|| Jai Sri Gurudev ||
Sri Adichunchanagiri Shikshana Trust (R)

SJC INSTITUTE OF TECHNOLOGY

VTU Affiliated, AICTE Approved, Accredited by NAAC & NBA, Gold Rated by QS I-Gauge
Chickballapur - 562 101, Karnataka

Estd:1986

www.sjcit.ac.in

Department of Computer Science and Engineering

Course File

Scheme	2018
Batch	2020
Academic year	2023 - 2024
Semester	VII
Subject Code & Title	18CS744 & Cryptography
Students enrolled	150+01=151
Allotted Faculties	Prof. Ajay.N & Prof. Rashmi. K.A
Course coordinator	Prof. Ajay.N

Faculty In-charge for CIE

IA – 1	IA – 2	IA – 3
Prof. Ajay.N	Prof. Rashmi. K.A	Prof. Rashmi. K.A

SEE Pass %

	Before Revaluation	After Revaluation
Section A	46: 97.82%	46: 97.82%
Section B	33: 96.96% 16: 100%	33: 96.96% 16: 100%
Section C	56: 100%	56: 100%
Average	98.67%	98.67%

11/3/24

11/3/24
Signature of the Course coordinator

20/4/24
Signature of the HoD
Professor & HOD,
Department of Computer Science & Engg.
S.J.C. Institute of Technology
Chickballapur-562 101

||Jai Sri Gurudev||

S. J. C Institute of Technology, Chickballapur

Department of Computer Science & Engineering

Calendar of Events

(August -2023 to February -2024)

Sl. No	Date / Month	Events	Faculty In – charge
1.	August -2023	Internship (VII semester)	Prof. Swetha T & Prof. Narendra Babu C
2.	04-10-2023 to 06-10-2023	Project Synopsis Presentation	Dr. Shrihari M R ,Dr. Seshaiah M & Dr. Harshavardhan D
3.	25-10-2023 to 27-10-2023	Tutorial-1 (VII semester)	All Faculty Members
4.	02-11-2023 to 04-11-2023	C IE -1 (VII & I semester)	Prof. Girish BG & Dr. Harshavardhan D
5.	24-11-2023 to 25-11-2023	Project Phase-1 Presentation	Dr. Shrihari M R ,Dr. Seshaiah M & Dr. Harshavardhan D
6.	27-11-2023 to 29-11-2023	Tutorial-2 (VII & I semester) Tutorial-1 (III semester)	All Faculty Members
7.	04-12-2023 to 06-12-2023	CIE-2 (VII & I semester) CIE-1(III semester)	Prof. Girish BG & Dr. Harshavardhan D
8.	09-12-2023	Guest Lecture (BDA)	Prof. Srinath GM, Prof. Swetha T & Prof. Chanadana K R
9.	23-12-2023	Parent Teacher Meeting (III semester)	Prof. Gavina C G and all Mentors
10.	23-12-2023	Mini Project Exhibition (Cryptography)	Prof. Ajay N & Prof. Rashmi K A
11.	23-12-2023	Designing the Interface Competition (UID)	Prof. Girish B G, Prof. Divakar K M & Prof. Mamatha G
12.	26-12-2023 to 28-12-2023	Tutorial-3 (VII & I semester) Tutorial-2 (III semester) Tutorial-1 (V	All Faculty Members
13.	01-01-2024 to 03-01-2024	CIE-3 (VII & I semester) CIE-2(III semester) CIE-1(V semester)	Prof. Girish BG & Dr. Harshavardhan D

14.	13-01-2024	Parent Teacher Meeting(V semester)	Prof. Gavina C G and all Mentors
15.	13-01-2024	LEX and YACC Tool Demonstration (AT&CD)	Dr. Manjunatha Kumar B H, Dr. Seshaiah M & Dr. Shrihari MR
16.	13-01-2024	Demonstration of AI & ML Algorithms	Dr. Harshavardhan D, Prof. Bhavya RA & Prof. Gavina CG
17.	13-01-2024	Coding Contest (DSC& OOPS with JAVA)	Dr. Shrihari M R, Prof. Manjunath PV & Prof. Dhanushree AN
18.	29-01-2023 to 31-01-2023	Tutorial-3 (IIII semester) Tutorial-2 (V semester)	All Faculty Members
19.	01-02-2024 to 03-02-2024	CIE-3(III semester) CIE-2(V semester)	Prof. Girish BG & Dr. Harshavardhan D
20.	24-02-2024	Mini Project Exhibition (Computer Networks)	Prof.Manjunth S, Dr. Murthy SVN & Prof. Suresh Kumar HS
21.	26-02-2023 to 28-02-2023	Tutorial-3 (V semester)	All Faculty Members
22.	February-2024	Mini Project Evaluation (DBMS)	Dr. Seshaiah M, Prof. Girish BG & Prof.Kiran Kumar PN
23.	04-03-2024 to 06-03-2024	CIE-3(V semester)	Prof. Girish BG & Dr. Harshavardhan D
24.	December	Department Festival (Technotsav)	All Faculty Members
25.	Every Month Second and Fourth Saturday	BGS Memorial Lecture Series	Prof. Ashok KN

Prepared By: **Prof. Girish B G**

Approved By: **Dr. Manjunatha Kumar B H**
HOD, CSE

|| JAI SRI GURUDEV ||

Sri Adichunchanagiri Shikshana Trust (R)

SJC INSTITUTE OF TECHNOLOGY

CALENDAR OF EVENTS FOR THE ACADEMIC YEAR 2022-2023 (EVEN Semester)

(Affiliated to Visvesvaraya Technological University, Belagavi & Approved by AICTE, New Delhi)

Accredited by NAAC A+ and NBA (CE, ME, CSE, ECE, ISE & AE), Gold rated by QS-I Gauge Certified

Week No.	ಆಗಸ್ಟ್ 2023							No. of Working Days	AUGUST 2023
	MON	TUE	WED	THU	FRI	SAT	SUN		
		1	2	3	4	5	6	5	
	7	8	9	10	11	12	13	6	Aug 7th HOD's/IC Meeting
1	14	15	16	17	18	19	20	5	Aug 14th HOD's/IC Meeting, Aug 14th Internship Program for VII Sem B.E., Aug 15th Independence Day
2	21	22	23	24	25	26	27	6	Aug 21th HOD's/IC Meeting, Aug 26th SEED Activity
3	28	29	30	31				4	Aug 28th HOD's/IC Meeting

Week No.	ಸೆಪ್ಟೆಂಬರ್ 2023							No. of Working Days	SEPTEMBER 2023
	MON	TUE	WED	THU	FRI	SAT	SUN		
4					1	2	3	2	
5	4	5	6	7	8	9	10	6	Sep 4th HOD's/IC Meeting, Sep 4th Induction Program for 1 Sem B.E.
6	11	12	13	14	15	16	17	6	Sep 11th HOD's/IC Meeting, Sep 11th Commencement of Classes for VII Sem B.E.
7	18	19	20	21	22	23	24	5	Sep 18th Ganesh Chaturthi, Sep 21th Commencement of Classes for I Sem B.E.
8	25	26	27	28	29	30		5	Sep 25th HOD's/IC Meeting, Sep 30th SEED Activity, Sep 28th Eid-Milad

Week No.	ಅಕ್ಟೋಬರ್ 2023							No. of Working Days	OCTOBER 2023
	MON	TUE	WED	THU	FRI	SAT	SUN		
9							1	0	
10	2	3	4	5	6	7	8	5	Oct 2nd Gandhi Jayanthi, Oct 5th & 6th Project Review Phase I
11	9	10	11	12	13	14	15	5	Oct 9th HOD's/IC Meeting, Oct 14th Mahalaya Amavasye
12	16	17	18	19	20	21	22	6	Oct 16th HOD's/IC Meeting
13	23	24	25	26	27	28	29	3	Oct 23rd Ayudhapooja, Oct 24th Vijayadasami, Oct 25th to 27th Tutorial 1 for VII & I Sem B.E., Oct 28th Valmiki Jayanti
14	30	31						2	Oct 30th HOD's/IC Meeting

Week No.	ನವೆಂಬರ್ 2023							No. of Working Days	NOVEMBER 2023
	MON	TUE	WED	THU	FRI	SAT	SUN		
15			1	2	3	4	5	3	Nov 1st Kannada Rajyothsava, Nov 2nd to 4th CIE 1 for VII & I Sem B.E.
16	6	7	8	9	10	11	12	6	Nov 6th HOD's/IC Meeting, Nov 12th Naraka Chaturdashi
17	13	14	15	16	17	18	19	5	Nov 13th HOD's/IC Meeting, Nov 14th Balipadyami, Sep 16th & 17th Project Review Phase I
18	20	21	22	23	24	25	26	6	Nov 20th HOD's/IC Meeting, Nov 25th SEED Activity
19	27	28	29	30				3	Nov 27th HOD's/IC Meeting, Nov 27th to 29th Tutorial 2 for VII & I Sem B.E., Nov 30th Kanakadasa Jayanthi

Week No.	ಡಿಸೆಂಬರ್ 2023							No. of Working Days	DECEMBER 2023
	MON	TUE	WED	THU	FRI	SAT	SUN		
20					1	2	3	2	
21	4	5	6	7	8	9	10	6	Dec 04th HOD's/IC Meeting, Dec 4th to 6th CIE I1 for VII & I Sem B.E.
22	11	12	13	14	15	16	17	6	Dec 11th HOD's/IC Meeting, Dec 14th & 15th Project Review Phase I
24	18	19	20	21	22	23	24	6	Dec 18th HOD's/IC Meeting, Dec 23rd SEED Activity
25	25	26	27	28	29	30	31	5	Dec 25th Christmas, Dec 26th to 28th Tutorial 3 for VII & I Sem B.E.

Week No.	ಜನವರಿ 2024							No. of Working Days	JANUARY 2024
	MON	TUE	WED	THU	FRI	SAT	SUN		
26	1	2	3	4	5	6	7	6	Jan 01th HOD's/IC Meeting, Jan 1th to 3rd CIE II1 for VII & I Sem B.E., Ja 6th Last working day for VII Sem & 1 Sem B.E.
27	8	9	10	11	12	13	14	6	Jan 08th HOD's/IC Meeting, Jan 8th Commencement of Practical Exam for VII Sem & 1 Sem B.E.
28	15	16	17	18	19	20	21	5	Jan 15th Makara Sankranti,
29	22	23	24	25	26	27	28	5	Jan 22nd HOD's/IC Meeting, Jan 22nd Commencement of Theory Exa for VII Sem & 1 Sem B.E. Jan 26th Republic Day, Jan 27th SEED Activity
30	29	30	31					3	Jan 29th HOD's/IC Meeting

Meeting's	Commencement & Last Working Day	Seed Activity	CIE	Induction/Internship	Holiday

Commencement of EVEN Semester Classes for VIII Sem B.E. 13.02.2024 & II Sem B.E. 19.02.2024

VISION	MISSION
Preparing Competent Engineering and Management Professional to Serve the Society	• Providing Students with a Sound Knowledge in Fundamentals of their branch of Study. • Promoting Excellence in Teaching, Training, Research and Consultancy. • Exposing Students to Emerging Frontiers in various domains enabling Continuous Learning. • Developing Entrepreneurial acumen to venture into Innovative areas. • Imparting Value based Professional Education with a sense of Social Responsibility.

Dr. THYAGARAJ N R
Chief Coordinator, IQAC

Dr. G. T. RAJU
PRINCIPAL

ವಿಶ್ವೇಶ್ವರಯ್ಯ ತಾಂತ್ರಿಕ ವಿಶ್ವವಿದ್ಯಾಲಯ
("ವಿ ತಿ ಯು ಅಧಿನಿಯಮ ೧೯೯೪" ರ ಅಡಿಯಲ್ಲಿ ಕರ್ನಾಟಕ ಸರ್ಕಾರದಿಂದ ಸ್ಥಾಪಿತವಾದ ರಾಜ್ಯ ವಿಶ್ವವಿದ್ಯಾಲಯ)
VISVESVARAYA TECHNOLOGICAL UNIVERSITY
(State University of Government of Karnataka Established as per the VTU Act, 1994)
"JnanaSangama" Belagavi-590018, Karnataka, India

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

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

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

DATE: 25 AUG 2023

NOTIFICATION

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

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

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

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

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

Please Note:

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

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

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

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

Sd/-

REGISTRAR

To,

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

Copy to.

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

25/08/23

REGISTRAR

CRYPTOGRAPHY (Effective from the academic year 2018 -2019) SEMESTER – VII			
Course Code	**18CS744**	**CIE Marks**	40
Number of Contact Hours/Week	3:0:0	**SEE Marks**	60
Total Number of Contact Hours	40	**Exam Hours**	03
CREDITS –3			

Course Learning Objectives: This course (18CS744) will enable students to:

- Define cryptography and its principles
- Explain Cryptography algorithms
- Illustrate Public and Private key cryptography
- Explain Key management, distribution and ceritification
- Explain authentication protocols
- Tell about IPSec

Module – 1	**Contact Hours**
Classical Encryption Techniques Symmetric Cipher Model, Cryptography, Cryptanalysis and Brute-Force Attack, Substitution Techniques, Caesar Cipher, Monoalphabetic Cipher, Playfair Cipher, Hill Cipher, Polyalphabetic Cipher, One Time Pad. **Block Ciphers and the data encryption standard:** Traditional block Cipher structure, stream Ciphers and block Ciphers, Motivation for the feistel Cipher structure, the feistel Cipher, The data encryption standard, DES encryption, DES decryption, A DES example, results, the avalanche effect, the strength of DES, the use of 56-Bit Keys, the nature of the DES algorithm, timing attacks, Block cipher design principles, number of rounds, design of function F, key schedule algorithm **Textbook 1: Ch. 2.1,2.2, Ch. 3** **RBT: L1, L2**	08
Module – 2	
Public-Key Cryptography and RSA: Principles of public-key cryptosystems. Public-key cryptosystems. Applications for public-key cryptosystems, requirements for public-key cryptosystems. public-key cryptanalysis. The RSA algorithm, desription of the algorithm, computational aspects, the security of RSA. **Other Public-Key Cryptosystems:** Diffie-hellman key exchange, The algorithm, key exchange protocols, man in the middle attack,Elgamal Cryptographic systems **Textbook 1: Ch. 9, Ch. 10.1,10.2** **RBT: L1, L2**	08
Module – 3	
Elliptic curve arithmetic, abelian groups, elliptic curves over real numbers, elliptic curves over Zp, elliptic curves overGF(2m), Elliptic curve cryptography, Analog of Diffie-hellman key exchange, Elliptic curve encryption/ decryption, security of Elliptic curve cryptography, Pseudorandom number generation based on an asymmetric cipher, PRNG based on RSA. **Key Management and Distribution:** Symmetric key distribution using Symmetric encryption, A key distribution scenario, Hierarchical key control, session key lifetime, a transparent key control scheme, Decentralized key control, controlling key usage, Symmetric key distribution using asymmetric encryption, simple secret key distribution, secret key distribution with confidentiality and authentication, A hybrid scheme, distribution of public keys, public announcement of public keys, publicly available directory,public key	08

authority, public keys certificates. **Textbook 1: Ch. 10.3-10.5, Ch.14.1 to 14.3** **RBT: L1, L2**	
Module – 4	
X-509 certificates. Certificates, X-509 version 3, public key infrastructure .**User Authentication:** Remote user Authentication principles, Mutual Authentication, one wayAuthentication, remote user Authentication using Symmetric encryption, Mutual Authentication, one way Authentication, Kerberos, Motivation , Kerberos version 4, Kerberos version 5, Remote user Authentication using Asymmetric encryption, Mutual Authentication, one way Authentication. **Electronic Mail Security:** Pretty good privacy, notation, operational; description, S/MIME, RFC5322, Multipurpose internet mail extensions, S/MIME functionality, S/MIME messages, S/MIME certificate processing, enhanced security services, Domain keys identified mail, internet mail architecture, E-Mail threats, DKIM strategy, DKIM functional flow. **Textbook 1: Ch. 14.4, Ch. 15.1 to 15.4, Ch.19** **RBT: L1, L2**	08
Module – 5	
IP Security: IP Security overview, applications of IPsec, benefits of IPsec, Routing applications, IPsec documents, IPsec services, transport and tunnel modes, IP Security policy, Security associations, Security associations database, Security policy database, IP traffic processing, Encapsulating Security payload, ESP format, encryption and authentication algorithms, Padding, Anti replay service **Transport and tunnel modes**, combining security associations, authentication plus confidentiality, basic combinations of security associations, internet key exchange, key determinations protocol, header and payload formats, cryptographic suits. **Textbook 1: Ch. 20.1 to 20.3** **RBT: L1, L2**	08
Course outcomes: The students should be able to:	
• Define cryptography and its principles • Explain Cryptography algorithms • Illustrate Public and Private key cryptography • Explain Key management, distribution and ceritification • Explain authentication protocols • Tell about IPSec	
Question paper pattern: • The question paper will have ten questions. • There will be 2 questions from each module. • Each question will have questions covering all the topics under a module. • The students will have to answer 5 full questions, selecting one full question from each module.	
Text Books:	
1. William Stallings: Cryptography and Network Security, Pearson 6th edition.	
Reference Books:	
1. V K Pachghare: Cryptography and Information Security, PHI 2nd Edition.	

26/9/23

Professor & HOD,
Department of Computer Science & Engg
S.J.C. Institute of Technology
Chickballapur-562 101

VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI
Scheme of Teaching and Examination 2018 – 19
Choice Based Credit System (CBCS) AND Outcome Based Education (OBE)
(Effective from the academic year 2018 – 19)

VII SEMESTER

Sl. No	Course and Course code		Course Title	Teaching Department	Teaching Hours /Week			Examination				Credits
					Theory Lecture	Tutorial	Practical/ Drawing	Duration in hours	CIE Marks	SEE Marks	Total Marks	
					L	T	P					
1	PCC	18CS71	Artificial Intelligence and Machine Learning	CS / IS	4	--	--	03	40	60	100	4
2	PCC	18CS72	Big Data Analytics	CS / IS	4	--	--	03	40	60	100	4
3	PEC	18CS73X	Professional Elective – 2	CS / IS	3	--	--	03	40	60	100	3
4	PEC	18CS74X	Professional Elective – 3	CS / IS	3	--	--	03	40	60	100	3
5	OEC	18CS75X	Open Elective –B	CS / IS	3	--	--	03	40	60	100	3
6	PCC	18CSL76	Artificial Intelligence and Machine Learning Laboratory	CS / IS	--	--	2	03	40	60	100	2
7	Project	18CSP77	Project Work Phase – 1	CS / IS	--	--	2	--	100	--	100	1
8	INT	--	Internship	(If not completed during the vacation of VI and VII semesters, it has to be carried out during the intervening vacations of VII and VIII semesters								
				TOTAL	17	--	04	18	340	360	700	20

Note: PCC: Professional core, PEC: Professional Elective, OEC: Open Elective, INT: Internship.

Professional Elective - 2

Course code under 18CS73X	Course Title
18CS731	Software Architecture and Design Patterns
18CS732	High Performance Computing
18CS733	Advanced Computer Architecture
18CS734	User Interface Design

Professional Electives – 3

Course code under 18CS74X	Course Title
18CS741	Digital Image Processing
18CS742	Network management
18CS743	Natural Language Processing
18CS744	Cryptography
18CS745	Robotic Process Automation Design & Development

Open Elective –B (Not for CSE / ISE Programs)

18CS751	Introduction to Big Data Analytics
18CS752	Python Application Programming
18CS753	Introduction to Artificial Intelligence
18CS754	Introduction to Dot Net framework for Application Development

Students can select any one of the open electives offered by any Department (Please refer to the list of open electives under 18CS75X).
Selection of an open elective is not allowed provided,

- The candidate has studied the same course during the previous semesters of the programme.
- The syllabus content of open elective is similar to that of Departmental core courses or professional electives.
- A similar course, under any category, is prescribed in the higher semesters of the programme.

Registration to electives shall be documented under the guidance of Programme Coordinator/ Adviser/Mentor.

Project work: Based on the ability/abilities of the student/s and recommendations of the mentor, a single discipline or a multidisciplinary project can be assigned to an individual student or to a group having not more than 4 students. In extraordinary cases, like the funded projects requiring students from different disciplines, the project student strength can be 5 or 6.

CIE procedure for Project Work Phase - 1:

(i) Single discipline: The CIE marks shall be awarded by a committee consisting of the Head of the concerned Department and two senior faculty members of the Department, one of whom shall be the Guide. The CIE marks awarded for the project work phase -1, shall be based on the evaluation of the project work phase -1 Report (covering Literature Survey, Problem identification, Objectives and Methodology), project presentation skill and question and answer session in the ratio 50:25:25.The marks awarded for the Project report shall be the same for all the batch mates.

(ii) Interdisciplinary: Continuous Internal Evaluation shall be group wise at the college level with the participation of all guides of the college. Participation of external guide/s, if any, is desirable. The CIE marks awarded for the project work phase -1, shall be based on the evaluation of project work phase -1 Report, project presentation skill and question and answer session in the ratio 50:25:25.The marks awarded for the project report shall be the same for all the batch mates.

Internship: All the students admitted to III year of BE/B.Tech shall have to undergo mandatory internship of 4 weeks during the vacation of VI and VII semesters and /or VII and VIII semesters. A University examination shall be conducted during VIII semester and the prescribed credit shall be included in VIII semester. Internship shall be considered as a head of passing and shall be considered for the award of degree. Those, who do not takeup/complete the internship shall be declared fail and shall have to complete during subsequent University examination after satisfying the internship requirements

AICTE activity Points: In case students fail to earn the prescribed activity Points, Eighth semester Grade Card shall be issued only after earning the required activity Points. Students shall be admitted for the award of degree only after the release of the Eighth semester Grade Card.

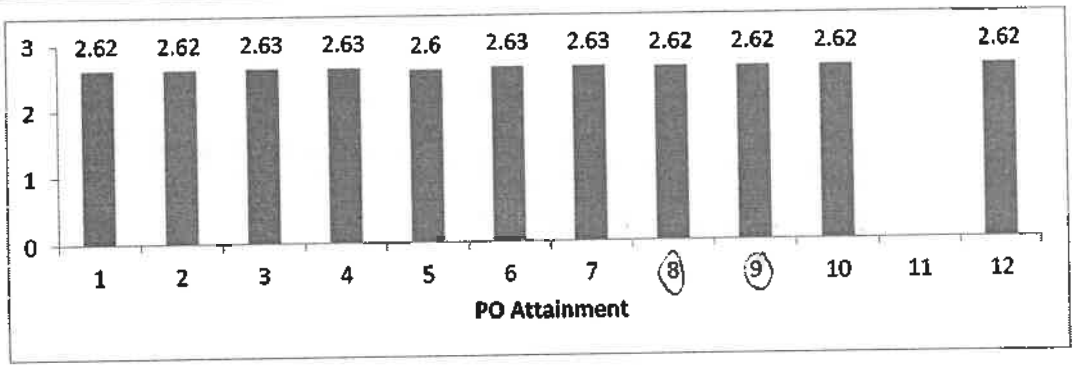
SJCIT/NBA/ CO-PO-PSO REPT/ 2023-24	S J C INSTITUTE OF TECHNOLOGY Chickballapur - 562 101 Department of Computer Science and Engineering						
Course Title	Cryptography					Course Code	C404
Subject Code	18CS744	Semester	7	Section	ABC	Emp.ID	1254
Faculty Name	Prof. Ajay N					No.students	151

Summary of CO attainments of Sub: 18CS744 Based on TYPE-1 Academic Year:2023-24

CO	CID_CO	CIE			SEE			CES			TOT_Attainment		
		S_AT	T_ST	ATN	S_AT	T_ST	ATN	S_AT	T_ST	ATN	ATN	%	Status
CO1	C404.1	145	151	2.9	113	151	2.2	120	121	3	2.6	88	YES
CO2	C404.2	150	151	3	113	151	2.2	113	121	2.8	2.7	89	YES
CO3	C404.3	151	151	3	113	151	2.2	56	121	1.4	2.5	84	YES
CO4	C404.4	151	151	3	113	151	2.2	120	121	3	2.7	90	YES
CO5	C404.5	146	151	2.9	113	151	2.2	120	121	3	2.6	88	YES

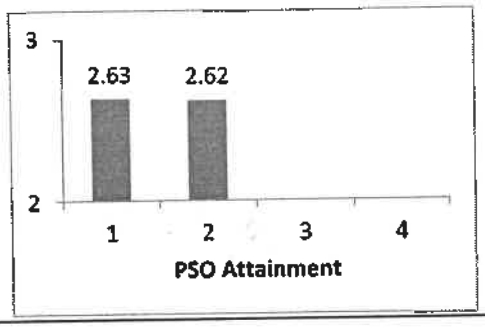
Summary of PO attainments of Sub: 18CS744 Based on TYPE-1 Academic Year:2023-24

PO Number	1	2	3	4	5	6	7	8	9	10	11	12
Direct ATNT(D)	2.62	2.62	2.63	2.63	2.65	2.63	2.63	2.62	2.62	2.62		2.62
Indirect ATNT(ID)	2.64	2.6	2.55	2.55	2.1	2.55	2.55	2.64	2.64	2.64		2.64
Total-ATNT	2.62	2.62	2.63	2.63	2.6	2.63	2.63	2.62	2.62	2.62		2.62
Total-ATNT (%)	87	87	88	88	87	88	88	87	87	87		87
Rel. to Mapping	13.1	11.3	7	3.5	1.7	3.5	3.5	8.7	4.4	4.4		8.7



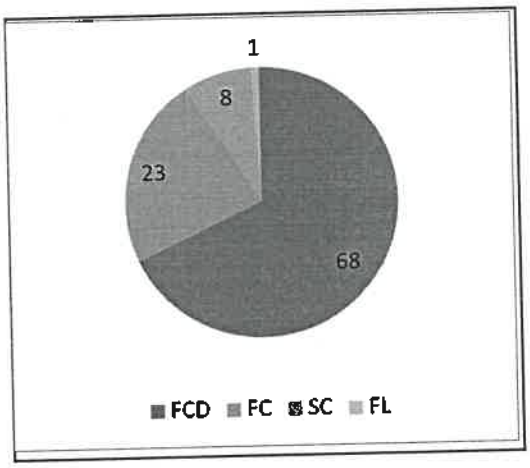
Summary of PSO attainments in Year:2023-24

