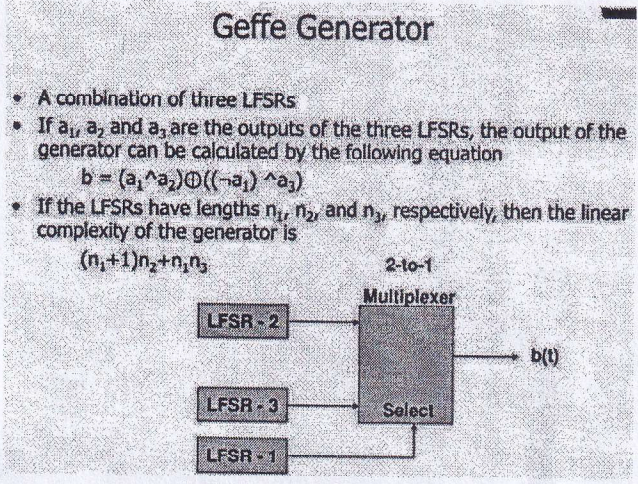
4M

2b.



4M

3a.

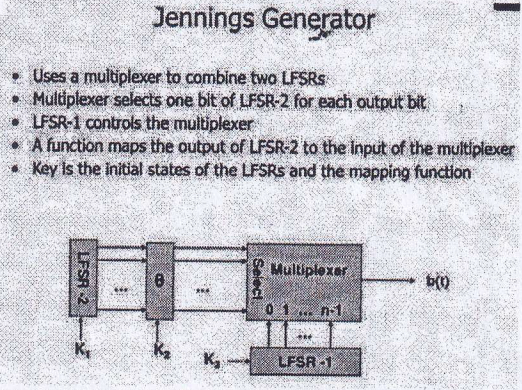


4M

3c.

Bilateral Stop and Go Generator

- This generator uses two LFSRs, both of length 'n'.
- The output of the generator is the XOR of the outputs of each LFSR.
- If the output of LFSR-2 at time t-1 is 0 and at time t-2 is 1, then LFSR-2 does not clock at time 't'.
- Conversely, if the output of LFSR-1 at time t-1 is 0 and the output at t-2 is 1, and if LFSR-1 clocked at time 't', then LFSR-2 does not clock at time 't'.
- The linear complexity of this system is equal to the period.



4M

3a)

$$\Delta = \begin{bmatrix} a-7 \\ 5-3 \end{bmatrix} = \frac{2}{2} = 1$$

$$x_{p+q} = \Delta^2 - \alpha_p - \alpha_q = 1^2 - 3 - 5$$

$$\Rightarrow 1 - 8 = -7 \pmod{11} \Rightarrow 4$$

$$y_{p+q} = \Delta(x_p - x_{p+q}) - y_p$$

$$= 1(3 - (-7)) - 7$$

$$= 1(3+7) - 7 \Rightarrow 10 - 7 = 3$$

$$p+q = (4, 3)$$

$$y_{2p} = 4, x_{2p} = 3$$

$$2p = (3, 4)$$

4b.

$$2p = p+p$$

$$= (3, 2) + (3, 2)$$

$$\Delta = \frac{3x^2 + 9}{2 \cdot 4p} = \frac{3(3)^2 + 9}{2(7)} = \frac{3(9) + 9}{14} = \frac{33 + 9}{14}$$

$$[\Delta] = \frac{33}{14} \pmod{11} \Rightarrow \begin{pmatrix} 2 \\ 13 \end{pmatrix} \pmod{11} \Rightarrow \begin{pmatrix} 2 \\ 2 \end{pmatrix} \pmod{11}$$

$$2 \times 3^2 \pmod{11}$$

$$2 \times 9 \pmod{11}$$

$$\Delta \pmod{11} \Rightarrow 8$$

$$2p = p(1, 2) + p(1, 2)$$

$$\Delta \Rightarrow \frac{3x^2 + 9}{2 \cdot 4p} \Rightarrow \frac{3(1)^2 + 9}{2(3)} \Rightarrow \frac{3+9}{6} \Rightarrow \frac{12}{6} \pmod{11}$$

$$\Rightarrow \frac{2}{3} \pmod{11} \Rightarrow 2 \times 3^2 \pmod{11}$$

$$\Delta_{2p} \Rightarrow 2 \times 4 \pmod{11} \Rightarrow 8 \pmod{11} = 8$$

4M

$$y_A = \Delta(x_p - x_{2p}) - y_p \Rightarrow 8(1-3) - 3 = 8(-2) - 3$$

$$= -16 - 3 \Rightarrow -19 \pmod{11} \Rightarrow -8 \pmod{11} \Rightarrow 3$$

$$y_A = 3$$

use B:

private key  $n_B = 1$

public key  $P_B = n_B G \Rightarrow 1(1, 3) = (1, 3)$

$P_B = (1, 3)$

private key  $n_B = 1$

public key  $P_B = n_B G = 1(1, 3) = (1, 3)$

$P_B = (1, 3)$

private use A

$n_A = 2$

public key  $P_A = n_A G \Rightarrow 2 \cdot (1, 3) \Rightarrow (2, 6)$

$$\Delta \Rightarrow \frac{3x^2 + 9}{2 \cdot 4p} \Rightarrow \frac{3(1)^2 + 9}{2(3)} \Rightarrow \frac{12}{6}$$

$$\Rightarrow 2 \times 3^2 \pmod{11} \Rightarrow 2 \times 9 \pmod{11}$$

$$\Rightarrow 8 \pmod{11} \Rightarrow 8$$

$\Delta = 8$

use B =  $(n_B, P_B) \Rightarrow (1, (1, 3))$

encryption:

$$C = [kM + P_B K]$$

secret key  $K=1$

$$C = [1(1, 3) + 1(1, 3)]$$

$$C = [(1, 3), (1, 3) + (1, 3)]$$

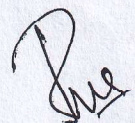
$C = [(1, 3), (2, 6)]$

4b.

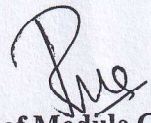
$$X_A = 1, X_B = 1, Y_A = G X_A = (2, 2), X_B = 2, Y_B = 2(2, 2) = (4, 4), = 5,$$

$$K_A = Y_B X_A = G X_A Y_B = (4, 4)(1) = (4, 4), K_B = Y_A X_B = (2, 2)$$

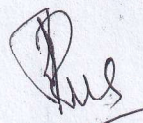
4M



Signature of Course In charge



Signature of Module Coordinator



Signature of HOD



**K.S. INSTITUTE OF TECHNOLOGY, BENGALURU - 560109**  
**THIRD INTERNAL TEST QUESTION PAPER 2023-24 EVEN SEMESTER**

**KSIT**  
A UNIVERSITY OF TECHNOLOGY

**SET: B**

USN									
-----	--	--	--	--	--	--	--	--	--


Degree : B. E.,  
 Branch : E&CE  
 Course Title : Cryptography  
 Duration : 60 Minutes

Semester : VI  
 Course Code : 21EC642  
 Date : 31<sup>st</sup> July 2024  
 Max Marks : 20

Note: Answer **ONE** full question from each part.

K-Levels: K1-Remembering, K2-Understanding, K3-Applying, K4-Analyzing, K5-Evaluating, K6-Creating

Q No.	Questions	Marks	CO	K-Level
<b>PART-A</b>				
1(a)	Make use of Linear Feedback shift register and explain the working of given $g(x)=1+x^2+x^3$ and find the period & Key generated. Consider initial key value as 1,0,0	4	CO5	K3
(b)	Explain the concept of Generalized Geffe generator with an example and definelinearity complex and correlation attack.	4	CO5	K2
(c)	Explain Beth Piper Stop & Go generator & Self-Decimated Generators with a neat diagram.	4	CO5	K2
<b>OR</b>				
2(a)	Make use of Linear Feedback shift register and explain the working of given $g(x)=1+x+x^3$ and solve the period & Key generated. Consider initial key value as 1,0 0 ...	4	CO5	K3
(b)	Explain Additive Generators and FISH additive generator.	4	CO5	K2
(c)	Explain NANOTEQ and RAMBUTAN	4	CO5	K2
<b>PART -B</b>				
3(a)	For the given Elliptical equation $Y^2=X^3+2X+8$ in $z_{11}$ field if the given $G(2,8)$ . Solve public key of user A and B .given $n_A=1, n_B=2$ , plain text $(2,6), K=1$ .	4	CO4	K3
(b)	Make use of an Elliptic Curve Arithmetic on the curve of $E_{23}(1,1), p=(3,10)q=(9,7)$ , Solve $2P+Q$ and explain ECC.	4	CO4	K3
<b>OR</b>				
4(a)	Solve $P+Q$ and $2P, 2Q$ .given $P=(2,7)$ & $Q=(4,10)$ for $GF(7)$ .	4	CO4	K3
(b)	Solve cipher text for message(1,6) given $E_{23}(1,0)$ .consider $n=50, K=1, G(2,8)$ . solve Private and Public key for user A and B $G(4,2)$ and private Key of User A is 1 and B is 2 and Explain ECC encryption algorithm.	4	CO4	K3

  
 Name & Signature of  
 Course In charge

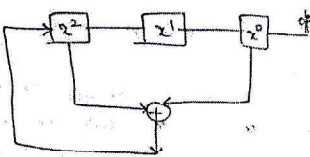

  
 Name & Signature of  
 Module Coordinator

  
 HOD ECE

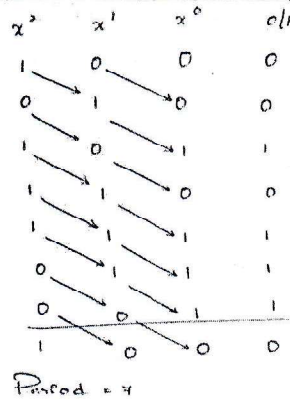
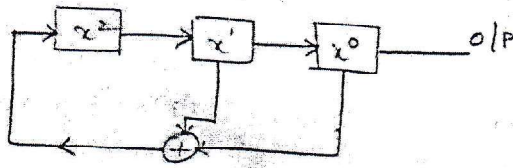
  
