Pandit Deendayal Energy University
School of Technology
Department of Computer Science and Engineering
Odd Semester 2023-2024
Course student handout file
INDEX

Name of the course: Information Security	**Course Code:**20CP304T
Program: B.Tech. **Branch: CSE**	**Semester:5th** **Academic Year: 2023-24**
Name of Course Coordinator: Dr. Rutvij H. Jhaveri	
Subject Teachers (Division wise/Batch wise): Elective Course **1. Dr. Nishant Doshi, Dr. Hargeet Kaur** **2. -**	

Date:

Signature of Subject Teachers **Signature of Department Coordinator (IQAC)** **Signature of Head of the Department**

1. Departmental Vision & Mission

Vision

"To contribute to the society by imparting transformative education and producing globally competent professionals having multidisciplinary skills and core values to do futuristic research & innovations."

Mission

- To accord high quality education in the continually evolving domain of Computer Engineering by offering state-of-the-art undergraduate, postgraduate, doctoral programmes.
- To address the problems of societal importance by contributing through the talent we nurture and research we do:
- To collaborate with industry and academia around the world to strengthen the education and multidisciplinary research ecosystem.
- To develop human talent to its fullest extent so that intellectually competent and imaginatively exceptional leaders can emerge in a range of computer professions.

2. Program educational objectives (PEOs) of Department

The Program Educational Objectives of B.Tech. (Computer Engineering) program are:

1. To prepare graduates who will be successful professionals in industry, government, academia, research, entrepreneurial pursuit and consulting firms
2. To prepare graduates who will make technical contribution to the design, development and production of computing systems
3. To prepare graduates who will get engage in lifelong learning with leadership qualities, professional ethics and soft skills to fulfill their goals
4. To prepare graduates who will adapt state of the art development in the field of computer engineering

3. Program Outcomes (POs)

Undergraduate engineering program are designed to prepare graduates to attain the following program outcomes:

1. Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
2. Problem analysis: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

3. Design / development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
4. Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
5. Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.
6. The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
7. Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
8. Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
9. Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
10. Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
11. Project management and finance: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
12. Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

4. Program Specific Outcomes (PSOs)

The graduates of CSE department will be able to:

1. Develop computer engineering solutions for specific needs in different domains applying the knowledge in the areas of programming, algorithms, hardware-interface, system software, computer graphics, web design, networking and advanced computing.
2. Analyze and test computer software designed for diverse needs.
3. Pursue higher education, entrepreneurial ventures and research.