PSO Number	1	2	3	4
Direct ATNT(D)	2.63	2.62		
Indirect ATNT(ID)	2.67	2.6		
Total-ATNT	2.63	2.62		
Total-ATNT (%)	88	87		
Rel. to Mapping	5.3	4.4		



SJCIT/NBA/ SEE-REPT/ 2023-24	S J C INSTITUTE OF TECHNOLOGY Chickballapur - 562 101 Department of Computer Science and Engineering						
Course Title	Cryptography					Course Code	C404
Subject Code	18CS744	Semester	7	Section	ABC	Emp.ID	1254
Faculty Name	Prof. Ajay N					No.students	151

Result Analysis of Subject Code -18CS744 - for the Academic year 2023-24



Result Analysis of Section: 7 - ABC				
No. Students	Pass	%	Fail	%
151	149	99	2	1

Class Analysis of Section: 7 - ABC			
No. Students	151	%	Grade Point
FCD	103	68	10,9,8
FC	34	23	7
SC	12	8	6,4
FL	2	1	0

Max. and Avg. Marks					
CIE	AVG	SEE	AVG	TOT	AVG
40	36	60	38	100	75

CO Attainment in SEE	
Sum_AT	378
T_students	151
Avg.ATNT	2.5
Sum_AT(=3)	113
AT(=3)%	75
Attainment	YES

ANALYSIS OF GRADE POINT AND GRADE LETTER							
Grade Letter	S	A	B	C	D	E	F
Grade Point	10	9	8	7	6	4	0
No.of Students	14	37	52	34	11	1	1
% of Students	9	25	34	23	7	1	1

CIE and SEE correlation Coefficient	0.48

Course Coordinator Remarks on Semester End Results for the Academic Year2023-24

Attainment Acheived

3/6/24
Signature of Course Coordinator

3/6/24.
Signature HOD/DAC

SJCIT/NBA/ SEE-REPT/ 2023-24	S J C INSTITUTE OF TECHNOLOGY Chickballapur - 562 101 Department of Computer Science and Engineering						
Course Title	Cryptography					Course Code	C404
Subject Code	18CS744	Semester	7	Section	ABC	Emp.ID	1254
Faculty Name	Prof. Ajay N					No.students	151

		Format for Entry of Semester End Examination Marks						40	60	100
Sl.	USN	NAME	CIE	SEE	TOT	Result	Class	ATNT	Grade	Rank
1	1SJ20CS001	ABHILASH N G	38	38	76	PASS	FCD	3	8	20
2	1SJ20CS002	ABHINAV KUMAR	38	22	60	PASS	FC		7	35
3	1SJ20CS007	ADITYA IYER	29	45	74	PASS	FCD	3	8	22
4	1SJ20CS008	ADITYA VIJAY N V	36	33	69	PASS	FC	3	7	27
5	1SJ20CS009	AKASH K N	28	35	63	PASS	FC	3	7	33
6	1SJ20CS011	ANANYA G R	40	44	84	PASS	FCD	3	9	12
7	1SJ20CS013	ANJAN KUMAR S	40	50	90	PASS	FCD	3	10	6
8	1SJ20CS016	ANUSHA S V	37	41	78	PASS	FCD	3	8	18
9	1SJ20CS017	ARFA THAREEN K	40	47	87	PASS	FCD	3	9	9
10	1SJ20CS018	ARJUN KASHYAP S	39	27	66	PASS	FC	1	7	30
11	1SJ20CS019	ARUNA P U	40	47	87	PASS	FCD	3	9	9
12	1SJ20CS020	ASHA M	40	38	78	PASS	FCD	3	8	18
13	1SJ20CS021	ASHWARYA	34	44	78	PASS	FCD	3	8	18
14	1SJ20CS022	BACHU GURU SAI KIRAN REDDY	30	39	69	PASS	FC	3	7	27
15	1SJ20CS024	BHANUPRASAD D R	40	39	79	PASS	FCD	3	8	17
16	1SJ20CS025	BHARGAVI D S	40	51	91	PASS	FCD	3	10	5
17	1SJ20CS026	BHAVANA S	40	41	81	PASS	FCD	3	9	15
18	1SJ20CS027	BINDHU SHREE G V	37	48	85	PASS	FCD	3	9	11
19	1SJ20CS029	CALLURU HARIHARA PALLAVI	40	41	81	PASS	FCD	3	9	15
20	1SJ20CS030	CHAITHRASHREE M	36	30	66	PASS	FC	2	7	30
21	1SJ20CS031	CHAITRA B D	40	48	88	PASS	FCD	3	9	8
22	1SJ20CS032	CHANDAN GOWDA N	38	27	65	PASS	FC	1	7	31
23	1SJ20CS035	CHANDU RAJ N	37	32	69	PASS	FC	2	7	27
24	1SJ20CS037	CHETHAN C V	39	37	76	PASS	FCD	3	8	20
25	1SJ20CS038	CHETHAN KUMAR D C	37	29	66	PASS	FC	1	7	30
26	1SJ20CS041	DAARIVEMULA SNEHA	36	38	74	PASS	FCD	3	8	22
27	1SJ20CS042	DEEKSHITHA B C	40	41	81	PASS	FCD	3	9	15
28	1SJ20CS043	DEEPAK U	27	15	42	FAIL				44
29	1SJ20CS044	DEEPTHI B L	31	33	64	PASS	FC	3	7	32
30	1SJ20CS045	DEERAJ C	34	33	67	PASS	FC	3	7	29
31	1SJ20CS046	DEVI PRASAD G M	39	59	98	PASS	FCD	3	10	1
32	1SJ20CS047	DHANUSH REDDY H M	39	40	79	PASS	FCD	3	8	17
33	1SJ20CS048	DUDDELA GANESH REDDY	35	36	71	PASS	FCD	3	8	25
34	1SJ20CS051	GANESH BABU BAKALE	36	33	69	PASS	FC	3	7	27
35	1SJ20CS052	GAURAV SINGH	32	30	62	PASS	FC	2	7	34
36	1SJ20CS053	HARSHAVARDHAN R	38	39	77	PASS	FCD	3	8	19
37	1SJ20CS054	HARSHITHA K	40	48	88	PASS	FCD	3	9	8
38	1SJ20CS056	HEMA H	36	37	73	PASS	FCD	3	8	23
39	1SJ20CS057	HEMA K A	40	38	78	PASS	FCD	3	8	18
40	1SJ20CS058	HEMALATHA A	32	32	64	PASS	FC	2	7	32

SJCIT/NBA/ SEE-REPT/ 2023-24	S J C INSTITUTE OF TECHNOLOGY Chickballapur - 562 101 Department of Computer Science and Engineering						
Course Title	Cryptography					Course Code	C404
Subject Code	18CS744	Semester	7	Section	ABC	Emp.ID	1254
Faculty Name	Prof. Ajay N					No.students	151

41	1SJ20CS060	HRUSHIKESH S	39	51	90	PASS	FCD	3	10	6
42	1SJ20CS061	ITHA SAI SREEHARI	37	33	70	PASS	FCD	3	8	26
43	1SJ20CS062	JITHENDRA G	32	26	58	PASS	SC		6	37
44	1SJ20CS063	K A AJAY	40	41	81	PASS	FCD	3	9	15
45	1SJ20CS065	K PRATHUSHA	40	42	82	PASS	FCD	3	9	14
46	1SJ20CS066	KALAVA VENKATA MIHEER KASY	33	38	71	PASS	FCD	3	8	25
47	1SJ20CS070	KIRAN K S	40	41	81	PASS	FCD	3	9	15
48	1SJ20CS071	KISHORE G S	39	36	75	PASS	FCD	3	8	21
49	1SJ20CS072	KOLLAMARAM KEERTHI REDDY	40	52	92	PASS	FCD	3	10	4
50	1SJ20CS074	LIKHITHASHREE D N	40	39	79	PASS	FCD	3	8	17
51	1SJ20CS075	M L SOUMIKA	40	54	94	PASS	FCD	3	10	3
52	1SJ20CS076	M N MADHU	26	31	57	PASS	SC	2	6	38
53	1SJ20CS077	MALLADI SRIKARA SAI ADITYA	37	37	74	PASS	FCD	3	8	22
54	1SJ20CS078	MALLIKASHREE N	35	49	84	PASS	FCD	3	9	12
55	1SJ20CS079	MANASA SINDHU P	40	41	81	PASS	FCD	3	9	15
56	1SJ20CS080	MANASWI M	35	23	58	PASS	SC		6	37
57	1SJ20CS081	MANISH KUMAR	39	39	78	PASS	FCD	3	8	18
58	1SJ20CS082	MANJUSRI N	33	32	65	PASS	FC	2	7	31
59	1SJ20CS083	MANUJA C R	40	45	85	PASS	FCD	3	9	11
60	1SJ20CS084	MARUTHI CHANDRA MOURYA A	22	13	35	FAIL			0	45
61	1SJ20CS085	MAYURI S	40	51	91	PASS	FCD	3	10	5
62	1SJ20CS087	MEGHANA R	35	37	72	PASS	FCD	3	8	24
63	1SJ20CS088	MEGHAVATHI M V	40	31	71	PASS	FCD	2	8	25
64	1SJ20CS089	MONIKA K	40	49	89	PASS	FCD	3	9	7
65	1SJ20CS091	MYTREYE H B	40	48	88	PASS	FCD	3	9	8
66	1SJ20CS092	NAGASHREE C R	40	50	90	PASS	FCD	3	10	6
67	1SJ20CS094	NAVYA L	40	37	77	PASS	FCD	3	8	19
68	1SJ20CS095	NEERAJ Y M	32	30	62	PASS	FC	2	7	34
69	1SJ20CS096	NEHA B S	40	40	80	PASS	FCD	3	9	16
70	1SJ20CS097	PEDARAPU CHENNAKESAVA RED	39	42	81	PASS	FCD	3	9	15
71	1SJ20CS098	NIKITHA S A	40	58	98	PASS	FCD	3	10	1
72	1SJ20CS099	NOOR FATHIMA M	40	35	75	PASS	FCD	3	8	21
73	1SJ21CS400	AMBARISH K C	32	23	55	PASS	SC		6	40
74	1SJ20CS176	CHIRAG S	40	41	81	PASS	FCD	3	9	15
75	1SJ21CS406	MONITH L	37	38	75	PASS	FCD	3	8	21
76	1SJ21CS416	VIJAY RAGAVAN N	38	27	65	PASS	FC	1	7	31
77	1SJ21CS415	VAISHNAVI N	39	34	73	PASS	FCD	3	8	23
78	1SJ21CS404	KISHOR T M	37	29	66	PASS	FC	1	7	30
79	1SJ21CS413	SHIVAKUMAR K	37	28	65	PASS	FC	1	7	31
80	1SJ20CS102	PRAJWAL MURALI S	34	43	77	PASS	FCD	3	8	19
81	1SJ20CS104	PRATHAM GOWDA H S	30	46	76	PASS	FCD	3	8	20
82	1SJ20CS105	PREETHAM H K	20	29	49	PASS	SC	1	6	41

SJCIT/NBA/ SEE-REPT/ 2023-24	S J C INSTITUTE OF TECHNOLOGY Chickballapur - 562 101 Department of Computer Science and Engineering							
Course Title	Cryptography					Course Code	C404	
Subject Code	18CS744	Semester	7	Section	ABC	Emp.ID	1254	
Faculty Name	Prof. Ajay N					No.students	151	

83	1SJ20CS106	PREETHI M	40	49	89	PASS	FCD	3	9	7
84	1SJ20CS108	RACHAMADUGU HARI DHEERAJ	33	29	62	PASS	FC	1	7	34
85	1SJ20CS110	RAJAN KUMAR GUPTA	40	36	76	PASS	FCD	3	8	20
86	1SJ20CS111	RAKSHITH D S	38	39	77	PASS	FCD	3	8	19
87	1SJ20CS113	RAKSHITHA K V	40	45	85	PASS	FCD	3	9	11
88	1SJ20CS114	RAKSHITHA R	40	38	78	PASS	FCD	3	8	18
89	1SJ20CS116	REVANTHRAJA M	40	56	96	PASS	FCD	3	10	2
90	1SJ20CS117	RISHIKESH L	36	39	75	PASS	FCD	3	8	21
91	1SJ20CS179	SHWETHA R	29	39	68	PASS	FC	3	7	28
92	1SJ20CS177	RAMYA H	37	26	63	PASS	FC		7	33
93	1SJ21CS401	BALA SUBRAMANYAM D P	32	30	62	PASS	FC	2	7	34
94	1SJ21CS403	Kavya S	29	35	64	PASS	FC	3	7	32
95	1SJ21CS402	JAYASUDHA	24	32	56	PASS	SC	2	6	39
96	1SJ20CS118	ROHAN M	34	42	76	PASS	FCD	3	8	20
97	1SJ20CS119	ROHAN S	24	34	58	PASS	SC	3	6	37
98	1SJ20CS120	ROOPASHREE K N	40	38	78	PASS	FCD	3	8	18
99	1SJ20CS121	S P PREETHI	38	43	81	PASS	FCD	3	9	15
100	1SJ20CS122	SAHANA SHREE N	40	26	66	PASS	FC		7	30
101	1SJ20CS123	SAI SUJAY K	31	32	63	PASS	FC	2	7	33
102	1SJ20CS124	SAI SUNAY K	28	39	67	PASS	FC	3	7	29
103	1SJ20CS125	SAI SUPREETH REDDY P	39	34	73	PASS	FCD	3	8	23
104	1SJ20CS126	SALLAUDDIN AYUB BEIG	39	47	86	PASS	FCD	3	9	10
105	1SJ20CS127	SANJANA K L	38	35	73	PASS	FCD	3	8	23
106	1SJ20CS128	SANJANA S	38	53	91	PASS	FCD	3	10	5
107	1SJ20CS130	SANKALANA C M	37	44	81	PASS	FCD	3	9	15
108	1SJ20CS131	SATHI GRASHMA ANISWA	40	38	78	PASS	FCD	3	8	18
109	1SJ20CS132	SATISH G	40	26	66	PASS	FC		7	30
110	1SJ20CS133	SHASHANK M J	34	44	78	PASS	FCD	3	8	18
111	1SJ20CS134	SHASHANK M N	39	35	74	PASS	FCD	3	8	22
112	1SJ20CS136	SHIRISHA N	39	50	89	PASS	FCD	3	9	7
113	1SJ20CS137	SHRAVYA D K	40	47	87	PASS	FCD	3	9	9
114	1SJ20CS138	SHREEKAR BHARADWAJ M N	32	40	72	PASS	FCD	3	8	24
115	1SJ20CS139	SHREYAS N	37	45	82	PASS	FCD	3	9	14
116	1SJ20CS140	SHWETHASHREE K V	37	41	78	PASS	FCD	3	8	18
117	1SJ20CS141	SKANDA KUMAR C S	35	27	62	PASS	FC	1	7	34
118	1SJ20CS142	SRUJAN V	36	34	70	PASS	FCD	3	8	26
119	1SJ20CS143	SUCHITHRA K S	40	39	79	PASS	FCD	3	8	17
120	1SJ20CS144	SUCHITRA N L	40	45	85	PASS	FCD	3	9	11
121	1SJ20CS145	SUDHARANI R	40	44	84	PASS	FCD	3	9	12
122	1SJ20CS146	SUHAS V	34	31	65	PASS	FC	2	7	31
123	1SJ20CS147	SUPRAJA B	40	27	67	PASS	FC	1	7	29
124	1SJ20CS148	SURAJ	35	39	74	PASS	FCD	3	8	22

SJCIT/NBA/ SEE-REPT/ 2023-24	S J C INSTITUTE OF TECHNOLOGY Chickballapur - 562 101 Department of Computer Science and Engineering							
Course Title	Cryptography						Course Code	C404
Subject Code	18CS744	Semester	7	Section	ABC		Emp.ID	1254
Faculty Name	Prof. Ajay N						No.students	151

125	1SJ20CS149	SURBHI KUMARI	30	42	72	PASS	FCD	3	8	24
126	1SJ20CS151	SWETHA D S	38	43	81	PASS	FCD	3	9	15
127	1SJ20CS152	TARUN K H	40	41	81	PASS	FCD	3	9	15
128	1SJ20CS153	TEJAS GOWDA H A	39	25	64	PASS	FC		7	32
129	1SJ20CS154	TEJAS V A	38	33	71	PASS	FCD	3	8	25
130	1SJ20CS155	THARUN REDDY K V	32	42	74	PASS	FCD	3	8	22
131	1SJ20CS156	USHA B S	39	44	83	PASS	FCD	3	9	13
132	1SJ20CS158	VADDE NANDINI	39	53	92	PASS	FCD	3	10	4
133	1SJ20CS159	VANDANA C K	40	45	85	PASS	FCD	3	9	11
134	1SJ20CS160	VANDANA R	40	38	78	PASS	FCD	3	8	18
135	1SJ20CS161	VANDANA S R	40	50	90	PASS	FCD	3	10	6
136	1SJ20CS162	VARALAKSHMI P S	39	50	89	PASS	FCD	3	9	7
137	1SJ20CS163	VARSHITHA R	40	45	85	PASS	FCD	3	9	11
138	1SJ20CS164	VARSHITHA V	40	51	91	PASS	FCD	3	10	5
139	1SJ20CS165	VENKATESH BABU G S	38	40	78	PASS	FCD	3	8	18
140	1SJ20CS168	VIJAYAKUMAR	28	37	65	PASS	FC	3	7	31
141	1SJ20CS169	VINUTHA C R	38	37	75	PASS	FCD	3	8	21
142	1SJ20CS170	VISHWANATH K	39	38	77	PASS	FCD	3	8	19
143	1SJ20CS171	VIVEK K S	27	32	59	PASS	SC	2	6	36
144	1SJ20CS172	Y HARIPRIYA	38	33	71	PASS	FCD	3	8	25
145	1SJ20CS173	YALLATURU PRANAY KUMAR RE	31	24	55	PASS	SC		6	40
146	1SJ20CS174	YASHASWINI K M	40	41	81	PASS	FCD	3	9	15
147	1SJ20CS175	ZEBA SULTHANA A	32	27	59	PASS	SC	1	6	36
148	1SJ20CS178	KOWSHIK R G	34	32	66	PASS	FC	2	7	30
149	1SJ21CS407	NAGARJUN K R	21	22	43	PASS	SC		4	43
150	1SJ21CS409	PAVAN KALYAN V R	27	21	48	PASS	SC		6	42
151	1SJ21CS414	SUHAS D P	35	41	76	PASS	FCD	3	8	20

..... *** END *** .....

|| Jai Sri Gurudev ||
Sri Adichunchanagiri Shikshana Trust ®

SJC INSTITUTE OF TECHNOLOGY

Chickballapur – 562 101

Estd: 1986

Department of Computer Science and Engineering
LESSON PLAN

SUBJECT TITLE	**CRYPTOGRAPHY**		
SUBJECT TYPE	**PROFESSIONAL ELECTIVE**		
SUBJECT CODE	**18CS744**		
ACADEMIC YEAR	**2023-2024 (ODD SEMESTER)**	**BATCH**	**2020-2024**
SCHEME	**CBCS scheme (Effective from the academic year 2018 -2019)**		
SEMESTER & SECTION	**VII & 'B & C'**		
IA MARKS	**40**	***EXAM MARKS***	**60**
NUMBER OF LECTURE HOURs/WEEK	**3**	***TOTAL NUMBER OF LECTURE HOURS***	**40**
FACULTY NAME	**Prof. Ajay N & Prof. Rashmi K A**	***NO. OF TIMES HANDLED***	**02**

COURSE LEARNING OBJECTIVES: This course will enable students to

1. Define cryptography and its principles
2. Explain Cryptography algorithms
3. Illustrate Public and Private Key cryptography
4. Explain Key management, distribution and certification
5. Explain authentication protocols
6. Tell about IPSec

Course Outcomes: At the end of this course, students are able to:

CO1	Comprehend basic cryptographic techniques and its principles.
CO2	Apply mathematical concepts for different cryptographic algorithms.
CO3	Analyze symmetric and asymmetric cryptographic algorithms.
CO4	Illustrate the application of user authentication algorithms.
CO5	Identify security issues in network, transport and application layers and outline appropriate security protocols.

CO-PO MATRIX

COURSE OUTCOMES	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	-	-	-	-	-	2	1	1	-	2	1	1
CO2	3	2	2	1	1	1	1	2	1	1	-	2	2	2
CO3	3	3	2	1	1	1	1	2	1	1	-	2	1	1
CO4	3	3	2	1	-	1	1	2	1	1	-	2	1	-
CO5	3	3	2	1	-	1	1	2	1	1	-	2	1	1

CO-PO MAPPING JUSTIFICATION

18CS744	CO1	PO1	3	Able to apply the knowledge acquired to classify the different cryptographic techniques.
		PO2	2	Understanding the cryptographic techniques helps the students to identify and formulate the problems based on the techniques.
		PO8	2	This knowledge helps us to use effective engineering practices such as testing, survey etc. before choosing the best algorithm
		PO9	1	Understand the cryptographic Function effectively as an individual, and as a member or leader in diverse teams.
		PO10	1	This knowledge helps to communicate our ideas and suggestion in a more effective manner to the community
		PO12	2	These concepts are fundamental to CS and can be used in research and other innovative ideas.
	CO2	PO1	3	Able to apply the knowledge acquired to classify the Mathematical concepts of different cryptographic techniques.
		PO2	2	Understanding the encryption techniques helps the students to identify and formulate the problems based on the techniques.
		PO3	2	The knowledge help in designing solutions and analysing its complexity.
		PO4	1	By studying the existing cryptographic algorithms students can conduc investigations of complex problems and provide valid conclusions.
		PO5	1	This knowledge helps in identifying the best tools needed to develop the algorithm
		PO6	1	Apply reasoning informed by the contextual knowledge to safety issues and the consequent responsibilities.
		PO7	1	Understand the impact of the cryptographic solutions in societal and environmental contexts, and demonstrate the knowledge and need for sustainable development.
		PO8	2	This knowledge helps us to use effective engineering practices such as testing , survey etc. before choosing the best algorithm
		PO9	1	Understand the cryptographic Function effectively as an individual, and as a member or leader in diverse teams.
		PO10	1	This knowledge helps to communicate our ideas and suggestion in a more effective manner to the community
		PO12	2	These concepts are fundamental to CS and can be used in research and other innovative ideas.
	CO3	PO1	3	Applies the knowledge of mathematics behind cryptographic technique, students can find solutions for engineering problem.
		PO2	3	Using the knowledge in basic mathematics students can analyze and formulate solutions for some problems
		PO3	2	The knowledge help in designing solutions and analyzing its complexity.
		PO4	1	By studying the existing cryptographic algorithms students can conduct investigations of complex problems and provide valid conclusions.
		PO5	1	This knowledge helps in identifying the best tools needed to develop the algorithm
		PO6	1	Apply reasoning informed by the contextual knowledge to safety issues and the consequent responsibilities.
		PO7	1	Understand the impact of the cryptographic solutions in societal and environmental contexts, and demonstrate the knowledge and need for sustainable development.
		PO8	2	Will be follow the ethics in security application like hacking.
		PO9	1	Understand the cryptographic algorithm effectively as an individual, and as a member or leader in diverse teams.
		PO10	1	This knowledge helps to communicate our ideas and suggestion in a more effective manner to the community.
		PO12	2	These concepts are fundamental to CS and can be used in research and other innovative ideas.
	CO4	PO1	3	Understanding different authentication schemes

		PO2	3	Different authentication schemes helps the students to identify and formulate the problems based on the techniques
		PO3	2	The knowledge help in designing solutions and analyzing its complexity
		PO4	1	By studying the existing authentication schemes students can conduct investigations of complex problems and provide valid conclusions.
		PO6	1	Apply reasoning informed by the contextual knowledge to safety issues and the consequent responsibilities.
		PO7	1	Understand the impact of the authentication schemes solutions in societal and environmental contexts, and demonstrate the knowledge and need for sustainable development.
		PO8	2	Will be follow the ethics in security application like hacking.
		PO9	1	Understand the authentication schemes effectively as an individual, and as a member or leader in diverse teams.
		PO10	1	This knowledge helps to communicate our ideas and suggestion in a more effective manner to the community.
		PO12	2	These concepts are fundamental to CS and can be used in research and other innovative ideas.
	CO5	PO1	3	Understanding various security issues over internet.
		PO2	3	Understanding various security issues helps the students to identify and formulate the problems based on the techniques.
		PO3	2	The knowledge help in designing solutions and analyzing its complexity.
		PO4	1	By studying the existing security issues students can conduct investigations of complex problems and provide valid conclusions.
		PO6	1	Apply reasoning informed by the contextual knowledge to safety issues and the consequent responsibilities.
		PO7	1	Understand the impact of the security scheme solutions in societal and environmental contexts, and demonstrate the knowledge and need for sustainable development.
		PO8	2	Will be follow the ethics in security application like hacking.
		PO9	1	Understand the security issues effectively as an individual, and as a member or leader in diverse teams.
		PO10	1	This knowledge helps to communicate our ideas and suggestion in a more effective manner to the community.
		PO12	2	These concepts are fundamental to CS and can be used in research and other innovative ideas.