 Principal

Degree : B. E  
 Branch : E&CE  
 Course Title : Cryptography

Semester: VI A & B  
 Course Code: 21EC642  
 Max Marks: 20

Q No.	Points	Marks																																				
1 a	<p><math>f(x) = x^3 + x^2 + 1</math></p> <p><math>3^2 = 9 - 1 = 8</math></p> <table border="1" style="display: inline-table; vertical-align: top;"> <tr><td><math>x^2</math></td><td><math>x^1</math></td><td><math>x^0</math></td><td>o/p</td></tr> <tr><td>1</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>1</td><td>1</td><td>0</td><td>0</td></tr> <tr><td>1</td><td>1</td><td>1</td><td>1</td></tr> <tr><td>0</td><td>1</td><td>1</td><td>1</td></tr> <tr><td>1</td><td>0</td><td>1</td><td>1</td></tr> <tr><td>0</td><td>1</td><td>0</td><td>0</td></tr> <tr><td>0</td><td>0</td><td>1</td><td>1</td></tr> <tr><td>1</td><td>0</td><td>0</td><td></td></tr> </table>  <p>Period = 7      weight of the code = 4</p>	$x^2$	$x^1$	$x^0$	o/p	1	0	0	0	1	1	0	0	1	1	1	1	0	1	1	1	1	0	1	1	0	1	0	0	0	0	1	1	1	0	0		4M
$x^2$	$x^1$	$x^0$	o/p																																			
1	0	0	0																																			
1	1	0	0																																			
1	1	1	1																																			
0	1	1	1																																			
1	0	1	1																																			
0	1	0	0																																			
0	0	1	1																																			
1	0	0																																				
1b	<p align="center"><b>Generalized Geffe Generator</b></p> <p align="center"><b>Linear Complexity</b></p> <ul style="list-style-type: none"> <li>• Definition:          An LFSR is said to generate a sequence <math>s</math> if there is some initial state for which the output sequence of the LFSR is <math>s</math>. An LFSR is said to generate a finite sequence <math>s^n</math> if there is some initial state for which the output sequence of the LFSR has <math>s^n</math> as its first <math>n</math> terms.</li> <li>• Definition:          The linear complexity of an infinite binary sequence <math>s</math>, denoted <math>L(s)</math>, is defined as follows:         <ul style="list-style-type: none"> <li>- if <math>s</math> is the zero sequence <math>s = 0, 0, 0, \dots</math>, then <math>L(s) = 0</math></li> <li>- if no LFSR generates <math>s</math>, then <math>L(s) = \infty</math></li> <li>- otherwise, <math>L(s)</math> is the length of the shortest LFSR that generates <math>s</math>.</li> </ul> </li> </ul> <p>Correlation Attack: Cryptographers try to get a high linear complexity by combining the output of several output sequences in some nonlinear manner. The danger is that one or more of the internal output sequences often just outputs of individual LFSRs can be correlated with the combined keystream and attacked using linear algebra. This is called a correlation attack.</p>	4M																																				
1c	<p align="center"><b>Self-Decimated Generators</b></p> <p align="center"><b>Beth Piper Stop and Go Generator</b></p> <ul style="list-style-type: none"> <li>• It uses the output of one LFSR to control the clock of another LFSR.</li> <li>• The clock input of LFSR-2 is controlled by the output of LFSR-1, So that LFSR-2 can change its state at time 't' only if the output of LFSR-1 was 1 at time t-1.</li> <li>• The linear complexity of the generator is not yet proved in general case.</li> <li>• But, it falls to a correlation attack.</li> </ul>  <p align="right">(2x2M)</p>	4M																																				

2a.



4M

2b.

Additive Fibonacci generators (AFG) are widely used in cybersecurity devices to generate pseudorandom sequences of bits or numbers. By itself, such a generator is not cryptographically strong. Nevertheless, using it is fundamental to create a completely secure and resistant cryptanalysis algorithm. (2M)

4M

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 plain text. The algorithm is named as it is because it is a Fibonacci shrinking generator. (2M)

NANOTEQ:

2c.

- Nanoteq is a South African electronics company.
- This is their algorithm that has been fielded by the South African police to encrypt their fax transmissions and for other uses as well.
- It uses 127 bit LFSR with a fixed feedback polynomial; the key is the initial state of the feedback register.
- The 127 bits of the register are reduced to single key stream bit using 25 primitive cells.
- Each input of the function is XORed with some bit of the key.
- There is also a secret permutation that depends on the particular implementation. This algorithm is only available in hardware (2M)
- RAMBUTAN: It has 112 bit key and can operate in three modes ECB, CBC and 8 bit CFB. This strongly indicates that it is a block algorithm, but rumours point elsewhere.
- It is LFSR streamcipher.
- it has 5 shift registers each one of a different length around 80 bits.
- The feedback polynomials or family sparse with only about 10 taps each.
- Each shift register provides for inputs very large and complex non linear function which eventually spits out a single bit. (2M)

4M

3a.

$$n_A = 1$$

$$P_A = n_A G \Rightarrow 1(2, 8) = (2, 8)$$

$$n_B = 2$$

$$P_B = n_B G \Rightarrow 2(2, 8) \Rightarrow (2, 8) + (2, 8)$$

$$\Delta = \frac{3(2)^2 + 2}{2(8)} \Rightarrow \frac{3(4) + 2}{16} \Rightarrow \frac{12 + 2}{16}$$

$$\Delta \Rightarrow \frac{14}{8} \pmod{11} \Rightarrow 7 \times 8^{-1} \pmod{11}$$

$$c = [c_x \ c_y]$$

$$c_y = P_m + K P_B$$

$$\Rightarrow (2, 8) + 1(7, 7) + 1(10, 7) \Rightarrow (2, 6) + (10, 7)$$

$$\Delta = \frac{7-6}{10-2} \Rightarrow \frac{1}{8} \Rightarrow 8^{-1} \pmod{11} \Rightarrow 8 \times 8 \pmod{11} \Rightarrow 7$$

$$\Delta = 7$$

$$x_c \Rightarrow \Delta^2 - x_p - x_q \Rightarrow 7^2 - 2 - 10 \Rightarrow 49 - 12 \Rightarrow 37 \pmod{11}$$

$$x_c = 4$$

$$y_c \Rightarrow \Delta(x_p - x_q) - 4p \Rightarrow 7(2 - 10) - 8$$

$$\Rightarrow -20 \pmod{11}$$

$$y_c = 2$$

$$C_y = P_m + K P_B$$

$$c = [c_x \ c_y] = [4, 2]$$

$$c_x \Rightarrow K G \Rightarrow 1(2, 8)$$

$$c = [(2, 8) \ (4, 2)]$$

$$\Delta = 5$$

$$x \Rightarrow \Delta^2 - x_p - x_q$$

$$\Rightarrow 5^2 - 2 - 2 \Rightarrow 25 - 4 = 21 \pmod{11}$$

$$x_B \Rightarrow 10$$

$$y = \Delta(x_p - x_q) - 4p \Rightarrow 5(2 - 10) - 8$$

$$\Rightarrow -48 \pmod{11}$$

$$y_B = 7$$

$$P_B = (10, 7)$$

4M

3b.

$$\Delta \Rightarrow \frac{3(3)^2 + 1}{2(10)} \Rightarrow \frac{3(9) + 1}{20} \Rightarrow \frac{28}{20}$$

$$\Rightarrow 5 \times 20^{-1} \pmod{23}$$

$$\Rightarrow 4^{-1} \pmod{23}$$

$$\Delta \Rightarrow 6$$

$$x_{2p} \Rightarrow 6^2 - 3 - 3 \Rightarrow 36 - 6 \Rightarrow 30 \pmod{23}$$

$$\Rightarrow 7$$

$$y_{2p} \Rightarrow 6(3 - 3) - 10 \Rightarrow -28 - 10 \Rightarrow 8 \pmod{23}$$

$$y_{2p} = 12$$

4M

$$\Delta_{2p+q} \Rightarrow (7, 12) + (9, 7)$$

$$\Delta \Rightarrow \frac{7-12}{9-7} \Rightarrow \frac{-5}{2} \Rightarrow \frac{-5}{2} \pmod{23}$$

$$\Rightarrow -5 \times 12 \pmod{23}$$

$$\Rightarrow -60 \pmod{23}$$

$$\Delta \Rightarrow 9$$

4M

4a.

$$\Delta = \frac{10-7}{4-2} \Rightarrow \frac{3}{2} \pmod{7}$$

$$\Rightarrow 12 \pmod{7} = 5$$

$$\Delta = 5$$

$$\Delta_{2p} \Rightarrow (2, 2) + (2, 2)$$

$$\Delta = \frac{3(2)^2 + 1}{2(7)} \Rightarrow \frac{3(4) + 1}{14} \Rightarrow \frac{13}{14} \pmod{7}$$

$$\Rightarrow \frac{6}{14} \pmod{7} \Rightarrow \frac{3}{7} \pmod{7}$$

$$\Delta = 0$$

4b.

$$\Delta_{29} \Rightarrow \frac{3(4)^2+1}{2(10)} \Rightarrow \frac{3(16)+1}{20} \Rightarrow \frac{49}{20} \pmod{29} \Rightarrow \frac{9}{20} \pmod{29}$$

$$\Delta_{29} = 0$$

$$x_{29} \Rightarrow 0^2 - 4 - 4 \Rightarrow -8 \pmod{29} \Rightarrow 6$$

$$y_{29} \Rightarrow 0(4-6) - 10 \Rightarrow -10 \pmod{29} \Rightarrow 19$$

Use A

$$n_A = 2$$

$$2 < 50$$

$$P_B = n_B q \Rightarrow 2(3, 8) \Rightarrow (2, 8) + (2, 8)$$

$$\Delta = \frac{3(2)^2+1}{2(8)} \Rightarrow \frac{3(4)+1}{16} \Rightarrow \frac{13}{16} \pmod{23}$$

$$\Rightarrow \frac{13}{16} \pmod{23} \Rightarrow 13 \times 16^{-1} \pmod{23}$$

$$\Rightarrow 13 \times 3 \pmod{23}$$

$$\Rightarrow 39 \pmod{23}$$

$$\Delta \Rightarrow 08$$

$$x = \Delta^2 - x_p - x_p \Rightarrow 8^2 - 2 - 2^2$$

$$\Rightarrow 60 \pmod{23}$$

$$x \Rightarrow 14$$

$$y = \Delta(x_p - x) - 4p \Rightarrow 8(2 - 14) - 8$$

$$\Rightarrow -104 \pmod{23}$$

$$y = 11$$

$$P_A = (14, 11)$$

4M



Signature of Course In charge



Signature of Module Coordinator



Signature of HOD





# K. S. INSTITUTE OF TECHNOLOGY

#14, Raghuvanahalli, Kanakapura Main Road, Bengaluru-5600109

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING


2023-24 EVEN SEMESTER


List of students who are identified as slow learners and their marks in every internal

Subject and Subject Code: Cryptography (21EC642)

Semester and Section: VI B

Sl No	USN	NAME	First Test Marks (20)	Remedial Class Dates & Attendance		Improvement Test marks	Second Test Marks (20)	Remedial Class Dates & Attendance		Improvement Test Marks (20)	Third Test Marks (20)	Final (60)
				06/06/24	13/06/24			04/07/24	11/07/24			
1	1KS21EC076	RITESH KUMAR SINHA	06	P	P	-	AB	P	P	14	12	32
2	1KS21EC080	S SHAJITH ALI	05	P	P	-	04	P	P	-	05	14
3	1KS21EC099	SUNEETHA	04	P	P	-	09	P	P	-	14	27
4	1KS21EC107	THEJAS.H.V	07	P	P	-	08	P	P	-	16	34
5	1KS21EC109	UDAYA KUMAR.S.R	02	P	P	5	04	P	P	-	7	16
6	1KS21EC113	VARSHITH.S	04	P	P	11	04	P	P	-	10	25
7	1KS21EC114	VEERESH.K.N	08	P	P	-	07	P	P	-	14	29
8	1KS21EC407	PRAJWAL PATIL.B.S	08	P	P	-	06	P	P	6	10	24
9	1KS21EC411	SUDEEP.P	02	P	P	7	05	P	P	-	7	19