5. Academic Calendar

PANDIT DEENDAYAL ENERGY UNIVERSITY
Academic Calendar: 2023-24

Odd Semester: UG Sem.1/3/5/7 & PG Sem. 1/3 (FoET) & UG Sem. 1/3/5/7 & PG Sem 1/3 (FoLS)	
Particulars	Date
Semester Registration & Commencement of classes-FoET & FoLS- 1st Sem	17th July (Mon) 2023
Semester Registration, Department Orientation & Commencement of classes for 3/5/7 Sem – FoET & FoLS	24th Jul (Mon). 2023
Evaluation of Rural Internship/CSSI & Evaluation of Industry Orientation, & Evaluation of Industrial Internship	7th (Mon)-11th (Fri)Aug. 2023
Independence Day Celebration	15th Aug. (Thes) 2023
Attendance Review-1 (After 4 week)	17th (Thur)-18th (Fri) Aug. 2023
Internal Assesment-1 (Quiz, Test, Assignment etc.)** Student mentoring week – 1	21st (Mon)-25th (Fri)Aug. 2023
Mid Semester Examination / Project Phase 1 Review	11th Sept. (Mon) 2023 Onwards
Attendance Review-2 (After 8 week)	14th (Thur)-15th (Fri)Sept 2023
Parent Teacher Meeting (Saturday)	23rd Sept.(Sat) 2023
Last date of showing evaluated answer books of Mid Semester Examination	27th Sept. (Wed) 2023
Declaration of Mid Semester Exam Result	6th Oct. (Fri) 2023
360 Degree Feedback from Students by School Admin	9th (Mon)-13th (Fri)Oct. 2023
Attendance Review-3 (After 12 week)	12th (Thur)-13th (Fri)Oct 2023
Rangtaal – Navratri Celebration	13th Oct.(Fri) 2023
Internal Assesment-2 (Quiz, Test, Assignment etc)** Student mentoring week – 2	25th (Wed)-31st (Tues)Oct. 2023
Tesseract – The Science & Technical Fest	03(Fri)-04(Sat)-05(Sun) Nov. 2023
Declaration of Detention list of students (during 13th Week)	By 20th Oct (Fri) 2023
Diwali Vacation	13th (Mon)-17th (Fri) Nov. 2023
Classes End	21st (Tues) Nov. 2023
Practical Examinations, submission of Term Work and Seminars	22nd Nov.(Wed) 2023 Onwards
Dissertation presentation for UG and PG for FOLS	22nd Nov.(Wed) 2023 onwards
End Semester Examinations - FoET& FoLS	28th Nov.(Tues) 2023 Onwards
Last date of Submission of Marks of End sem. Exam	15th Dec. (Fri) 2023
Rural Internship for FoLS students	During Dec 2023
Project Phase I Exam for PG program of FoET & Progress Review for Ph. D.	18th (Mon)-22nd (Fri)Dec. 2023
Winter Break	26th (Tues)-29th (Fri)Dec. 2023
Alumni Day	29th Dec (Fri) 2023
Even Semester: UG Sem. 2/4/6/8 & PG Sem. 2/4 (FoET) & UG Sem.2/4/6/8 & PG Sem. 2/4 (FoLS)	
Next semester registration	27th (Wed)-30th (Sat) Dec. 2023
Start of Next Semester	1st Jan. (Mon) 2024

- This calendar is subject to change under any unforeseen situation.
- All the students should start attending the classes from the day of commencement of respective semester subject to fulfillment of the semester progression rules.
- **Internal assessment shall be in parallel to the regular teaching schedule.
- Attendance Rule: Please attend all lectures and laboratories without fail. Attendance is compulsory as per the PDEU norms, the student must maintain 80% attendance.

6. Class Time Table and Faculty Time Table with office hours

Class Time Table

Div 6

Faculty Time Table : Dr. Rutvij H. Jhaveri

Rutvij H Jhaveri
Computer Science & Engineering

Autumn Semester 2023 w.e.f : 24th July 2023

Day	08:00-09:00	09:00-10:00	10:00-11:00	11:00-12:00	12:00-13:00	13:00-14:00	14:00-15:00	15:00-16:00	16:00-17:00	17:00-18:00	18:00-19:00
Monday		G1 (23CP301P) E204, CP(5) - L							G1 (23CP301P) F-203, CP(5) - P		
		G1 (23CP301P) E204, CP(5) - L							G1 (23CP301P) F-203, CP(5) - P		
		G1G2 (23CP301P) E204, CP(5) - L							G1 (23CP301P) F-203, CP(5) - P		
		G1G2 (23CP301T) E204, CP(5) - L							G1 (23CP301P) F-203, CP(5) - P		
		G1G2 (23CP301T) E204, CP(5) - L							G1 (23CP301P) F-203, CP(5) - P		
		G1G2 (23CP301T) E204, CP(5) - L							G1 (23CP301P) F-203, CP(5) - P		
Tuesday		G1 (23CP301P) E204, CP(5) - L					G11 (20CP304P) F-104, CP(5) - P			G1G2 (F-303, CP(5) -	
		G1 (23CP301P) E204, CP(5) - L									
		G1G2 (23CP301P) E204, CP(5) - L									
		G1G2 (23CP301T) E204, CP(5) - L									
		G1G2 (23CP301T) E204, CP(5) - L									
		G1G2 (23CP301T) E204, CP(5) - L									