CO-PSO MAPPING JUSTIFICATION

18CS744	CO1	PSO1	1	The graduates of the programme are able to analyze encryption method.
		PSO2	1	The graduates of the programme are able to use diverse knowledge of real time security attacks.
	CO2	PSO1	2	The graduates of the programme are able to analyze the cryptographic technique in the network.
		PSO2	2	Graduates will apply the knowledge of cryptography to analyze the solution.
	CO3	PSO1	1	The graduates of the programme are able to apply the knowledge of security mechanism.
		PSO2	1	Graduates will apply the learnt knowledge throughout their life for developing cryptography algorithm by following ethics.
	CO4	PSO1	1	The graduates of the programme are able to analyze authentication scheme.
	CO5	PSO1	1	Graduates will apply the knowledge acquired on various security applications over internet.
		PSO2	1	The graduates of the programme are able to use various security applications over internet

DELIVERY PLAN WITH DETAILS

MODULE – 1

Lecture #	Topic	Mode of Delivery (Please Tick √)				Date of Delivery	COs Covered
		1	2	3	4		
1	Vision/Mission/PO/CO, Introduction + Syllabus,	√	√			12/09/23	
2	Bridge class	√	√			12/09/23	
3	Classical Encryption Techniques Symmetric Cipher Model,	√	√			13/09/23	CO1
4	Cryptography, Cryptanalysis and Brute-Force Attack, Substitution Techniques,	√	√			15/09/23	CO1
5	Caesar Cipher, Monoalphabetic Cipher, Playfair Cipher,	√	√			19/09/23	CO1
6	Hill Cipher, Polyalphabetic Cipher, One Time Pad. Block Ciphers and the data encryption standard: Traditional block Cipher structure, stream Ciphers and block Ciphers,	√	√			20/09/23	CO1
7	Motivation for the feistel Cipher structure, the feistel Cipher,	√	√			22/09/23	CO1
8	The data encryption standard, DES encryption, DES decryption, A DES example, results, the avalanche effect,	√	√	√		23/09/23	CO1
9	the strength of DES, the use of 56-Bit Keys, the nature of the DES algorithm, timing attacks,	√	√	√		25/09/23	CO1
10	Block cipher design principles, number of rounds, design of function F, key schedule algorithm	√	√			26/09/23 27/09/23	CO1

Text Book: William Stallings: Cryptography and Network Security, Pearson 6th edition.
Chapters: Ch. 2.1,2.2, Ch. 3
RBT: L1, L2

Signatures		#HOURS	Allotted	Taken
	Faculty: 4/10/23		08	10
	HoD: 4/10/23			
Remarks	Executed.			

MODULE – 2

Lecture #	Topic	Mode of Delivery (Please Tick √)				Date of Delivery	COs Covered
		1	2	3	4		
1.	Public-Key Cryptography and RSA: Principles of public-key cryptosystems. Public-key cryptosystems.	√	√			03.10.23	CO2
2.	Applications for public-key cryptosystems,	√	√			09.10.23	CO2
3.	Requirements for public-key cryptosystems. Public-key cryptanalysis.	√	√			10.10.23	CO2
4.	The RSA algorithm, description of the algorithm,	√	√	√	√	11.10.23	CO2
5.	Computational aspects, the security of RSA.	√	√			16.10.23	CO2
6.	Other Public-Key Cryptosystems: Diffie-Hellman key exchange,	√	√			17.10.23	CO2

7.	The algorithm, key exchange protocols, man in the middle attack,	√	√			18.10.23	CO2
8.	Elgamal Cryptographic systems	√	√			27.10.23	CO2

Text Book: William Stallings: Cryptography and Network Security, Pearson 6th edition.
Chapters: Ch. 9, Ch. 10.1,10.2
RBT: L1, L2

Signatures	**Faculty:** 27.10.23	**#HOURS**	**Allotted**	**Taken**
	HoD: 27/10/23		08	08
Remarks	Executed.			

MODULE – 3

Lecture #	Topic	Mode of Delivery (Please Tick √)				Date of Delivery	COs Covered
		1	2	3	4		
1.	Elliptic curve arithmetic, abelian groups, elliptic curves over real numbers, elliptic curves over Zp, elliptic curves overGF(2m), Elliptic curve cryptography,	√	√			30.10.23	CO3
2.	Analog of Diffie-hellman key exchange, Elliptic curve encryption/ decryption, security of Elliptic curve cryptography,	√	√			31.10.23	CO3
3.	Pseudorandom number generation based on an asymmetric cipher, PRNG based on RSA.	√	√			08.11.23	CO3
4.	Key Management and Distribution: Symmetric key distribution using Symmetric encryption, A key distribution scenario,	√	√			18.11.23	CO3
5.	Hierarchical key control, session key lifetime, a transparent key control scheme,	√	√			20.11.23	CO3
6.	Decentralized key control, controlling key usage, Symmetric key distribution using asymmetric encryption,	√	√			21.11.23	CO3
7.	simple secret key distribution, secret key distribution with confidentiality and authentication,	√	√			22.11.23	CO3
8.	A hybrid scheme, distribution of public keys, public announcement of public keys, publicly available directory,public key	√	√			22.11.23	CO3

Text Book: William Stallings: Cryptography and Network Security, Pearson 6th edition.
Chapters: Ch. 10.3-10.5, Ch.14.1 to 14.3
RBT: L1, L2

Signatures	**Faculty:** 05.12.23	**#HOURS**	**Allotted**	**Taken**
	HoD: 5/12/23.		08	08
Remarks	Executed.			

MODULE – 4

Lecture #	Topic	Mode of Delivery (Please Tick √)	Date of Delivery	COs Covered

		1	2	3	4		
1.	X-509 certificates. Certificates, X-509 version 3, public key infrastructure.	√	√			27.11.23	CO4
2.	User Authentication: Remote user Authentication principles, Mutual Authentication, one way Authentication, remote user Authentication using Symmetric encryption.	√	√			28.11.23	CO4
3.	Mutual Authentication, one way Authentication, Kerberos, Motivation, Kerberos version 4, Kerberos version 5,	√	√			29.11.23	CO4
4.	Remote user Authentication using Asymmetric encryption, Mutual Authentication,	√	√			08.12.23	CO4
5.	One way Authentication. Electronic Mail Security: Pretty good privacy, notation, operational; description, S/MIME, RFC5322,	√	√			09.12.23	CO4
6.	Multipurpose internet mail extensions, S/MIME functionality, S/MIME messages, S/MIME certificate processing,	√	√			11.12.23	CO4
7.	enhanced security services, Domain keys identified mail, internet mail architecture,	√	√			12.12.23	CO4
8.	E-Mail threats, DKIM strategy, DKIM functional flow	√	√			13.12.23	CO4

Text Book: William Stallings: Cryptography and Network Security, Pearson 6th edition.
Chapters: Ch. 14.4, Ch. 15.1 to 15.4, Ch.19
RBT: L1, L2

Signatures	**Faculty:** 13/12/23	**#HOURS**	**Allotted**	**Taken**
	HoD: 14/12/23		08	08
Remarks	Executed.			

MODULE – 5

Lecture #	Topic	Mode of Delivery (Please Tick √) 1	2	3	4	Date of Delivery	COs Covered
1.	IP Security: IP Security overview, applications of IPsec, benefits of IPsec,	√	√			15.12.23	CO5
2.	Routing applications, IPsec documents, IPsec services, transport and tunnel modes, IP Security policy,	√	√			18.12.23	CO5
3.	Security associations, Security associations database, Security policy database, IP traffic processing,	√	√			19.12.23	CO5
4.	Encapsulating Security payload, ESP format, encryption and authentication algorithms, Padding, Anti replay service	√	√			22.12.23	CO5
5.	Transport and tunnel modes, combining security associations, authentication plus confidentiality,	√	√			23.12.23	CO5
6.	basic combinations of security associations, internet key exchange,	√	√			26.12.23	CO5

7.	key determinations protocol, header and payload formats,	√	√			27.12.23	CO5
8.	Cryptographic suits.	√	√			27.12.23	CO5

Text Book: William Stallings: Cryptography and Network Security, Pearson 6th edition.
Chapters: Ch. 20.1 to 20.3
RBT: L1, L2

Signatures	**Faculty:** 29.12.23	**#HOURS**	**Allotted**	**Taken**
	HoD: 1/1/24		08	07
Remarks	Executed.			

Text Books: 1. William Stallings: Cryptography and Network Security, Pearson 6th edition.
Reference Books: 1. V K Pachghare: Cryptography and Information Security, PHI 2nd Edition,

(Note: Mode of Delivery : 1:Black Board 2:PPT 3:Video 4:Demo/Hands-on)

INTERNAL/ASSIGNMENT/QUIZ SCHEDULE

TEST and QUIZ		COs and Portions Covered		ASSIGNMENT	
Test# and Quiz#	**DATE**	**CO**	**Modules**	**Assignment#**	**DATE**
T1 & Q1	06.11.23	CO1 & CO2	Module-1, Module-2	**A1**	24.11.23
T2 & Q2	05.12.23	CO2, CO3 & 4	Module-3, Module-4	**A2**	18.12.23
T3 & Q3	03.01.24	CO4, CO5	Module-5	**A3**	04.01.24

SUMMARY

Signatures With Date	**Faculty:**	**Total #HOURS**	**Allotted**	**Taken**
	HoD: 1/1/24		40	41
Remarks	Completed 100% Syllabus.			

ENCLOSURES

1. **Syllabus**
2. **CO Attainment**
3. **Gap Analysis**
4. **Special lectures/talks arranged if any**

Feedback by PAC

* Result Achieved 98.67%
* 100% Syllabus coverage
* Attained the all CO's
* Conducted the project Based learning to fill the Gaps

3/6/24 **Faculty**

3/6/24 **Course coordinator**

3/06 **PAC**

3/6/24 **HOD**

|| Jai Sri Gurudev ||
Sri Adichunchanagiri Shikshana Trust ®

Estd: 1986

SJC INSTITUTE OF TECHNOLOGY

Chickballapur – 562 101

Department of Computer Science & Engineering
ASSIGNMENT

SUBJECT TITLE	**Cryptography**		
SUBJECT TYPE	**ELECTIVE**		
SUBJECT CODE	**18CS744**		
ACADEMIC YEAR	**2023-24**	**BATCH**	**2020**
SCHEME	**2018**		
SEMESTER	**VII**		
FACULTY NAME and DESIGNATION	**Prof. Ajay N & Prof. Rashmi K A, Assistant Professor**		

Module -1

Q. No.	***Questions***	***Bloom's LL***	***COs***
1	Given the Caesar's cipher Build the plaintext from the Cipher text, DOLFHLPZRQGHUODQG	L3	CO1
2	Construct the bits number 1, 16, 33 and 48 at the output of the first round of the DES decryption, assuming that the cipher text block is composed of all ones and the external key is composed of all ones.	L3	CO1
3	Encrypt the message "we are all together" using a double transposition cipher with 4 rows and 4 columns. Using the row permutations (1,2,3,4) -> (2,4,1,3) and column permutation (1,2,3,4) -> (2,4,1,3)	L3	CO1
4	Prove that DES decryption is the inverse of DES encryption.	L4&L5	CO1
5	Write a program that can encrypt and decrypt using the general Caesar cipher.	L4&L5	CO1

Module -2

Q. No.	***Questions***	***Blooms LL***	***COs***
1	Compare Conventional and Public-Key Encryption.	L3	CO2
2	Apply RSA algorithm for the following, perform the encryption and decryption. i. p=3, q=11, e=7, M=5 ii. p=5, q=11, e=3, M=9	L3	CO2
3	Illustrate the Diffie-Hellman key exchange with an example.	L3	CO2

4	Analyze the countermeasures to be used against the timing attack.	L4&L5	CO2
5	User A and B use the Diffie-Hellman's key exchange technique with a common prime q=71 and primitive root of α=7. Solve the following: i. if user A has private key X_A=5, Solve Y_A ii. if user B has private key X_B=12, Solve Y_B	L4&L5	CO2

Module -3

Q. No.	Questions	Bloom's LL	COs
1	Experiment with an example, how ECC Diffie-Hellman key exchange done.	L3	CO3
2	Select an example, discuss elliptic curves over real numbers.	L3	CO3
3	Compare two families of elliptic curves used in cryptographic applications.	L3	CO3
4	For $E_{11}(1,7)$, consider the point G=(3,2). Compute the multiple of G from 2G through 13G.	L4&L5	CO3
5	Consider the elliptic curve $E_7(2,1)$; that is, the curve is defined by $y^2=x^3+2x+1$ with a modulus of p=7. Determine all of the points in $E_7(2,1)$.	L4&L5	CO3

Module -4

Q. No.	Questions	Bloom's LL	COs
1	Construct the NIST model for Electronic user authentication architecture model.	L3	CO4
2	Build functional modules and standardized protocols used between them in the Internet Mail architecture.	L3	CO4
3	Summarize the S/MIME services	L3	CO4
4	Suppose N different systems use the IBM cryptographic subsystem with host master keys KMH[i](i=1,2,…..N). Devise a method for communicating between systems without requiring the system to either share a common host master key or to divulge their individual host master keys.	L4&L5	CO4
5	Suppose that, in PCBC mode, blocks C_i and C_{i+1} are interchanged during transmission. Show that this affects only the decrypted blocks P_i and P_{i+1} but not subsequent blocks.	L4&L5	CO4

Module -5

Q. No.	Questions	Bloom's LL	COs
1	Construct the basic combinations of security associations with different cases.	L3	CO5
2	Make use of scope of ESP encryption and authentication, draw a diagram for Authentication Header.	L3	CO5
3	Write a note on applications of IPsec.	L3	CO5
4	Suppose that the current replay window spans from 120 to 530. a. If the next incoming authenticated packet has sequence number 105, what will the receiver do with the packet, and what will be the parameters of the window after that? b. If instead the next incoming authenticated packet has sequence	L4&L5	CO5

	number 440, what will the receiver do with the packet, and what will be the parameters of the window after that? c. If instead the next incoming authenticated packet has sequence number 540, what will the receiver do with the packet, and what will be the parameters of the window after that?		
5	End-to-end authentication and encryption are desired between two hosts. Develop the diagram that show each of the following. i. Transport adjacency with encryption applied before authentication. ii. A transport SA bundled inside a tunnel SA with encryption applied before authentication. iii. A transport SA bundled inside a tunnel SA with authentication applied before encryption.	L4&L5	CO5

||JAI SRI GURUDEV||

S.J.C. INSTITUTE OF TECHNOLOGY, CHICKBALLAPUR

Department of Computer Science & Engineering

QUIZ QUESTIONS

Sem: 7TH SEM **Sub Name:** CRYPTOGRAPHY [18CS744]

1. _____ is the science and art of transferring messages to make them secure and immune to attacks.
   A. CryptographyB. CryptoanalysisC. either (a) or (b)D. neither (a) or (b)

2. The _____ is the original message before transformation.
   A. ciphertext **B. plaintext** C. secret-testD. none of the above

3. The _____ is the message after transformation.
   A. ciphertext B. plaintext C. secret-testD. none of the above

4. A (n) _____ algorithm transforms plaintext to ciphertext
   A. encryption B. decryptionC. either (a) or (b)D. neither (a) or (b)

5. A (n) _____ algorithm transforms ciphertext to plaintext
   A. encryption **B. decryption**C. either (a) or (b)D. neither (a) or (b)

6. A combination of an encryption algorithm and decryption algorithm is called a _____.
   A cipher B. secret C. key D. none of these

7. The _____ number or a set of numbers on which the cipher operates.
   A cipher B. secret **C. key** D. none of these

8. In a(n) _____ cipher, the same key is used by both the sender and receiver.
   A. symmetric-key B. asymmetric-key C. either (a) or (b) D. neither (a) or (b)

9. In a(n) _____, the key is called the secret key.
   A. symmetric-key B. asymmetric-key C. either (a) or (b) D. neither (a) or (b)

10. In an asymmetric- key cipher, the receiver uses the _____ key.
    A. private B. public C. either (a) or (b) D. neither (a) or (b)

11. A modern cipher is usually a complex _____ cipher made of a combination of different simple ciphers.
    A. round B. circle **C. square** D. none of the above

12. DES is a(n) _____ method adopted by U.S. government
    A. symmetric-key B. asymmetric-key C. either (a) or (b) D. neither (a) or (b)

13. DES has initial and final permutation block and _____ rounds.
    A. 14 B. 15 **C. 16** D. none of the above

14. The DES function has _____ components
    A. 2 B. 3 **C. 4** D. 5

15. _____ DES was designed to increase the size of the DES key.
    A. Double **B. Triple** C. Quadruple D. none of the above

16. The man-in-the-middle attack can endanger the security of the Diffie-Hellman method if two parties are not
    A. **authenticated** B. joined C. submit D. separate

17. Session keys are transmitted after being encrypted by
A. make-shift keys B. temporary keys **C. master keys** D. section

18. Which of the following is not a type of symmetric-key cryptography technique?
A. Caesar cipher B. data encryption standard (des) **C. Diffie Hellman cipher**
D. Playfair cipher

19. How many bytes of the secret key is generated using Diffie-Hellman encryption/decryption scheme?
A. **256** B. 871 C. 1024 D. 962

20. The certificate message is required for any agreed-on key exchange method except
A. ephemeral Diffie – Hellman B. **anonymous Diffie- Hellman** C. fixed Diffie- Helmand.
D. RSA

21..Which of the following public key distribution systems is most secure?
a) **Public-Key Certificates** b) Public announcementsc) Publicly available directories
d) Public-Key authority

22. Communication between end systems is encrypted using a key, often known as
a) temporary key b) section key c) line key **d) session key**

23SSM stands for
a) Secure Security Module b) **Session Security Module** c) Service Session Module
d) Session Service Module

24. Which of these is not a type of session key?
a) PIN-encryption key b) File- encryption key **c) Session encryption key**
d) Data encryption key

25. PRNG stands for
a) Personal Random Number Generation b) **Pseudo Random Number Generation**
c) Primitive Number Generators d) Private Number Generators

26. What are man in the middle attacks?
a. Users are forced to use a second server which causes the attack
b. **Users are forced to divert to a fake site where the attack takes place**
c. Users are fooled by similar GUI and data is extracted from them. d. None of the mentioned

27. ElGamal encryption system is _____
A.symmetric key encryption algorithm B.asymmetric key encryption algorithm
C.not an encryption algorithm D.block cipher method

28. A digital signature needs a
A. Private-key system B. Shared-key system **C. Public-key system** D. All of them

29. A session symmetric key between two parties is used
A. **Only once** B. Twice C. Multiple times D. Conditions dependent

30. The certificate message is required for any agreed-on key exchange method except
_____

a) Ephemeral Diffie-Hellman b) **Anonymous Diffie-Hellman** c) Fixed Diffie-Hellman
d) RSA

31.The man-in-the-middle attack can endanger the security of the Diffie-Hellman method if two parties are not
A. **authenticated**B. joinedC. submitD. separate

32.Session keys are transmitted after being encrypted by
A. make-shift keysB. temporary keysC. **master keys**D. section

33.Which of the following is not a type of symmetric-key cryptography technique?
A. Caesar cipherB. data encryption standard (des)C. **Diffie Hellman cipher**D. Playfair cipher

34. How many bytes of the secret key is generated using Diffie-Hellman encryption/decryption scheme?
A. **256**B. 871C. 1024D. 962

35. The certificate message is required for any agreed-on key exchange method except
A. ephemeral Diffie– HellmanB. **anonymous Diffie- Hellman**C. fixed Diffie- Helmand.
D. RSA

36. Which of the following public key distribution systems is most secure?
a) **Public-Key Certificates**b) Public announcementsc) Publicly available directories
d) Public-Key authority

37. Communication between end systems is encrypted using a key, often known as
a) temporary keyb) section keyc) line keyd) **session key**

38. SSM stands for
a) Secure Security Moduleb) **Session Security Module**c) Service Session Module
d) Session Service Module

39. Which of these is not a type of session key?
a) PIN-encryption keyb) File- encryption keyc) **Session encryption key**
d) Data encryption key

40. PRNG stands for
a) Personal Random Number Generationb) **Pseudo Random Number Generation**
c) Primitive Number Generatorsd) Private Number Generators

41. What are man in the middle attacks?
a. Users are forced to use a second server which causes the attack
b. **Users are forced to divert to a fake site where the attack takes place**
c. Users are fooled by similar GUI and data is extracted from them.
d. None of the mentioned

42. ElGamal encryption system is _____
A.symmetric key encryption algorithm B.asymmetric key encryption algorithm
C.not an encryption algorithm D.block cipher method

43. A digital signature needs a
A. Private-key system B. Shared-key system C. **Public-key system** D. All of them

44. A session symmetric key between two parties is used
A. **Only once**B. Twice C. Multiple times D. Conditions dependent

45. The certificate message is required for any agreed-on key exchange method except _____

a) Ephemeral Diffie-Hellman b) **Anonymous Diffie-Hellman** c) Fixed Diffie-Hellman d) RSA

|| Jai Sri Gurudev ||
Sri Adichunchanagiri Shikshana Trust ®

Estd: 1986

SJC INSTITUTE OF TECHNOLOGY

Chickballapur – 562 101

Department of Computer Science and Engineering

QUESTION BANK

SUBJECT TITLE	**Cryptography**		
SUBJECT TYPE	**ELECTIVE**		
SUBJECT CODE	**18CS744**		
ACADEMIC YEAR	**2023-24**	**BATCH**	**2020**
SCHEME	**2018**		
SEMESTER	**VII**		
FACULTY NAME and DESIGNATION	**Prof. Ajay N & Prof. Rashmi K A, Assistant Professor**		

Module -1

Q. No.	*Questions*	*Bloom's LL*	*COs*
1	Name the Five essential ingredients of a symmetric cipher model.	L1	CO1
2	Why is the Caesar cipher substitution technique vulnerable to a brute force cryptanalysis?	L1	CO1
3	Which parameters and design choices determine the actual algorithm of a Feistal cipher?	L1	CO1
4	Using the letter encodings table, the following cipher text message was encrypted with a one-time pad: KITLKE Letter: e, h, i, k, l, r, s, t Binary: 000, 001, 010, 011, 100, 101, 110, 111 i. If the plaintext is "thrill", demonstrate the key? ii. If the plaintext is "tiller", demonstrate the key?	L2	CO1
5	Encrypt the message "we are all together" using a double transposition cipher with 4 rows and 4 columns. Using the row permutations (1,2,3,4) -> (2,4,1,3) and column permutation (1,2,3,4) -> (2,4,1,3)	L2	CO1
6	Explain the Avalanche effect.	L2	CO1
7	Given the Caesar's cipher Build the plaintext from the Cipher text, DOLFHLPZRQGHUODQG	L3	CO1

8	Construct the bits number 1, 16, 33 and 48 at the output of the first round of the DES decryption, assuming that the cipher text block is composed of all ones and the external key is composed of all ones.	L3	CO1
9	A ciphertext has been generated with an affine cipher. The most frequent letter of the ciphertext is "B", and the second most frequent letter of the ciphertext is "U". Break this code.	L4	CO1
10	Write a program that can encrypt and decrypt using the general Caesar cipher.	L5&L6	CO1

Module -2			
Q. No.	***Questions***	***Bloom's LL***	***COs***
1	List five possible approaches to attacking the RSA algorithm.	L1	CO2
2	What are the roles of the public and private keys?	L1	CO2
3	How can a probable-message attack be used for public-key cryptanalysis?	L1	CO2
4	Explain with an explain the Elgamal Cryptographic System	L2	CO2
5	Illustrate the Diffie-Hellman key exchange with a neat diagram.	L2	CO2
6	Summarize Man-in-the-Middle Attack with neat diagram	L2	CO2
7	Compare Conventional and Public-Key Encryption.	L3	CO2
8	Apply RSA algorithm for the following, perform the encryption and decryption. i. p=3, q=11, e=7, M=5 ii. p=5, q=11, e=3, M=9	L3	CO2
9	Analyze the countermeasures to be used against the timing attack.	L4	CO2
10	Alice and Bob use the Diffie-Hellman's key exchange technique with a common prime q=23 and primitive root of α=5. a. if Bob has public key Y_B=10, Find the Bob's private key Y_B? b. if Alice has a public key Y_A=8, Find the shared key K with Bob? c. Prove that 5 is a primitive root of 23.	L5&L6	CO2

Module -3			
Q. No.	***Questions***	***Bloom's LL***	***COs***
1	What are Abelian groups? Explain the geometric description of addition in Elliptic curves.	L1	CO3
2	What is the zero point of an elliptic curve?	L1	CO3

3	What is the sum of three points on an elliptic curve that lie on a straight line?	L1	CO3
4	Compare two families of elliptic curves used in cryptographic applications.	L2	CO3
5	Discuss the techniques involved in distribution of public keys.	L2	CO3
6	With the aid of diagram, describe the key distribution scenario.	L2	CO3
7	Experiment with an example, how ECC Diffie-Hellman key exchange done.	L3	CO3
8	Select an example, discuss elliptic curves over real numbers.	L3	CO3
9	For $E_{11}(1,7)$, consider the point G=(3,2). Compute the multiple of G from 2G through 13G.	L4	CO3
10	Consider the elliptic curve $E_7(2,1)$; that is, the curve is defined by $y^2=x^3+2x+1$ with a modulus of p=7. Determine all of the points in $E_7(2,1)$.	L5&L6	CO3

Module -4			
Q. No.	***Questions***	***Bloom's LL***	***COs***
1	What are the four general means of authentication?	L1	CO4
2	List few examples of replay attacks.	L1	CO4
3	What are the two types of protocol used for transferring email?	L1	CO4
4	Explain with neat diagram, the general format of X.509 certificate.	L2	CO4
5	Briefly describe the S/MIME message content types.	L2	CO4
6	Summarize the S/MIME services.	L2	CO4
7	Construct the NIST model for Electronic user authentication architecture model.	L3	CO4
8	Build functional modules and standardized protocols used between them in the Internet Mail architecture.	L3	CO4
9	Suppose N different systems use the IBM cryptographic subsystem with host master keys KMH[i](i=1,2,.....N). Devise a method for communicating between systems without requiring the system to either share a common host master key or to divulge their individual host master keys.	L4	CO4
10	Suppose that, in PCBC mode, blocks C_i and C_{i+1} are interchanged during transmission. Show that this affects only the decrypted blocks P_i and P_{i+1} but not subsequent blocks.	L5&L6	CO4

Module -5			
Q. No.	***Questions***	***Bloom's LL***	***COs***
1	List the benefits of IPsec.	L1	CO5
2	What services are provided by IPsec?	L1	CO5
3	Why does ESP include a padding field?	L1	CO5
4	Describe with neat diagram encapsulating security payload format.	L2	CO5
5	Discuss IPsec architecture with neat diagram	L2	CO5
6	Explain the applications of IPsec.	L2	CO5
7	Construct the basic combinations of security associations with different cases.	L3	CO5
8	Make use of scope of ESP encryption and authentication, draw a diagram for Authentication Header.	L3	CO5
9	Suppose that the current replay window spans from 120 to 530. a. If the next incoming authenticated packet has sequence number 105, what will the receiver do with the packet, and what will be the parameters of the window after that? b. If instead the next incoming authenticated packet has sequence number 440, what will the receiver do with the packet, and what will be the parameters of the window after that? c. If instead the next incoming authenticated packet has sequence number 540, what will the receiver do with the packet, and what will be the parameters of the window after that?	L4	CO5
10	End-to-end authentication and encryption are desired between two hosts. Develop the diagram that show each of the following. i. Transport adjacency with encryption applied before authentication. ii. A transport SA bundled inside a tunnel SA with encryption applied before authentication. iii. A transport SA bundled inside a tunnel SA with authentication applied before encryption.	L5&L6	CO5

||JAI SRI GURUDEV||

SJC INSTITUTE OF TECHNOLOGY, CHICKBALLAPUR

Department of Computer Science & Engineering

TUTORIAL-I

Sem: 7th SEM **Sub Name:** CRYPTOGRAPHY [18CS744] **Date:** 27.10.2023

1. Discuss the simplified model of conventional cryptosystem with neat diagram.
2. Why is the Caesar cipher substitution technique vulnerable to a brute force cryptanalysis?
3. Which parameters and design choices determine the actual algorithm of a Feistal cipher?
4. Using the letter encodings table, the following cipher text message was encrypted with a Cipher text: KITLKE

Letter	e	h	i	k	l	r	S	t
Binary	000	001	010	011	100	101	110	111

   i. If the plaintext is "thrill", demonstrate the key?
   ii. If the plaintext is "tiller", demonstrate the key?
5. Define Substitution and Transposition techniques. Explain the Avalanche effect.
6. Apply the Caesar's cipher method, build the plaintext from the Cipher text, DOLFHLPZRQGHUODQG
7. Prove that DES decryption is the inverse of DES encryption.
8. Apply the hill cipher technique, encryption and decryption the plaintext "PAYMOREMONEY" using the key K=[17 17 5, 21 18 21, 2 2 19].
9. Explain the playfair cipher and its rules for the following example.
   Keyword: MONARCHY plain text: Cryptography.
10. Explain the Feistel cipher encryption and decryption with neat diagram.
11. Describe the general depiction of DES encryption algorithm with neat diagram.
12. Apply the playfair cipher, do the encryption and decryption for the given plain text is "Hide the gold under the carpet" and keyword is "NESO ACADEMY".
13. List and explain the types of attacks on encrypted messages.
14. Describe the following with an example
    i. Vernam Cipher ii. Vigenere Cipher iii. One-Time Pad
15. Analyse the countermeasures to be used against the timing attack.
16. Describe RSA algorithm. Apply RSA algorithm for the following, perform the encryption and decryption.
    i. p=3, q=11, e=7, M=5
    ii. p=5, q=11, e=3, M=9
17. Compare Conventional and Public-Key Encryption
18. What are the roles of the public and private keys?
19. List and describe four possible approaches to attacking the RSA algorithm.
20. Explain Public-Key Cryptosystems.