  
Signature of the Faculty

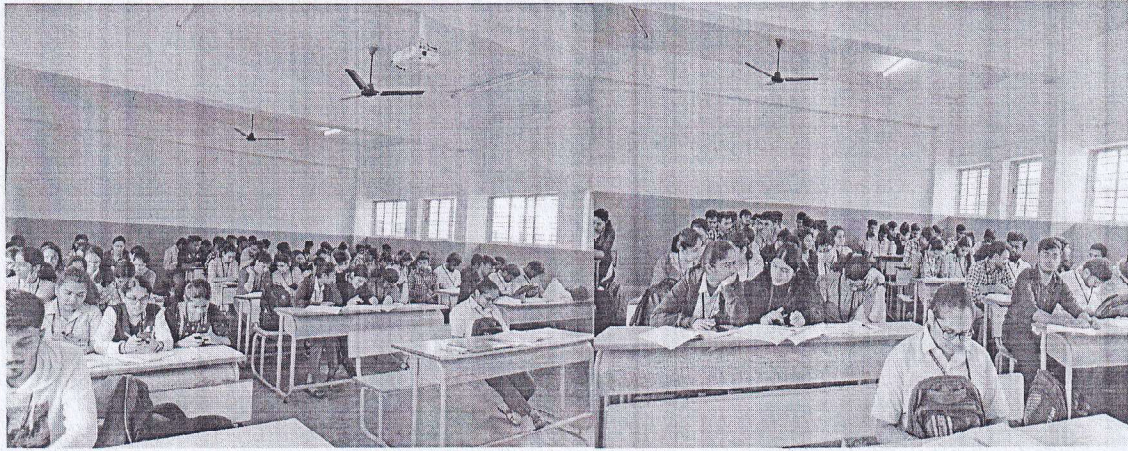
  
Signature of the HOD



**K.S. INSTITUTE OF TECHNOLOGY, BANGALORE - 560109**  
**DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING**  
**PEDAGOGY REPORT**

<b>Academic Year</b>	<b>2023-24 (EVEN)</b>
<b>Name of the Faculty</b>	<b>V.Sangeetha Dr.P.N.Sudha</b>
<b>Course Name /Code</b>	<b>Cryptography/21EC642</b>
<b>Semester/Section</b>	<b>VI/A&amp;B</b>
<b>Activity Name</b>	<b>Quiz</b>
<b>Topic Covered</b>	<b>Cryptography Basics,AES,DES</b>
<b>Date</b>	<b>24/7/2024</b>
<b>No. of Participants</b>	<b>90 students</b>
<b>Objectives/Goals</b>	<ul style="list-style-type: none"> <li>To apply the knowledge on different topics in Cryptography.</li> <li>To improve the self-learning skills of students.</li> </ul>
<b>ICT Used</b>	<b>Google forms</b>
<b>Appropriate Method/Instructional materials/Exam Questions</b>	
<ul style="list-style-type: none"> <li>MCQs:</li> </ul> <p>1) Which of the following is not a type of symmetric-key cryptography technique?  2) A mechanism used to encrypt and decrypt data. Conventional cryptography also known as ... encryption.  4) The Data Encryption Standard (DES) is an example of a ...  5) Public key cryptography is a ... cryptosystem.  6) Security Goals of Cryptography are  7) Cipher in cryptography is ...  8) The private key in asymmetric key cryptography is kept by ...  9) Which one of the following algorithms is not used in asymmetric-key cryptography?  10) A key is a value that works with a cryptographic algorithm to produce a specific cipher text.  11) The DES (Data Encryption Standard) cipher follows the feistel structure. Which of the following properties are not shown by the feistel structure?  12) Among the following given options, choose the strongest encryption technique?  13) What is the full-form of RSA in the RSA encryption technique?  14) Consider the following steps, The above steps are performed in each round of which of the following ciphers?  15) Decryption is a process to unveil the _____.  16) _____ ciphers encrypt uniformly sized blocks of data.  17) Which of the following cipher techniques include the involvement of matrix operations in their algorithms of encryption and decryption?  18) Which of the following ciphers is a block cipher?  19) In the case of symmetric key encryption, the secret key that both the parties possess can be anything such as a _____.  20) Which of the following cannot be chosen as a key in the Caesar cipher?</p>	
<b>Relevant PO's</b>	1,2,5,9,10
<b>Significance of Results/Outcomes</b>	<ul style="list-style-type: none"> <li>Students learnt and improved their creativity and communication skills.</li> <li>Students understand the basic concepts and developed modern tool usage.</li> </ul>
<b>Reflective Critique</b>	<ul style="list-style-type: none"> <li>The activity improved the learning and communication skills of students.</li> <li>The activity provided a platform for students to apply their knowledge on different concepts in Cryptography and apply their skills in future work as individual.</li> </ul>

**Proofs (Photographs/Videos/Reports/Charts/Models)**



Signature of Course In-charge

Signature of HOD-ECE



**K.S. INSTITUTE OF TECHNOLOGY, BANGALORE - 560109**  
**DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING**  
**PEDAGOGY REPORT**

<b>Academic Year</b>	2023-24 (EVEN)																																																														
<b>Name of the Faculty</b>	V.Sangeetha																																																														
<b>Course Name /Code</b>	Cryptography/21EC642																																																														
<b>Semester/Section</b>	VI/B																																																														
<b>Activity Name</b>	Mini Project																																																														
<b>Topic Covered</b>	Encryption , Decryption, Symmetric, Asymmetric cipher																																																														
<b>Date</b>	8/7/2024 to 11/7/2024																																																														
<b>No. of Participants</b>	50																																																														
<b>Objectives/Goals</b>	<ul style="list-style-type: none"> <li>To apply the knowledge on different topics in Cryptography.</li> <li>To improve the self-learning skills of students.</li> <li>To improve the communication skills of students.</li> <li>To improve the Creative skills of students</li> </ul>																																																														
<b>ICT Used</b>	Laptop																																																														
<b>Appropriate Method/Instructional materials/Exam Questions</b> <ul style="list-style-type: none"> <li>Students teams formed and assigned different topics from CCN to develop model.</li> <li>Students discussed about the model and ideas have been shared among students.</li> <li>Title of the Mini Project as follows: <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td colspan="2"><b>Title of the Mini Project</b></td> </tr> <tr><td>Caesar cipher using matlab</td><td></td></tr> <tr><td>Hash algorithm using C</td><td></td></tr> <tr><td>Rail fence Cipher using C</td><td></td></tr> <tr><td>Play Fair cipher using C++</td><td></td></tr> <tr><td>Euler's Toient Function</td><td>GCD of two num using Python</td></tr> <tr><td>Vernam cipher using C++</td><td>Caesar cipher using C++</td></tr> <tr><td>Play fair cipher using C</td><td>Elliptic Curve Algorithm</td></tr> <tr><td>Construction of multiplicative table and its inverse using C</td><td>Hill cipher using C</td></tr> <tr><td></td><td>DH Algorithm using C</td></tr> <tr><td>Vernam cipher Algorithm using C</td><td>Eulers theorem using matlab</td></tr> <tr><td>Mono Alphabetic cipher using C</td><td>Simple substitution cipher using C</td></tr> <tr><td>Vigenere cipher using C++</td><td>Additive table and its inverse using Python</td></tr> <tr><td>RSA Algorithm using python</td><td>Euler's Theorem</td></tr> <tr><td>Caesar cipher encryption using python</td><td>Euclidian algorithm using C</td></tr> <tr><td>Finding gcd for two numbers using c++</td><td>Eulers theorem using C</td></tr> <tr><td>Hill cipher using python</td><td>Caesar cipher using matlab</td></tr> <tr><td>Polynomial Arithmetic</td><td>Vigenere cipher using C</td></tr> <tr><td>Extended Euclidean Algorithm using c</td><td>Vigenere cipher using python</td></tr> <tr><td>Diffie Hellman Key Exchange</td><td>Rail fence using Python</td></tr> <tr><td></td><td>DH Algorithm using Python</td></tr> <tr><td>Twofish algorithm using matlab</td><td>Multiplicative inverse using Python</td></tr> <tr><td>Hill Cipher</td><td>Diffie Hellman Algorithm</td></tr> <tr><td></td><td>Pseudo Random sequence using C++</td></tr> <tr><td>Hill cipher using C++</td><td>Caesar Cipher using Python</td></tr> <tr><td>Hill cipher using matlab</td><td>Euclidian algorithm</td></tr> <tr><td>Construction of multiplicative table and its inverse using C</td><td>Fermet's Theorem</td></tr> <tr><td>Multiplicative table and find its inverse using python</td><td>Pseudo Random sequence using Python</td></tr> <tr><td>Play fair cipher using Python</td><td></td></tr> <tr><td>GCD of two num using c</td><td></td></tr> <tr><td>Caesar cipher encryption using c</td><td></td></tr> </table> </li> </ul>		<b>Title of the Mini Project</b>		Caesar cipher using matlab		Hash algorithm using C		Rail fence Cipher using C		Play Fair cipher using C++		Euler's Toient Function	GCD of two num using Python	Vernam cipher using C++	Caesar cipher using C++	Play fair cipher using C	Elliptic Curve Algorithm	Construction of multiplicative table and its inverse using C	Hill cipher using C		DH Algorithm using C	Vernam cipher Algorithm using C	Eulers theorem using matlab	Mono Alphabetic cipher using C	Simple substitution cipher using C	Vigenere cipher using C++	Additive table and its inverse using Python	RSA Algorithm using python	Euler's Theorem	Caesar cipher encryption using python	Euclidian algorithm using C	Finding gcd for two numbers using c++	Eulers theorem using C	Hill cipher using python	Caesar cipher using matlab	Polynomial Arithmetic	Vigenere cipher using C	Extended Euclidean Algorithm using c	Vigenere cipher using python	Diffie Hellman Key Exchange	Rail fence using Python		DH Algorithm using Python	Twofish algorithm using matlab	Multiplicative inverse using Python	Hill Cipher	Diffie Hellman Algorithm		Pseudo Random sequence using C++	Hill cipher using C++	Caesar Cipher using Python	Hill cipher using matlab	Euclidian algorithm	Construction of multiplicative table and its inverse using C	Fermet's Theorem	Multiplicative table and find its inverse using python	Pseudo Random sequence using Python	Play fair cipher using Python		GCD of two num using c		Caesar cipher encryption using c	
<b>Title of the Mini Project</b>																																																															
Caesar cipher using matlab																																																															
Hash algorithm using C																																																															
Rail fence Cipher using C																																																															
Play Fair cipher using C++																																																															
Euler's Toient Function	GCD of two num using Python																																																														
Vernam cipher using C++	Caesar cipher using C++																																																														
Play fair cipher using C	Elliptic Curve Algorithm																																																														
Construction of multiplicative table and its inverse using C	Hill cipher using C																																																														
	DH Algorithm using C																																																														
Vernam cipher Algorithm using C	Eulers theorem using matlab																																																														
Mono Alphabetic cipher using C	Simple substitution cipher using C																																																														
Vigenere cipher using C++	Additive table and its inverse using Python																																																														
RSA Algorithm using python	Euler's Theorem																																																														
Caesar cipher encryption using python	Euclidian algorithm using C																																																														
Finding gcd for two numbers using c++	Eulers theorem using C																																																														
Hill cipher using python	Caesar cipher using matlab																																																														
Polynomial Arithmetic	Vigenere cipher using C																																																														
Extended Euclidean Algorithm using c	Vigenere cipher using python																																																														
Diffie Hellman Key Exchange	Rail fence using Python																																																														
	DH Algorithm using Python																																																														
Twofish algorithm using matlab	Multiplicative inverse using Python																																																														
Hill Cipher	Diffie Hellman Algorithm																																																														
	Pseudo Random sequence using C++																																																														
Hill cipher using C++	Caesar Cipher using Python																																																														
Hill cipher using matlab	Euclidian algorithm																																																														
Construction of multiplicative table and its inverse using C	Fermet's Theorem																																																														
Multiplicative table and find its inverse using python	Pseudo Random sequence using Python																																																														
Play fair cipher using Python																																																															
GCD of two num using c																																																															
Caesar cipher encryption using c																																																															
<b>Relevant PO's</b>	1,2,5,9,10																																																														
<b>Significance of Results/Outcomes</b>	<ul style="list-style-type: none"> <li>Students learnt and improved their creativity and communication skills.</li> <li>Students understand the concepts and developed team build activity.</li> </ul>																																																														
<b>Reflective Critique</b>	<ul style="list-style-type: none"> <li>The activity improved the learning and communication skills of students.</li> <li>The activity provided a platform for students to apply their knowledge on different concepts in Cryptography future work as individual.</li> </ul>																																																														