Wednesday									G10 (20CP304P) E203, CP(5) - P		
Thursday		G1 (23CP301P) F-203, CP(5) - P									
		G1 (23CP301P) F-203, CP(5) - P									
		G1 (23CP301P) F-203, CP(5) - P									
		G3 (23CP301P) F-203, CP(5) - P									
		G3 (23CP301P) F-203, CP(5) - P									
		G3 (23CP301P) F-203, CP(5) - P									
Friday		G1 (23CP301P) F-203, CP(5) - P	G11G12 (20CP304T) D102, CP(5) - L								
		G1 (23CP301P) F-203, CP(5) - P									
		G1 (23CP301P) F-203, CP(5) - P									
		G2 (23CP301P) F-203, CP(5) - P									
		G2 (23CP301P) F-203, CP(5) - P									
		G2 (23CP301P) F-203, CP(5) - P									

Location Abbr.	Location Name
D102	D, Lecture Hall
E203	E, Lecture Hall
E204	E, Lecture Hall
F-104	F, Data Analytics Lab
F-203	F, Security & Comp. Lab
F-303	F, Lecture Hall

Subject Abbr.	Subject Name
20CP304T	Information Security
20CP304P	Information Security - Lab.
23CP301P	Advanced Python
23CP301T	Advanced Python

Office Hours: Monday 2:00 to 4:00 pm

7. Course Outcomes (COs), Course Syllabus, Pre requisites for the course

20CP304T					Information Security					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
2	0	0	2	2	25	50	25	-	-	100

COURSE OBJECTIVES

- To understand the concept of security requirements, security attacks, and security policy.
- To understand the mathematical concepts for cryptographic algorithms.
- To understand the security mechanisms available to protect the data.
- To understand the security analysis of cryptographic algorithms.

UNIT 1 INTRODUCTION AND NUMBER THEORY **7 Hrs.**

Basics of Information Security, Classical Ciphers and Cryptanalysis, Introduction to Steganography. Introduction to Number Theory.

UNIT 2 SYMMETRIC KEY CRYPTOGRAPHY **7 Hrs.**

Feistel Structure, Advanced Encryption Standard, Data Encryption Standard, Modern Block Ciphers, Modes of Operation, Synchronous and Asynchronous Stream Ciphers, Use of Modern Block Ciphers and Stream Ciphers.

UNIT 3PUBLIC KEY CRYPTOGRAPHY

Introduction to Public Key Cryptography, Diffie-Hellman Key Exchange, RSA Cryptosystem, RSA Cryptanalysis. Elliptic Curve Cryptography. **6 Hrs.**

UNIT 4HASH FUNCTION AND DIGITAL SIGNATURE **6 Hrs.**

Introduction to Hash Function, MD5, SHA, Message Authentication Code, Digital Signature, Authentication Protocols.

Max. 26 Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Differentiate between cryptography and cryptanalysis.
CO2- Explain the mathematical concepts for cryptographic algorithms.
CO3- Apply symmetric encryption techniques for data security.
CO4- Analyze the security strength of public key cryptosystem.
CO5- Use Hashing algorithm for Digital signature.
CO6- Express the importance of authentication protocols.

TEXT/REFERENCE BOOKS

1. William Stallings, "Cryptography and Network Security Principles and Practice", Pearson Education
2. Atul Kahate, “Cryptography and Network Security”, Tata McGraw-Hill Education
3. Behrouz A. Forouzan, “Cryptography and Network Security”, McGraw-Hill Education
4. Wenbo Mao, “Modern Cryptography: Theory and Practice”, Prentice Hall.
5. Bruce Schneier, “Applied Cryptography: Protocols, Algorithms, and Source Code in C”, Wiley Computer Publishing.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 3 Hrs**

