Name of Institute: Indus Institute of Technology & Engineering
Name of Faculty: Roshni Patel

Course code:
Course name: Cryptography and Network Security
Pre-requisites: General ease with algorithms and elementary probability theory, maturity with mathematical proofs.
Credit points: 4
Offered Semester: VII

Course coordinator (weeks 01 - 15)
Full name: Roshni V Patel
Department with sitting location: Department of Computer Engineering (4th Floor Faculty Room, Bhanvar Building)
Email: roshnipatel.ce@indusuni.ac.in
Consultation times: 3:00 to 4:30 pm

Students will be contacted throughout the session via mail with important information relating to this course.

Course Objectives
By participating in and understanding all facets of this course a student will:

1. To know the methods of conventional encryption.
2. To understand and be critically aware of security threats and the available security mechanisms for combating security breaches.
3. To Critically discuss and understand the concepts of authentication and authorization, intrusion detection and information security techniques.
4. To know the network security tools and applications and also to understand the system level security used.

Course Outcomes (CO)
On successful completion of this subject content, the student should:
CO 1: Basics of Cryptography and Network Security.
CO 2: Illustrate various Public key cryptographic techniques.
CO3: Evaluate the authentication and hash algorithms along with authentication applications.
CO 4: Summarize the intrusion detection and its solutions to overcome the attacks.
CO 5: To understand various protocols for network security to protect against the threats in the networks.
CO 6: Basic concepts of system level security.

Course Outline
Cryptographic algorithm, Hashing, authentication, authorization, intrusion detection.

Method of delivery

1. Chalk & Talk
2. PPT presentation

Study time

Lectures: 3 hours
Practical : 2 hours
Total: 5 hours/week

CO-PO Mapping (PO: Program Outcomes)

Course Outcome	Program Outcomes											
CO	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**
C0 1	3	-	2	-	2	2	2	3	2	-	1	-
C0 2	2	1	3	-	-	-	3	-	1	3	-	-
C0 3	2	3	2	2	-	-	2	2	2	-	3	-
C0 4	2	3	3	-	2	-	-	-	2	-	2	-
C0 5	-	2	-	-	2	2	2	-	2	-	-	-
C0 6	-	-	-	-	2	3	2	-	-	-	-	-
CE0705	**2.25**	**2.25**	**2.5**	**2**	**2**	**2.3**	**2.2**	**2.5**	**1.8**	**3**	**2**	**0**

Blooms Taxonomy and Knowledge retention (For reference)

(Blooms taxonomy has been given for reference)

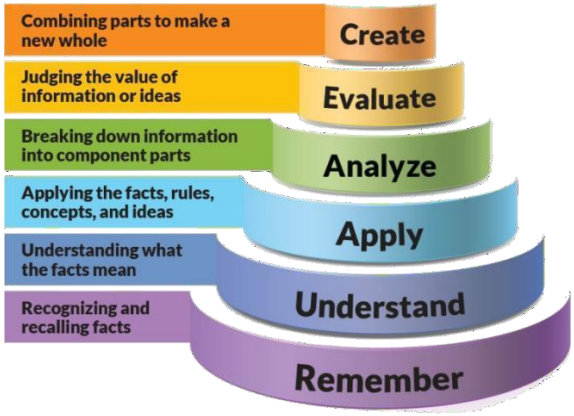


Figure 1: Blooms Taxonomy

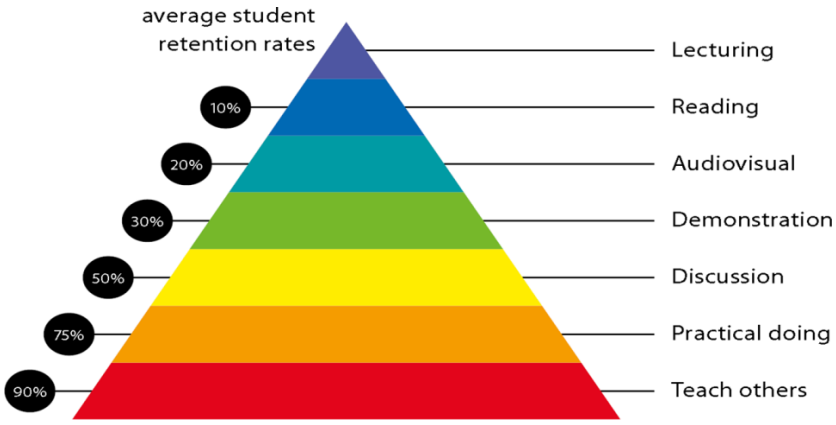


Figure 2: Knowledge retention

Graduate Qualities and Capabilities covered

(Qualities graduates harness crediting this Course)