# Proofs (Photographs/Videos/Reports/Charts/Models)



**Title:** VERNAM CIPHER  
**Name:** PREETHAMM  
**USN:** IKS21EC068  
**Theory /Algorithm:**  
**VERENAM CIPHER:**

Vernam Cipher is a method of encrypting alphabetic text. It is one of the Substitution techniques for converting plain text into cipher text. In this mechanism, we assign a number to each character of the Plain-Text, like (a=0, b=1, c=2... z=25). Method to take key: In the Vernam cipher algorithm, we take a key to unencrypt the plain text whose length should be equal to the length of the plain text.

**ALGORITHM:**

- > Assign a number to each character of the plain text and the key according to alphabetical order.
- > Bitwise XOR both the number (Corresponding plain-text character number and Key character number).
- > Subtract the number from 26 if the resulting number is greater than or equal to 26, if it fits then leave it.

**Mini Project Programme/Code:**

```
#include <bits/stdc++.h>
using namespace std; Long
mod(int a, int b)
{
    return (a % b + b) % b;
}
String encrypt(string key, string m)
{
    String result = "";
    // traverse text
    for (int i=0; i<m.length(); i++)
    {
        // apply transformation to each character
        Result += char(mod(int(m[i]-65+key[i]-65), 26)+65);
    }
    // Return the resulting string Return result;
}
String decrypt(string key, string m)
{
    String result = "";
    // traverse text
    for (int i=0; i<m.length(); i++)
    {
        Result += char(mod(int(m[i]-65)-(key[i]-65), 26)+65);
    }
    // Return the resulting string Return result;
}
int main() { String m;
    cout<<"Enter the message"<<"\n";
    cin>>m;
    String key;
    cout<<"Enter the key"<<"\n";
    cin>>key;
    String cipher = encrypt(key, m);
    cout<<"Encrypted message: "<<cipher<<"\n";
    cout<<"Decrypted message: "<<decrypt(key, cipher)<<"\n";
    return 0;
}
```

```
Result += char(mod(int(m[i]-65+key[i]-65), 26)+65);
}
// Return the resulting string Return result;
String decrypt(string key, string m)
{
    String result = "";
    // traverse text
    for (int i=0; i<m.length(); i++)
    {
        Result += char(mod(int(m[i]-65)-(key[i]-65), 26)+65);
    }
    // Return the resulting string Return result;
}
int main() { String m;
    cout<<"Enter the message"<<"\n";
    cin>>m;
    String key;
    cout<<"Enter the key"<<"\n";
    cin>>key;
    String cipher = encrypt(key, m);
    cout<<"Encrypted message: "<<cipher<<"\n";
    cout<<"Decrypted message: "<<decrypt(key, cipher)<<"\n";
    return 0;
}
```

**OUTPUT:**

```
Enter the message STUDENT
Enter the key
CLASS
Encrypted message: UEUWAG
Decrypted message: STUDENT
```

VISVESVARAYA TECHNOLOGICAL UNIVERSITY  
 Jyoti Sarvagata Heigava - 590118 Karnataka



MINI PROJECT REPORT ON  
 VERNAM CIPHER  
 Presented by  
 PREETHAMM (IKS21EC068)

Course Name: CRYPTOGRAPHY  
 Course Code: 21EC642



K. S. INSTITUTE OF TECHNOLOGY  
 #14, Raghunathalli, Kankaranur, main road  
 Hangeave - 599109  
 2023-2024

VISVESVARAYA TECHNOLOGICAL UNIVERSITY  
 Jyoti Sarvagata Heigava - 590118 Karnataka



MINI PROJECT REPORT ON  
 RAIL FENCE TECHNIQUE  
 Presented by  
 VIDYASHREE R (IKS21EC117)

Course Name: CRYPTOGRAPHY  
 Course Code: 21EC642



K. S. INSTITUTE OF TECHNOLOGY  
 #14, Raghunathalli, Kankaranur, main road  
 Hangeave - 599109  
 2023-2024

Signature of Course In-charge

Signature of HOD-ECE



<b>Academic Year</b>	<b>2023-24 (EVEN)</b>																																																								
<b>Name of the Faculty</b>	<b>V.Sangeetha</b>																																																								
<b>Course Name /Code</b>	<b>Cryptography/21EC642</b>																																																								
<b>Semester/Section</b>	<b>VI/B</b>																																																								
<b>Activity Name</b>	<b>Mini Project</b>																																																								
<b>Topic Covered</b>	<b>Encryption , Decryption, Symmetric, Asymmetric cipher</b>																																																								
<b>Date</b>	<b>8/7/2024 to 11/7/2024</b>																																																								
<b>No. of Participants</b>	<b>50</b>																																																								
<b>Objectives/Goals</b>	<ul style="list-style-type: none"> <li>• To apply the knowledge on different topics in Cryptography.</li> <li>• To improve the self-learning skills of students.</li> <li>• To improve the communication skills of students.</li> <li>• To improve the Creative skills of students</li> </ul>																																																								
<b>ICT Used</b>	<b>Laptop</b>																																																								
<p>Appropriate Method/Instructional materials/Exam Questions</p> <ul style="list-style-type: none"> <li>• Title of the Mini Project as follows:</li> </ul> <table border="0"> <tr><td>Title of the Mini Project</td><td>_____</td></tr> <tr><td>Caesar cipher using matlab</td><td>_____</td></tr> <tr><td>Hash algorithm using C</td><td>_____</td></tr> <tr><td>Rail fence Cipher using C</td><td>_____</td></tr> <tr><td>Play Fair cipher using C++</td><td>_____</td></tr> <tr><td>Euler's Totient Function</td><td>GCD of two num using Python</td></tr> <tr><td>Vernam cipher using C++</td><td>Caesar cipher using C++</td></tr> <tr><td>Play fair cipher using C</td><td>Elliptic Curve Algorithm</td></tr> <tr><td>Construction of multiplicative table and its inverse using C</td><td>Hill cipher using C</td></tr> <tr><td>Vernam cipher Algorithm using C</td><td>DH Algorithm using C</td></tr> <tr><td>Mono Alphabetic cipher using C</td><td>Eulers theorem using matlab</td></tr> <tr><td>Vigenere cipher using C++</td><td>Simple substitution cipher using C</td></tr> <tr><td>RSA Algorithm using python</td><td>Additive table and its inverse using Python</td></tr> <tr><td>Caesar cipher encryption using python</td><td>Euler's Theorem</td></tr> <tr><td>Finding gcd for two numbers using c++</td><td>Euclidian algorithm using C</td></tr> <tr><td>Hill cipher using python</td><td>Eulers theorem using C</td></tr> <tr><td>Polynomial Arithmetic</td><td>Caesar cipher using matlab</td></tr> <tr><td>Extended Euclidean Algorithm using c</td><td>Vigenere cipher using C</td></tr> <tr><td>Diffie Hellman Key Exchange</td><td>Vigenere cipher using python</td></tr> <tr><td>Twofish algorithm using matlab</td><td>Rail fence using Python</td></tr> <tr><td>Hill Cipher</td><td>DH Algorithm using Python</td></tr> <tr><td>Hill cipher using C++</td><td>Multiplicative inverse using Python</td></tr> <tr><td>Hill cipher using matlab</td><td>Diffie Hellman Algorithm</td></tr> <tr><td>Construction of multiplicative table and its inverse using C</td><td>Pseudo Random sequence using C++</td></tr> <tr><td>Multiplicative table and find its inverse using python</td><td>Caesar Cipher using Python</td></tr> <tr><td>Play fair cipher using Python</td><td>Euclidian algorithm</td></tr> <tr><td>GCD of two num using c</td><td>Fermat's Theorem</td></tr> <tr><td>Caesar cipher encryption using c</td><td>Pseudo Random sequence using Python</td></tr> </table>		Title of the Mini Project	_____	Caesar cipher using matlab	_____	Hash algorithm using C	_____	Rail fence Cipher using C	_____	Play Fair cipher using C++	_____	Euler's Totient Function	GCD of two num using Python	Vernam cipher using C++	Caesar cipher using C++	Play fair cipher using C	Elliptic Curve Algorithm	Construction of multiplicative table and its inverse using C	Hill cipher using C	Vernam cipher Algorithm using C	DH Algorithm using C	Mono Alphabetic cipher using C	Eulers theorem using matlab	Vigenere cipher using C++	Simple substitution cipher using C	RSA Algorithm using python	Additive table and its inverse using Python	Caesar cipher encryption using python	Euler's Theorem	Finding gcd for two numbers using c++	Euclidian algorithm using C	Hill cipher using python	Eulers theorem using C	Polynomial Arithmetic	Caesar cipher using matlab	Extended Euclidean Algorithm using c	Vigenere cipher using C	Diffie Hellman Key Exchange	Vigenere cipher using python	Twofish algorithm using matlab	Rail fence using Python	Hill Cipher	DH Algorithm using Python	Hill cipher using C++	Multiplicative inverse using Python	Hill cipher using matlab	Diffie Hellman Algorithm	Construction of multiplicative table and its inverse using C	Pseudo Random sequence using C++	Multiplicative table and find its inverse using python	Caesar Cipher using Python	Play fair cipher using Python	Euclidian algorithm	GCD of two num using c	Fermat's Theorem	Caesar cipher encryption using c	Pseudo Random sequence using Python
Title of the Mini Project	_____																																																								
Caesar cipher using matlab	_____																																																								
Hash algorithm using C	_____																																																								
Rail fence Cipher using C	_____																																																								
Play Fair cipher using C++	_____																																																								
Euler's Totient Function	GCD of two num using Python																																																								
Vernam cipher using C++	Caesar cipher using C++																																																								
Play fair cipher using C	Elliptic Curve Algorithm																																																								
Construction of multiplicative table and its inverse using C	Hill cipher using C																																																								
Vernam cipher Algorithm using C	DH Algorithm using C																																																								
Mono Alphabetic cipher using C	Eulers theorem using matlab																																																								
Vigenere cipher using C++	Simple substitution cipher using C																																																								
RSA Algorithm using python	Additive table and its inverse using Python																																																								
Caesar cipher encryption using python	Euler's Theorem																																																								
Finding gcd for two numbers using c++	Euclidian algorithm using C																																																								
Hill cipher using python	Eulers theorem using C																																																								
Polynomial Arithmetic	Caesar cipher using matlab																																																								
Extended Euclidean Algorithm using c	Vigenere cipher using C																																																								
Diffie Hellman Key Exchange	Vigenere cipher using python																																																								
Twofish algorithm using matlab	Rail fence using Python																																																								
Hill Cipher	DH Algorithm using Python																																																								
Hill cipher using C++	Multiplicative inverse using Python																																																								
Hill cipher using matlab	Diffie Hellman Algorithm																																																								
Construction of multiplicative table and its inverse using C	Pseudo Random sequence using C++																																																								
Multiplicative table and find its inverse using python	Caesar Cipher using Python																																																								
Play fair cipher using Python	Euclidian algorithm																																																								
GCD of two num using c	Fermat's Theorem																																																								
Caesar cipher encryption using c	Pseudo Random sequence using Python																																																								
<b>Relevant PO's</b>	<b>1,2,5,9,10</b>																																																								
<b>Significance of Results/Outcomes</b>	<ul style="list-style-type: none"> <li>• Students learnt and improved their creativity and communication skills.</li> <li>• Students understand the concepts and developed team build activity.</li> </ul>																																																								
<b>Reflective Critique</b>	<ul style="list-style-type: none"> <li>• The activity improved the learning and communication skills of students.</li> <li>• The activity provided a platform for students to apply their knowledge on different concepts in Cryptography future work as individual.</li> </ul>																																																								