Part A: 50 Marks

Part B: 50 Marks

8. Lesson Plan

Lecture No.	Topic to be covered	Teaching Aid to be used	Remarks (Text book/Unit No etc.)
1	Basics of Information Security	BW+PPT	Unit 1
2	Classical Ciphers and Cryptanalysis	BW+PPT	Unit 1
3	Substitution techniques	BW+PPT	Unit 1
4	Transposition techniques	BW+PPT	Unit 1
5	Introduction to Steganography	BW+PPT	Unit 1
6	Introduction to Number Theory	BW+PPT	Unit 1
7	Euler's Theorem and Fermat's Theorem	BW+PPT	Unit 1
8	Feistel Structure	BW+PPT	Unit 2
9	Advanced Encryption Standard	BW+PPT	Unit 2
10	Data Encryption Standard	BW+PPT	Unit 2
11	Modern Block Ciphers	BW+PPT	Unit 2
12	Modes of Operation	BW+PPT	Unit 2
13	Synchronous and Asynchronous Stream Ciphers	BW+PPT	Unit 2
14	Use of Modern Block Ciphers and Stream Ciphers	BW+PPT	Unit 2
15	Introduction to Public Key Cryptography	BW+PPT	Unit 3
16	Diffie-Hellman Key Exchange	BW+PPT	Unit 3
17	RSA Cryptosystem	BW+PPT	Unit 3
18	RSA Cryptanalysis	BW+PPT	Unit 3
19	Elliptic Curve Cryptography: Basics	BW+PPT	Unit 3
20	Elliptic Curve Cryptography: Numericals	BW+PPT	Unit 3
21	Introduction to Hash Function	BW+PPT	Unit 4
22	MD5	BW+PPT	Unit 4
23	SHA	BW+PPT	Unit 4
24	Message Authentication Code	BW+PPT	Unit 4
25	Digital Signature	BW+PPT	Unit 4
26	Authentication Protocols	BW+PPT	Unit 4

Legends : BW (Board Work), PPT (PowerPoint Slides)

9. Program Articulation Matrix and Course Articulation Matrix

Course Articulation Matrix

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
18CP304T.1	3	1	1	-	1	1	-	2	2	1	-	3	3	1	3
18CP304T.2	3	3	2	2	1	1	-	2	2	1	-	3	3	1	3
18CP304T.3	3	2	2	2	3	2	-	2	2	1	1	3	3	1	3
18CP304T.4	3	3	3	2	1	2	-	2	2	1	2	3	3	1	3
18CP304T.5	3	3	3	3	2	2	-	2	2	1	2	3	3	1	3
18CP304T.6	3	1	1	1	2	1	-	2	2	1	-	3	3	1	3
18CP304T	3.00	2.17	2.00	1.67	1.67	1.50	0.00	2.00	2.00	1.00	0.83	3.00	3.00	1.00	3.00

Program Articulation Matrix

PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PS01	PSO2	PSO3
3.00	2.17	2.00	1.67	1.67	1.50	0.00	2.00	2.00	1.00	0.83	3.00	3.00	1.00	3.00

Correlation levels 1, 2 or 3 as defined below:

1: Slight (Low)

2: Moderate (Medium)

3: Substantial (High)

10. Evaluation Scheme and Rubrics

Course code: 20CP304T **Course name:** Information Security

Course Outcomes (CO's): On completion of the course, student will be able to
CO1- **Differentiate** between cryptography and cryptanalysis.
CO2- **Explain** the mathematical concepts for cryptographic algorithms.
CO3- **Apply** symmetric encryption techniques for data security.
CO4- **Analyze** the security strength of public key cryptosystem.
CO5- **Use** Hashing algorithm for Digital signature.
CO6- **Express** the importance of authentication protocols.

CO Assessment Tools (Direct Assessment):
Various assessment tools used to evaluate CO's (Rubrics) and the frequency with which the assessment processes are carried out are listed below.

