2.1 Establish the correlation between the courses and the Program Outcomes (POs) and Program Specific Outcomes (PSOs) (15)

(Program Outcomes as mentioned in Annexure I and Program Specific Outcomes as defined by the Program)

- **Program Outcomes (POs):**

PO-1: Adequate knowledge of fundamentals of Information Security

PO-2: Ability to analyze a problem critically using scientific approach, relevant tools and techniques

PO-3: Appropriate research skills for exploring a new problem and solving it in best possible way

PO-4: Ability to work ethically and carry out the work with social responsibility

PO-5: Ability of life-long and continuous self learning

PO-6: Ability to carry out collaborative and multidisciplinary work in a professional environment

PO-7: Ability to identify strengths and weaknesses and continuously strive to improve oneself

- **Program Specific Outcomes (PSOs):**

PSO1: Students will be able to develop secure applications

PSO2: Students will be able to use tools and technologies in the field of information security

2.1.1 Course Outcomes (COs) (05)

After finalizing the structure and course names, COs are formulated by a faculty or the group of expert faculties for all of the courses. These COs are then discussed in DPPC. After that their mapping is carried out with POs. Entire CO-PO mapping is discussed and approved by DPPC and BoS.

The table shown below gives the course outcomes of the courses in the program curriculum for the year 2016-19.

Probability, Statistics and Queuing Theory	
CO 1	Demonstrate understanding of fundamental concepts in probability, statistics and queuing theory.
CO 2	Solve various problems on probability, statistics and queuing theory.
CO 3	Analyze the given probabilistic model of the problem.
CO 4	Use the techniques studied in probability, statistics and queuing theory to solve problems in domains such as data mining, machine learning, network analysis.
Foundation of Cryptography	
CO 1	Demonstrate an Understanding of modern concepts related to cryptography and cryptanalysis
CO 2	Analyze and use methods for cryptography and reflect about limits and applicability of these
CO 3	Reason about the details and design philosophy of modern symmetric and public key systems

CO 4	Have a better appreciation of the uses and limitations of the various categories of cryptographic algorithms and understand that great care is needed in their selection and use.
CO 5	Reason that security is a systems problem, and that technical methods such as cryptography can only form part of the solution
Information Theory and Coding	
CO 1	Demonstrate knowledge of information and entropy, and their use in information theory
CO 2	Demonstrate knowledge of principles data compression
CO 3	Demonstrate an Understanding of techniques of design and performance evaluation of error correcting codes
CO 4	Design and develop solutions for technical issues related to information coding
CO 5	Discuss emerging topics in information theory, coding and compression.
Network Security	
CO 1	Understand security issues related to networking vulnerabilities, firewalls, intrusion detection
CO 2	Identify infrastructure components including devices, topologies, protocols, systems software, management and security
CO 3	Design and develop solutions for technical issues related to networking and security problems.
CO 4	Apply footprinting, scanning, enumeration and similar techniques to discover network and system vulnerabilities
Wireless and Mobile Security	
CO 1	Demonstrate knowledge of security and privacy topics in wireless and mobile networking
CO 2	Understand the security and privacy problems in the realm of wireless networks and mobile computing
CO 3	Apply proactive and defensive measures to counter potential threats, attacks and intrusions
CO 4	Analyze the various categories of threats, vulnerabilities, countermeasures in the area of
CO 5	Design secured wireless and mobile networks that optimize accessibility whilst minimizing vulnerability to security risks
CO 6	Research in the field of mobile and wireless security and privacy
Machine Learning	
CO 1	Design hypothesis model for any real-life problems.
CO 2	Apply linear regression, logistic regression and regularization to any machine learning problem.
CO 3	Apply learning techniques like decision tress, bayesian theory, clustering, SVM, ANN,etc., to solve a real-life problem.
CO 4	Evaluate and perform diagnoses of any machine learning system.
CO 5	Apply learned machine learning techniques to Information security domains

Table 2.1.1 Course outcomes of the courses in the program curriculum for the year 2016-19