# Proofs (Photographs/Videos/Reports/Charts/Models)



**Title:** VERNAM CIPHER  
**Name:** PREETHAM M  
**USN:** IKS21EC068  
**Theory /Algorithm:**  
**VERENAM CIPHER:**

Vernam Cipher is a method of encrypting alphabetic text. It is one of the Substitution techniques for converting plain text into cipher text. In this mechanism, we assign a number to each character of the Plain-Text like (a = 0, b = 1, c = 2 ... z = 25). Method to take key: In the Vernam cipher algorithm, we take a key to encrypt the plain text whose length should be equal to the length of the plain text.

**ALGORITHM:**

- Assign a number to each character of the plain text and the key according to alphabetical order.
- Either XOR both the number (Corresponding plain-text character number and Key character number).
- Subtract the number from 26 if the resulting number is greater than or equal to 26, if it int then leave it.

**Mini Project Programme/Code:**

```
#include <bits/stdc++.h>
using namespace std; Long
mod(int a, int b)
{
    return (a % b + b) % b;
}
String encrypt(string key, string m)
{
    String result = "";
    // traverse text
    For (int i=0; i<m.length(); i++)
    {
        // apply transformation to each character
```

```
Result += char(mod((m[i]-65+key[i]-65), 26)+65);
}
// Return the resulting string Return result;
}
String decrypt(string key, string m)
{
    String result = "";
    // traverse text
    For (int i=0; i<m.length(); i++)
    {
        Result += char(mod((m[i]-65)-(key[i]-65), 26)+65);
    }
    // Return the resulting string Return result;
}
int main() { String m;
    cout<<"Enter the message"<<"\n";
    cin>>m;
    String key;
    cout<<"Enter the key"<<"\n"; cin>>key;
    String cipher = encrypt(key, m); cout<<"Encrypted message:
    "<<cipher<<"\n";
    cout<<"Decrypted message: "<<decrypt(key, cipher)<<"\n"; return 0;
}
```

**OUTPUT:**  
 Enter the message STUDENT  
 Enter the key  
 CLASS  
 Encrypted message: UUEUYWAG  
 Decrypted message: STUDENT

VISVESVARAYA TECHNOLOGICAL UNIVERSITY  
 Jyana Sangama Belgavi - 590118, Karnataka



MINI PROJECT REPORT ON  
 VERNAM CIPHER  
 Presented by  
 PREETHAM M (IKS21EC068)  
 Course Name: CRYPTOGRAPHY  
 Course Code:21EC642



K. S. INSTITUTE OF TECHNOLOGY  
 #14, Raghuvanahalli, Nanakapura math road,  
 Bangalore - 560109  
 2023-2024

VISVESVARAYA TECHNOLOGICAL UNIVERSITY  
 Jyana Sangama Belgavi - 590118, Karnataka



MINI PROJECT REPORT ON  
 RAIL FENCE TECHNIQUE  
 Presented by  
 VIDYASHREE R (IKS21EC117)  
 Course Name: CRYPTOGRAPHY  
 Course Code: 21EC642



K. S. INSTITUTE OF TECHNOLOGY  
 #14, Raghuvanahalli, Nanakapura math road,  
 Bangalore - 560109  
 2023-2024

*V.S.*  
 Signature of Course In-charge

*P. Jay*  
 Signature of HOD-ECE



**K.S. INSTITUTE OF TECHNOLOGY, BANGALORE – 560109**  
**Department of Electronics & Communication Engineering**  
**2023-24 Even Semester**

Course Name: Cryptography  
Semester/sec: VI B

Course Code: 21EC642

**CONTENT BEYOND SYLLABUS**

Sl.No	USN	Name of the Student	Title of the Mini Project
1	1KS21EC062	PRAJWAL D	ceaser cipher using matlab
2	1KS21EC064	PRAJWAL H S	Hash algorithm using C
3	1KS21EC065	PRAJWAL R	Rail fence Cipher using C
4	1KS21EC066	PRATHAM R SHANBHAG	Play Fair cipher using C++
5	1KS21EC067	PRAYAG SINGH S	Euler's Toient Function
6	1KS21EC068	PREETHAM M	Vernam cipher using C++
7	1KS21EC069	PREKSHA S	Play fair cipher using C
8	1KS21EC070	PUNITII M	Construction of multiplicative table and its inverse using C
9	1KS21EC071	RAGHAVENDRA NARAYAN PUJAR	Vernam cipher Algorithm using C
10	1KS21EC073	RAKSHITHA M R	Mono Alphabetic cipher using C
11	1KS21EC074	RAYADURG JOISH SHRIYA	Vigenere cipher using C++
12	1KS21EC076	RITESH KUMAR SINHA	RSA Algorithm using python
13	1KS21EC077	RITHIKA M	Ceaser cipher encryption using python
14	1KS21EC080	S SHAJITH ALI	Finding gcd for two numbers using c++
15	1KS21EC081	SAGAR G S	Hill cipher using python
16	1KS21EC083	SAMHITHA PRAKASH	Polynomial Arithmetic
17	1KS21EC084	SANJANA V	Extended Euclidean Algorithm using c
18	1KS21EC086	SANJAY N	Diffie Hellman Key Exchange
19	1KS21EC088	SATHYAM KUMAR MANDAL S	Twofish algorithm using matlab
20	1KS21EC090	SHASHANK C U	Hill Cipher
21	1KS21EC091	SHREYAS RAGHAVENDRA V	Hill cipher using C++
22	1KS21EC092	SHWETHA V	Hill cipher using matlab
23	1KS21EC093	SINDHU M NIMBAL	Construction of multiplicative table and its inverse using C
24	1KS21EC095	SPOORTHY M U	Multiplicative table and find its inverse using python
25	1KS21EC099	SUNEETHA	Play fair cipher using Python
26	1KS21EC100	SUNEHA S	GCD of two num using c
27	1KS21EC101	SUPREETH A	Ceaser cipher encryption using c
28	1KS21EC102	SURABHI K R	GCD of two num using Python
29	1KS21EC104	TARUN M	Ceaser cipher using C++
30	1KS21EC105	TEJASHREE N	Elliptic Curve Algorithm
31	1KS21EC106	THARUN K V	Hill cipher using C
32	1KS21EC107	THEJAS H V	DH Algorithm using C



33	1KS21EC108	THUSHAR CHERIAN	Eulers theorm using matlab
34	1KS21EC109	UDAYA KUMAR S R	Simple substitution cipher using C
35	1KS21EC110	VAISHNAVI B A	Additive table and its inverse using Python
36	1KS21EC111	VARSHA JAYAKUMAR	Euler's Theorem
37	1KS21EC112	VARSHA S DAVASKAR	Euclidian algorithm using C
38	1KS21EC113	VARSHITH S	Eulers theorm using C
39	1KS21EC114	VEERESH K N	Ceaser cipher using matlab
40	1KS21EC115	VIDYA I	Vigenere cipher using C
41	1KS21EC116	VIDYA RAWAL D	Vigenere cipher using python
42	1KS21EC117	VIDYASHREE R	Rail fence using Python
43	1KS21EC118	VIJAY YADAV R	DH Algorithm using Python
44	1KS21EC120	VYSHAK G R	Multiplicative inverse using Python
45	1KS21EC121	YASHWANTH.M	Diffie Hellman Algorithm
46	1KS22EC407	PRAJWAL PATIL B S	Pseudo Random sequence using C++
47	1KS22EC408	SANGEETHA H M	Ceaser Cipher using Phython
48	1KS22EC409	SOUNDARYA S	Euclidian algorithm
49	1KS22EC410	SOWMYA A M	Fermet's Theorem
50	1KS22EC411	SUDEEP P	Pseudo Random sequence using Python



<b>Course: Cryptography</b>	<b>Course Code:21EC642</b>	<b>Type: Core</b>
<b>Course In Charge: V.Sangeetha</b>	<b>Academic year:2023-24</b>	

**EXHAUSTIVE QUESTION BANK**

**Module-1**

- 1) Explain the Euclid's algorithm for determining the GCD of two positive integers. Find the GCD of (24140,16762), GCD(UNS,127), GCD(124,421)
- 2) Explain extended Euclidean algorithm and find multiplicative inverse of (your USN,1111),
- 3) Find the multiplicative inverse of
  - 1234 mod 4321
  - 24140 and 40902USN and 171
- 4) Using play fair cipher with the key largest encrypt the message "Must see you today"
- 5) Obtain additive and multiplicative table for GF(5),GF(7) and find additive and multiplicative inverse for all the integers.
- 6) Find the multiplicative inverse of  $(x^7+x+1) \bmod (x^8+x^4+x^3+x+1)$
- 7) State the axioms of field and Obtain additive and multiplicative table for GF(2<sup>2</sup>) & find additive and multiplicative inverse for all the elements.
- 8) Check whether  $(X^4+X^3+X^2+1)$  is irreducible and Solve multiplicative invers for  $(X^3+X+1) \bmod (X^2+X+1)$ .
- 9) Construct  $Z_8$  additive and multiplicative table and Solve all additive and multiplicative inverse elements.
- 10) Mention all modular arithmetic properties & obtain additive & multiplicative table for Mod5 and Solve all additive & multiplicative inverse for the same.
- 11) Solve GCD  $[a(x),b(x)]$  for  $a(x) = x^6+x^5+x^4+x^3+x^2+x+1$  and  $b(x) = x^4+x^2+x+1$  and write all modular arithmetic properties.