27/10/23

Signature of the Faculty

Signature of the HoD 27/10/23

|| Jai Sri Gurudev ||
Sri Adichunchanagiri Shikshana Trust (R)

SJC INSTITUTE OF TECHNOLOGY

VTU Affiliated, AICTE Approved, Accredited by NAAC & NBA, Gold Rated by QS I-Gauge
Chickballapur - 562 101, Karnataka

Estd:1986

www.sjcit.ac.in

Department of Computer Science and Engineering

Date: 01.01.2024

Sem: VII **Sub: Cryptography (18CS744)**

Agenda:

1. Syllabus Coverage.
2. Demonstrate the Mini Projects.
3. Study Materials.
4. Assignment.
5. CO-PO Attainment

Sl #	Faculty Name	Section	Signature
1	Prof. Rashmi K A	A & B	Rashmi 1/1/24
2	Prof. Ajay N	B & C	01.01.24

Meeting Discussion:

1. Syllabus coverage A, B & C: 100%.
2. Demonstrate the Mini Project on 20.12.2023.
3. Share the study materials to students.
4. Deadline for submitting assignment-3 on or before 05.01.2024.
5. As per the PAC member's suggestion, we are conducted the activity to fill the gap.
6. Major Issue:
   a. Preetham H K (1SJ20CS105) secured test-1: 0(zero) marks, test-2 absent. He was not attended improvement test also. Even communicated to him, not responded.

01.01.24
Signature of the Course Co-ordinator

1/1/24.
Signature of the HoD
Professor & HOD,
Department of Computer Science & Engg.,
S.J.C. Institute of Technology,
Chickballapur-562 101

|| Jai Sri Gurudev ||
Sri Adichunchanagiri Shikshana Trust (R)

SJC INSTITUTE OF TECHNOLOGY

VTU Affiliated, AICTE Approved, Accredited by NAAC & NBA, Gold Rated by QS I-Gauge
Chickballapur - 562 101, Karnataka

Estd:1986

www.sjcit.ac.in

Department of Computer Science and Engineering

Date: 16.11.2023

Sem: VII **Sub: Cryptography (18CS744)**

Agenda:

1. Syllabus Coverage for Test 2.
2. Mini Projects.
3. Study Materials.
4. Assignment/Seminar.

Sl #	Faculty Name	Section	Signature
1	Prof. Rashmi K A	A & B	
2	Prof. Ajay N	B & C	16/11/23

Meeting Discussion:

1. Plan to Coverage the Syllabus for Test-2 is Module-3 and Module-4.
2. For Bright Students: Plan to form a group, assign topic and complete it on or before 3rd internals.
3. Share the study materials to students.
4. Deadline for submitting assignment-1 on or before 25.11.2023.
5. For Slow learners: Share previous year question paper with scheme and solution.

16/11/23
Signature of the Course Co-ordinator

16/11/23
Signature of the HoD
Professor & HOD,
Department of Computer Science & Engg.
S.J.C. Institute of Technology
Chickballapur-562 101

|| Jai Sri Gurudev ||
Sri Adichunchanagiri Shikshana Trust (R)

SJC INSTITUTE OF TECHNOLOGY

VTU Affiliated, AICTE Approved, Accredited by NAAC & NBA, Gold Rated by QS I-Gauge
Chickballapur - 562 101, Karnataka

Estd:1986

www.sjcit.ac.in

Department of Computer Science and Engineering

Date: 25.09.2023

Sub: Cryptography (18CS744)

Sem: VII

Agenda:

1. Lesson Plan
2. CO PO Mapping
3. Syllabus Coverage for Test 1

Sl #	Faculty Name	Section	Signature
1	Prof. Rashmi K A	A& B	25/9/23
2	Prof. Ajay N	B &C	25/9/23

Meeting Discussion:

1. Prepare the Lesson plan as per syllabus and Start the module-1, 2, 3, 4 and 5.
2. Discussed CO-PO mapping.
3. Plan to Coverage the Syllabus for Test-1 is Module-1 and Module-2.

T1 – Ajay N (BP, SS)
T2 & T3 – Rashmi KA (BP, SS)

25/9/23
Signature of the Course Co-ordinator

26/9/23.
Signature of the HoD

Professor & HOD,
Department of Computer Science & Engg.
S.J.C. Institute of Technology.
Chickballapur-562 101

||JAI SRI GURUDEV||

SJC INSTITUTE OF TECHNOLOGY, CHICKBALLAPUR

Department of Computer Science & Engineering

TUTORIAL-II

Sem: 7th SEM **Sub Name:** CRYPTOGRAPHY [18CS744] **Date:** 1.12.2023

1. Summarize the Elgamal Cryptographic System with an example.
2. Illustrate the Diffie-Hellman key exchange with a neat diagram.
3. Summarize Man-in-Middle Attack with neat diagram.
4. User A and B use the Diffie-Hellman's key exchange technique with a common prime q=71 and primitive root of α=7. Solve the following:
   i. if user A has private key X_A=5, Solve Y_A
   ii. if user B has private key X_B=12, Solve Y_B
   iii. Show that 7 is a primitive root of 71
5. What are Abelian groups? Explain geometric description of addition in Elliptic curves.
6. Discuss the techniques involved in distribution of keys.
7. With an aid of diagram, describe the key distribution scenario.
8. Examine two pseudorandom number generator (PRNG) designs based on pseudorandom functions.
9. Select an example, discuss elliptic curves over real numbers.
10. Explain automatic key distribution for connection oriented protocol.
11. Explain X.509 Certificates and formats.
12. Explain Public Key Infrastructure.
13. Explain Symmetric Key Distribution using Asymmetric Encryption.
14. Illustrate the ECC Diffie-Hellman key exchange with a neat diagram.

01/12/23

Signature of the Faculty

Signature of the HoD 1/12/23

Continuous Internal Evaluation (CIE) Question Paper- CBCS Scheme

|Jai Sri Gurudev||

SJC Institute of Technology

Department: Computer Science and Engineering

CIE: 1st Internal

Course Name & Code: Cryptography & 18CS744

Semester: VII

Section: A, B & C

Date: 06.11.2023

Time: 2.00 PM to 3.30 PM

Max Marks: 50+10(MCQ)

Instructions: Answer the following questions.

Q.NO.	Questions	Marks	CO	PO	RBTL
1	Discuss the simplified model of conventional cryptosystem with neat diagram.	10	CO1	PO1	L2
	OR				
2	List and Describe the types of attacks on encrypted messages.	10	CO1	PO1	L2
3	Apply the hill cipher techniques, encryption and decryption the plaintext "PAYMOREMONEY" using the key K=[17 17 5, 21 18 21, 2 2 19]	10	CO2	PO2	L3
	OR				
4	Write and Apply RSA algorithm for the following, perform the encryption and decryption. i. p=3, q=11, e=7, M=5 ii. p=5, q=11, e=3, M=9	10	CO2	PO2	L3
5	Compare Conventional and Public-Key Encryption and also write a note on Public-Key Cryptosystem: Authentication and Secrecy.	10	CO1	PO1	L2
	OR				
6	List four possible approaches to attacking the RSA algorithm and also Analyse the countermeasures to be used against the timing attack in the RSA algorithm.	10	CO1	PO2	L2
7	Describe the playfair cipher algorithm. Apply the playfair cipher technique, do the encryption and decryption for the given plain text is "instruments" and keyword is "MONARCHY".	10	CO2	PO2	L3
	OR				
8	Discuss the avalanche effect. Apply the playfair cipher technique, do the encryption and decryption for the given plain text is "Hide the gold under the carpet" and keyword is "NESO ACADEMY".	10	CO2	PO2	L3
9	Summarize the Feistel cipher encryption and decryption with neat diagram.	10	CO1	PO1	L2
	OR				
10	Illustrate the general depiction of DES encryption algorithm with neat diagram.	10	CO1	PO1	L2

CO1	Comprehend basic cryptographic techniques and its principles.
CO2	Apply mathematical concepts for different cryptographic algorithms.

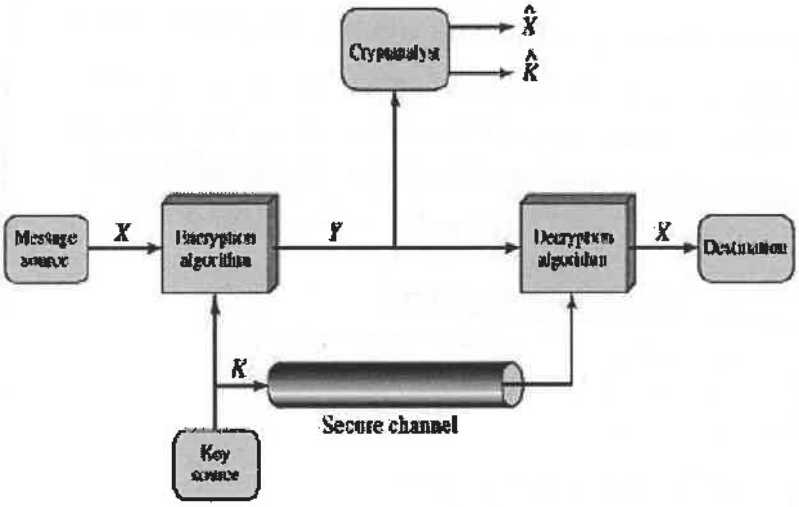
Multiple Choice Questions					
1	The _____ is the original message before transformation. A. ciphertext B. plaintext C. secret-test D. none of the above	1	CO1	PO1	L1
2	The _____ is the message after transformation. A. ciphertext B. plaintext C. secret-test D. none of the above	1	CO1	PO1	L1
3	_____ is the science and art of transferring messages to make them secure and immune to attacks. A. Cryptography B. Cryptoanalysis C. either (a) or (b) D. neither (a) or (b)	1	CO1	PO1	L1
4	In a(n) _____ cipher, the same key is used by both the sender and receiver. A. symmetric-key B. asymmetric-key C. either (a) or (b) D. neither (a) or (b)	1	CO1	PO1	L1
5	In an asymmetric- key cipher, the receiver uses the _____ key. A. private B. public C. either (a) or (b) D. neither (a) or (b)	1	CO1	PO1	L1
6	A modern cipher is usually a complex _____ cipher made of a combination of different simple ciphers. A. round B. circle C. square D. none of the above	1	CO1	PO1	L1
7	DES is a(n) _____ method adopted by U.S. government A. symmetric-key B. asymmetric-key C. either (a) or (b) D. neither (a) or (b)	1	CO2	PO1	L1
8	DES has initial and final permutation block and _____ rounds. A. 14 B. 15 C. 16 D. none of the above	1	CO2	PO1	L1
9	_____ DES was designed to increase the size of the DES key. A. Double B. Triple C. Quadruple D. none of the above	1	CO2	PO1	L1
10	Three security goals are A. Confidentiality, cryptography and non repudation B. Confidentiality, encryption and decryption C. Confidentiality, integrity and availability D. None of these	1	CO1	PO1	L1

31/10/23 Course Coordinator Signature	31/10/23 Reviewer Signature	31/10/23 HOD Signature

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Scheme & Solutions- TEST- I **Date: 06.11.2023**

Semester: VII (Professional Elective) **Subject Title:** Cryptography **Subject Code:** 18CS744

Question Number	Solution	Marks Allocated
1	Simplified model of conventional cryptosystem  	5 marks
	Explanation Carries	5 marks
2	**Type of Attack** / **Known to Cryptanalyst** Ciphertext only: • Encryption algorithm • Ciphertext Known plaintext: • Encryption algorithm • Ciphertext • One or more plaintext-ciphertext pairs formed with the secret key Chosen plaintext: • Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key Chosen ciphertext: • Encryption algorithm • Ciphertext • Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key Chosen text: • Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key	5 marks
	Explanation Carries	5 marks

Subject Code: 18CS744

Subject Title: Cryptography

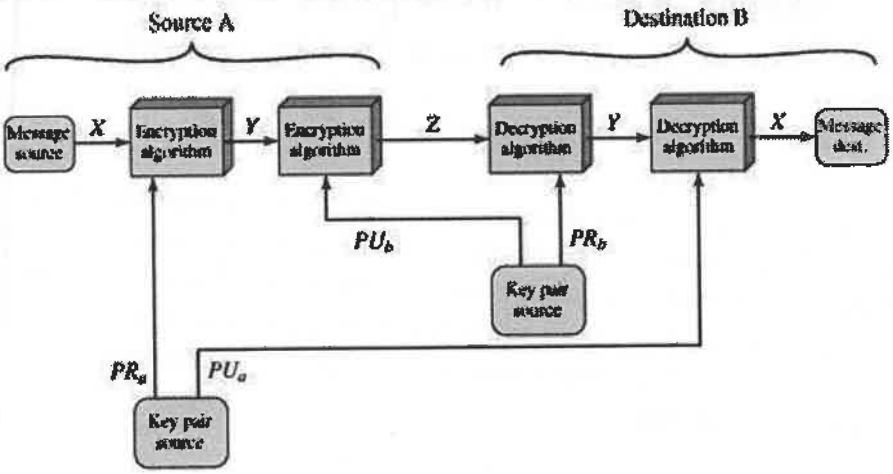
Question Number	Solution	Marks Allocated
3	Plaintext = paymore money $K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$ paymore money = (15, 0, 24, 12, 14, 17, 4, 12, 14, 13, 4, 24) (15, 0, 24) K = (303, 303, 531) mod 26 = (17, 17, 11) = RRL (12, 14, 17) K = (532, 490, 677) mod 26 = (12, 22, 1) = MWB (4, 12, 14) K = (348, 312, 538) mod 26 = (10, 0, 18) = KAS (13, 4, 24) K = (353, 341, 605) mod 26 = (15, 3, 7) = PDH Ciphertext = RRLMWBKASPDH $K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$ $P = CK^{-1} \bmod 26.$ (17, 17, 11) K^{-1} = (15, 0, 24) = pay (12, 22, 1) K^{-1} = (12, 14, 17) = mor (10, 0, 18) K^{-1} = (4, 12, 14) = emo (15, 3, 7) K^{-1} = (13, 4, 24) = ney.	5 marks 5 marks
4	**Key Generation.** 1. Select two prime numbers p & q. 2. Calculate n = p×q. 3. Calculate Φ(n) = (p-1)×(q-1) 4. Choose a value for e. such that 1 < e < Φ(n) & gcd(Φ(n),e) = 1 5. Calculate d = e^{-1} mod Φ(n) Let p = 3 , q= 11 n = p × q = 3 × 11 = 33 So n = 33. Φ(n) = (3-1)×(11-1)= 2×10 = 20. So Φ(n) = 20. So let e = 7 1<7<20 & gcd(7,20) = 1 d = e^{-1} mod Φ(n) i.e. ed = 1 mod Φ(n) ie, 7 × d = 1 mod 20 **7 × 3 mod 20** **so d = 3** So PU = {7,33} & PR = {3,33} Encryption: $C=M^e \bmod n = 5^7 \bmod 33 = 14$ Decryption: $M=C^d \bmod n = 14^3 \bmod 33 = 5$ ii .p=5, q=11, n=55, pi(n)=40, e=9, d=9 Encryption: C=49 Decryption: M=9	4 marks 3 marks 3 marks

Subject Title: Cryptography **Subject Code:** 18CS744

Question Number	Solution	Marks Allocated
5		

Conventional Encryption	Public-Key Encryption
Needed to Work: 1. The same algorithm with the same key is used for encryption and decryption. 2. The sender and receiver must share the algorithm and the key. *Needed for Security:* 1. The key must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.	*Needed to Work:* 1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption. 2. The sender and receiver must each have one of the matched pair of keys (not the same one). *Needed for Security:* 1. One of the two keys must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

5 marks



Public-Key Cryptosystem: Authentication and Secrecy

5 marks

Explanation

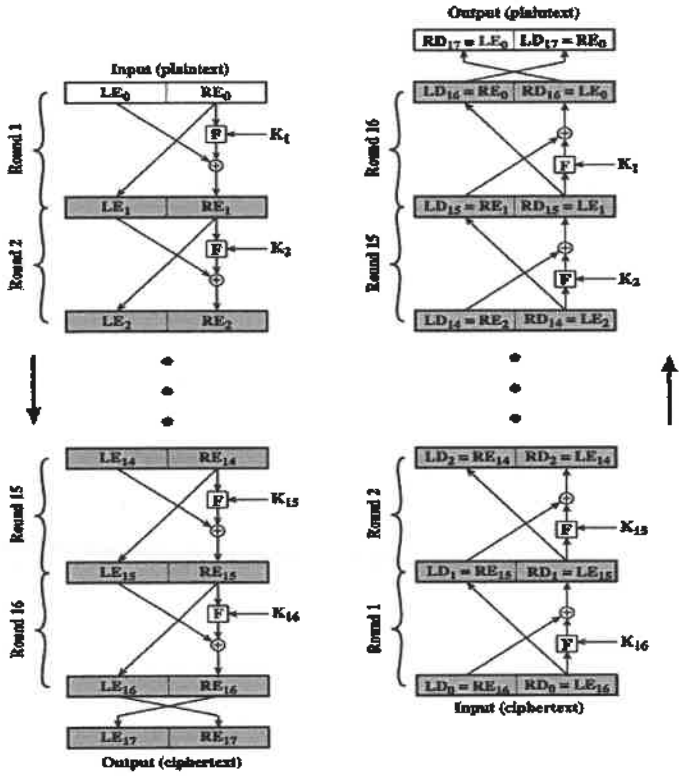
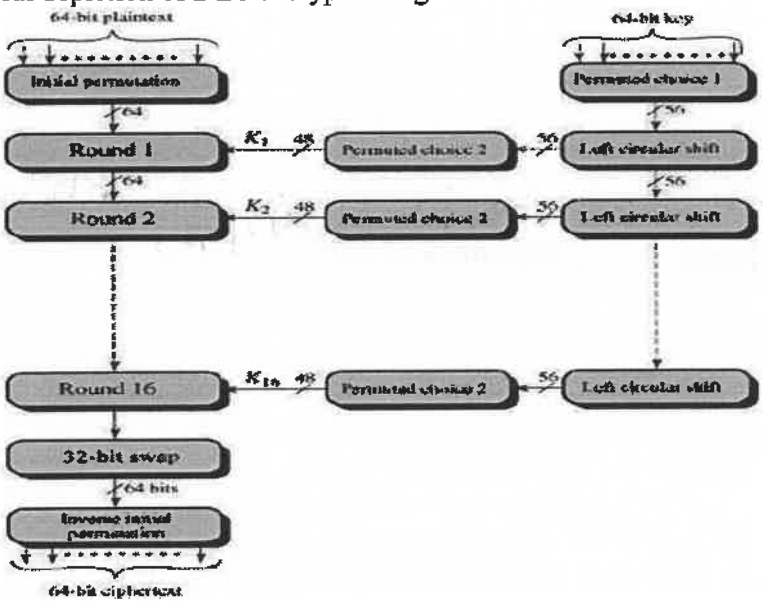
6	Four possible approaches to attacking the RSA algorithm 1. Brute force 2. Mathematical attacks 3.Timing attacks 4.Chosen ciphertext attacks	**4 marks**
	The countermeasures to be used against the timing attack in the RSA algorithm. i. **Constant exponentiation time** ii. **Random delay** iii. **Blinding**	**3 marks**
	Explanations	**3` marks**

Subject Code: 18CS744

Subject Title: Cryptography

Question Number	Solution	Marks Allocated
7	Explanation of playfair cipher with four rules to perform encryption.	3 marks
	plaintext - instruments in st ru me nt sz	
	Key = MONARCHY M O N A R C H Y B D E F G I/J K L P Q S T U V W X Z in → [i→g n→a] st → [s→t t→l] ru → [r→m u→z] me → [m→c e→l] nt → [n→r t→q] sz → [s→t z→x]	5 marks
	Ciphertext : gatlmzclrqtx	2 marks
8	**The Avalanche Effect** A desirable property of any encryption algorithm is that a small change in either the plaintext or the key should produce a significant change in the ciphertext. In particular, a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the ciphertext. If the change were small, this might provide a way to reduce the size of the plaintext or key space to be searched.	3 marks
	"Hide the gold under the carpet" Keyword : MESO ACADEMY M E S O A C D M Y B F G H I/J K L P Q R T U V W X Z	4 marks
	Encryption: Diagram : HI DE TH EQ OL DU ND ER TH EC AR PE TX Cipher : IK GD QK DP NR CV EC OP QK ND OT ND RI **Decryption:** works in reverse order	3 marks

Subject Title: Cryptography **Subject Code:** 18CS744

Question Number	Solution	Marks Allocated
9	**Feistel Encryption and Decryption (16 rounds)**  	5 marks
	Explanation Carries	5 marks
10	General depiction of DES encryption algorithm  	5 marks
	Explanation Carries	5 marks

Subject Code: 18CS744

Subject Title: Cryptography

Question Number	Solution	Marks Allocated
	MCQ 1.b 2.a 3.a 4.a 5.a 6.c 7.a 8.c 9.b 10.c	1*10=10 marks

31/1/23 **Signature of faculty**

Signature of Reviewer 2/1/23

Signature of HOD 2/1/23

Continuous Internal Evaluation (CIE) Question Paper- CBCS Scheme

|Jai Sri Gurudev||

SJC Institute of Technology

Department: Computer Science and Engineering

CIE: 2nd Internal

Course Name & Code: Cryptography & 18CS744

Semester: VII

Section: A, B & C

Date: 05.12.2023

Time: 2.00 PM to 3.30 PM

Max Marks: 50+10(MCQ)

Instructions: Answer the following questions.

Q.NO.	Questions	Marks	CO	PO	RBTL
1	Discuss the Elgamal Cryptographic System with a neat diagram.	10	CO2	PO1	L2
	OR				
2	List and Discuss the techniques involved in distribution of keys.	10	CO2	PO1	L2
3	Apply Diffie-Hellman's key exchange technique with a common prime q=71 and primitive root of α=7. Solve the following: i. if user A has private key X_A=5, Solve Y_A ii. if user B has private key X_B=12, Solve Y_B iii. Show that 7 is a primitive root of 71	10	CO2	PO1, 2,3	L3
	OR				
4	Illustrate the ECC Diffie-Hellman key exchange with a neat diagram	10	CO2	PO1, 2,3	L3
5	Explain Symmetric Key Distribution using Asymmetric Encryption	10	CO3	PO1	L2
	OR				
6	With an aid of diagram, describe the key distribution scenario	10	CO3	PO2	L2
7	What are Abelian groups? Explain geometric description of addition in Elliptic curves	10	CO2	PO2	L2
	OR				
8	Explain automatic key distribution for connection oriented protocol.	10	CO2	PO2	L2
9	Explain X.509 Certificates and formats.	10	CO4	PO1	L2
	OR				
10	Explain Public Key Infrastructure.	10	CO4	PO1	L2

CO2	Apply mathematical concepts for different cryptographic algorithms.
CO3	Analyze symmetric and asymmetric cryptographic algorithms.
CO4	Illustrate the application of user authentication algorithms.