2.1.2 COs-POs/PSOs matrices of courses selected in 2.1 (05)

Explanation of table to be ascertained The Mapping Level Contribution between COs-POs/PSOs are Categorized as follows:

3: High, 2: Medium, 1: Low, - : No correlation

Probability, Statistics and Queuing Theory									
COs	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PSO1**	**PSO2**
CO 1	3	0	1	0	1	0	0	1	0
CO 2	3	2	1	0	1	0	0	1	0
CO 3	3	3	2	0	1	0	0	1	0
CO 4	3	3	3	0	1	0	0	1	0
Average	3	2	1.8	0	1	0	0	1	0
Foundation of Cryptography									
COs	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PSO1**	**PSO2**
CO 1	3	2	1	1	1	0	0	1	0
CO 2	1	3	3	1	1	0	0	1	1
CO 3	1	2	3	1	1	0	0	1	0
CO 4	1	3	3	1	1	0	0	1	0
CO 5	0	2	2	0	0	0	0	1	0
Average	1.2	2.4	2.4	0.8	0.8	0	0	1	0.2
Information Theory and Coding									
COs	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PSO1**	**PSO2**
CO 1	3	1	1	0	0	0	0	1	-
CO 2	3	1	1	0	0	0	0	1	1
CO 3	3	1	1	0	0	0	0	1	-
CO 4	0	3	3	0	0	0	0	1	-
CO 5	0	1	1	0	3	0	0	1	1
Average	1.8	1.4	1.4	0	0.6	0	0	1	0.4
Network Security									
COs	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PSO1**	**PSO2**
CO 1	3	3	2	0	0	0	0	1	1
CO 2	2	2	2	0	0	0	0	1	1
CO 3	2	2	2	0	1	0	0	1	2
CO 4	3	3	2	0	1	0	0	1	2
Average	2.5	2.5	2	0	0.5	0	0	1	1.5
Wireless and Mobile Security									
COs	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PSO1**	**PSO2**
CO 1	3	2	2	1	0	0	0	1	1
CO 2	2	3	1	0	0	0	0	1	1

CO 3	2	3	2	1	1	0	0	1	1
CO 4	2	3	2	1	1	0	0	1	1
CO 5	2	3	2	0	1	0	0	1	1
CO 6	1	1	3	0	2	0	0	1	1
Average	2	2.5	2	0.5	1.3	0	0	1	1
Machine Learning									
COs	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PSO1**	**PSO2**
CO 1	0	3	2	0	1	0	0	1	1
CO 2	2	3	2	0	1	0	0	1	1
CO 3	2	3	3	0	1	0	0	1	1
CO 4	2	3	3	0	1	0	0	1	2
CO 5	2	3	3	0	1	0	0	1	2
Average	2	3	3	0	1	0	0	1	1.4

Table 2.1.2 COs-POs/PSOs matrices

Note:

1. Enter correlation levels 1, 2 or 3 as defined below:

1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High) It there is no correlation, put "-"

2.1.3 Program level Course-PO/PSOs Matrix of all Courses INCLUDING First year courses (05)

Sr. No.	Course Type	Course Code	Course Name
Semester I			
1	PSMC	IS-16001	Probability, Statistics and Queuing Theory
2	PSBC	IS-16002	Foundation of Cryptography
3	PCC	IS-16003	Advanced Operating System
4	PCC	IS-16004	Information Theory and Coding
5	DEC	IS(DE)-16003	Machine Learning
6	MLC	ML-16011	Research Methodology
7	MLC	ML-190	Humanities
8	LC	IS-16005	Security Lab
Semester II			
9	PCC	IS-16006	Network Security
10	PCC	IS-16007	Applied Cyber Security
11	DEC	IS(DE)-16004	Advanced Database and Information Retrieval
12	DEC	IS(DE)-16005	Cloud Computing and Security
13	DEC	IS(DE)-16007	Internet of Things
14	DEC	IS(DE)-16008	Web Systems &Technology
15	SLC	IS(DE)-18004	MOOC (Massive Open Online Course)