General Graduate Qualities	Specific Department of Computer Graduate Capabilities
Informed Have a sound knowledge of an area of study or profession and understand its current issues, locally and internationally. Know how to apply this knowledge. Understand how an area of study has developed and how it relates to other areas.	**1 Professional knowledge, grounding & awareness**
Independent learners Engage with new ideas and ways of thinking and critically analyze issues. Seek to extend knowledge through ongoing research, enquiry and reflection. Find and evaluate information, using a variety of sources and technologies. Acknowledge the work and ideas of others.	**2 Information literacy, gathering & processing**
Problem solvers Take on challenges and opportunities. Apply creative, logical and critical thinking skills to respond effectively. Make and implement decisions. Be flexible, thorough, innovative and aim for high standards.	**4 Problem solving skills**
Effective communicators Articulate ideas and convey them effectively using a range of media. Work collaboratively and engage with people in different settings. Recognize how culture can shape communication.	**5 Written communication** **6 Oral communication** **7 Teamwork**
Responsible Understand how decisions can affect others and make ethically informed choices. Appreciate and respect diversity. Act with integrity as part of local, national, global and professional communities.	**10 Sustainability, societal & environmental impact**

Practical work:

Practical list of this course covers implementation of cryptographic algorithms.

Lecture/tutorial times

Online Lectures (7 CE)	
Day	**Time**
Monday	11:10 - 12:10 pm
Tuesday	02:00 - 03:00 pm
Friday	11:10 - 12:10 pm

Attendance Requirements

The University norms states that it is the responsibility of students to attend all lectures, tutorials, seminars and practical work as stipulated in the course outline. Minimum attendance requirement as per university norms is compulsory for being eligible for semester examinations.

Details of referencing system to be used in written work

Text books

1. William Stallings, "Cryptography And Network Security - Principles and Practices", Prentice Hall of India, Third Edition, 2003.

Additional Materials

1. BehrouZ A. ForouZan. Tata McGraw-Hill Publishing Company Limited. NEW DELH ISBN 10: 1259064751 / ISBN 13: 9781259064753
2. Atul Kahate, "Cryptography and Network Security", Tata McGraw-Hill, 2003.
3. Charles P. Pfleeger, Shari Lawrence Pfleeger – Security in computing – Prentice Hall of India.
4. Bruce Schneier, "Applied Cryptography", John Wiley & Sons Inc, 2001.
5. Johannes A. Buchmann, Introduction to Cryptography, Undergraduate Text in Mathematics, Springer.
6. A. Das and C. E. Veni Madhavan, Public-Key Cryptography: Theory and Practice, Pearson Education Asia.

ASSESSMENT GUIDELINES

Your final course mark will be calculated from the following:

Marking Scheme

CIE	**60 Marks**
Mid semester Exam(21-Sep-2020)	40
Assignment:1	5
Assignment:2	5
Presentation/Quiz	5
Attendance>80%	5
ESE	**40 Marks**

SUPPLEMENTARY ASSESSMENT

Students who receive an overall mark less than 40% in internal component or less than 40% in the end semester will be considered for supplementary assessment in the respective components (i.e internal component or end semester) of semester concerned. Students must make themselves available during the supplementary examination period to take up the respective components (internal component or end semester) and need to obtain the required minimum 40% marks to clear the concerned components.

Practical Work Report/Laboratory Report:

A report on the practical work is due the subsequent week after completion of the class by each group.

Late Work

Late assignments will not be accepted without supporting documentation. Late submission of the reports will result in a deduction of -10% of the maximum mark per calendar day

Format

All assignments must be presented in a neat, legible format with all information sources correctly referenced. **Assignment material handed in throughout the session that is not neat and legible will not be marked and will be returned to the student.**

Retention of Written Work

Written assessment work will be retained by the Course coordinator/lecturer for two weeks after marking to be collected by the students.

University and Faculty Policies

Students should make themselves aware of the University and/or Faculty Policies

regarding plagiarism, special consideration, supplementary examinations and other educational issues and student matters.

Plagiarism - Plagiarism is not acceptable and may result in the imposition of severe penalties. Plagiarism is the use of another person's work, or idea, as if it is his or her own - if you have any doubts at all on what constitutes plagiarism, please consult your Course coordinator or lecturer. Plagiarism will be penalized severely.

Do not copy the work of other students.
Do not share your work with other students (except where required for a group activity or assessment)

.

Course schedule (subject to change)