Multiple Choice Questions					
1	The man-in-the-middle attack can endanger the security of the Diffie-Hellman method if two parties are not A. authenticated B. joined C. submit D. separate	1	CO2	PO1	L1
2	Session keys are transmitted after being encrypted by A. make-shift keys B. temporary keys C. master keys D. section	1	CO2	PO1	L1
3	Which of the following is not a type of symmetric-key cryptography technique? A. Caesar cipher B. Data Encryption Standard (DES) C. Diffie Hellman cipher D. Playfair cipher	1	CO2	PO1	L1
4	How many bytes of the secret key is generated using Diffie-Hellman encryption/decryption scheme? A. 256 B. 871 C. 1024 D. 962	1	CO2	PO1	L1
5	The certificate message is required for any agreed-on key exchange method except A. ephemeral Diffie – Hellman B. anonymous Diffie- Hellman C. fixed Diffie- Helmand. D. RSA	1	CO2	PO1	L1
6	Which of the following public key distribution systems is most secure? A) Public-Key Certificates B) Public announcements C) Publicly available directories D) Public-Key authority	1	CO3	PO1	L1
7	Communication between end systems is encrypted using a key, often known as A) temporary key B) section key C) line key D) session key	1	CO2	PO1	L1
8	What are man in the middle attacks? A. Users are forced to use a second server which causes the attack B. Users are forced to divert to a fake site where the attack takes place C. Users are fooled by similar GUI and data is extracted from them. D. None of the mentioned	1	CO2	PO1	L1
9	ElGamal encryption system is _____ A. symmetric key encryption algorithm B. asymmetric key encryption algorithm C. not an encryption algorithm D. block cipher method	1	CO3	PO1	L1
10	A digital signature needs a A. Private-key system B. Shared-key system C. Public-key system D. All of them	1	CO3	PO1	L1

01/12/23 Course Coordinator Signature	01/12/2023 Reviewer Signature	HOD Signature

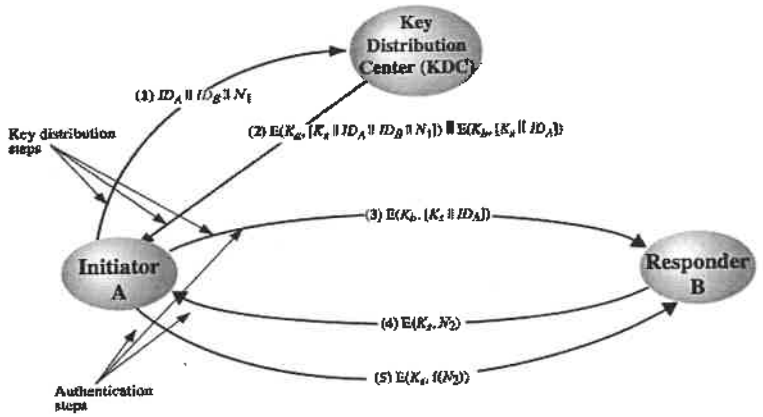
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Scheme & Solutions- TEST- II **Date: 05.12.2023**

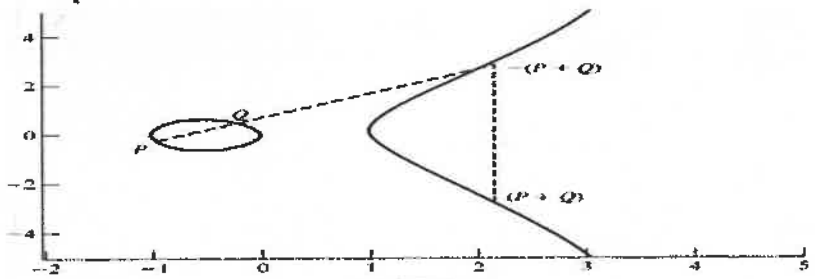
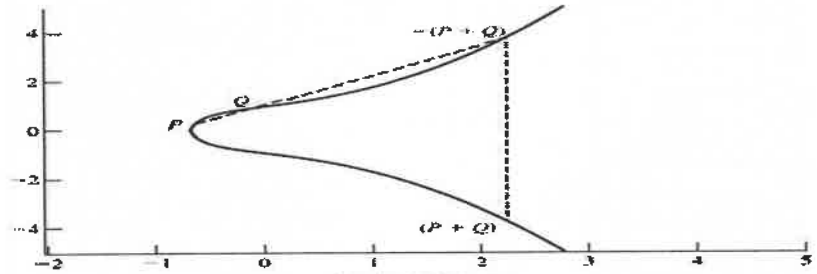
Semester: VII (Professional Elective) **Subject Title:** Cryptography **Subject Code:** 18CS744

Question Number	Solution	Marks Allocated
1	**The Elgamal Cryptography** **Global Public Elements** q — prime number α — $\alpha < q$ and α is a primitive root of q **Key Generation by Alice** Select private X_A — $X_A < q - 1$ Calculate Y_A — $Y_A = \alpha^{X_A} \bmod q$ Public key — $\{q, \alpha, Y_A\}$ Private key — X_A **Encryption by Bob with Alice's Public Key** Plaintext: — $M < q$ Select random integer k — $k < q$ Calculate K — $K = (Y_A)^k \bmod q$ Calculate C_1 — $C_1 = \alpha^k \bmod q$ Calculate C_2 — $C_2 = KM \bmod q$ Ciphertext: — (C_1, C_2) **Decryption by Alice with Alice's Private Key** Ciphertext: — (C_1, C_2) Calculate K — $K = (C_1)^{X_A} \bmod q$ Plaintext: — $M = (C_2 K^{-1}) \bmod q$	5 marks
	Explanation:	3 marks
	Example:	2 marks
2	**Distribution of Public Keys** ➢ can be considered as using one of: ● public announcement ● publicly available directory ● public-key authority ● public-key certificates	4 marks
	explanation for each one	6 marks
3	$\alpha=7$, $q=71$, $X_A=5$, $X_B=12$ i. $Y_A=\alpha^{X_A} \bmod q$ $= 7^5 \bmod 71$ $=51$ ii. $Y_B= \alpha^{X_B} \bmod q$ $= 7^{12} \bmod 71$ $=4$ $K=Y_B^{X_A} \bmod q$ $=4^5 \bmod 71$ $= 30$ iii. Show that 7 is a primitive root of 71	4 marks 2 marks
		4 marks

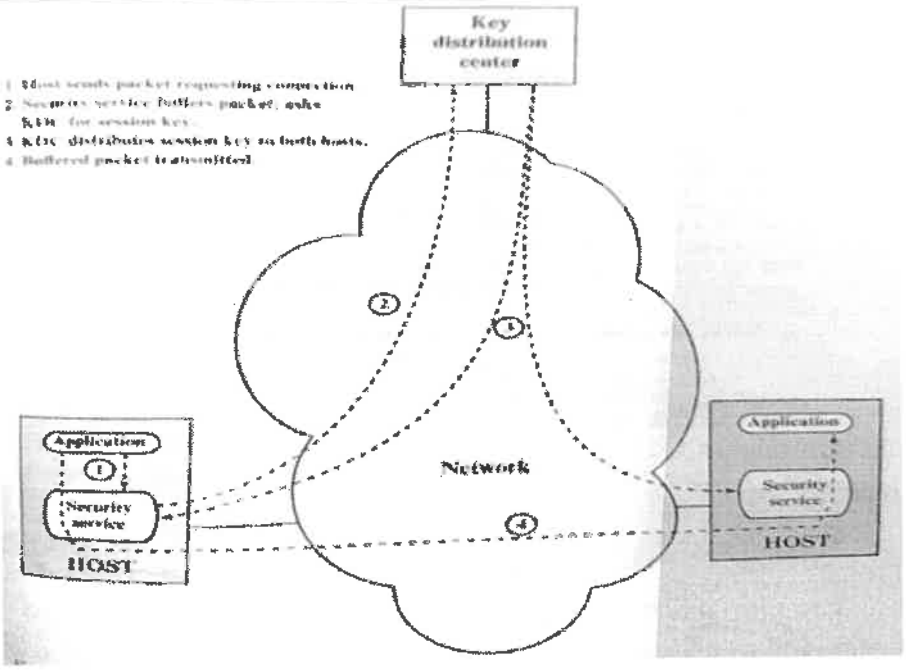
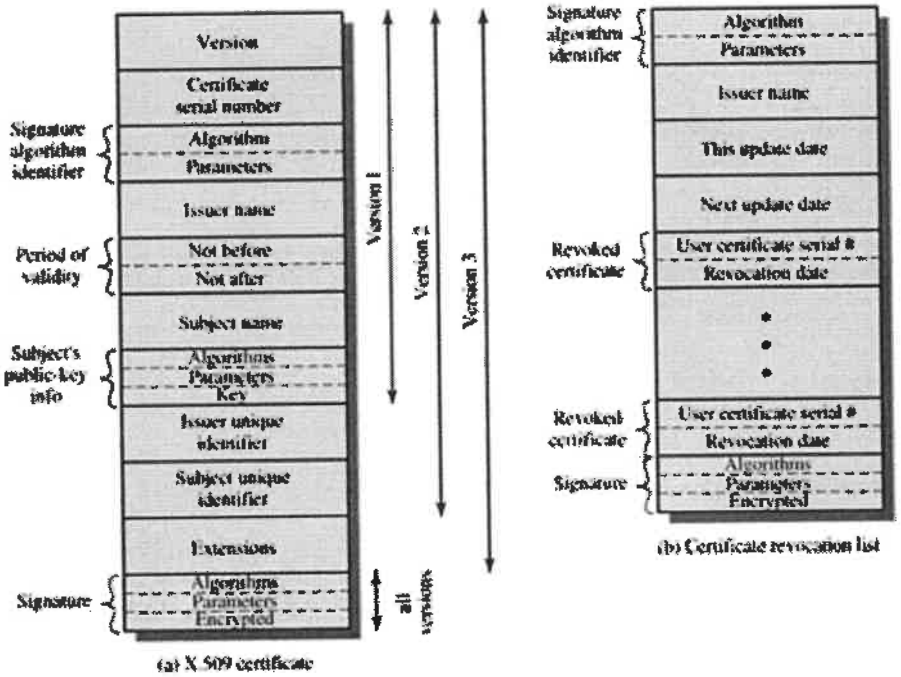
Subject Title: Cryptography **Subject Code:** 18CS744

Question Number	Solution	Marks Allocated
4	**Diffie Hellman key exchange** **Global Public Elements** q — prime number α — $\alpha < q$ and α a primitive root of q **User A Key Generation** Select private X_A — $X_A < q$ Calculate public Y_A — $Y_A = \alpha^{X_A} \bmod q$ **User B Key Generation** Select private X_B — $X_B < q$ Calculate public Y_B — $Y_B = \alpha^{X_B} \bmod q$ **Calculation of Secret Key by User A** $K = (Y_B)^{X_A} \bmod q$ **Calculation of Secret Key by User B** $K = (Y_A)^{X_B} \bmod q$	**5 marks**
	Explanation:	**3 marks**
	Example:	**2 marks**
5	**Symmetric Key Distribution using asymmetric encryption** i. Simple Secret Key Distribution ii. Secret Key Distribution with Confidentiality and Authentication iii. Hybrid Key Distribution	**3 marks**
	Explanations	**7 marks**
6		**5 marks**
	Explanation	**5 marks**

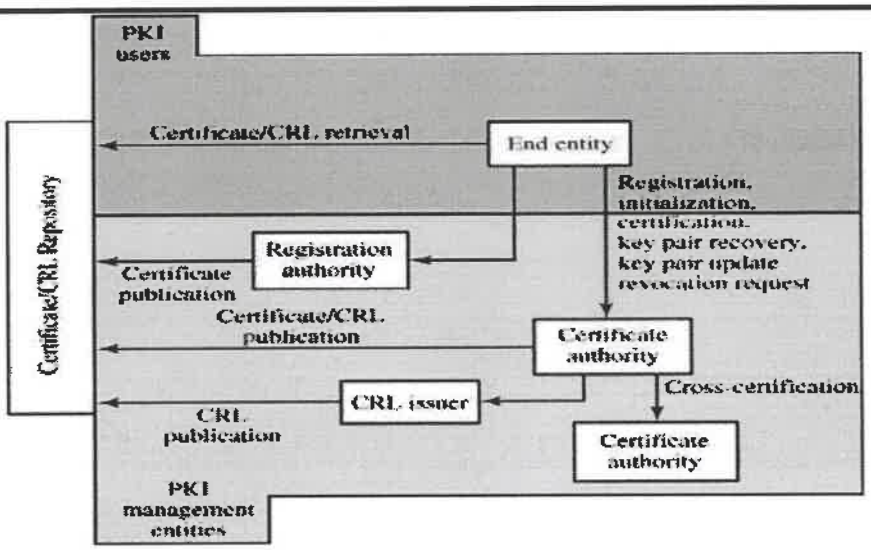
Subject Title: Cryptography **Subject Code:** 18CS744

Question Number	Solution	Marks Allocated
7	Elliptic curves are not ellipses. They are so named because they are described by cubic equations, similar to those used for calculating the circumference of an ellipse. In general, cubic equations for elliptic curves take the form $$y^2 + axy + by = x^3 + cx^2 + dx + e$$ where a, b, c, d, and e are real numbers and x and y take on values in the real numbers. For our purpose, it is sufficient to limit ourselves to equations of the form. $$y^2 = x^3 + ax + b$$ To plot such a curve, we need to compute $$y = \sqrt{x^3 + ax + b}$$ For given values of a and b, the plot consists of positive and negative values of y for each value of x. Thus each curve is symmetric about $y = 0$ **Example:**  (a) $y^2 = x^3 - x$  (b) $y^2 = x^3 + x + 1$	2 marks 2 marks 2 marks 2 marks 2 marks

Subject Title: Cryptography **Subject Code:** 18CS744

Question Number	Solution	Marks Allocated
8		5 marks
	Explanation	5 marks
9	 (a) X.509 certificate (b) Certificate revocation list	6 marks
	Explanation	5 marks

Subject Title: Cryptography **Subject Code:** 18CS744

Question Number	Solution	Marks Allocated
10		5 marks
	Explanation	5 marks
	Multiple Choice Questions **1.a** **2.c** **3.c** **4.b** **5.a** **6.d** **7.b** **8.c** **9.b** **10.b**	1*10=10 marks

05/12/23 **Signature of faculty** **Signature of Reviewer** 14/12/23 **Signature of HOD** 14/12/23

Continuous Internal Evaluation (CIE) Question Paper- CBCS Scheme

|Jai Sri Gurudev||

SJC Institute of Technology

Department: Computer Science and Engineering

CIE: 3rd Internal

Course Name & Code: Cryptography & 18CS744

Semester: VII **Section:** A, B & C

Date: 03.1.2024 **Time:** 2.00 PM to 3.30 PM **Max Marks:** 50

Instructions: Answer the following questions.

Q.NO.	Questions	Marks	CO	PO	RBTL
1	Infer the IP security applications and benefits with the help of IP security scenario.	10	CO5	PO2	L3
	OR				
2	Infer Kerberos Version 4 and 5.	10	CO5	PO2	L3
3	Interpret Remote User Authentication Principles	10	CO4	PO1	L3
	OR				
4	Demonstrate different combinations of security associations with cases.	10	CO4	PO1	L3
5	Infer transport-mode versus tunnel-mode encryption.	10	CO5	PO1	L3
	OR				
6	Discuss Pretty Good Privacy mail security protocol.	10	CO5	PO1	L2
7	Discuss the Internet key exchange (IKE) key determination features.	10	CO5	PO1	L2
	OR				
8	Discuss the S/MIME message content types.	10	CO5	PO1	L2
9	Outline with neat diagram encapsulating security payload format.	10	CO5	PO1	L2
	OR				
10	What services are provided by IPsec? List the benefits of IPsec	10	CO5	PO1	L2

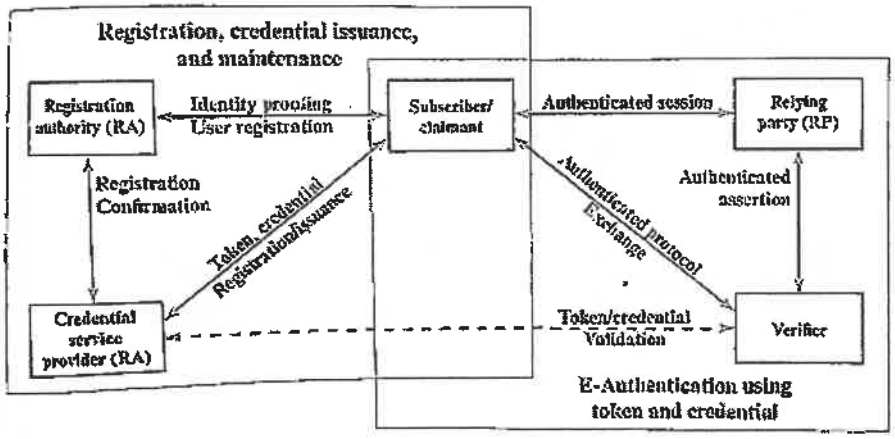
CO4	**Illustrate the application of user authentication algorithms.**
CO5	**Identify security issues in network, transport and application layers and outline appropriate security protocols.**

01.01.2024 **Course Coordinator Signature**	01/01/2024 **Reviewer Signature**	1/1/24 **`HOD Signature**

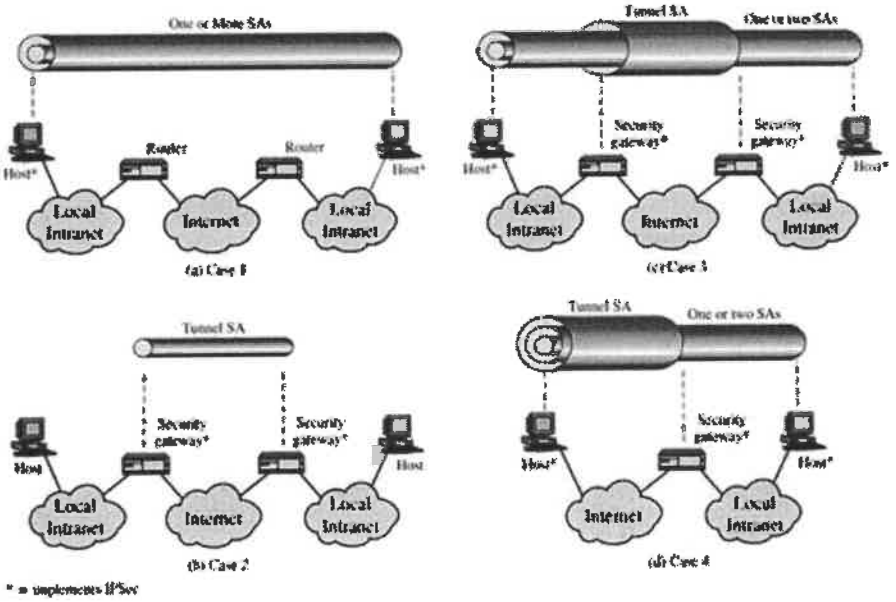
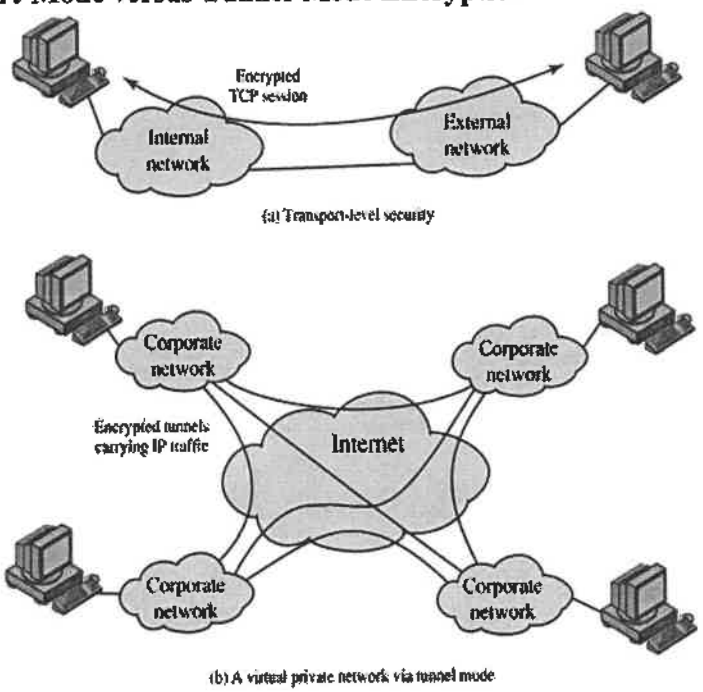
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Scheme & Solutions- TEST- III **Date: 03.01.2024**

Semester: VII (Professional Elective) **Subject Title:** Cryptography **Subject Code:** 18CS744

Question Number	Solution	Marks Allocated
1	**Applications of IPSec** • Secure branch office connectivity over the Internet. • Secure remote access over the Internet. • Establishing extranet and intranet connectivity with partners. • Enhancing electronic commerce security.	**4 marks**
	Explanation carries	**2 marks**
	Benefits • IPSec in a firewall is resistant to bypass • IPSec is below the transport layer (TCP, UDP) and so is transparent to applications • IPSec can be transparent to end users • IPSec can provide security for individual users if needed	**4 marks**
2	**Kerberos Versions 4 and 5** 1. Encryption system dependence 2. Internet protocol dependence 3. Message byte ordering 4. Ticket lifetime 5. Authentication forwarding 6. Inter realm authentication 7. Double encryption 8. PCBC encryption 9. Session keys 10. Password attacks Answer any five	**5*2=10 marks**
3		**5 marks**
	Explanation	**5 marks**

Subject Title: Cryptography **Subject Code:** 18CS744

Question Number	Solution	Marks Allocated
4	**Combinations of security associations with cases.**  	4 marks
	Explanation Carries	6 marks
5	**Transport-Mode versus Tunnel-Mode Encryption**  	4 marks
	Explanation Carries	6 marks

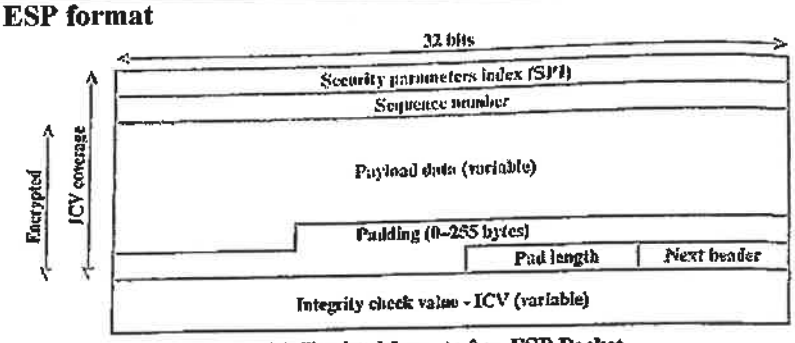
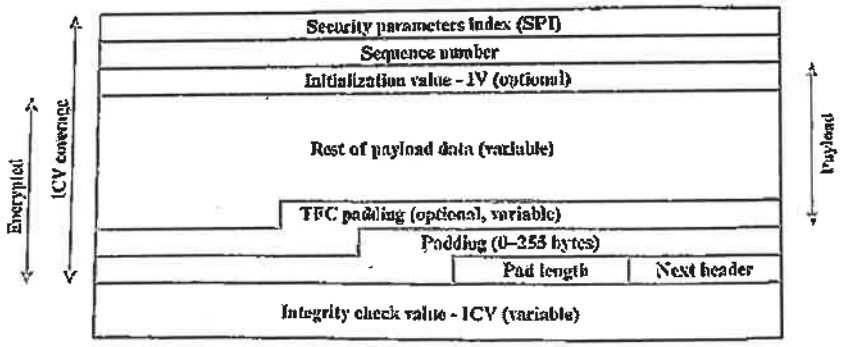
Subject Title: Cryptography **Subject Code:** 18CS744

Question Number	Solution	Marks Allocated
6	PGP has grown explosively and is now widely used. A number of reasons can be cited for this growth: 1. It is available free worldwide in versions that run on a variety of platforms, including Windows, UNIX, Macintosh, and many more. In addition, the commercial version satisfies users who want a product that comes with vendor support. 2. It is based on algorithms that have survived extensive public review and are considered extremely secure. Specifically, the package includes RSA, DSS, and Diffie-Hellman for public-key encryption; CAST-128, IDEA, and 3DES for symmetric encryption; and SHA-1 for hash coding. 3. It has a wide range of applicability, from corporations that wish to select and enforce a standardized scheme for encrypting files and messages to individuals who wish to communicate securely with others worldwide over the Internet and other networks. 4. It was not developed by, nor is it controlled by, any governmental or standards organization. For those with an instinctive distrust of "the establishment," this makes PGP attractive. 5. PGP is now on an Internet standards track (RFC 3156). Nevertheless, PGP still has an aura of an antiestablishment endeavor.	5 marks
	Notation	2 marks
	Description	3 marks
7	**Features of IKE key determination** The IKE key determination algorithm is characterized by five important features: 1. It employs a mechanism known as cookies to thwart clogging attacks. 2. It enables the two parties to negotiate a *group*; this, in essence, specifies the global parameters of the Diffie-Hellman key exchange. 3. It uses nonces to ensure against replay attacks. 4. It enables the exchange of Diffie-Hellman public key values. 5. It authenticates the Diffie-Hellman exchange to thwart man-in-the-middle attacks.	5 marks
	Explanation Carries	5 marks
8	**S/MIME Content Types**	

Type	Subtype	smime Parameter	Description
Multipart	Signed		A clear-signed message in two parts: one is the message and the other is the signature.
Application	pkcs 7-mime	signedData	A signed S/MIME entity.
	pkcs 7-mime	envelopedData	An encrypted S/MIME entity.
	pkcs 7-mime	degenerate signedData	An entity containing only public- key certificates.
	pkcs 7-mime	CompressedData	A compressed S/MIME entity
	pkcs 7-signature	signedData	The content type of the signature subpart of a multipart/signed message.