16	LC	IS-16009	Mini Project/Case study
17	MLC	MLC-16006	Intellectual Property Rights
18	LLC	LL-15001	Liberal Learning Course
Semester III			
19	Dissertation	IS-17002	Dissertation Phase I
Semester IV			
20	Dissertation	IS-17003	Dissertation Phase II

Table 2.1.3(a) List of Courses

Program level Course-Program Outcome (POs) matrix and Program Specific Outcomes (PSOs) of all courses for the above listed courses are given in the Table 2.1.3(b)

Mapping Matrix									
Course Code	**CO vs PO**							**CO vs PSO**	
	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PSO1**	**PSO2**
IS-16001	3	2	1.8	0	1	0	0	1	0
IS-16002	1.2	2.4	2.4	0.8	0.8	0	0	1	0.2
IS-16003	2.7	2.7	2	0	0.7	0	0	1	0.3
IS-16004	1.8	1.4	1.4	0	0.6	0	0	1	0.4
IS(DE)-16003	1.6	3	2.6	0	1	0	0	1	1.4
MLC-16011	0	1	2.7	0.5	2	0.5	0.2	1	0.2
MLC-190	0	0	0	2	1	1.2	0.4	0.2	0
IS-16005	1	2	0.5	0.3	1	1	1	2	2
IS-16006	2.5	2.5	2	0	0.5	0	0	1	1.5
IS-16007	1.6	1.6	1.2	2	0.4	0.4	0	2	1.4
IS(DE)-16004	1.5	1.5	1.7	0	0.8	0	0	1	0.3
IS(DE)-16005	1.8	2	1.5	0.3	0.8	0	0	1	0.8
IS(DE)-16007	2	2	2	0	2	0	0	0.8	1
IS(DE)-16008	2.4	2.2	1.4	0	0.4	0	0	1	1
IS(DE)-18004	2	2	2	0.3	1	0	0	1	1.7
IS-16009	1	2.3	1	1.5	0.8	0	1	1.5	2.3
MLC-16006	1	1	2	2	1	0	0	0	0.3
LL-15001	0	0	0	0	2	0	2	0	0
IS-17002	1	1.6	3	0.4	2.6	2.2	2	0	0.2
IS-17003	0.8	1.4	2.4	1.2	2	2.4	1.6	1	1

Table 2.1.3(b)

Note:

1. Enter Correlation Levels 1, 2 or 3 as defined below:

   1**: Slight (Low) 2: Moderate (Medium) 3: Substantial (High) If there is No Correlation, put "-"**

   It may be noted that contents of Table B.3.1.2 must be consistent with information availablein Table B.3.1.3 for all the courses.

2. Similar Table is to be prepared for PSOs

2.2. Attainment of Course Outcomes (60)

2.2.1. Describe the assessment processes used to gather the data upon which the evaluation of Course Outcome is based (20)

(Examples of data collection processes may include, but are not limited to, specific exam/tutorial questions, assignments, laboratory tests, project evaluation, student portfolios (A portfolio is a collection of artifacts that demonstrate skills, personal characteristics and accomplishments created by the student during study period), internally developed assessment exams, project presentations, oral exams etc.)

2.2.1.1. List of assessment processes:

Assessment Mechanism	Assessment Criteria	Frequency of Data	Relevance
End semester examination for each course	Average weighted performance of passed students	Once in a semester. At the end of semester	Used for CO calculations
Course feedback for all courses (theory as well as laboratory)	Average feedback of for each CO from all students who attended the course.	Once in a semester. At the end of semester	Used for CO calculations
Laboratory evaluation for each laboratory course	Average weighted performance of passed students	Once in a semester. At the end of semester	Used for CO calculations
Project work-external evaluation	Average weighted performance of passed students	Once in a year	Used for CO calculations

Table 2.2.1(a) Assessment processes

2.2.1.2. The Quality /relevance of assessment processes & tools used:

- **Quality assessment for theory courses:**
  - The examinations are conducted by the institute level exam cell as per the academic calendar published at the beginning of the academic year.
  - The department nominates a faculty as DCE (Department Controller of Examination) to help the exam cell for smooth conduction of the examinations.
  - The DCE prepares a list of external experts (from industry or academics) for paper setting and lab/project evaluation.
  - The DCE sends mails to the internal faculty member who conducted a particular theory course as well as an expert for the same course for submitting the question papers for the end semester examination.
  - The papers set by internal faculty members are reviewed by other faculty members to ensure correctness, appropriate coverage and desired quality of the question paper.
  - It is the prerogative of the exam cell to choose one of the papers from the two question papers,

where one is from the internal faculty and one is from the external expert, for the final examination.