## Module-2

- 1) With a neat sketch explain the model of Symmetric cryptosystem
- 2) Design to encrypt & decrypt the plain text "CRYPTO" using hill cipher technique with the key matrix  
$$K_1 = \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix} \quad K_2 = \begin{pmatrix} 2 & 3 \\ 3 & 6 \end{pmatrix}$$
- 3) Explain all the properties of Group, Ring & field and what is an abelian group
- 4) Encrypt the plain text MONDAY using Hill cipher with key [J E F H] and Solve inverse of the Key matrix.
- 5) Make use of Playfair algorithm and Explain it with an example.
- 6) Make use of Symmetric Crypto system and explain it with a neat diagram and define reducible and irreducible polynomial.
- 7) Make use of Symmetrical encryption model and explain it with a neat diagram and define Substitution Technique and Transposition technique.
- 8) Make use of playfair cipher ,Encrypt the plain text "ELECTRONICS" with a key INDIA also mention all the rules for encryption.
- 9) Make use of PlayFair cipher with the key largest encrypt the message "Must see you today"



<b>Course: Cryptography</b>	<b>Course Code:21EC642</b>	<b>Type: Core</b>
<b>Course In Charge: V.Sangeetha</b>	<b>Academic year:2023-24</b>	

**EXHAUSTIVE QUESTION BANK**

**MODULE-2**

- 1) Encrypt the plain text 'PAYMORE' using Hill cipher algorithm and find the cipher text.

Given Key K=

17	17	15
21	18	21
2	2	19

- 2) Compute the encrypted data given the plain text COMMUNICATION using Rail fence method & Key technique given KEY as 4132.
- 3) Define Monoalphabetic cipher & Polyalphabetic cipher.
- 4) Define Substitution and Transposition technique with an example also define Diffusion and Confusion technique.
- 5) Encrypt the plain text ECEDEPARTMENT using Rail fence method & Key technique given KEY as 4132
- 6) Write the process used in RSA algorithm for encrypting and decrypting the data
- 7) Define Authentication, Digital Signature, Confidentiality.
- 8) Explain the Transposition technique with an Example
- 9) Encrypt the message "WORK IS WORSHIP" using the key "MOTIVATION" using Vignere cipher.

**MODULE-3**

- 1) List the differences between Stream Cipher and Block Cipher.
- 2) Define the Confusion and diffusion terms in the context of cryptology
- 3) Explain with a neat diagram the operation performed in 1<sup>st</sup> & 10<sup>th</sup> round of AES algorithm.
- 4) State & prove Fermat's theorem
- 5) Using Fermats Theorem find  $3^{990} \bmod 91$  &  $3^{999} \bmod 10$  using it.
- 6) Explain the parameters of Feistel structure and design Feistel network for encryption & decryption.
- 7) State & prove Euler's theorem. Find  $\Phi(q)$  and  $P^{\Phi(q)} \bmod q$  given values  
1)  $P=3, q=7$       2)  $q=12, P=5$
- 8) Illustrate the Feistel encryption and decryption process with a neat diagram
- 9) Define Fermat's little theorem and find the value of X given  $X^{103} \equiv 4 \pmod{11}$  and find the remainder for  $2^{35} \bmod 7$  and  $7^{20} \bmod 21$
- 10) With a neat diagram explain round operation in DES encryption.
- 11) Draw a neat diagram of DES encryption & decryption process and explain the working principle for the same.
- 12) Explain Key expansion technique in AES algorithm

- 13) Define Euler's theorem and find Totient function for 36 & 700
- 14) Explain the concept of Substitution byte, Mix column & Shift row operation with neat diagram in AES algorithm.
- 15) Illustrate the round operation in DES algorithm & compare DES and AES algorithm.
- 16) Define a WORD in AES algorithm & illustrate the working of 'g' function in AES Key expansion algorithm with a neat diagram.
- 17) State Euler's theorem and find the result for  $3^{90} \bmod 91$  using the same.
- 18) Using Euler's theorem find the value of x .given  $x^{91} \bmod 11 = 4$  or  $x^9 - 4 \bmod 11$

#### Module-4

- 1) With a neat block diagram explain the Principles of Public-Key Cryptosystems with authentication
- 2) find cipher text given plain text as KS using the RSA algorithm given  $P=3$ ,  $Q=11$ ,  $e=7$
- 3) With a neat block diagram explain the Principles of Public-Key Cryptosystems with authentication and secrecy.
- 4) Explain RSA algorithm
- 5) find cipher text and plain text using the RSA algorithm given  $P=5$ ,  $Q=11$ ,  $e=3$  and encrypt the message  $M=EC$  and decrypt the same.
- 6) With a neat block diagram explain the Principles of Public-Key Cryptosystems with confidentiality.
- 7) If  $p=61$ ,  $q=53$  find private key and Public key and encrypt the message  $M=65$ .
- 8) Perform encryption using RSA algorithm given  $p=5$ ,  $q=11$ ,  $e=3$ ,  $M=9$  using the same RSA algorithm decrypt the cipher text  $C=21$ .



## K S INSTITUTE OF TECHNOLOGY, BANGALORE

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

Course: Cryptography	Course Code:21EC642	Type: Core
Course In Charge: V.Sangeetha	Academic year:2023-24	

### EXHAUSTIVE QUESTION BANK

#### MODULE-5

1. Write an explanatory note on linear feedback shift register with a neat diagram.
2. Explain Generalized Geffe generator & Alternating Stop & Go generator with a neat diagram.
3. Explain the application & working of A5 generator and Threshold generator.
4. Explain Bilateral Stop and Go generator and Jennings Generator
5. Write a note on Linear Congruential Generator with an example.
6. Explain Gifford generator & Geffe generator.
7. Explain the concept of Gifford generator with an example and define linearity complex and correlation factor
8. Explain Beth Piper Stop & Go generator & Alternating Stop & Go generator with a neat diagram.
9. Design & explain the working of Linear Feedback shift register given  $g(x)=1+x+x^4$  and find the period & Key generated. Consider initial key values as 10 0.
10. Explain Bilateral Stop and Go generator and Jennings Generator.
11. Explain Linear Congruential Generator & Geffe generator with an example with an example.
12. Design & explain the working of Linear Feedback shift register given  $g(x)=1+x+x^3$  and find the period & Key generated. Consider initial key values as 1,0,0.



**K.S. INSTITUTE OF TECHNOLOGY, BANGALORE**  
**DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING**

YEAR / SEMESTER / BRANCH	VI/ECE
COURSE TITLE	Cryptography
COURSE CODE	21EC642
ACADEMIC YEAR	2023-24

sl.no	USN	Name of the student					Assignm	Acitivity	Total(100)	Final(50)
			IA1	IA2	IA3		ent			
	<b>Max Marks</b>		20	20	20	60	20	20	100	50
1	1KS21EC062	PRAJWAL D	11	4	7	22	16	20	58	29
2	1KS21EC064	PRAJWAL H S	4	6	8	18	20	20	72	36
3	1KS21EC065	PRAJWAL R	12	6	14	32	20	20	78	39
4	1KS21EC066	PRATHAM R SHANBHAG	15	14	9	38	20	20	61	31
5	1KS21EC067	PRAJYAG SINGH S	9	6	8	23	18	20	93	47
6	1KS21EC068	PREETHAM M	16	18	19	53	20	20	79	40
7	1KS21EC069	PREKSHA S	15	10	14	39	20	20	62	31
8	1KS21EC070	PUNITH M	9	7	6	22	20	20	76	38
9	1KS21EC071	RAGHAVENDRA NARAYAN PUJAR	12	9	15	36	20	20	71	36
10	1KS21EC073	RAKSHITHA M R	12	8	11	31	20	20	94	47
11	1KS21EC074	RAYADURG JOISH SHRIYA	16	18	20	54	20	20	72	36
12	1KS21EC076	RITESH KUMAR SINHA	6	14	12	32	20	20	90	45
13	1KS21EC077	RITHIKA M	16	17	17	50	20	20	54	27
14	1KS21EC080	S SHAJITH ALI	5	4	5	14	20	20	86	43
15	1KS21EC081	SAGAR G S	17	12	17	46	20	20	70	35
16	1KS21EC083	SAMHITHA PRAKASH	11	8	11	30	20	20	79	40
17	1KS21EC084	SANJANA V	12	13	14	39	20	20	73	37
18	1KS21EC086	SANJAY N	16	6	11	33	20	20	74	37
19	1KS21EC088	SATHYAM KUMAR MANDAL S	14	11	9	34	20	20	84	42
20	1KS21EC090	SHASHANK C U	18	13	13	44	20	20	62	31
21	1KS21EC091	SHREYAS RAGHAVENDRA V	7	5	10	22	20	20	89	45
22	1KS21EC092	SHWETHA V	14	16	19	49	19	20	62	31
23	1KS21EC093	SINDHU M NIMBAL	10	5	8	23	19	20	78	39
24	1KS21EC095	SPOORTHY M U	12	14	13	39	20	20	67	34
25	1KS21EC099	SUNEETHA	4	9	14	27	20	20	72	36
26	1KS21EC100	SUNEHA S	10	12	10	32	20	20	88	44
27	1KS21EC101	SUPREETHA	14	17	17	48	20	20	78	39
28	1KS21EC102	SURABHI K R	10	13	15	38	19	20	67	34
29	1KS21EC104	TARUN M	9	4	15	28	20	20	78	39
30	1KS21EC105	TEJASHREE N	10	12	16	38	19	20	64	32
31	1KS21EC106	THARUN K V	5	6	14	25	20	20	74	37
32	1KS21EC107	THEJAS H V	10	8	16	34	20	20	74	37

33	IKS21EC108	THUSHAR CHERIAN	10	3	7	20	16	19	55	28
34	IKS21EC109	UDAYA KUMAR S R	5	4	7	16	20	20	56	28
35	IKS21EC110	VAISHNAVI B A	14	14	14	42	20	20	82	41
36	IKS21EC111	VARSHA JAYAKUMAR	18	9	17	44	20	20	84	42
37	IKS21EC112	VARSHA S DAVASKAR	10	10	13	33	20	20	73	37
38	IKS21EC113	VARSHITH S	11	4	10	25	20	20	65	33
39	IKS21EC114	VEERESH K N	8	7	14	29	20	20	69	35
40	IKS21EC115	VIDYA I	20	17	16	53	20	20	93	47
41	IKS21EC116	VIDYA RAWAL D	15	18	17	50	20	20	90	45
42	IKS21EC117	VIDYASHREE R	18	20	20	58	20	20	98	49
43	IKS21EC118	VIJAY YADAV R	6	1	11	18	20	20	58	29
44	IKS21EC120	VYSHAK G R	15	17	19	51	20	20	91	46
45	IKS21EC121	YASHWANTH.M	13	8	13	34	20	20	74	37
46	IKS22EC407	PRAJWAL PATIL B S	8	6	10	24	20	20	64	32
47	IKS22EC408	SANGEETHA H M	5	7	13	25	20	20	65	33
48	IKS22EC409	SOUNDARYA S	8	4	14	26	20	20	66	33
49	IKS22EC410	SOWMYA A M	9	4	10	23	20	20	63	32
50	IKS22EC411	SUDEEP P	7	5	7	19	20	20	59	30



# CBCS SCHEME

USN

1	K	S	2	2	E	C	4	0	8
---	---	---	---	---	---	---	---	---	---

21EC642

## Sixth Semester B.E. Degree Examination, June/July 2024 Cryptography

Time: 3 hrs.