		5 marks
	Explanation carries	5 marks

Subject Title: Cryptography **Subject Code:** 18CS744

Question Number	Solution	Marks Allocated
9	**ESP format**  (a) Top-level format of an ESP Packet  (b) Substructure of payload data	6 marks
10	**Explanation** The services are • Access control • Connectionless integrity • Data origin authentication • Rejection of replayed packets (a form of partial sequence integrity) • Confidentiality (encryption) • Limited traffic flow confidentiality	4 marks 5 marks
		5 marks

	AH	ESP (encryption only)	ESP (encryption plus authentication)
Access control	✔	✔	✔
Connectionless integrity	✔		✔
Data origin authentication	✔		✔
Rejection of replayed packets	✔	✔	✔
Confidentiality		✔	✔
Limited traffic flow confidentiality		✔	✔

Benefits

Signature of faculty 01/01/24

Signature of Reviewer 1/1/24
Professor & HOD,
Department of Computer Science & Engg
S.J.C. Institute of Technology
Chickballapur-562 101

Signature of HOD 1/1/24
Professor & HOD,
Department of Computer Science & Engg
S.J.C. Institute of Technology
Chickballapur-562 101

||JAI SRI GURUDEV||

SJC INSTITUTE OF TECHNOLOGY, CHICKBALLAPUR

Department of Computer Science & Engineering

TUTORIAL-III

Sem: 7th SEM **Sub Name:** CRYPTOGRAPHY [18CS744] **Date:** 26.12.2023

1. Explain overview of Kerberos authentication services.
2. Explain Pretty Good Privacy mail security protocol.
3. Briefly describe the S/MIME message content types.
4. Build functional modules and standardized protocols used between them in the Internet Mail architecture.
5. Distinguish between Kerberos Version 4 and 5.
6. Design the interrelationship of DNSSEC, SPF, DKIM, DMARC, DANE and S/MIME for assuring message authenticity and integrity.
7. What services are provided by IPsec? List the benefits of IPsec.
8. Describe with neat diagram encapsulating security payload format.
9. Discuss IPsec architecture with neat diagram
10. Construct the basic combinations of security associations with different cases.
11. Make use of scope of ESP encryption and authentication, draw a diagram for Authentication Header.
12. Distinguish between transport-mode versus tunnel-mode encryption. Explain Internet Key Exchange Protocol.

26/12/23 26/12/23

Signature of the Faculty

1/1/24.

Signature of the HoD

Professor & HOD,
Department of Computer Science & Engg.
S.J.C. Institute of Technology,
Chickballapur-562 101

CBCS SCHEME

18CS744

USN | | | | | | | | | | |

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. Using Hill Cipher technique, encrypt the plain text "Paymoremoney" using the key.

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

[Hint : a = 0 , b = 1 , ... z = 25]. **(08 Marks)**

b. Explain the playfair cipher and its rules for the following example.
Keyword : MONARCHY ; Plain text : Cryptography. **(08 Marks)**

c. Define Substitution and Transposition techniques. **(04 Marks)**

OR

2 a. Explain DES Encryption algorithm, with neat diagram. **(10 Marks)**

b. Explain Feistel encryption and Decryption algorithm, with neat diagram. **(10 Marks)**

Module-2

3 a. Explain Public – Key Cryptosystems. **(10 Marks)**

b. Explain the description of the RSA algorithm. **(10 Marks)**

OR

4 a. Explain the Diffie – Hellman key exchange algorithm. **(10 Marks)**

b. Describe Elgamal Cryptographic systems. **(10 Marks)**

Module-3

5 a. Explain Elliptic curve over real numbers. **(10 Marks)**

b. Describe Micali – Schnorr pseudorandom Bit generator with neat diagram. **(10 Marks)**

OR

6 a. Explain Key – distribution Scenario, with neat diagram. **(10 Marks)**

b. Explain Public – key authority technique proposed for the distribution of Public keys. **(10 Marks)**

Module-4

7 a. Describe Public key infrastructure, with neat diagram. **(10 Marks)**

b. Explain Remote User – Authentication Principles. **(10 Marks)**

OR

8 a. Describe in detail PGP (Pretty Good Privacy) Cryptographic functions. **(10 Marks)**

b. Explain DKIM (Domain Keys Identified Mail) functional flow with diagram. **(10 Marks)**

Module-5

9 a. Describe the application and benefits of IPsec. **(10 Marks)**

b. Describe IP Security Architecture, with neat diagram. **(10 Marks)**

OR

10 a. Explain Internet Key Exchange (IKE) Key determination features. **(10 Marks)**

b. Explain Basic Combinations of Security Associations. **(10 Marks)**

* * * * *

211118CS74438053

Visvesvaraya Technological University

Belagavi, Karnataka - 590 018

Signature of Scrutinizer

Scheme & Solutions

Subject Title : cryptography

Subject Code : 18CS744

Question Number	Solution	Marks Allocated
1(a)	Hill cipher technique encryption method. plain text " paymore money" Key $\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$ $C = KP \bmod 26$ The first three letters of the plaintext are represented by the vector (2 marks) pay mor emo ney Find cipher text for pay $C = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix} \bmod 26$ $= \begin{pmatrix} 17\times15 + 17\times0 + 5\times24 \\ 21\times15 + 18\times0 + 21\times24 \\ 2\times15 + 2\times0 + 19\times24 \end{pmatrix} \bmod 26$ $= \begin{pmatrix} 255+0+120 \\ 315+0+504 \\ 30+0+456 \end{pmatrix} \bmod 26$ $= \begin{pmatrix} 375 \\ 819 \\ 486 \end{pmatrix} \bmod 26$ $= \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix} = \begin{pmatrix} L \\ N \\ S \end{pmatrix}$ similarly find for remaining. 2+2+2 = 6 marks P.T. Paymoremoney C.T. LNSHDLEWMTRW So the cipher text after encryption is LNSHDLEWMTRW	8 marks

Subject Title : Cryptography Subject Code : 18CS 744

Question Number	Sub: Cryptography Solution	Marks Allocated
b.	playfair cipher rules (4 marks) To find ciphertext for the plain text "cryptography" (4 marks) Keyword : MONARCHY Divide plain text in digraph cr yp to gr ap hy Cipher text is : DM HQ PR KN OS YB 5x5	8 marks
c.	Definition of Substitution (2 marks) Definition of Transposition (2 marks)	4 marks
2 a.	Explanation of DES encryption algorithm (6 marks) Diagram of General Depiction of DES encryption Algorithm (4 marks)	10 marks
b.	Explanation of Feistel encryption & Decryption algorithm (6 marks) Diagram of Feistel encryption and Decryption (4 marks)	10 marks
	Module - 2	
3 a.	Explanation of public-key cryptosystems (6 marks) plaintext Encryption algorithm public & private keys Cipher text Decryption algorithms Diagrams of public key cryptosystem (4 marks)	10 marks
b.	Description of RSA Algorithms • Key generation (2 marks) • Encryption (4 marks) • Decryption (4 marks)	10 marks

Subject Title : Cryptography Subject Code : 18CS744

Question Number	Solution	Marks Allocated
4 a.	The Diffie-Hellman Key Exchange algorithm Explanation (5 marks) Global public elements (1 mark) User A key generation (1 mark) User B Key Generation (1 mark) Calculating of secret key by user 'A'. (1 mark) Calculating of secret key by user 'B' (1 mark)	10 marks
(b)	Elgamal cryptographic system steps to generate private key pair (6 marks) • Global public elements (1 mark) • Key generation by Alice (1 mark) • Encryption by Bob with Alice's public key (1 mark) • Decryption by Alice with Alice's private key (1 mark)	10 marks
5(a)	Elliptic curve over real numbers Explanation. Weierstrass equation: $y^2+axy+by=x^3+cx^2+dx+e$ where a,b,c,d,e are real numbers. (2 marks) To plot a curve we need to compute $y=\sqrt{x^3+ax+b}$ Examples of elliptic curves. (4 marks) Geometric description of Addition (2 marks) Algebraic Description of Addition. (2 marks)	10 marks
(b)	Micali-Schnorr pseudorandom Bit generator diagram (4 marks) Explanation (6 marks)	10 marks
6(a)	Key Distribution Scenario explanation (6 marks) Fae diagram (4 marks)	10 marks
(b)	public-key authority techniques Explanation ① public announcement ② publicly available directory	

Subject Title : Cryptography Subject Code : 18CS744

Question Number	Solution	Marks Allocated
	3) public-Key authority 4) public-Key certificates (2 marks) Explaination with diagram (2+2+2+2) = 8 marks	10 marks
	Module-4	
7 (a)	public Key Infrastructure Explaination 1) End Entity 2) certification authority (CA) 3) Registration authority (RA) 4) CRL issuer 5) Repository (4 marks) For Diagram (2 marks) PKIX management functions (4 marks) 1) Registration 2) Initialization 3) certification 4) Key pair recovery 5) Key pair update 6) Revocation Request 7) cross certification.	10 marks
(b)	Remote user-Authentication principles Explaination. [Identification & verification step] (4 marks) • Mutual Authentication (3 marks) • one way Authentication. (3 marks)	10 marks
8 (a)	PGP cryptographic functions Explaination (6 marks) a) Authentication only b) confidentiality only c) confidentiality and authentication. For diagrams (4 marks)	10 marks
(b)	DKIM Function flow Explaination (5 marks) For diagram (5 marks)	10 marks

Subject Title : Cryptography Subject Code : 18CS744

Question Number	Solution	Marks Allocated
	Module-5	
9 (a)	Applications of IP sec (5 marks) Benefits of IPSec (5 marks)	10 marks
(b)	IP Security Architecture Explaination (6 marks) For diagram (4 marks)	10 marks
10(a)	Internet Key Exchange Explaination of Key determination features (6 marks) IKE mandates that cookie generation satisfy three basic requirements (4 marks)	10 marks
(b)	Basic combinations of security Association Explainations (2 marks) Diagrams Case 1 (2 marks) Case 2 (2 marks) Case 3 (2 marks) Case 4 (2 marks)	10 marks

Modified

CBCS SCHEME

USN | | | | | | | | | | |

18CS744

Seventh Semester B.E. Degree Examination, Jan./Feb. 2023
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 Playfair Cipher Algorithm. Find the Ciphertext for plaintext = "instruments" with key = "MONARCHY". **(10 Marks)**

b. Explain with neat diagram Feistel Cipher structure for Encryption and Decryption. **(10 Marks)**

OR

2 a. Explain Hill Cipher Algorithm. Using Hill-Cipher perform encryption and decryption for plaintext = "paymoremoney" using key $K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$. **(10 Marks)**

b. Explain with neat diagram DES encryption algorithm. **(10 Marks)**

Module-2

3 a. Explain RSA algorithm. Using RSA algorithm perform encryption and decryption using $p = 17, q = 11, e = 7$ and $M = 88$. **(10 Marks)**

b. Explain Diffie-Hellman key exchange algorithm and also show that the calculations produce the identical results. **(10 Marks)**

OR

4 a. Explain Elgamal cryptosystem. Perform encryption and decryption using $q = 19$, $\alpha = 10$, $k = 6$, $M = 17$, $X_A = 5$ and $Y_A = 3$. **(10 Marks)**

b. Explain the requirements and applications for public key cryptography. **(10 Marks)**

Module-3

5 a. Explain the concept of PRNG based on RSA. **(10 Marks)**

b. Explain the distribution of public keys with public key Authority. **(10 Marks)**

OR

6 a. Explain with neat diagram control vector encryption and decryption. **(10 Marks)**

b. Explain distribution of public keys using public key certificates. **(10 Marks)**

Module-4

7 a. Explain X.509 certificate format. **(10 Marks)**

b. Bring out the differences between Kerberos version 4 and version 5 and also mention the technical deficiencies in Kerberos version 4 protocols. **(10 Marks)**

OR

8 a. Explain PKIX architectural model. **(10 Marks)**

b. Explain with neat diagram the key components of Internet Mail Architecture. **(10 Marks)**

Module-5

9 a. Explain the benefits and applications of IPsec. **(10 Marks)**

b. Explain the IP traffic processing for outbound and inbound packets. **(10 Marks)**

OR

10 a. Explain ESP packet format. **(10 Marks)**

b. Explain the concept of transport and tunnel modes. **(10 Marks)**

* * * * *

Re: Sir, scheme updated regarding

"Nagappa Bhajantri" <bhajan3nu@gmail.com> January 31, 2023 11:22 AM

To: boe@vtu.ac.in

Respected sir,
Here mentioned 7th sem CSE/ISE both the elective courses schemes
1) 18CS742-Network Management
2) 18CS744-Cryptography
are updated & may not need any changes

Thanking you
Dr. Nagappa Bhajantri
BoE chairman IS/CS Board

On Mon, 30 Jan, 2023, 4:56 pm , <boe@vtu.ac.in> wrote:

" APPROVED "

Registrar (Evaluation)
Visvesvaraya Technological University
BELAGAVI - 590018

211118CS74438058

Visvesvaraya Technological University

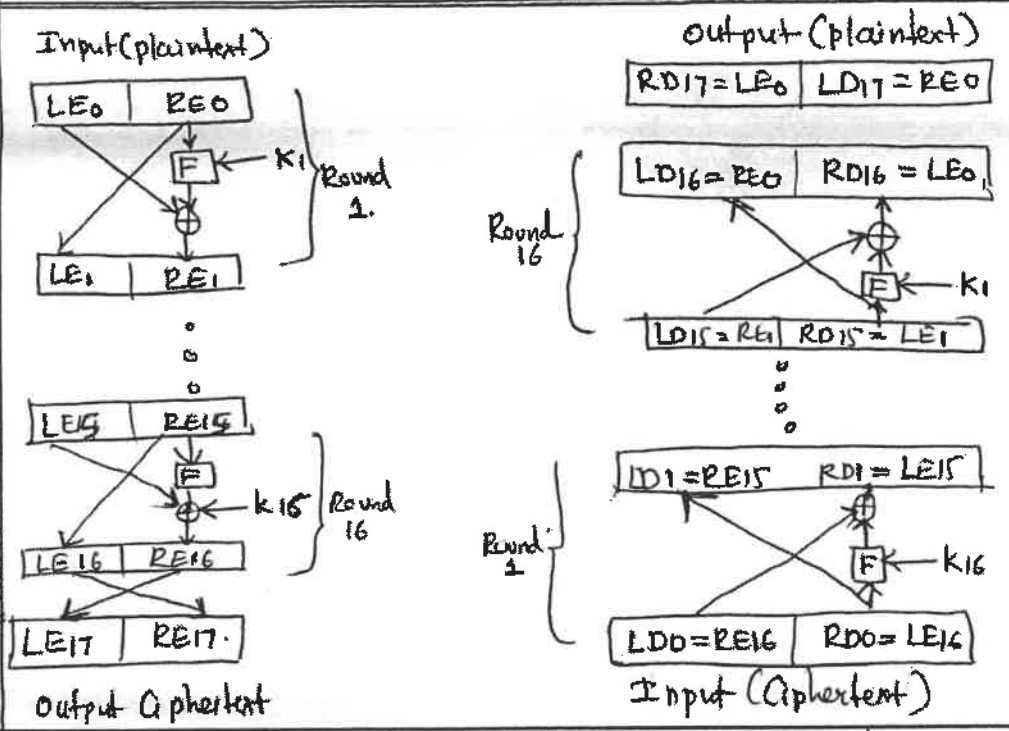
Belagavi, Karnataka - 590 018

Signature of Scrutinizer

Scheme & Solutions

Subject Title : Cryptography

Subject Code : 18CS744

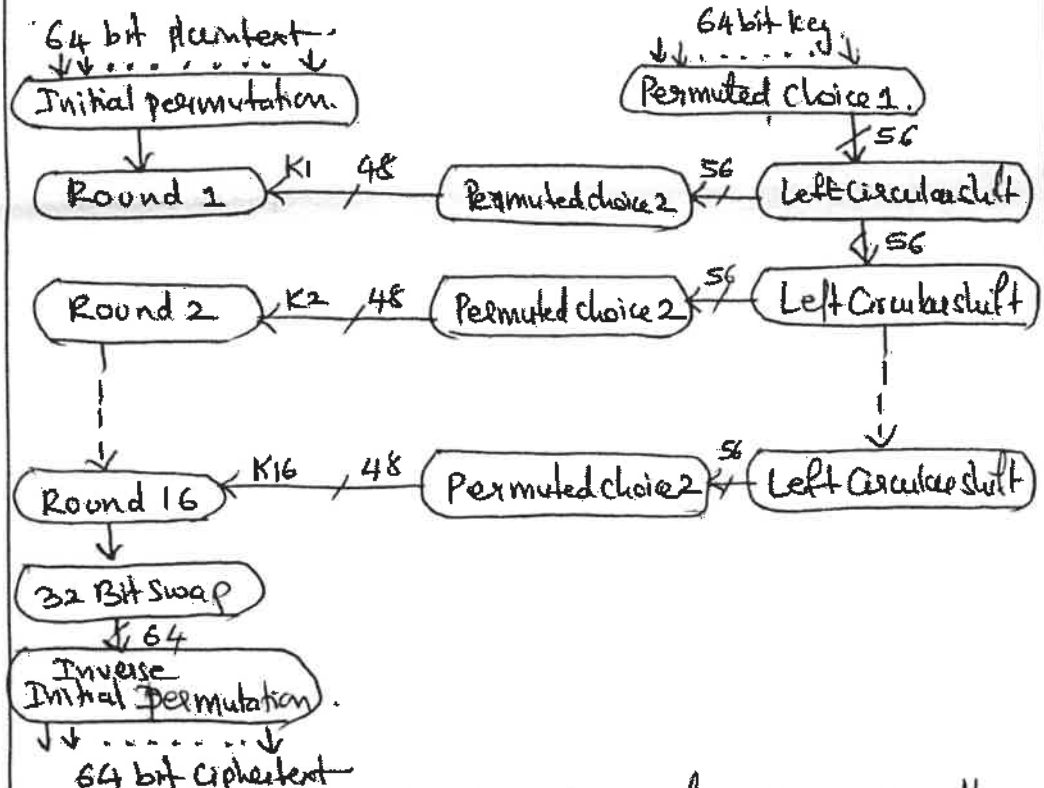
Question Number	Solution	Marks Allocated
1a.	Explanation of playfair cipher with four rules to perform encryption. plaintext - instruments in st ru me nt sz key = MONARCHY M O N A R C H Y B D E F G I/J K L P Q S T U V W X Z in → [i→g n→a] st → [s→t t→l] ru → [r→m u→z] me → [m→c e→l] nt → [n→r t→q] sz → [s→t z→x] Ciphertext : gatlmzclrqtx	05 marks 05 marks
1b.		05 marks

Explanation of Feistel Cipher Structure —— 05 marks.

APPROVED

Registrar (Evaluation)
Visvesvaraya Technological University
BELAGAVI - 590018

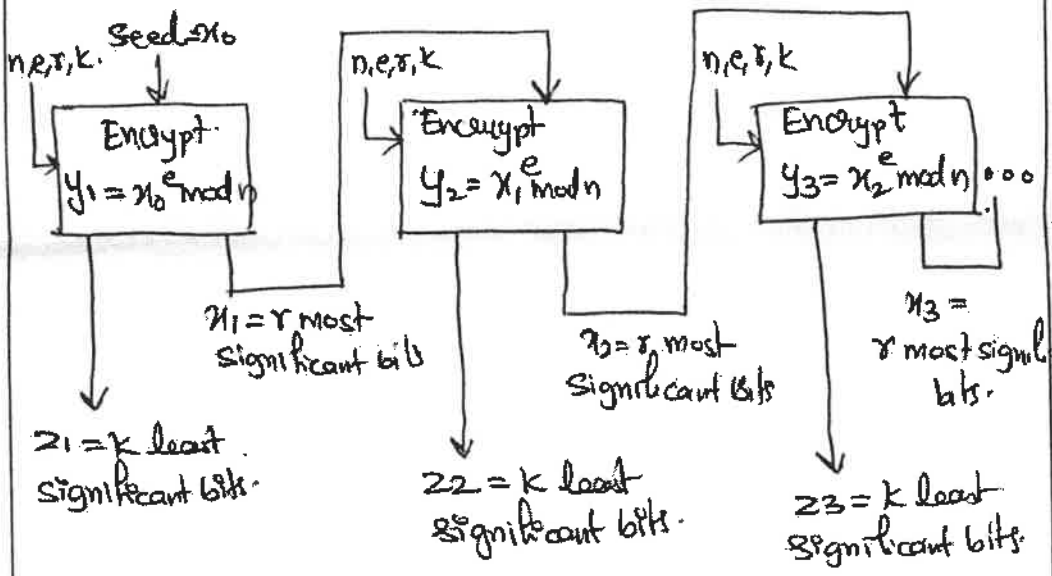
Subject Title : Cryptography. Subject Code : 18CS744

Question Number	Solution	Marks Allocated
2a	Explanation of Hill Cipher Algorithm. →	05 marks
	plaintext = paymore money $K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$	
	paymore money = (15, 0, 24, 12, 14, 17, 4, 12, 14, 13, 4, 24)	
	(15, 0, 24) K = (303, 303, 531) mod 26 = (17, 17, 11) = RRL	
	(12, 14, 17) K = (532, 490, 677) mod 26 = (12, 22, 1) = MWB	
	(4, 12, 14) K = (348, 312, 538) mod 26 = (10, 0, 18) = KAS	05 marks
	(13, 4, 24) K = (353, 341, 605) mod 26 = (15, 3, 7) = PDH	
	$\boxed{\text{Ciphertext} = \text{RRLMWBKASPDH}}$	
	$K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$ $\boxed{P = CK^{-1} \bmod 26.}$	
	(17, 17, 11) K^{-1} = (15, 0, 24) = pay	
	(12, 22, 1) K^{-1} = (12, 14, 17) = mor	
	(10, 0, 18) K^{-1} = (4, 12, 14) = emo	
	(15, 3, 7) K^{-1} = (13, 4, 24) = ney.	
2b		04 marks.
	Explanation of DES Algorithm	06 marks

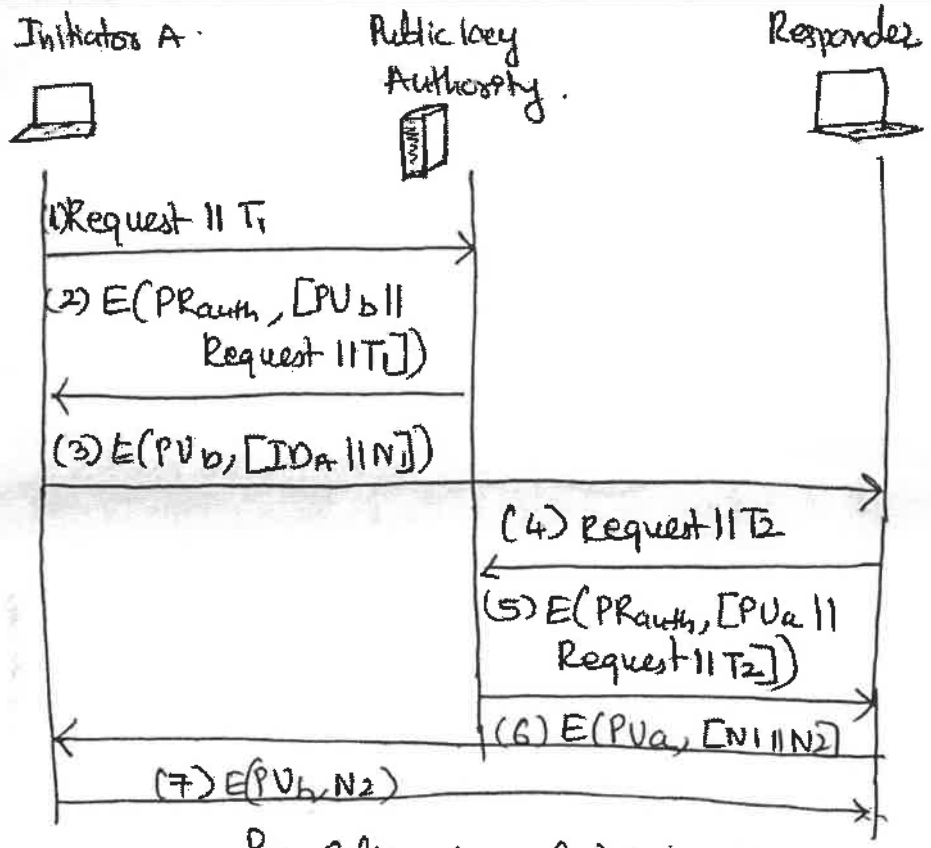
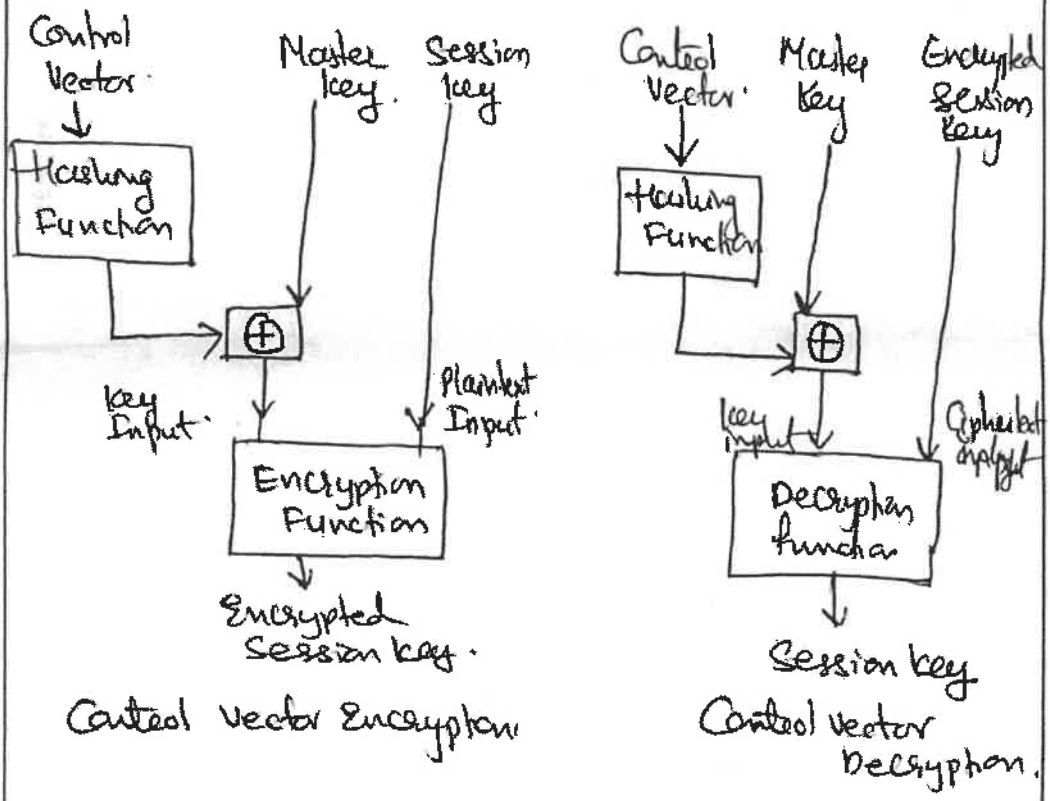
Subject Title : Cryptography Subject Code : 18CS144