- The evaluated answer sheets of the internal as well as end semester examinations are shown to the students so that students are convinced about fair evaluation.
- The course-in-charge faculty member decides the grade ranges and comes up with the grade distribution (how many students in each grade etc). A departmental committee, DPPC (Department Post-Graduate Program Committee) may suggest changes in the grade ranges and distribution so that there is no bias in grading. After approval from the DPPC, marks and grade ranges are entered in the central MIS. The MIS team is responsible for generation and publishing the result.

➢ **Quality assessment of laboratory courses:**

- A list of laboratory assignments for each laboratory course is prepared at the time of curriculum revision by the course-in-charge faculty member(s). The assignments are discussed and deliberated in curriculum revision meetings attended by external experts. After the assignments are finalized, they are published as part of the curriculum document available on the college site. It is ensured that the assignments are related to the contents of the related theory courses and would make students apply theory to solve real life problems.
- The faculty members are supposed to use the list available as part of the curriculum as a guideline and update the assignments if needed.
- The instructor evaluates the assignments periodically and keeps a record of the performance of each student.
- The final evaluation is done at the end of the semester by calling an external expert.
- The grading strategy is same as the one used for theory courses and is described above.

➢ **Quality assessment of completed projects/prototype:**

- An internal panel evaluates the project 3 months ahead of the tentative final evaluation to check readiness. Students are given suggestions for remaining tasks in their projects, contents of the report and final presentation.
- The departmental project co-ordinators publish a standard report template which students are expected to use to maintain uniformity in reports.
- Students are expected to submit a plagiarism report generated by using some standard tool along with the soft copy of the report. The project guide accepts the report only if the similarity index is below the acceptable threshold.
- The departmental project co-ordinators decide the external expert depending upon the domain of

the project for external evaluation and share the project report with the expert well in advance before the final evaluation.

- In the final evaluation, the external expert evaluates the project on various accounts such as quality of literature survey, the scientific/technical challenges involved in the chosen project topic, quality of design and implantation of the proposed solution, quality of the project report and project presentation.
- The expert gives marks in consultation with the internal project guide which later get converted to appropriate grades.

➢ **Intermediate Evaluation/Examinations:**

- For theory courses, two tests of 20 marks each are conducted before the end semester examination. The end semester examination carries 60% weightage.
- For laboratory courses, the instructor evaluates assignments from time to time.
- For project work, a pre-final evaluation is done by a panel of faculty members to decide readiness of the project work for final evaluation.
- The marks obtained in the intermediate evaluation/examinations contribute to the aggregate score which is used in deciding the final grade of a student in the course.
- For every course relative grading is in practice.

Grade Ranges	Grade Points	Letter Grade
Grade ranges are decided by DPPC and vary from time to time and course to course as relative grading is in practice	10	AA
	9	AB
	8	BB
	7	BC
	6	CC
	5	CD
	4	DD
	0	FF

Table 2.2.1(b) Grade Point Range

2.2.2 Course Outcome Assessment Procedure (40)

The procedure is explained with an example subject from the curriculum. This procedure is to be carried out for all theory courses.