Assessment Method	Assessment Tool	Description	Marks	Mapping with CO	Contribution to CO's
Direct	Mid-sem	MCQ/Analytical/ Output-based/ questions on syllabus covered from Unit I, Unit II	50	CO1/CO2/CO3 CO4/CO5/CO6	It fractionally contributes to 50% weightage of Direct Assessment to CO attainment. (50/2)
Direct	MCQ/Class Assignment	MCQ/ Analytical/ Output-based/ Theoretical questions on syllabus covered	25	CO1/CO2/CO3 CO4/CO5/CO6	It contributes to 100% weightage of Direct Assessment to CO attainment.
Direct	End-Sem Examination	**Topics to be covered:** Unit I, II, III, IV	100	CO1,CO2, CO3,CO4, CO5, CO6	It contributes to 50% weightage of Direct Assessment to CO attainment. (100/2)
	Total 100 Marks				

11. Tutorials, Assignments, Case Studies, Quiz, Presentations etc.

a. Topic wise PPTs as well as other study material (including question bank) for All units 1 to 4 made available online on Teams Platform
b. Quiz papers for all divisions and Assignment is attached as separate sheet.
a. Remedial Presentation details along with the date wise conduction is attached in separate sheet.

12. Copy of Mid and End Semester Examination Question Papers (Old and Current), solution of current examination with stage-wise marking scheme

MID SEMESTER EXAMINATION

Pandit Deendayal Energy University

(Formerly Pandit Deendayal Petroleum University)

Mid Semester Examination - September 2022

B. Tech. (Computer Science & Engineering)

Semester - V

Date: 27.09.2022

Course Name : Information Security **Time: 2 hours**

Course Code : 20CP304T **Max. Marks: 50**

Instructions:

1. Do not write anything other than your roll number on question paper.
2. Assume suitable data wherever essential and mention it clearly.
3. Writing appropriate units, nomenclature, and drawing neat sketches/schematics wherever required is an integral part of the answer.

Ques. No.	Description	Marks	CO Mapped	BL
Q.1	Distinguish between the following: i. Passive and Active attacks ii. Data authentication and Data confidentiality iii. Substitution and Transposition cipher iv. Stream cipher and Block cipher v. Cryptography and Steganography	02*5	CO-1	L-2
Q. 2	i. State Fermat's Theorem. ii. Solve the following equations for **X** **X**≡ 2 (mod 5) **X**≡ 3 (mod 7) **X**≡ 10 (mod 11)	2+8	CO-2	L-3
Q.3	i. Construct playfair matrix with the key "ELEPHANT" ii. Demonstrate the playfair cipher by showing encryption on the plain text: "GREEN BALLOON" using the key in Q.3 i. iii. Identify two disadvantages of playfair cipher. iv. Give example of an autokey system. Name the cipher which makes use of this system.	2+4+2+2	CO-3	L-4
Q. 4	i. Describe fiestel cipher structure (encryption only) with a neat sketch. ii. Discuss avalanche effect. Also name any two encryption algorithms that perform strong avalanche effect.	05*2	CO-3	L-2
	OR			
	Describe Advanced Encryption Standard.	10	CO-3	L-2
Q. 5	i. Explain meet-in-the-middle attack? In which encryption model do we encounter this attack? ii. Choose another encryption model that can be used to counter meet-in-the-middle attack. Discuss the	05*2	CO-3	L-4

	encryption and decryption steps in the chosen model using a neat sketch.			
	OR			
	Describe 5 block cipher modes of operations. Compare the strength and weakness of all modes.	10	CO-3	L-4

Note: Solution is attached as a separate sheet

END SEMESTER EXAMINATION

Pandit Deendayal Energy University

(Formerly Pandit Deendayal Petroleum University)

End Semester Examination - December 2022

B. Tech. (Computer Science & Engineering)

Semester - V

Date: 06.12.2022

Course Name : Information Security **Time: 3 hours**

Course Code : 20CP304T **Max. Marks: 100**

Instructions:

4. Q.1 to Q.5 are compulsory. Attempt any one sub-question A or B in Q.6 to Q.10.
5. Do not write anything other than your roll number on question paper.
6. Assume suitable data wherever essential and mention it clearly.
7. Writing appropriate units, nomenclature, and drawing neat sketches/schematics wherever required is an integral part of the answer.