Question Number	Solution	Marks Allocated
3a	Explanation of RSA Algorithm. $p=17$ $q=11$ $e=7$. $n = p \times q = 17 \times 11 = 187$. $\phi(n) = (p-1)(q-1) = (16 \times 10) = 160$. $de \equiv 1 \pmod{160}$ and $d < 160$. $d \cdot 7 \equiv 1 \pmod{160}$ $d = 23$ because $23 \times 7 = 161 \bmod 160 = 1$. Public key $= \{7, 187\}$ Private key $= \{23, 187\}$ Encryption: $C = M^e \bmod n$ $88^7 \bmod 187 = 11$ Decryption $M = C^d \bmod n$ $= 11^{23} \bmod 187 = 88$.	05 marks 05 marks
3b.	Explanation of Diffie Hellman Key Exchange algorithm. Calculation $K = (Y_B)^{X_A} \bmod q$. $= (\alpha^{X_B} \bmod q)^{X_A} \bmod q$. $= (\alpha^{X_B})^{X_A} \bmod q$. $= \alpha^{X_B \cdot X_A} \bmod q$. $= (\alpha^{X_A})^{X_B} \bmod q$. $= (\alpha^{X_A} \bmod q)^{X_B} \bmod q$. $= Y_A^{X_B} \bmod q$.	07 marks. 03 marks
4a	Explanation of Elgamal Cryptosystem. (Key generation Encryption, Decryption). $q = 19$ $\alpha = 10$. $X_A = 5$ $Y_A = \alpha^{X_A} \bmod q = 10^5 \bmod 19 = 3$ $\boxed{Y_A = 3}$ $\boxed{\text{Private key} = 5}$ $\boxed{\text{Public key } \{q, \alpha, Y_A\} = \{19, 10, 3\}}$	05 marks

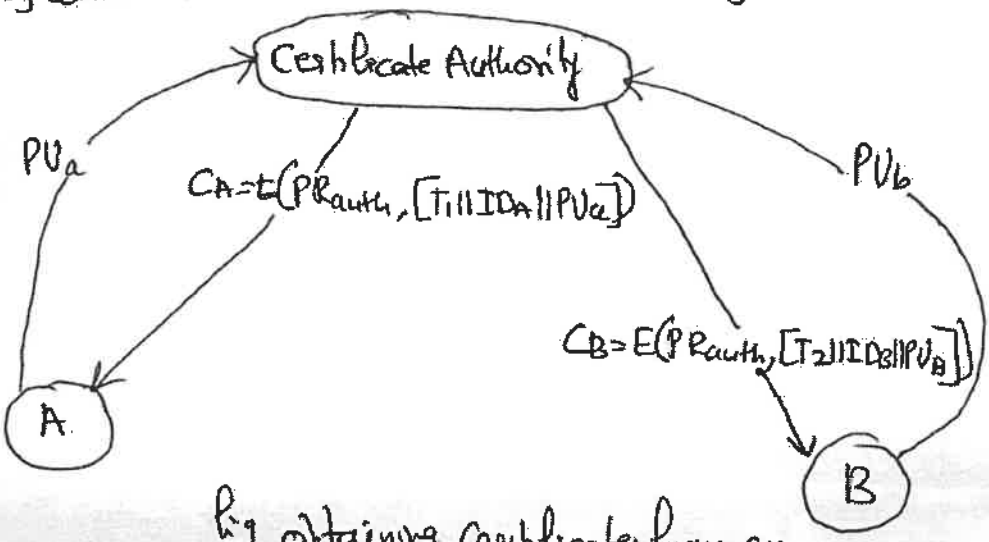
Subject Title : Subject Code :

Question Number	Solution	Marks Allocated
	$M = 17$. <u>Encryption</u> $K = 6$. $K = (Y_A)^K \bmod q = 3^6 \bmod 19 = 729 \bmod 19 = 7$. $C_1 = \alpha^K \bmod q = 10^6 \bmod 19 = 11$ $C_2 = KM \bmod q = 7 \times 17 \bmod 19 = 119 \bmod 19 = 5$ Ciphertext $(C_1, C_2) = (11, 5)$ <u>Decryption</u>. $K = (C_1)^{X_A} \bmod q = 11^5 \bmod 19 = 161051 \bmod 19 = 7$ $K^{-1} = 11$ $M = (C_2 K^{-1}) \bmod q = 5 \times 11 \bmod 19 = 17$	05 marks
4b	Requirements for public key cryptography Applications for public key cryptography	06 marks 04 marks
5a	Explanation of PRNG. Based on RSA (Setup, Seed, Generate, output) and parameters)  	07 marks 03 marks.
5b.	Diagram of Public key distribution Scenario Explanation of steps.	03 marks. 07 marks

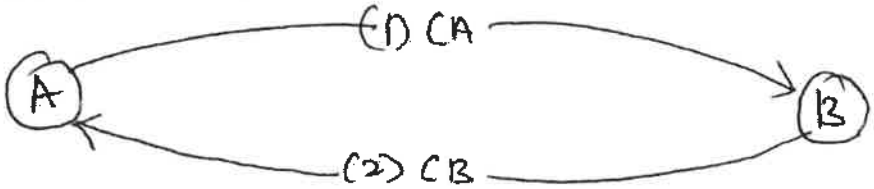
Subject Title : Cryptography Subject Code : 18CS744

Question Number	Solution	Marks Allocated
5b	 Fig Public key distribution Scenario.	
6a	 Explanation of Control Vector Encryption & Decryption	03 marks 07 marks

6b: Explanation of Distribution of public keys with Public key certificate. — 07 marks

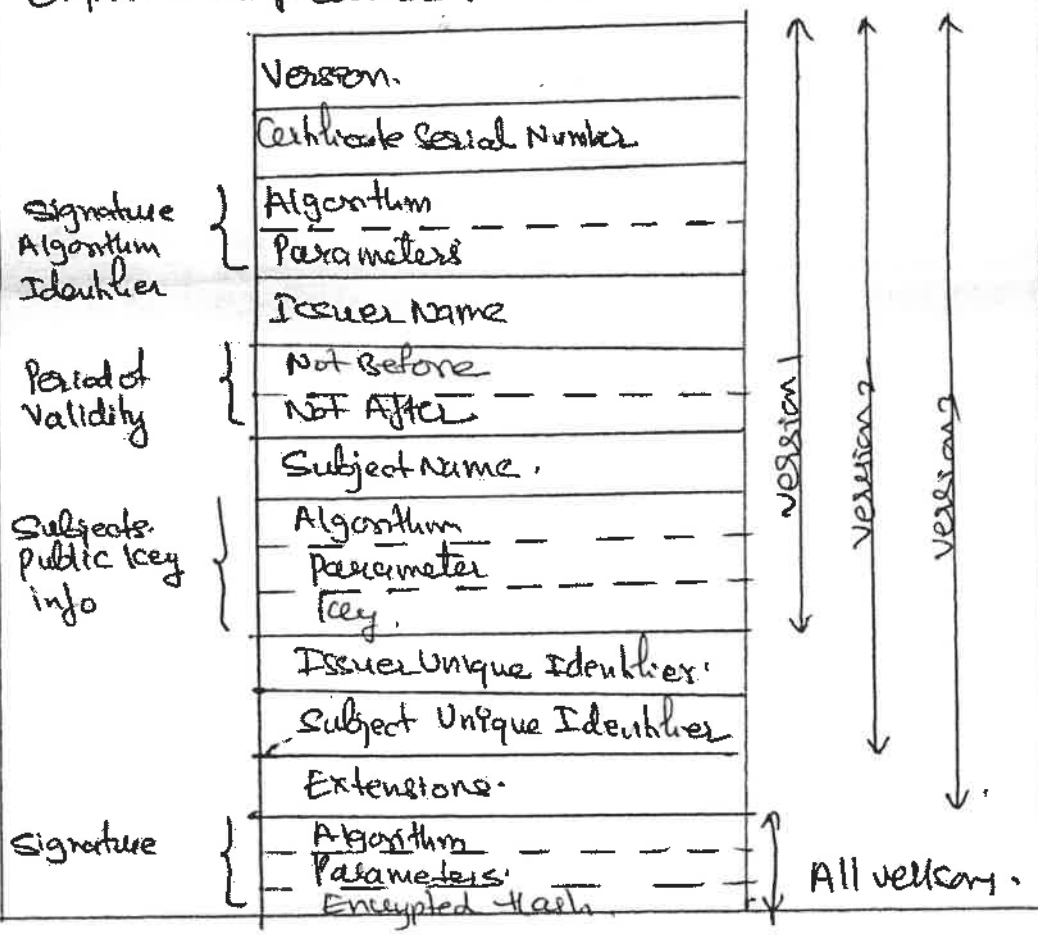


(i) obtaining Certificates from CA. — 02 marks



(ii) Exchanging Certificates. — 01 mark

7a. Explanation of Certificate format → — 06 marks



— 04 marks

Subject Title: Cryptography. Subject Code: 18CS744.

7b	Differences between Version 4 & 5 of Kerberos.	06 marks
	~~Application~~ Technical Deficiencies of Version 4	04 marks
8a	Explanation of PKIX Architectural model.	06 marks
	Diagram	04 marks
8b	Explanation of Internet mail Architecture	06 marks
	Diagram.	04 marks
9a	Benefits of IPSec.	06 marks
	Applications of IPSec.	04 marks
9b	IP Traffic processing for OutBound packets (diagram + Explanation)	05 marks
	IP Traffic processing for Inbound packets (diagram + Explanation)	05 marks
10a	ESP packet format	04 marks
	Explanation.	06 marks
10b	Explanation of Transport & Tunnel mode	10 marks

"APPROVED"

Registrar (Evaluation)
Visvesvaraya Technological University
BELAGAVI - 590018

|| Jai Sri Gurudev ||

S.J.C Institute of Technology, Chickballapur

Department of Computer Science & Engineering

Remedial Class for Slow Learners

Date: 20.12.2023

Subject Code: 18CS744 **Subject Name: Cryptography** **Sem /Sec: VII/B&C**

Topics Discussed:-

* Key management & Distribution
* X.509 Certificate
* IP Security. overview application of IPSec, benefits

Student attendance:-

Sl. #	USN	Name
1.	1SJ20CS119	ROHAN S
2.	1SJ20CS123	SAI SUJAY K
3.	1SJ20CS124	SAI SUNAY K
4.	1SJ20CS132	SATISH G
5.	1SJ20CS171	VIVEK K S
6.	1SJ20CS173	Y PRANAY KUMAR REDDY
7.	1SJ20CS179	SHWETHA R
8.	1SJ21CS401	BALA SUBHRAMANYAM D P
9.	1SJ21CS402	JAYASUDHA Y S
10.	1SJ21CS403	KAVYA S
11.	1SJ21CS407	NAGARJUN K R
12.	1SJ21CS409	PAVAN KALYAN V R
13.	1SJ21CS414	SUHAS D P

Outcome:

Students are able to understand the above topics.

20/12/23

Signature of the Subject Teacher

HOD 20/12/23

|| Jai Sri Gurudev ||

S.J.C Institute of Technology, Chickballapur

Department of Computer Science & Engineering

Remedial Class for Slow Learners

Date: 09.12.2023

Subject Code:18CS744 **Subject Name:Cryptography** **Sem/Sec: VII/B&C**

Topics Discussed:-

* RSA algorithm
* Diffie-Hellman key exchange
* Elgamal Cryptographic system

Student attendance:-

Sl. #	USN	Name
1.	1SJ20CS119	ROHAN S
2.	1SJ20CS123	SAI SUJAY K
3.	1SJ20CS124	SAI SUNAY K
4.	1SJ20CS132	SATISH G
5.	1SJ20CS171	VIVEK K S
6.	1SJ20CS173	Y PRANAY KUMAR REDDY
7.	1SJ20CS179	SHWETHA R
8.	1SJ21CS401	BALA SUBHRAMANYAM D P
9.	1SJ21CS402	JAYASUDHA Y S
10.	1SJ21CS403	KAVYA S
11.	1SJ21CS407	NAGARJUN K R
12.	1SJ21CS409	PAVAN KALYAN V R
13.	1SJ21CS414	SUHAS D P

Outcome:

Students are able to solve the problems related to RSA, Diffie-Hellman & Elgamal

9/12/23

Signature of the Subject Teacher

HOD 9/12/23

|| Jai Sri Gurudev ||

S.J.C Institute of Technology, Chickballapur

Department of Computer Science & Engineering

Remedial Class for Slow Learners

Date: 18.11.2023

Subject Code:18CS744 **Subject Name:Cryptography** **Sem/Sec: VII/B&C**

Topics Discussed:-

* Symmetric cipher model
* Caesar cipher, playfair cipher, Hill cipher
* polyalphabetic cipher
* DES encryption & decryption

Student attendance:-

Sl. #	USN	Name
1.	1SJ20CS119	ROHAN S
2.	1SJ20CS123	SAI SUJAY K
3.	1SJ20CS124	SAI SUNAY K
4.	1SJ20CS132	SATISH G
5.	1SJ20CS171	VIVEK K S
6.	1SJ20CS173	Y PRANAY KUMAR REDDY
7.	1SJ20CS179	SHWETHA R
8.	1SJ21CS401	BALA SUBHRAMANYAM D P
9.	1SJ21CS402	JAYASUDHA Y S
10.	1SJ21CS403	KAVYA S
11.	1SJ21CS407	NAGARJUN K R
12.	1SJ21CS409	PAVAN KALYAN V R
13.	1SJ21CS414	SUHAS D P

Outcome: Students are able solve the problem and understand the DES concepts.

18/11/23

Signature of the Subject Teacher

HOD 18/11/23

||Jai Sri Gurudev||

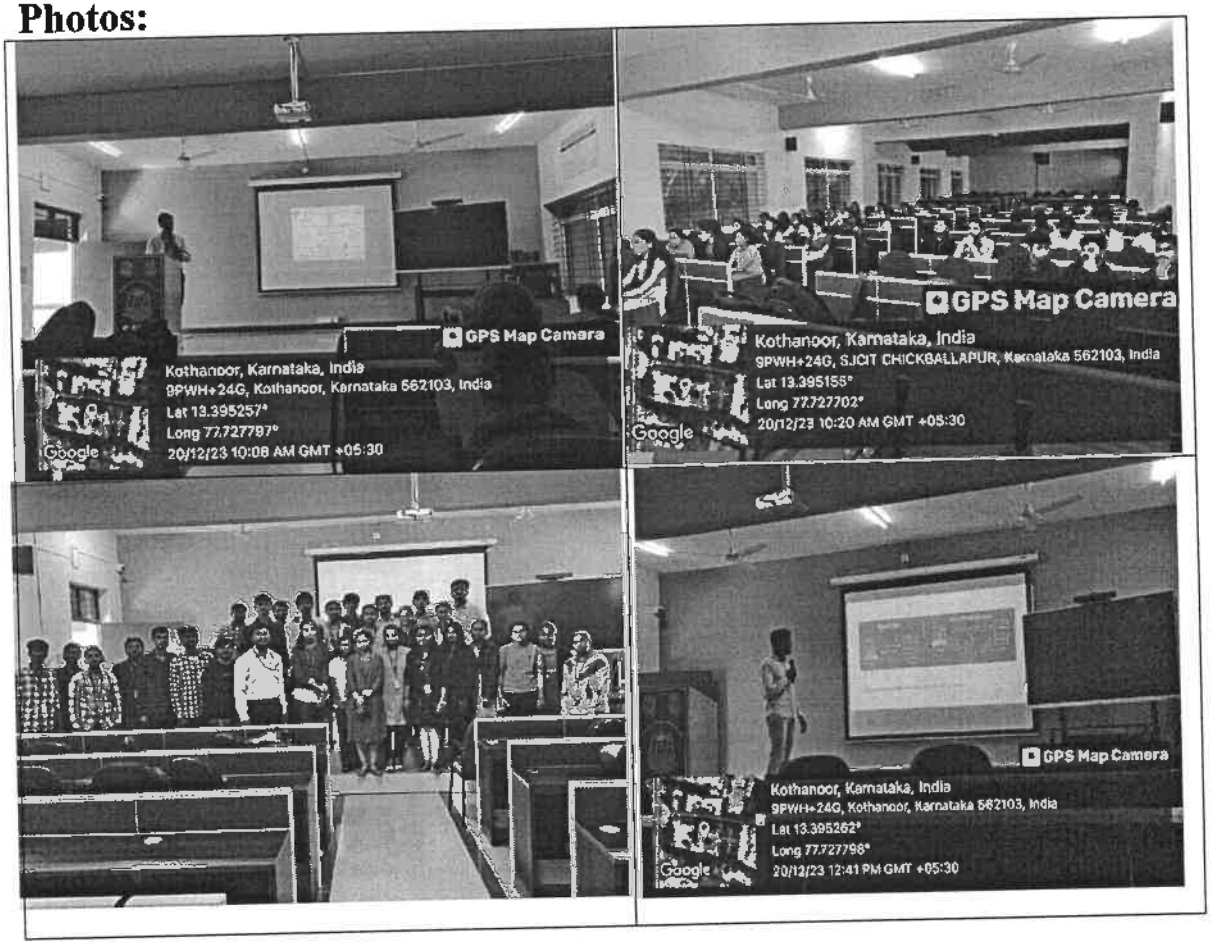
SJC Institute of Technology, Chickaballpur
Department of Computer Science & Engineering
Mini Project Exhibition Details

Sem: VII **Subject Name: Cryptography (18CS744)**

Sl #	Group No.	USN	Name	Topics	Photos
1.	1	1SJ20CS152	TARUN K H	Secure Hashing Algorithm	
2.		1SJ20CS125	SAI SUPREETH REDDY P		
3.		1SJ20CS134	SHASHANK M N		
4.	2	1SJ20CS153	TEJAS GOWDA H A	Man in the Middle Attack	
5.		1SJ20CS154	TEJAS V A		
6.		1SJ20CS155	THARUN REDDY K V		
7.	3	1SJ20CS127	SANJANA K L	Data Encryption Standard	
8.		1SJ20CS172	Y HARIPRIYA		
9.		1SJ20CS140	SHWETHASHREE KV		
10.	4	1SJ20CS143	SUCHITRA K S	Message Authentication Code	
11.		1SJ20CS161	VANDANA S R		
12.		1SJ20CS169	VINUTHA C R		
13.	5	1SJ20CS106	PREETHI M	Diffie Hellman Key Exchange Algorithm	
14.		1SJ20CS121	S P PREETHI		

15.	6	1SJ20CS122	SAHANASHREE N	Advanced Encryption Standard	
16.		1SJ20CS144	SUCHITRA N L		
17.		1SJ20CS174	YASHASWINI K M		
18.	7	1SJ20CS116	REVANTH RAJA	Elliptical Curve Cryptography	
19.		1SJ20CS111	RAKSHITH D S		
20.		1SJ20CS102	PRAJWAL MURULI S		
21.	8	1SJ20CS114	RAKSHITHA R	RSA Algorithm	
22.		1SJ20CS113	RAKSHITHA K V		

Photos:




GPS Map Camera
Kothanoor, Karnataka, India
9PWH+24G, Kothanoor, Karnataka 562103, India
Lat 13.395261°
Long 77.727819°
20/12/23 12:25 PM GMT +05:30
Google

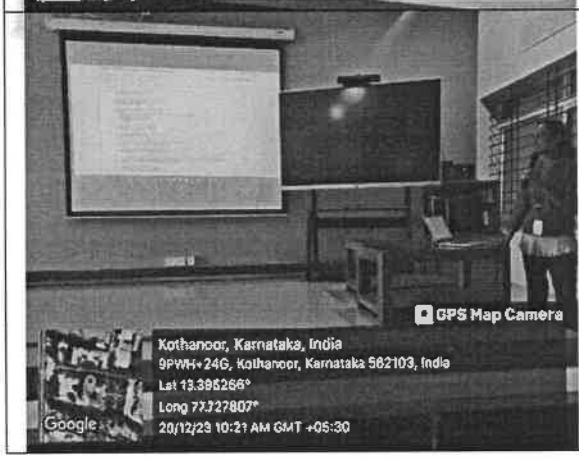

GPS Map Camera
Kothanoor, Karnataka, India
9PWH+24G, Kothanoor, Karnataka 562103, India
Lat 13.395281°
Long 77.727799°
20/12/23 12:03 PM GMT +05:30
Google

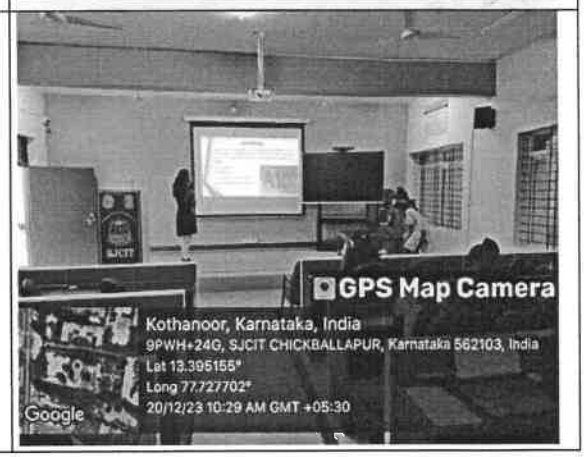

GPS Map Camera
Kothanoor, Karnataka, India
9PWH+24G, Kothanoor, Karnataka 562103, India
Lat 13.395265°
Long 77.727803°
20/12/23 11:56 AM GMT +05:30
Google


SJCIT
GPS Map Camera
Kothanoor, Karnataka, India
9PWH+24G, Kothanoor, Karnataka 562103, India
Lat 13.395282°
Long 77.727806°
20/12/23 11:18 AM GMT +05:30
Google


GPS Map Camera
Kothanoor, Karnataka, India
9PWH+24G, Kothanoor, Karnataka 562103, India
Lat 13.395261°
Long 77.727809°
20/12/23 11:02 AM GMT +05:30
Google


GPS Map Camera
Kothanoor, Karnataka, India
9PWH+24G, Kothanoor, Karnataka 562103, India
Lat 13.395262°
Long 77.727808°
20/12/23 10:47 AM GMT +05:30
Google


GPS Map Camera
Kothanoor, Karnataka, India
9PWH+24G, Kothanoor, Karnataka 562103, India
Lat 13.395266°
Long 77.727807°
20/12/23 10:21 AM GMT +05:30
Google


SJCIT
GPS Map Camera
Kothanoor, Karnataka, India
9PWH+24G, SJCIT CHICKBALLAPUR, Karnataka 562103, India
Lat 13.395155°
Long 77.727702°
20/12/23 10:29 AM GMT +05:30
Google

Poster:

|| Jai Sri Gurudev ||

Adichunchanagiri Shikshana Trust(R.)

SJC INSTITUTE OF TECHNOLOGY

Chickballapur- 562101, Karnataka, India

INSTITUTION'S INNOVATION COUNCIL

Department of Computer Science and Engineering

Organizing

Mini Project Exhibition on "Cryptography"

20th Dec, 2023 ***10:00AM to 12:00PM*** ***CSE Seminar Hall***

Coordinators	Convener	Organising Chair	Program Chair
Prof. Ajay N & Prof. Rashmi K A Dept. of CSE	Dr. Manjunatha Kumar B H Prof. & HoD, Dept. of CSE	Mr.Suresha J Registrar	Dr.G.T. Raju Principal

20/12/23

Signature of the Subject Teacher

1/1/24

Signature of the HoD

S J C INSTITUTE OF TECHNOLOGY

DEPARTMENT OF Computer Science &Engineering

Name of the staff: Ajay N /Rashmi K A
Subject: Cryptography
Semester/Sec: VII Sem A, B & C

Sub Code: 18CS744

GAPS IN THE SYLLABUS - TO MEET INDUSTRY/PROFESSION REQUIREMENTS:

Sl. No.	Description Proposed	Actions
1	Zero Knowledge	Content Beyond Syllabus
2	Cryptographic game theory	Content Beyond Syllabus
3	Concurrent zero knowledge	Content Beyond Syllabus

Gaps in PO Attainment:

POs	ACTION PLANNED TO FILL THE GAP
PO9: Individual and teamwork	Mini-Project
PO10: Communication	Project Demonstration
PO11: Project management and finance	--

ACTION PLAN FOR NEXT ACADEMIC:

Change in the teaching methodology follows:

- More concentrate on find security algorithm with illustrative example
- Conducting revision classes in a semester to make them to remember with examples.

Counseling the students

- Counseling the weaker students to find out where they are lagging and finding difficulty in understanding the concepts in the course.