Subject Name: Foundation of Cryptography

I. Course Outcomes:

CO Number	CO Description
CO-1	Demonstrate an understanding of modern concepts related to cryptography and cryptanalysis
CO-2	Analyze and use methods for cryptography and reflect about limits and applicability of these methods
CO-3	Reason about the details and design philosophy of modern symmetric and public key systems
CO-4	Have a better appreciation of the uses and limitations of the various categories of cryptographic algorithms and understand that great care is needed in their selection and use
CO-5	Reason that security is a systems problem, and that technical methods such as cryptography can only form part of the solution

Table 2.2.2(a) CO Table

II. CO to PO Mapping:

CO List	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6	PO-7	PSO1	PSO2
CO-1	3	2	1	1	1	-	-	1	-
CO-2	1	3	3	1	1	-	-	1	1
CO-3	1	2	3	1	1	-	-	1	-
CO-4	1	3	3	1	1	-	-	1	-
CO-5	-	2	2	-	-	-	-	1	-

Table 2.2.2(b) CO-PO Mapping

Attainment Levels:

1- Partially **2- Moderately** **3 - Fully**

III. CO Assessment Tools:

Two Factors considered

1. **Direct:**
   1. Result from MIS
   2. ESE Questions to CO mapping
2. **Indirect:**
   1. Course Exit Survey

Procedure followed for getting Course Outcome attainment

CO = I*0.3+ R*0.5 + Q*0.2

Where,

I – Course Exit Survey (Indirect)
R – Result from MIS (Direct)
Q – Questions to CO mapping (Direct)

I - Course Exit Survey (Indirect)

Following survey form is used for collecting the feedback from students for each of the COs.

M. Tech (Computer Engineering: Information Security) Year 2018-19

Exit Survey for Course Outcome Attainment
Following questionnaire is provided to get your feedback on attainment of course outcomes for all the courses you studied during your first year of M.Tech. Below every subject name, the expected outcomes are listed. For each outcome you have to rate to what extent the outcome was achieved on the scale of 1 to 5 as below:

1. <= 10%
2. >10% and <= 40%,
3. >40% and <= 60%,
4. >60% and <=90%,
5. >90% and <=100%

* Required

1. **MIS Number** *

_____

1. Foundations of Cryptography

2. **CO-1: Demonstrate an Understanding of modern concepts related to cryptography and cryptanalysis** *
   Mark only one oval.
   - ◯ 1
   - ◯ 2
   - ◯ 3
   - ◯ 4
   - ◯ 5

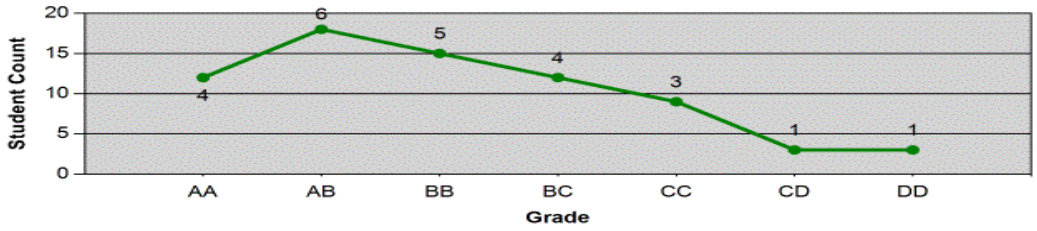
3. **CO-2: Analyze and use methods for cryptography and reflect about limits and applicability of these** *
   Mark only one oval.
   - ◯ 1
   - ◯ 2
   - ◯ 3
   - ◯ 4
   - ◯ 5

R – Result from MIS (Direct)

R: Direct from MIS Result Report Sample calculation:

You will get AVG GP from MIS (last page of Result)

R = Sum (Grade Point * Number of Students) / Total Number of Students * 100



Subject Grade Range

Start Range	End Range	Grade	Grade Point
74	100	AA	10
61	73	AB	9
53	60	BB	8
47	52	BC	7
41	46	CC	6
35	40	CD	5
31	34	DD	4
0	30	FF	0

HOD
Signature

Signature
Vinod Keshaorao Pachghare

Values of R will be common to all COs of your subjects

Grade Point	No. of Students	Total Grade Points
10	4	40
9	6	54
8	5	40
7	4	28
6	3	18
5	1	5
4	1	4
Average		**78.75**

Q - From Question wise marks

Sample Question Paper: Foundation of Cryptograhpy

COLLEGE OF ENGINEERING PUNE

(An Autonomous Institute of Govt. of Maharashtra)

END SEM - EXAMINATION

(IS-16002) Foundation of Cryptography

Course: **M.Tech (Information Security, Semester-I,**

Academic Year: 2017-18 Date:06/12/2017

Duration: 3 hr. Max. Marks: 60.