Max. Marks: 100

Note: Answer any FIVE full questions, choosing ONE full question from each module.

### Module-1

- 1 a. Explain the division algorithm with an example. (07 Marks)
- b. Define Ring. State six properties of Rings. (07 Marks)
- c. Explain the Euclidean algorithm. Calculate the GCD(60, -24) (06 Marks)

OR

- 2 a. Lists the properties of modular arithmetic for integer in  $2n$  with expression. (07 Marks)
- b. Explain the polynomial arithmetic. Find polynomial arithmetic over  $GF(2)$  for  $f(x) = x^7 + x^5 + x^4 + x^3 + x + 1$  and  $g(x) = x^3 + x + 1$ . (07 Marks)
- c. Develop set of tables for polynomial arithmetic modulo of  $x^3 + x + 1$  over  $GF(2^3)$ . (06 Marks)

### Module-2

- 3 a. Draw and explain model of symmetric encryption. (07 Marks)
- b. Explain the playfair cipher and its rules for the following keyword : "MONARCHY" plaintext : "Cryptography". (07 Marks)
- c. Explain the vernam Cipher with a neat diagram. (06 Marks)

OR

- 4 a. Draw and explain model of symmetric cryptosystem. (07 Marks)
- b. Explain the Caesar Cipher technique Encrypt plaintext "Cryptography" with key = 3. (06 Marks)
- c. Using Hill Cipher algorithm Encrypt the plaintext "paymoremoney" using the key,

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

(07 Marks)

### Module-3

- 5 a. State and prove Euler's theorem. (05 Marks)
- b. Explain the DES encryption algorithm with neat diagram. (10 Marks)
- c. Explain Block Cipher with neat diagram. (05 Marks)

OR

- 6 a. Explain Feistel encryption and decryption with neat diagram. (10 Marks)
- b. State and prove Fermat's theorem. (05 Marks)
- c. Explain Euler's Totient function. Determine (i)  $\phi(37)$  and  $\phi(35)$ . (05 Marks)

### Module-4

- 7 a. Bring out differentiate between conventional encryption and public-key encryption. Explain the requirement of public-key cryptography. (10 Marks)
- b. Explain RSA algorithm. Using RSA algorithm perform encryption and decryption using  $p = 17$ ,  $q = 11$ ,  $e = 7$  and  $M = 88$ . (10 Marks)

OR

- 8 a. Explain the Diffie-Hellman key exchange algorithm. Evaluate a Diffie-Hellman key exchange for  $q = 23$  and  $\alpha = 9$ .
- If User A has private key  $X_A = 4$   
What is A's public key  $Y_A = ?$
  - If User B has private key  $X_B = 3$   
What is B's public key  $Y_B = ?$
  - What is shared key?
- b. Describe Elgamal cryptographic system.

(10 Marks)

(10 Marks)

Module-5

- 9 a. Write short notes on, (i) NANOTEQ (ii) A5 (iii) Linear Congruential generator.
- b. Explain Additive generator.
- c. With a neat diagram, explain Threshold generator.

(10 Marks)

(06 Marks)

(04 Marks)

OR

- 10 a. Explain linear feedback shift register with a neat diagram.
- b. With a neat diagram, explain Geffe generator and Jennings generator.
- c. Explain Gifford with a neat diagram.

(06 Marks)

(10 Marks)

(04 Marks)

\* \* \* \* \*

# CBCS SCHEME

USN

--	--	--	--	--	--	--	--	--	--

18EC744

## Seventh Semester B.E. Degree Examination, Feb./Mar. 2022 Cryptography

Time: 3 hrs.

Max. Marks: 100

Note: Answer any FIVE full questions, choosing ONE full question from each module.

### Module-1

- 1 a. Draw the model of symmetric cryptosystem and explain in detail. (08 Marks)  
b. Using Hill Cipher technique encrypt and decrypt the plain text "Pay more money" (12 Marks)

Using the key, 
$$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

$$17(18 \times 19 - 42) - 17(21 \times 19 - 42) + 5(42 - 36)$$

OR

- 2 a. Explain Euclidean algorithm for determining of GCD. If  $a = 24140$ ,  $b = 16762$  solve using Euclidean algorithm to find GCD (a, b). (08 Marks)  
b. Mention the modular arithmetic operation properties and prove the same. (08 Marks)  
c. Find  $11^7 \pmod{13}$  using modular Arithmetic. (04 Marks)

### Module-2

- 3 a. With a neat diagram, explain feistel encryption and decryption model. (08 Marks)  
b. With a neat diagram, explain DES encryption algorithm. (08 Marks)  
c. List the design features of feistel network. (04 Marks)

OR

- 4 a. Explain with a neat diagram AES encryption and decryption process. (08 Marks)  
b. Explain AES key expansion algorithm write the Pseudo code for the same. (08 Marks)  
c. Describe the AES shift Rows Transformation. (04 Marks)

### Module-3

- 5 a. What are Groups? Explain in detail with respect to its properties. (06 Marks)  
b. Write a note on finite field of the form  $GF(P)$ . (06 Marks)  
c. Find the additive and multiplicative inverse of  $GF(8)$ . (08 Marks)

OR

- 6 a. State and prove Fermat's Theorem. Also find  $7^{18} \pmod{19}$  using it. (08 Marks)  
b. With suitable explanation prove Euler's Theorem. (07 Marks)  
c. Explain discrete logarithms for modular Arithmetic. (05 Marks)

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.  
2. Any revealing of identification, appeal to evaluator and/or equations written eg. 42:18 = 50, will be treated as malpractice.

**Module-4**

- 7 a. With a neat diagram, explain public-key cryptosystem secrecy and Authentication. (10 Marks)  
b. Explain the steps involved for encryption and Decryption for RSA Algorithm. (06 Marks)  
c. Perform encryption using RSA algorithm for  $p = 5$ ,  $q = 11$ ,  $e = 3$ ,  $m = 9$ . (04 Marks)

**OR**

- 8 a. Explain Diffie-Hellman key exchange algorithm. (07 Marks)  
b. Explain Elliptic curve over real numbers. (07 Marks)  
c. Explain Elliptic curve cryptography. (06 Marks)

**Module-5**

- 9 a. Write an explanatory note on Linear Feedback shift registers. (10 Marks)  
b. Explain the following with necessary diagrams :  
i) Generalized Geffe Generator  
ii) Threshold Generator  
iii) Alternating stop and go generator. (10 Marks)

**OR**

- 10 a. Explain Additive Generators. Also explain fish and pike Additive Generator. (10 Marks)  
b. With a neat diagram, explain the concept of Gifford. (06 Marks)  
c. Write a short note on A5. (04 Marks)

\*\*\*\*\*

# CBCS SCHEME

USN

--	--	--	--	--	--	--	--	--	--

18EC744

## Seventh Semester B.E. Degree Examination, July/August 2022 Cryptography

Time: 3 hrs.

Max. Marks: 100

Note: Answer any FIVE full questions, choosing ONE full question from each module.

### Module-1

- 1 a. Describe the simplified model of Symmetric encryption scheme and its ingredients. (15 Marks)  
b. Explain Euclidean algorithm to find the GCD of two integers. (05 Marks)

OR

- 2 a. With suitable example, explain the Substitution Cipher. (08 Marks)  
b. Explain the Transposition Cipher. (07 Marks)  
c. Write the properties of Modular Arithmetic. (05 Marks)

### Module-2

- 3 a. Describe the overall scheme for DES algorithm and its salient features. (15 Marks)  
b. What are the strengths of DES algorithm? (05 Marks)

OR

- 4 a. Present an overview of the general structure of Advanced Encryption standard. (10 Marks)  
b. Describe the AES key expansion algorithm. (10 Marks)

### Module-3

- 5 a. Distinguish between Groups, Rings and Fields. (12 Marks)  
b. Define Discrete Logarithms with an example. (08 Marks)

OR

- 6 a. With examples, describe Fermat's and Euler's theorem. (12 Marks)  
b. Define the fields of the form  $GF(P)$ . (08 Marks)

### Module-4

- 7 a. Present an overview of the RSA algorithm. (10 Marks)  
b. Describe Elliptic Curve Cryptography. (10 Marks)

OR

- 8 a. Describe Diffie – Hellman key exchange algorithm. (10 Marks)  
b. What are the basic principles of Public key Cryptography? (05 Marks)  
c. What are the possible approaches to attack the RSA algorithms? (05 Marks)

### Module-5

- 9 a. Explain LFSR and how the Shift register sequences are used in cryptography. (10 Marks)  
b. Write note on : Design and Analysis of Stream Cipher. (10 Marks)

OR

- 10 Write short note on :  
a. Geffe generator. (06 Marks)  
b. A5 to encrypt GSM. (06 Marks)  
c. NANOTEQ and RAMBUTAN. (08 Marks)

\* \* \* \* \*

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.  
2. Any revealing of identification, appeal to evaluator and /or equations written eg. 42+8 = 50, will be treated as malpractice.

# CBCS SCHEME

USN

--	--	--	--	--	--	--	--	--	--

17TE71

## Seventh Semester B.E. Degree Examination, Jan./Feb.2021 Cryptography and Network Security

Time: 3 hrs.

Max. Marks: 100

Note: Answer any FIVE full questions, choosing ONE full question from each module.