Ques. No.	Description	Marks	CO Mapped	BL
Q. 1	a) State true or false against the following statements i. In RSA, p and q should differ in length only by a few digits. ii. Data Authentication Code (DAC) is calculated by using the cipher block chaining (CBC) mode of operation on triple DES with an initialization vector of zero. iii. Symmetric key encryption is slower than asymmetric key encryption. iv. DES encrypts 64-bit blocks using a 56-bit key and produces a 64-bit ciphertext. b) Differentiate between the following: i. Monoalphabetic and polyalphabetic cipher ii. Synchronous and Asynchronous stream ciphers.	4+6	CO-1	L-1
Q. 2	a) List the criteria defined by NIST for AES. b) What is trapdoor one-way function? c) Discuss the merits of counter mode over output feedback mode. d) State Euler's Theorem.	2*5	CO-4	L-1

	e) What do you mean by discrete logarithm?			
Q. 3	a) Using p=11, q=17, d=23 and e=7 in the Rivest, Shamir, Adleman (RSA) algorithm, what is the value of cipher text for a plain text 5? b) Find the inverse of 135 in GF(61) using extended Euclidean Theorem.	3+7	CO-4	L-3
Q. 4	a) Describe the trapdoor function used in elliptic curve cryptography (ECC). b) You want to secretly send a message to your friend using public key cryptography. Which one would you prefer: RSA or ECC? Justify your choice. c) Name any 5 categories of possible attacks on RSA.	3+2+5	CO-4	L-2
Q. 5	a) Identify the security service(s) offered by the models described in i. FIGURE 1 ii. FIGURE2 iii. FIGURE 3 b) Give suggestions to improve the cryptography model described in FIGURE 3 so that it is resistant to release of message content attack. c) Give one example (only example, no definition required) to explain the following: i. Denial of service attack ii. Avalanche effect iii. Brute-force attack iv. A prime number can have more than one primitive roots. v. Access control	3+2+5	CO-6	L-4