Student MIS No.:

Instructions:

1. **All Questions are Compulsory.**
2. **Make appropriate assumptions wherever necessary.**
3. **Figures to the right indicate the full marks.**
4. **Mobile phones and programmable calculators are strictly prohibited.**
5. **Writing anything on question paper is not allowed.**
6. **Exchange/Sharing of stationery, calculator etc. not allowed.**
7. **Write your PRN Number on Question Paper.**

			Marks	COs
Q.1.	**a)**	Suppose the cryptanalyst has learned that n = 84773093 and Φ(n)=84754668. Find out the two factors of n.	**[6]**	**CO-3**
	b)	Explain following terms with respect to security with required countermeasures. 1. Confidentiality 2. Integrity 3. Authentication	**[6]**	**CO-1**
Q.2.	**(a)**	Find at least three different numbers n between 15 to 30 such that φ(n) = 12.	**[3]**	**CO-3**
	(b)	Use Chinese Reminder theorem and Find all solutions of $x^3 - x + 1 \equiv 0 \pmod{35}$.	**[3]**	**CO-3**
	(c)	Find the last 2 digits of $(7^7)^{1000}$.	**[3]**	**CO-3**
	(d)	Find integers p, and q such that 2322p + 654q = 6 and also find the GCD(2322, 654).	**[3]**	**CO-3**

Q.3. **(a)** We use the Diffie-Hellman Key exchange with private keys X and Y and public keys $Z_1 = a^X \bmod p$ and $Z_2 = a^Y \bmod p$. We assume $p = 71$ and $a = 7$. **[6]** **CO-5**

1) Give two possible pairs (X; Y) such that the common key $K = 1$.
2) An attacker knows that the product $Z_1 * Z_2 = 7 \bmod p$. Give two possible pairs (X; Y) that satisfy the attackers knowledge.

OR

(b) chosen plaintext attack is on Hill Cipher with $P = C = Z^2_7$. Suppose the plaintext be "ESSENTIALA" and the message is encoded using: E = 0, S = 1, N = 2, T = 3, I = 4, A = 5 and L = 6. The ciphertext is "TNSLIIALEI". Find the key used in this cipher. **[6]** **CO-4**

(c) Compare and contrast the Electronic Cook Book (ECB) and Ciphertext Block Chaining (CBC) modes of operation for block ciphers with respect to the following (use diagrams if necessary): **[6]** **CO-1**

- Encryption
- Decryption
- Error propagation
- Detection of deleted ciphertext blocks
- Potential for repeated ciphertext blocks

Q.4 **(a)** Explain the significance of padding in Message Digest 5 (MD5). Explain how padding is done in MD5 with proper example. If the message size is 786, how many numbers of bits are required for padding this message? Justify your answer. **[6]** **CO-5**

(b) Explain Differential cryptanalysis and Linear Cryptanalysis of DES algorithm. **[6]** **CO-2**

OR

(c) Write a short note on Bitcoin cryptocurrency. **[6]** **CO-1**

Q.5. **(a)** The output of the shift row step fig (1-a) and the state matrix fig (1-b) of AES are as given below **[9]** **CO-2**

$$\begin{bmatrix} 62 & 74 & d3 & 59 \\ 83 & 74 & c6 & 4d \\ 5e & 5d & 88 & e6 \\ 8f & cf & fc & 2d \end{bmatrix}$$

Output of the shift row

Fig. 1 (a)

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

State Matrix

Fig. 1 (b)

Find the output of the mix column step of AES. [Only first two rows are expected]

(b) Fill the following table. **[3]** **CO-1**

Sr. No.	Name of the Algorithm	Key Length	Number of Rounds
1.	DES		
2.	Simplified IDEA		
3.	AES		