### Module-1

- 1 a. Explain the procedure to calculate GCD using Euclid's algorithm. Determine the GCD of (24140, 16,762) using Euclid's algorithm. (06 Marks)
- b. Encrypt the message "Work is workshop" using, play fair cipher with the keyboard "COMPUTER" and decrypt the cipher text to recover the original message. Give the rules for encryption and decryption. (08 Marks)
- c. Develop a set of additive and multiplications tables for modulo 9. (06 Marks)

OR

- 2 a. Construct the finite field  $GF(2^4)$  multiplication table using the polynomial arithmetic modulo  $(x^4 + x + 1)$ , show the calculation steps. (06 Marks)
- b. Using extended Euclidean, find the multiplicative inverse of 550 mod 1769. (06 Marks)
- c. Define the following:
  - (i) Groups, rings and fields.
  - (ii) Fermat's and Euler's theorem.
  - (iii) Cryptology, Cryptoanalysis, Cryptography. (08 Marks)

### Module-2

- 3 a. Compare AES to DES for each of the following elements of DES :
  - (i) XOR of subkey material with the input of the f function.
  - (ii) XOR of the f function output with the left half of the block.
  - (iii) f function
  - (iv) Permutation P
  - (v) Swapping of half of the block. (06 Marks)
- b. Consider the elliptic curve defined over  $E_{2,3}(1, 1)$ . Let  $P = (3, 10)$  and  $Q = (9, 7)$ . Find  $(P+Q)$  and  $2P$ . (08 Marks)
- c. Given  $p = 19$ ,  $q = 23$ ,  $m = 5$  and  $e = 3$ . Use RSA algorithm to find  $n$ ,  $\phi(n)$ ,  $d$  and  $C(m)$ . Also find  $M$  from decryption. (06 Marks)

OR

- 4 a. What are the 4 tasks performed in each round of AES cipher? Explain. (06 Marks)
- b. Users A and B use the Diffie Hellman key exchange technique, a common prime  $q = 11$  and a primitive root  $\alpha = 7$ 
  - (i) If user A has private key  $X_A = 3$ . What is A's public key  $Y_A$ ?
  - (ii) If user B has private key  $X_B = 6$ . What is B's public key  $Y_B$ ? What is the shared secret key? Write the algorithm as well? (06 Marks)
- c. Given the plaintext [000102030405060708090A0B0C0D0E0F] and the key [01010101010101010101010101010101]. Show the (a) State matrix (b) Initial round key (c) Sub Bytes (d) Shift rows (e) Mix columns output states. (08 Marks)

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.  
2. Any revealing of identification, appeal to evaluator and/or equations written eg.  $4+8=50$ , will be treated as malpractice.

**Module-3**

- 5 a. Explain MD5 algorithm steps. Compare it with SHA-1. (08 Marks)  
 b. Discuss the key components of digital signature algorithm. (06 Marks)  
 c. Explain the HMAC algorithm with a neat diagram. (06 Marks)

**OR**

- 6 a. Explain the Discrete Logarithm signature scheme. (06 Marks)  
 b. Describe SHA 512 algorithm in detail. (06 Marks)  
 c. Explain the following:  
 (i) Hash function and its requirements.  
 (ii) Role of compression function in Hash functions.  
 (iii) Difference between weak and strong collision resistance.  
 (iv) Advantages of HMAC over other hash based schemes. (08 Marks)

**Module-4**

- 7 a. Describe the four protocols defined by secure socket layer. (06 Marks)  
 b. Explain the Secure Shell (SSH) architecture. (06 Marks)  
 c. Explain the various phases of 802.11i. (08 Marks)

**OR**

- 8 a. Explain the parameters defined in SSL connection. (06 Marks)  
 b. Bring out the differences between SSL and TLS. (06 Marks)  
 c. Explain HTTPS elements encrypted connection initiation and connection closure. (08 Marks)

**Module-5**

- 9 a. Explain the services provided by PGP and the reasons for using PGP. (06 Marks)  
 b. Explain Encapsulating security pay load header. (06 Marks)  
 c. Explain the preparation of enveloped Data S/MIME entity. Write the functions of S/MIME and Enhanced Security Services of S/MIME. (08 Marks)

**OR**

- 10 a. Explain the IPsec architecture. (06 Marks)  
 b. Describe the following :  
 (i) Differences between Tunnel mode and Transport mode of IPsec.  
 (ii) Scope of ESP encryption and authentication. (08 Marks)  
 c. Explain IKE key determination protocol. (06 Marks)

\* \* \* \* \*

USN

--	--	--	--	--	--	--	--

## Seventh Semester B.E. Degree Examination, Jan./Feb. 2021 Cryptography

Time: 3 hrs.

Max. Marks: 100

**Note: Answer any FIVE full questions, choosing ONE full question from each module.**

### Module-1

- 1 a. What is Divisibility? Explain the division algorithm with suitable example. (06 Marks)
- b. Explain with examples the properties of modular Arithmetic. (06 Marks)
- c. Write a note on Finite field of the Form  $GF(P)$ . (08 Marks)

OR

- 2 a. Write the Arithmetic addition modulo and multiplication module for  $GF(2^4)$ . (06 Marks)
- b. With suitable example, explain the polynomial Arithmetic with co-efficient in  $Z_p$ . (08 Marks)
- c. What are Groups? Explain in detail with respect to its properties. (06 Marks)

### Module-2

- 3 a. With a neat sketch, explain the model of symmetric cryptosystems. (06 Marks)
- b. For the keyword "ELECTRONICS", Give the cipher text for the plain text "COMMUNICATION ENGINEERING", using play fair cipher. Explain the rules for play fair cipher. (10 Marks)
- c. Explain with an example, how the transposition technique is used to convert PT to CT. (04 Marks)

OR

- 4 a. What is Stegnography? Explain different methods adopted in stegnography. (06 Marks)
- b. Explain simplified DES algorithm with a neat block diagram. (08 Marks)
- c. Explain with suitable sketch, the concept of Feistel encryption and decryption. (06 Marks)

### Module-3

- 5 a. List and explain the algorithm and characteristics implementation and AES. (08 Marks)
- b. Explain the Key-Block-Round combination analysis in AES. (06 Marks)
- c. Explain the concept of AES encryption single Round stages. (06 Marks)

OR

- 6 a. Explain in detail the nonlinear shift Register. (06 Marks)
- b. Write an explanatory note on Linear Feed Back Shift Registers. (10 Marks)
- c. Compare different LFSR based stream ciphers for its cryptographic weaknesses. (04 Marks)

### Module-4

- 7 a. Find the GCD of (1970, 1066) using Euclid's method. (04 Marks)
- b. With suitable explanation prove Euler's theorem. (07 Marks)
- c. Explain Chaises Remainder Theorem and its features. (09 Marks)

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.  
2. Any revealing of identification, appeal to evaluator and /or equations written eg,  $42+8=50$ , will be treated as malpractice.



OR

- 8 a. Explain the complete steps involved for encryption key Generation and Decryption for RSA algorithm. (08 Marks)
- b. What is Key Management? Explain DH key exchange mechanism. (08 Marks)
- c. Users A and B use the DH key exchange technique. A common prime  $Q = 353$  and a primitive root  $\alpha = 3$ , If A select private key  $X_A = 97$  and B selects private key  $X_B = 233$ , then, what is public key  $Y_A$  of A and public key  $Y_B$ . Calculate shared secret key 'K'. (04 Marks)

Module-5

- 9 a. What are one way Hash Functions? Explain in detail one way hash function using symmetric block algorithms. (08 Marks)
- b. Write an explanatory note on MAC. (06 Marks)
- c. Briefly explain the security threats on Hash function and MAC. (06 Marks)

OR

- 10 a. Explain in detail Direct Digital Signature and Arbitrated Digital Signature. (08 Marks)
- b. Explain with suitable sketch, Discrete Logarithm signature scheme. (06 Marks)
- c. Briefly, explain the signing and verifying the Digital Signature Algorithm (DSA). (06 Marks)

\*\*\*\*\*

$$Q = 353$$

$$\alpha = 3$$

$$X_A = 97 \quad Y_A = 40$$

$$X_B = 233$$

$$Y_B = 233 \text{ mod } 353$$

$$[3^{10}]^{10} [98]^{10} = [98^2]^{10}$$

$$73^3, 73^2$$

$$11.$$

$$21$$

2 of 2

$$248 = 21^2 \times 67$$

$$\begin{matrix} 100 & 20 & 2 & 23 \\ (3) & = & (21) & . & 3 \\ \downarrow & & \downarrow & & \downarrow \\ (3) & & (3) & & (3) \\ 1981 & . & 3 & & 94 \times 3 = 67 \end{matrix}$$

# CBCS SCHEME

USN

--	--	--	--	--	--	--	--	--	--

17TE7

## Seventh Semester B.E. Degree Examination, July/August 2022 Cryptography and Network Security

Time: 3 hrs.

Max. Marks: 100

*Note: Answer any FIVE full questions, choosing ONE full question from each module.*

### Module-1

- 1 a. Explain the concept of divisibility and the division algorithm. (10 Marks)  
b. State and prove Fermat's and Euler's theorem for public-key cryptography. (10 Marks)

OR

- 2 a. Construct the addition, multiplication and inverses table for Arithmetic in  $GF(2^3)$ . (06 Marks)  
b. Mention the Modular Arithmetic Operation properties and prove the same. (08 Marks)  
c. Explain the following terminologies:  
(i) Symmetric Algorithms (ii) Asymmetric Algorithms (06 Marks)

### Module-2

- 3 a. With a neat diagram, explain DES encryption process. (10 Marks)  
b. Explain with a neat diagram the detailed structure of AES cipher. (10 Marks)

OR

- 4 a. Explain the Requirements of public-key cryptography. (06 Marks)  
b. Describe the RSA algorithm with an example. (08 Marks)  
c. Explain Elliptic curves over  $Z_p$ . (06 Marks)

### Module-3

- 5 a. Explain the concept of N-Hash with a neat diagram. (10 Marks)  
b. Explain the following one-way hash functions using symmetric block algorithms:  
(i) Tandem and Abreast Davies Meyer (ii) MDC-2 and MDC-4 (10 Marks)

OR

- 6 a. With a neat diagram, explain the operation Secure Hash Algorithm (SHA). (10 Marks)  
b. Explain Discrete Logarithm Signature Schemes. (10 Marks)

### Module-4

- 7 a. Give a comparison on Treats on the web. (06 Marks)  
b. Explain the Record Protocol of Secure Sockets Layer (SSL). (08 Marks)  
c. Explain the Alert codes supported by Transport Layer Security (TLS). (06 Marks)

OR

- 8 a. Explain the phase 1 (Establish Security Capabilities) of Handshake Protocol. (10 Marks)  
b. Describe the concept of HTTPs. (10 Marks)

### Module-5

- 9 a. Explain Pretty Good Privacy (PGP) for providing cryptographic functions like authentication, confidentiality and both with a neat diagram. (10 Marks)  
b. What are the two databases of IP Security policy and explain them. (10 Marks)

OR

- 10 a. Illustrate the working of transport and tunnel mode Encapsulating Security Payload (ESP). (10 Marks)  
b. With a neat diagram, describe Header and Payload Formats of Internet Key Exchange (IKE). (10 Marks)

\*\*\*\*\*

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.  
2. Any revealing of identification, appeal to evaluator and/or equations written eg. 42+8 = 50, will be treated as malpractice.