WEB SOURCE REFERENCES:

1. https://nptel.ac.in/courses

Signature of Faculty

Signature of HoD 4/1/24

||Jai Sri Gurudev||

S J C INSTITUTE OF TECHNOLOGY, CHICABALLAPUR

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Other Assessments

Sem/Sec: VII 'A' & 'B' **Subject: Cryptography**

1. **MCQ (10 Marks)**

2. **Assignment Evaluation Rubrics (10 Marks)**

Symbolic Representation of Rubrics	Marks Indication	Total
A	Answer up to the question / Description (2 – 4) Marks	4
B	Examples / Figures / Tables (2 – 4) Marks	4
C	Explanation/Formula / Calculations (2 Mark)	2

3. **Mini Project Rubrics (10 Marks)**

Sl. No.	Criteria	Marks	Scale of Assessment		
			Satisfactory-1	Good - 2	Excellent - 3
D	Objectives, Existing method with proposed method	2	Incomplete justification to the objectives proposed; Steps are mentioned but unclear; without justification to objectives.	All objectives of the proposed work are well defined; Steps to be followed to solve the defined problem are clearly specified.	--
E	Technical Description of the project	3	Incomplete explanation of the key concepts and in-sufficient description of the technical requirements of the project.	Complete explanation of the key concepts but in-sufficient description of the technical requirements of the project.	Complete explanation of the key concepts and strong description of the technical requirements of the project.
F	Project Report	2	1. Project report is according to the Specified format butsome mistakes. 2.In-sufficient references	1. Project report is according to the specified format. 2. References are appropriate and mentioned well.	--
G	Demonstration and Queries(IA)	3	Lacks sufficient knowledge and awareness	Fair knowledge and awareness related to the project.	Extensive knowledge and awareness related to the project.

Student List with MCQ and Assignment Assessment:

SL No	USN	STUDENT NAME	Test-1				Test-2				Final		Total (10 M)
			MCQ-1 (10 M)	Assignment-1 (10 M)			MCQ-2 (10 M)	Assignment-2 (10 M)			MCQ(4 M)	Assignment (6 M)	
				A	B	C		A	B	C			
1	1SJ20CS001	Abhilash N G	10	4	4	2	10	4	4	2	4	6	10
2	1SJ20CS002	Abhinav Kumar	10	4	4	2	10	4	4	2	4	6	10
3	1SJ20CS007	Aditya Iyer	10	4	4	2	10	4	4	2	4	6	10
4	1SJ20CS008	Aditya Vijay	10	4	4	2	10	4	4	2	4	6	10
5	1SJ20CS009	Akash K N	10	4	4	2	10	4	4	2	4	6	10
6	1SJ20CS013	Anjan Kumar S	10	4	4	2	10	4	4	2	4	6	10
7	1SJ20CS017	Arfa Thareen K	10	4	4	2	10	4	4	2	4	6	10
8	1SJ20CS021	Ashwarya	10	4	4	2	10	4	4	2	4	6	10
9	1SJ20CS022	BGSai kiran Reddy	10	4	4	2	10	4	4	2	4	6	10
10	1SJ20CS026	Bhavana S	10	4	4	2	10	4	4	2	4	6	10
11	1SJ20CS027	Bindhu Shree G V	10	4	4	2	10	4	4	2	4	6	10
12	1SJ20CS029	C Pallavi	10	4	4	2	10	4	4	2	4	6	10
13	1SJ20CS030	Chaitra Shree M	10	4	4	2	10	4	4	2	4	6	10
14	1SJ20CS032	Chandan Gowda N	10	4	4	2	10	4	4	2	4	6	10
15	1SJ20CS035	Chandu Raj N	10	4	4	2	10	4	4	2	4	6	10
16	1SJ20CS037	Chethan C V	10	4	4	2	10	4	4	2	4	6	10
17	1SJ20CS038	Chethan Kumar D C	10	4	4	2	10	4	4	2	4	6	10
18	1SJ20CS041	Daavimela Sneha	10	4	4	2	10	4	4	2	4	6	10
19	1SJ20CS043	Deepak U	10	4	4	2	10	4	4	2	4	6	10
20	1SJ20CS044	Deepthi B L	10	4	4	2	10	4	4	2	4	6	10
21	1SJ20CS048	D Ganesh Reddy	10	4	4	2	10	4	4	2	4	6	10
22	1SJ20CS051	Ganesh Barkela	10	4	4	2	10	4	4	2	4	6	10
23	1SJ20CS052	Gaurav Singh	10	4	4	2	10	4	4	2	4	6	10
24	1SJ20CS053	Harshvardhan R	10	4	4	2	10	4	4	2	4	6	10
25	1SJ20CS056	Hema H	10	4	4	2	10	4	4	2	4	6	10
26	1SJ20CS057	Hema K A	10	4	4	2	10	4	4	2	4	6	10
27	1SJ20CS058	Hemalatha A	10	4	4	2	10	4	4	2	4	6	10
28	1SJ20CS060	Hrushikesh S	10	4	4	2	10	4	4	2	4	6	10

29	1SJ20CS062	Jithendra	10	4	4	2	10	4	4	2	4	6	10
30	1SJ20CS063	K A Ajay	10	4	4	2	10	4	4	2	4	6	10
31	1SJ20CS065	K Prathusha	10	4	4	2	10	4	4	2	4	6	10
32	1SJ20CS070	Kiran K S	10	4	4	2	10	4	4	2	4	6	10
33	1SJ20CS071	Kishore G S	10	4	4	2	10	4	4	2	4	6	10
34	1SJ20CS072	Keerthi K	10	4	4	2	10	4	4	2	4	6	10
35	1SJ20CS074	Likhithashree	10	4	4	2	10	4	4	2	4	6	10
36	1SJ20CS075	M L Soumika	10	4	4	2	10	4	4	2	4	6	10
37	1SJ20CS076	M N Madhu	10	4	4	2	10	4	4	2	4	6	10
38	1SJ20CS078	Mallika Shree	10	4	4	2	10	4	4	2	4	6	10
39	1SJ20CS080	Manaswi M	10	4	4	2	10	4	4	2	4	6	10
40	1SJ20CS081	Manish Kumar	10	4	4	2	10	4	4	2	4	6	10
41	1SJ20CS082	Manjusri N	10	4	4	2	10	4	4	2	4	6	10
42	1SJ20CS083	Manuja C R	10	4	4	2	10	4	4	2	4	6	10
43	1SJ20CS084	Maruthi Chandra Mourya	10	4	4	2	10	4	4	2	4	6	10
44	1SJ20CS085	Mayuri S	10	4	4	2	10	4	4	2	4	6	10
45	1SJ20CS087	Meghana R	10	4	4	2	10	4	4	2	4	6	10
46	1SJ20CS088	Meghavathi M V	10	4	4	2	10	4	4	2	4	6	10
47	1SJ20CS089	Monika K	10	4	4	2	10	4	4	2	4	6	10
48	1SJ20CS091	Mythreye H B	10	4	4	2	10	4	4	2	4	6	10
49	1SJ20CS092	Nagashree C R	10	4	4	2	10	4	4	2	4	6	10
50	1SJ20CS094	Navya L	10	4	4	2	10	4	4	2	4	6	10
51	1SJ20CS095	Neeraj Y M	10	4	4	2	10	4	4	2	4	6	10
52	1SJ20CS096	Neha B S	10	4	4	2	10	4	4	2	4	6	10
53	1SJ20CS098	Nikitha S	10	4	4	2	10	4	4	2	4	6	10
54	1SJ20CS099	Noor Fathima M	10	4	4	2	10	4	4	2	4	6	10
55	1SJ20CS176	Chirag S	10	4	4	2	10	4	4	2	4	6	10
56	1SJ21CS400	Ambarish K C	10	4	4	2	10	4	4	2	4	6	10
57	1SJ21CS404	Kishore T M	10	4	4	2	10	4	4	2	4	6	10
58	1SJ21CS406	Monith L	10	4	4	2	10	4	4	2	4	6	10
59	1SJ21CS413	Shiva Kumar K	10	4	4	2	10	4	4	2	4	6	10
60	1SJ19CS105	Nandu Priya	10	4	4	2	10	4	4	2	4	6	10

Student List with MCQ and Mini Project:

Sl #	USN	Student Name	Test-1	Test-2	Test-3				Final		Total Marks (10 M)
			MCQ-1 (10 M)	MCQ-2 (10 M)	Mini Project (10 M)				MCQ (4 M)	Mini Project (6 M)	
					D	E	F	G			
1.	1SJ20CS061	Itha Sai Sreehari	10	10	2	3	2	3	4	6	10
2.	1SJ20CS066	K V Miheer Kasyap	10	10	2	3	2	3	4	6	10
3.	1SJ20CS077	M Srikada Sai Aditya	10	10	2	3	2	3	4	6	10
4.	1SJ20CS097	P.Chennakessava Reddy	10	10	2	3	2	3	4	6	10
5.	1SJ20CS024	Bhanuprasad D R	10	10	2	3	2	3	4	6	10
6.	1SJ20CS025	Bharagavi D S	10	10	2	3	2	3	4	6	10
7.	1SJ20CS054	Harshitha K	10	10	2	3	2	3	4	6	10
8.	1SJ20CS018	Arjun Kashyap S	10	10	2	3	2	3	4	6	10
9.	1SJ20CS045	Deeraj C	10	10	2	3	2	3	4	6	10
10.	1SJ20CS047	Dhanu Reddy H N	10	10	2	3	2	3	4	6	10
11.	1SJ20CS019	Aruna P U	10	10	2	3	2	3	4	6	10
12.	1SJ20CS031	Chaitra B D	10	10	2	3	2	3	4	6	10
13.	1SJ20CS042	Deekshitha B C	10	10	2	3	2	3	4	6	10

14.	1SJ20CS011	Ananya G R	10	10	2	3	2	3	4	6	10
15.	1SJ20CS016	Anusha S V	10	10	2	3	2	3	4	6	10
16.	1SJ20CS020	Asha M	10	10	2	3	2	3	4	6	10
17.	1SJ20CS046	Deviprasad G M	10	10	2	3	2	3	4	6	10
18.	1SJ21CS415	Vaishnavi N	10	10	2	3	2	3	4	6	10
19.	1SJ21CS416	Vijay Ragavan N	10	10	2	3	2	3	4	6	10

Signature of the Subject Teacher

Signature of the HoD 2/2/24

||Jai Sri Gurudev||

S J C INSTITUTE OF TECHNOLOGY, CHICABALLAPUR
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
Other Assessments

Sem/Sec: VII 'B' & C **Subject: Cryptography**

1. **MCQ (10 Marks)**

2. **Assignment Evaluation Rubrics (10 Marks)**

Symbolic Representation of Rubrics	Marks Indication	Total
A	Answer up to the question / Description (2 – 4) Marks	4
B	Examples / Figures / Tables (2 – 4) Marks	4
C	Explanation/Formula / Calculations (2 Mark)	2

3. **Mini Project Rubrics (10 Marks)**

Sl. No.	Criteria	Marks	Scale of Assessment		
			Satisfactory-1	Good - 2	Excellent - 3
D	Objectives, Existing method with proposed method	2	Incomplete justification to the objectives proposed; Steps are mentioned but unclear; without justification to objectives.	All objectives of the proposed work are well defined; Steps tobe followed to solve the defined problem are clearly specified.	--
E	Technical Description of the project	3	Incomplete explanation of the key concepts and in-sufficient description of the technical requirements of the project.	Complete explanation of the key concepts but in-sufficient description of the technical requirements of the project.	Complete explanation of the key concepts and strong description of the technical requirements of the project.
F	Project Report	2	1. Project report is according to the specified format but some mistakes. 2.In-sufficient references	1. Project report is according to the specified format. 2. References are appropriate and mentioned well.	--
G	Demonstration and Queries(IA)	3	Lacks sufficient knowledge and awareness	Fair knowledge and awareness related to the project.	Extensive knowledge and awareness related to the project.

Student List with MCQ and Assignment Assessment:

SL No	USN	STUDENT NAME	Test-1				Test-2				Final		Total (10 M)
			MCQ-1 (10 M)	Assignment-1 (10 M)			MCQ-2 (10 M)	Assignment-2 (10 M)			MCQ(4 M)	Assignment (6 M)	
				A	B	C		A	B	C			
1.	1SJ20CS104	PRATHAM GOWDA H S	10	4	4	2	10	4	4	2	4	6	10
2.	1SJ20CS105	PREETHAM H K	10	4	4	2	10	4	4	2	4	6	10
3.	1SJ20CS108	RACHAMADUGU HARI DHEERAJ	10	4	4	2	10	4	4	2	4	6	10
4.	1SJ20CS110	RAJAN KUMAR GUPTA	10	4	4	2	10	4	4	2	4	6	10
5.	1SJ20CS117	RISHIKESH L	10	4	4	2	10	4	4	2	4	6	10
6.	1SJ20CS118	ROHAN M	10	4	4	2	10	4	4	2	4	6	10
7.	1SJ20CS119	ROHAN S	10	4	4	2	10	4	4	2	4	6	10
8.	1SJ20CS120	ROOPASHREE K N	10	4	4	2	10	4	4	2	4	6	10
9.	1SJ20CS123	SAI SUJAY K	10	4	4	2	10	4	4	2	4	6	10
10.	1SJ20CS124	SAI SUNAY K	10	4	4	2	10	4	4	2	4	6	10
11.	1SJ20CS126	SALLAUDDIN AYUB BEIG	10	4	4	2	10	4	4	2	4	6	10
12.	1SJ20CS128	SANJANA S	10	4	4	2	10	4	4	2	4	6	10
13.	1SJ20CS130	SANKALANA C M	10	4	4	2	10	4	4	2	4	6	10
14.	1SJ20CS131	SATHI GRASHMA ANISWA	10	4	4	2	10	4	4	2	4	6	10
15.	1SJ20CS132	SATISH G	0	0	0	0	0	0	0	0	0	0	0
16.	1SJ20CS133	SHASHANK M J	10	4	4	2	10	4	4	2	4	6	10
17.	1SJ20CS136	SHIRISHA N	10	4	4	2	10	4	4	2	4	6	10
18.	1SJ20CS137	SHRAVYA D K	10	4	4	2	10	4	4	2	4	6	10
19.	1SJ20CS138	SHREEKAR BHARADWAJ M N	10	4	4	2	10	4	4	2	4	6	10
20.	1SJ20CS139	SHREYAS N	10	4	4	2	10	4	4	2	4	6	10
21.	1SJ20CS141	SKANDA KUMAR C S	10	4	4	2	10	4	4	2	4	6	10
22.	1SJ20CS142	SRUJAN V	10	4	4	2	10	4	4	2	4	6	10
23.	1SJ20CS145	SUDHARANI R	10	4	4	2	10	4	4	2	4	6	10
24.	1SJ20CS146	SUHAS V	10	4	4	2	10	4	4	2	4	6	10
25.	1SJ20CS147	SUPRAJA B	10	4	4	2	10	4	4	2	4	6	10
26.	1SJ20CS148	SURAJ	10	4	4	2	10	4	4	2	4	6	10
27.	1SJ20CS149	SURBHI KUMARI	10	4	4	2	10	4	4	2	4	6	10
28.	1SJ20CS151	SWETHA D S	10	4	4	2	10	4	4	2	4	6	10
29.	1SJ20CS156	USHA B S	10	4	4	2	10	4	4	2	4	6	10
30.	1SJ20CS158	VADDE NANDINI	10	4	4	2	10	4	4	2	4	6	10
31.	1SJ20CS159	VANDANA C K	10	4	4	2	10	4	4	2	4	6	10
32.	1SJ20CS160	VANDANA R	10	4	4	2	10	4	4	2	4	6	10
33.	1SJ20CS162	VARALAKSHMI P S	10	4	4	2	10	4	4	2	4	6	10
34.	1SJ20CS163	VARSHITHA R	10	4	4	2	10	4	4	2	4	6	10
35.	1SJ20CS164	VARSHITHA V	10	4	4	2	10	4	4	2	4	6	10
36.	1SJ20CS165	VENKATESH BABU G S	10	4	4	2	10	4	4	2	4	6	10
37.	1SJ20CS168	VIJAYAKUMAR	10	4	4	2	10	4	4	2	4	6	10
38.	1SJ20CS170	VISHWANATH K	10	4	4	2	10	4	4	2	4	6	10
39.	1SJ20CS171	VIVEK K S	10	4	4	2	10	4	4	2	4	6	10
40.	1SJ20CS173	YALLATURU PRANAY KUMAR REDDY	10	4	4	2	10	4	4	2	4	6	10

41.	1SJ20CS175	ZEBA SULTHANA A	10	4	4	2	10	4	4	2	4	6	10
42.	1SJ20CS177	RAMYA H	10	4	4	2	10	4	4	2	4	6	10
43.	1SJ20CS178	KOWSHIK R G	10	4	4	2	10	4	4	2	4	6	10
44.	1SJ20CS179	SHWETHA R	10	4	4	2	10	4	4	2	4	6	10
45.	1SJ21CS401	BALA SUBRAMANYAM D P	10	4	4	2	10	4	4	2	4	6	10
46.	1SJ21CS402	YASHADARA YS	10	4	4	2	10	4	4	2	4	6	10
47.	1SJ21CS403	KAVYA S	10	4	4	2	10	4	4	2	4	6	10
48.	1SJ21CS407	NAGARJUN K R	10	4	4	2	10	4	4	2	4	6	10
49.	1SJ21CS409	PAVAN KALYAN V R	10	4	4	2	10	4	4	2	4	6	10
50.	1SJ21CS414	SUHAS D P	10	4	4	2	10	4	4	2	4	6	10

Student List with MCQ and Mini Project:

Sl #	USN	Student Name	Test-1	Test-2	Test-3				Final		Total Marks (10 M)
			MCQ-1 (10 M)	MCQ-2 (10 M)	Mini Project (10 M)				MCQ (4 M)	Mini Project (6 M)	
					D	E	F	G			
1.	1SJ20CS102	PRAJWAL MURULI S	10	10	2	3	2	3	4	6	10
2.	1SJ20CS106	PREETHI M	10	10	2	3	2	3	4	6	10
3.	1SJ20CS111	RAKSHITH D S	10	10	2	3	2	3	4	6	10
4.	1SJ20CS113	RAKSHITHA K V	10	10	2	3	2	3	4	6	10
5.	1SJ20CS114	RAKSHITHA R	10	10	2	3	2	3	4	6	10
6.	1SJ20CS116	REVANTH RAJA	10	10	2	3	2	3	4	6	10
7.	1SJ20CS121	S P PREETHI	10	10	2	3	2	3	4	6	10
8.	1SJ20CS122	SAHANASHREE N	10	10	2	3	2	3	4	6	10
9.	1SJ20CS125	SAI SUPREETH REDDY P	10	10	2	3	2	3	4	6	10
10.	1SJ20CS127	SANJANA K L	10	10	2	3	2	3	4	6	10
11.	1SJ20CS134	SHASHANK M N	10	10	2	3	2	3	4	6	10
12.	1SJ20CS140	SHWETHASHREE KV	10	10	2	3	2	3	4	6	10
13.	1SJ20CS143	SUCHITHRA K S	10	10	2	3	2	3	4	6	10
14.	1SJ20CS144	SUCHITRA N L	10	10	2	3	2	3	4	6	10
15.	1SJ20CS152	TARUN K H	10	10	2	3	2	3	4	6	10
16.	1SJ20CS153	TEJAS GOWDA H A	10	10	2	3	2	3	4	6	10
17.	1SJ20CS154	TEJAS V A	10	10	2	3	2	3	4	6	10
18.	1SJ20CS155	THARUN REDDY K V	10	10	2	3	2	3	4	6	10
19.	1SJ20CS161	VANDANA S R	10	10	2	3	2	3	4	6	10
20.	1SJ20CS169	VINUTHA C R	10	10	2	3	2	3	4	6	10
21.	1SJ20CS172	Y HARIPRIYA	10	10	2	3	2	3	4	6	10
22.	1SJ20CS174	YASHASWINI K M	10	10	2	3	2	3	4	6	10

19/1/24

Signature of the Subject Teacher

25/1/24

Signature of the HoD

Professor & HOD,
Department of Computer Science & En
S.J.C. Institute of Technolo
Chickballapur-562 1

S.J.C. INSTITUTE OF TECHNOLOGY, CHICKBALLAPUR

Branch : CS Semester : 7

Sl NO.	USN	18CS744
1	1SJ19CS105	20
2	1SJ20CS001	38
3	1SJ20CS002	38
4	1SJ20CS003	-
5	1SJ20CS004	-
6	1SJ20CS005	-
7	1SJ20CS006	-
8	1SJ20CS007	29
9	1SJ20CS008	36
10	1SJ20CS009	28
11	1SJ20CS010	-
12	1SJ20CS011	40
13	1SJ20CS012	-
14	1SJ20CS013	40
15	1SJ20CS014	-
16	1SJ20CS015	-
17	1SJ20CS016	37
18	1SJ20CS017	40
19	1SJ20CS018	39
20	1SJ20CS019	40
21	1SJ20CS020	40
22	1SJ20CS021	34
23	1SJ20CS022	30
24	1SJ20CS023	-
25	1SJ20CS024	40
26	1SJ20CS025	40
27	1SJ20CS026	40
28	1SJ20CS027	37
29	1SJ20CS028	-
30	1SJ20CS029	40
31	1SJ20CS030	36
32	1SJ20CS031	40
33	1SJ20CS032	38
34	1SJ20CS033	-
35	1SJ20CS034	-
36	1SJ20CS035	37

Sl NO.	USN	18CS744
37	1SJ20CS036	-
38	1SJ20CS037	39
39	1SJ20CS038	37
40	1SJ20CS039	-
41	1SJ20CS040	-
42	1SJ20CS041	36
43	1SJ20CS042	40
44	1SJ20CS043	27
45	1SJ20CS044	31
46	1SJ20CS045	34
47	1SJ20CS046	39
48	1SJ20CS047	39
49	1SJ20CS048	35
50	1SJ20CS049	-
51	1SJ20CS050	-
52	1SJ20CS051	36
53	1SJ20CS052	32
54	1SJ20CS053	38
55	1SJ20CS054	40
56	1SJ20CS055	-
57	1SJ20CS056	36
58	1SJ20CS057	40
59	1SJ20CS058	32
60	1SJ20CS059	-
61	1SJ20CS060	39
62	1SJ20CS061	37
63	1SJ20CS062	32
64	1SJ20CS063	35
65	1SJ20CS064	-
66	1SJ20CS065	40
67	1SJ20CS066	33
68	1SJ20CS067	-
69	1SJ20CS068	-
70	1SJ20CS069	-
71	1SJ20CS070	40
72	1SJ20CS071	39
73	1SJ20CS072	40
74	1SJ20CS073	-
75	1SJ20CS074	40

Sl NO.	USN	18CS744
76	1SJ20CS075	40
77	1SJ20CS076	26
78	1SJ20CS077	37
79	1SJ20CS078	35
80	1SJ20CS079	-
81	1SJ20CS080	35
82	1SJ20CS081	39
83	1SJ20CS082	33
84	1SJ20CS083	40
85	1SJ20CS084	22
86	1SJ20CS085	40
87	1SJ20CS086	-
88	1SJ20CS087	35
89	1SJ20CS088	40
90	1SJ20CS089	40
91	1SJ20CS090	-
92	1SJ20CS091	40
93	1SJ20CS092	40
94	1SJ20CS094	40
95	1SJ20CS095	32
96	1SJ20CS096	40
97	1SJ20CS097	39
98	1SJ20CS098	40
99	1SJ20CS099	39
100	1SJ20CS101	-
101	1SJ20CS102	35
102	1SJ20CS103	-
103	1SJ20CS104	30
104	1SJ20CS105	20
105	1SJ20CS106	40
106	1SJ20CS108	33
107	1SJ20CS109	-
108	1SJ20CS110	30
109	1SJ20CS111	40
110	1SJ20CS113	40
111	1SJ20CS114	40
112	1SJ20CS115	-
113	1SJ20CS116	36
114	1SJ20CS117	29

Sl NO.	USN	18CS744
115	1SJ20CS118	34
116	1SJ20CS119	24
117	1SJ20CS120	40
118	1SJ20CS121	38
119	1SJ20CS122	40
120	1SJ20CS123	31
121	1SJ20CS124	28
122	1SJ20CS125	39
123	1SJ20CS126	39
124	1SJ20CS127	38
125	1SJ20CS128	38
126	1SJ20CS129	-
127	1SJ20CS130	37
128	1SJ20CS131	40
129	1SJ20CS132	20
130	1SJ20CS133	34
131	1SJ20CS134	39
132	1SJ20CS136	39
133	1SJ20CS137	40
134	1SJ20CS138	32
135	1SJ20CS139	37
136	1SJ20CS140	37
137	1SJ20CS141	35
138	1SJ20CS142	36
139	1SJ20CS143	40
140	1SJ20CS144	40
141	1SJ20CS145	40
142	1SJ20CS146	34
143	1SJ20CS147	40
144	1SJ20CS148	35
145	1SJ20CS149	30
146	1SJ20CS150	-
147	1SJ20CS151	38
148	1SJ20CS152	40
149	1SJ20CS153	39
150	1SJ20CS154	38
151	1SJ20CS155	32
152	1SJ20CS156	39
153	1SJ20CS157	-

Sl NO.	USN	18CS744
154	1SJ20CS158	39
155	1SJ20CS159	40
156	1SJ20CS160	40
157	1SJ20CS161	40
158	1SJ20CS162	39
159	1SJ20CS163	40
160	1SJ20CS164	40
161	1SJ20CS165	38
162	1SJ20CS167	-
163	1SJ20CS168	28
164	1SJ20CS169	38
165	1SJ20CS170	39
166	1SJ20CS171	27
167	1SJ20CS172	38
168	1SJ20CS173	31
169	1SJ20CS174	40
170	1SJ20CS175	32
171	1SJ20CS176	40
172	1SJ20CS177	37
173	1SJ20CS178	34
174	1SJ20CS179	25
175	1SJ21CS400	32
176	1SJ21CS401	32
177	1SJ21CS402	24
178	1SJ21CS403	29
179	1SJ21CS404	37
180	1SJ21CS405	-
181	1SJ21CS406	37
182	1SJ21CS407	21
183	1SJ21CS408	-
184	1SJ21CS409	27
185	1SJ21CS410	-
186	1SJ21CS411	-
187	1SJ21CS412	-
188	1SJ21CS413	37
189	1SJ21CS414	35
190	1SJ21CS415	39
191	1SJ21CS416	38

19/1/24

19/1/24