OR

Q.5. **(a)** Use RSA algorithm to encrypt the message M = 9726. The parameters given are: n = 11413, e = 3533. Also find out the value of d, the decryption exponent. **[6]** **CO-3**

(b) Generate the key for decryption from the following encryption key for IDEA algorithm. **[6]** **CO-2**

Key: 10101001110111110110010111000011

Table 2.2.2(c) CO Mapping from Question Paper

IV. Student Semester Result:

Sr. No.	MIS No.	Name of Student	Q-1	Q-2	Q-3	Q-4	Q-5
1	121742001	BHATTI BHAKTI RAVINDRA	5	6	1	6	3
2	121742002	BHIRUD BHAGYASHRI PURUSHOTTAM	5	9	6	10	5
3	121742003	CHAUDHARI GANESH RAMDAS	3	4	6	10	3
4	121742004	CHOUDHARI AYESHA RASOOL SAB	3	6	1	10	5
5	121742005	DEVYANI GURJAR	12	9	3	10	11
6	121742006	EKBOTE ONKAR ARUN	9	9	6	12	5
7	121742007	GUNDLA SUSHANT SUDARSHAN	6	9	0	10	7
8	121742008	HINGASPURE PRASHIK PUNDLIKRAO	6	9	1	9	3
9	121742009	JADE SHEETAL GAUTAM	2	5	2	7	1
10	121742010	JOSHI ANIRUDDHA NARENDRA	5	0	2	12	5
11	121742011	JUHI NAZISH	3	5	2	8	1
12	121742012	KHYADGI POOJA LAXMAN	6	8	0	12	3
13	121742013	NIPANIKAR MAYUR PANDURANG	4	5	6	10	0
14	121742014	PALAK AGRAWAL	6	8	12	12	9
15	121742015	PATIL ANUJA ASHOK	6	1	0	7	3
16	121742016	PRAPTI D KOLPE	3	3	1	8	6
17	121742017	SHAIKH VIKAR ANSAR	5	8	2	10	3
18	121742018	SHIVADE SHUBHAM MURLIDHAR	6	1	1	10	2
19	121742019	SHREYA BRAHMANAND TIWARI	4	5	12	12	3
20	121742020	SHRUTI SATISH KULKARNI	11	6	2	12	8
21	121742021	SONAR AKSHAY GOVARDHANRAO	5	4	5	6	5
22	121742022	TEJAS KHAJANCHEE	2	9	6	12	5
23	121742023	THAKURDESAI HRISHIKESH MANOHAR	4	5	10	12	4
24	121742024	VRUSHALI PANZADE	3	6	10	10	2
		AVG	**5.16**	**5.8**	**4.04**	**9.9**	**4.3**
		AVG	**43.05**	**51.38**	**33.68**	**82.29**	**35.41**

V. Question average Calculations

Q1- AVG = ∑ Marks In Column 1 * 100/ (Total No of Students * Percent Max Marks Of Q1)

= (124) *100/ (24*12) = 43.05

Q2- AVG = ∑ Marks In Column 2 * 100/ (Total No of Students * Max Marks Of Q2)

= (148) *100/ (24*12) = 51.38

Q3- AVG = ∑ Marks In Column 1 * 100/ (Total No of Students * Percent Max Marks Of Q1)

= (97) *100/ (24*12) = 33.68

Q4- AVG = ∑ Marks In Column 1 * 100/ (Total No of Students * Percent Max Marks Of Q1)

= (237) *100/ (24*12) = 82.29

Q5- AVG = ∑ Marks In Column 1 * 100/ (Total No of Students * Percent Max Marks Of Q1)

= (102) *100/ (24*12) = 35.41

VI. CO-Question Mapping Table with its calculations

CO-1	CO-2	CO-3	CO-4	CO-5
Q-1,Q-3, Q-4, Q.5	Q-4, Q.5	Q-1, Q-2, Q-5	Q.-3	Q-3, Q.4
48.6075	58.85	43.28	33.68	57.985

VII. Final Calculations:

Use below formula to calculate the final CO values for all the COs and submit it to the department.