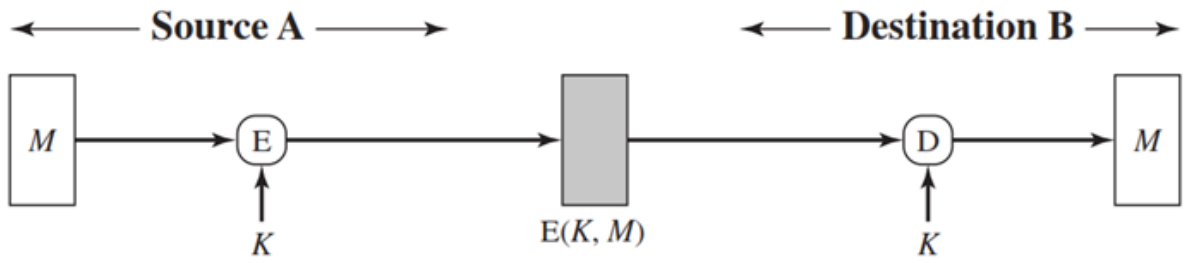

FIGURE 1

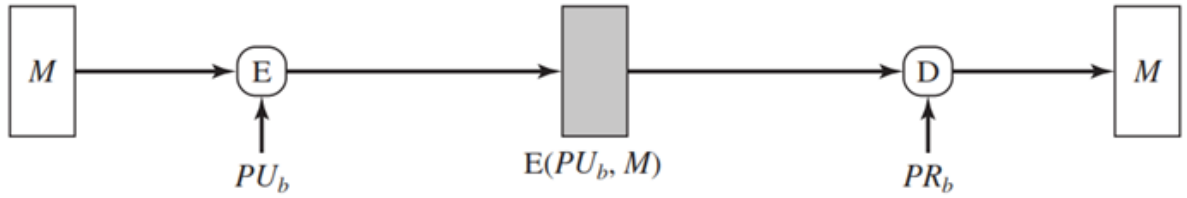

FIGURE 2

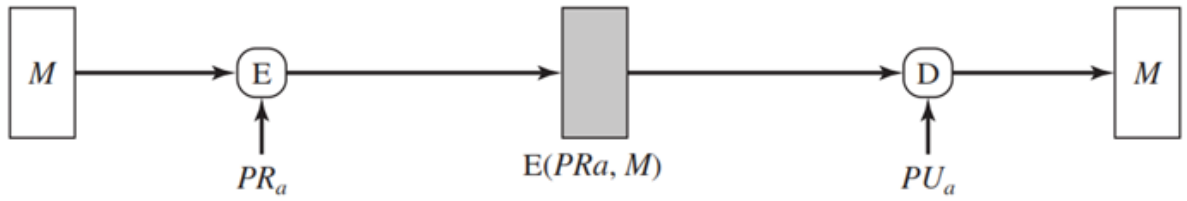

FIGURE 3

Q. 6 A	State and prove Fermat's Theorem.	10	CO-2	L-3
	OR			
Q. 6 B	Solve the following equations for **X** using Chinese Remainder Theorem. **X**≡ 3 (mod 5); **X**≡ 1 (mod 7);**X**≡ 6 (mod 8)	10	CO-2	L-3
Q. 7 A	a) Explain one-time pad cryptosystem. b) List two major advantages of block ciphers over stream ciphers. Suggest any method of converting a stream cipher into block cipher. c) Describe feistel cipher structure with a neat sketch.	2+3+5	CO-3	L-2
	OR			
Q. 7 B	a) Differentiate between substitution and transposition cipher. b) Name any 4 substitution cipher techniques. c) Give detailed explanation of encryption and decryption of any one transposition cipher with the help of an example.	2+2+6	CO-3	L-2
Q. 8 A	Comment on the weaknesses in DES due to a) Design of S-box b) Design of D-box c) Key size	10	CO-3	L-4
	OR			
Q. 8 B	a) What is the need of S-box? Explain two types of S-boxes.	5+5	CO-3	L-4

	b) What is the need of D-box? How many types of D-boxes can be used in modern block ciphers?			
Q. 9 A	Prove the secret exchange of key proposed by Diffie Hellman.	10	CO-4	L-3
	OR			
Q. 9 B	Explain with an example how meet in the middle attack is possible in Diffie Hellman key exchange.	10	CO-4	L-3
Q. 10A	a) Elaborate the steps for digital signature creation (only creation, no verification) using Digital Signature Algorithm. b) What security service(s) do the following methods provide : i. Hashing ii. MAC iii. Digital Signature	5+5	CO-5	L-2
	OR			
Q. 10B	a) Mention 5 properties/ requirements of a hash function in information security. b) Identify the requirements in a cryptography model that avoid the following: i. Traffic analysis ii. Timing modification iii. Disclosure iv. Source repudiation iv. Masquerade	5+5	CO-5	L-2

Note: Solution is attached as a separate sheet

13. Course covered beyond syllabus

Materials from national and international level like NPTEL, Web resources, etc. is shared related to subject domain.

14. Actual Engagement of Class

15. Attendance Record (Up to Mid Semester Examination and Up to End semester Examination)

Attendance Records for the students has been attached in the separate sheet.

16. Details for Remedial Classes (list and identification of slow learners, actions taken)

Separate Sheet is attached for the remedial classes for slow learners.

17. Justification for Course Outcome mapping with Exams and Assessments

18. Result of students (marks of mid, end and internal assessment components)

Separate sheet for the ESE, MSE and IA marks for the students has been attached.

19. Direct Attainment of COs and POs and interpretation (Result analysis)

20. Indirect Attainment of POs through Course Exit Survey (Just before end sem. exam)

21. Final Attainment of COs and POs and interpretation (Result analysis), Actions to be taken if COs and POs are not achieved

22. Sample answer scripts of mid sem., end sem. exam and assignments of Good, Better and Best performing students (at least five copies of each assessment tool)

23. Class notes (Lecture PPT & Lab manual etc.) in Soft/ Hard copy