CO = R*0.5+ Q*0.3 + I*0.2

VIII. Rubric for CO Attainment:

Following formula is used for the calculation of average CO-attainment:

CO-Attainment = 0.5 * R + 0.3 * Q + 0.2 * I

R: Weighted average grade of passed students converted to percentile score

Q: Average marks obtained for all the questions which correspond to a CO

I: The rating given by students for the fulfilment of a CO as part of the course-exit survey.

IX. Final CO Attainment for the course Foundations of Cryptography:

COs	R	R x 0.5	Q	Q x 0.3	I (Feedback)	I x 0.2	Final CO = R*0.5
CO 1	78.75	39.38	48.6075	14.58	84.2	16.84	**70.8**
CO 2	78.75	39.38	58.85	17.66	85	17	**74.04**
CO 3	78.75	39.38	43.28	12.98	83.4	16.68	**69.04**
CO 4	78.75	39.38	33.68	10.1	87.6	17.52	**67**
CO 5	78.75	39.38	57.985	17.4	85.8	17.16	**73.94**

2.2.3. Record the attainment of Course Outcomes of all courses with respect to set attainmentlevels (40)

Verify the attainment levels as per the benchmark set for all courses Program shall have set Course Outcome attainment levels for all courses (The attainment levels shall be set considering average performance levels in the university examination or any higher value set as target for the assessment years. Attainment level is to be measured in terms of student performance in internal assessments with respect to the Course Outcomes of a course in addition to the performance in the University examination) Measuring Course Outcomes attained through University Examinations Target may be stated in terms of percentage of students getting more than the university average marks or more as selected by the Program in the final examination. For cases where the university does not provide useful indicators like average or median marks etc., the program may choose an attainment level on its own with justification. The attainment of Course Outcomes of all courses is shown in the table.2.2.2(b) and (a) sample for the course Foundations of Cryptography is described in Table 2.2.2(a):

COs Attainment for all the subjects during the academic year 2018-19

Sr. No.	Subject Code	COs	% of COs Attainment
1	IS-16001	CO 1	65.78
		CO 2	66.92
		CO 3	62.19
		CO 4	59.2
2	IS-16002	CO 1	71.48
		CO 2	69.92
		CO 3	68.18
		CO 4	65.72
		CO 5	66.32
3	IS-16003	CO 1	79.5
		CO 2	72.3
		CO 3	70.42
4	IS-16004	CO 1	73.25
		CO 2	75.22
		CO 3	74.24
		CO 4	71.33
		CO 5	73.11
5	IS(DE)-16003	CO 1	74.08
		CO 2	74.61
		CO 3	76.32
		CO 4	72.96
		CO 5	71.53
6	IS-16005	CO 1	85.18
		CO 2	84.66
		CO 3	85.50
		CO 4	85.66
7	IS-16006	CO 1	80.4

		CO 2	81.9
		CO 3	78.9
		CO 4	81.6
8	IS-16007	CO 1	70.48
		CO 2	69.58
		CO 3	70.98
		CO 4	70.17
		CO 5	70.39
9	IS(DE)-16004	CO 1	75.68
		CO 2	67.48
		CO 3	75.08
		CO 4	76.68
		CO 5	71.68
		CO 6	80.48
10	IS(DE)-16005	CO 1	Not offered
		CO 2	
		CO 3	
		CO 4	
11	IS(DE)-16007	CO 1	79.85
		CO 2	77.19
		CO 3	64.28
		CO 4	68.27
12	IS(DE)-16008	CO 1	Not offered
		CO 2	
		CO 3	
		CO 4	
		CO 5	
13	IS(DE)-18004	CO 1	81.4
		CO 2	79
		CO 3	81.8
14	IS-16009	CO 1	83.18
		CO 2	82.34
		CO 3	84.18
		CO 4	83.34
15	IS-17002	CO 1	88.71
		CO 2	90.79
		CO 3	88.87
		CO 4	88.51
		CO 5	88.87
16	IS-17003	CO 1	83.52
		CO 2	82.88
		CO 3	83.52
		CO 4	84.48
		CO 5	84.80

Table 2.2.3a COs Attainment for all the course