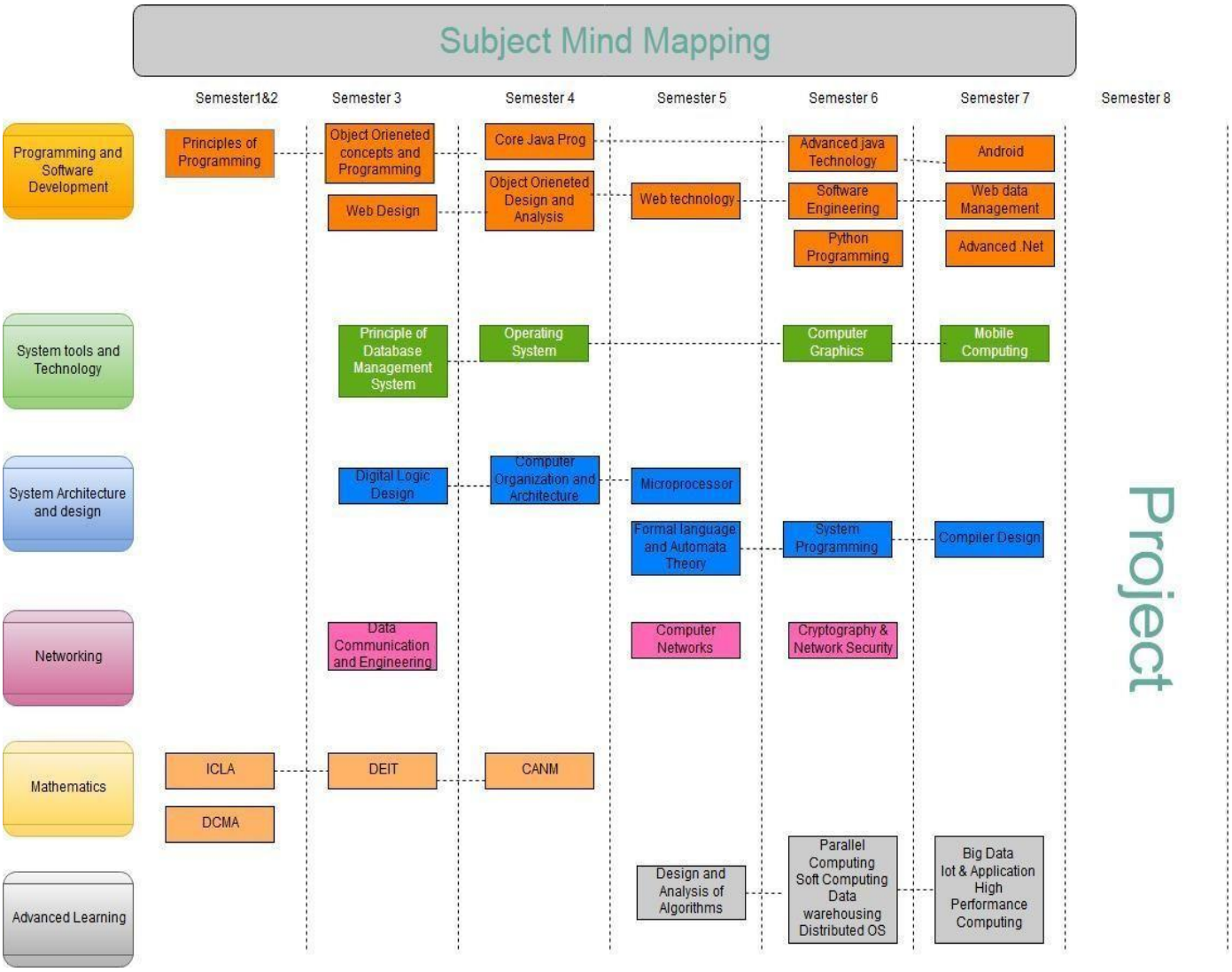
(Mention quiz, assignment submission, breaks etc as well in the table under the Teaching Learning Activity Column)

	Week #	Topic & contents	CO Addressed
	Weeks 1	**Fundamentals:** Security Concepts: Introduction, The need for security, Principles of security, Introduction to security attacks - services and mechanism, the OSI security architecture	CO-1
	Weeks 2	A model for Network Security, Classical Encryption techniques, Cipher principles, cryptanalysis.	CO-1
	Week 3	**Block ciphers:** Block cipher design principles and modes of operation, Fiestel cipher structure, Overview on S-Box Design Principles, DES and its variants	CO-4
	Week 4	RC5, IDEA, Blowfish, Advanced Encryption Standard (AES) Algorithm.	CO-1
	Week 5	Public Key Cryptography: Asymmetric key Ciphers: Principles of public key cryptosystems, RSA algorithm, Elgamal Cryptography	CO-2
	Week 6	Diffie-Hellman Key Exchange, Knapsack Algorithm, Key Management, KDC, Elliptic Curve Architecture and Cryptography.	CO-2
	Week 7	**Hash Function:** Message Authentication Codes, Hash Functions, Security of Hash Functions, MD5 message Digest algorithm, Secure Hash Algorithm	CO-3
	Week 8	RIPEMD, HMAC, Digital certificate. Digital Signatures,	CO-3
	Week 9	Authentication Protocols, Digital Signature Standards, Application Authentication Techniques Like Kerberos, X.509 Directory Authentication Services, PGP.	CO-3

	Week 10	**IPSec** architecture, Applications of IPSec, Benefits of IPSec, IPSec protocols, Authentication Header, Encapsulation Security Payload, Combining Security Association,	CO-5
	Week 11	**Web Security** Requirement, Web Security threats, Secure Socket Layer, Secure Electronic Transaction.	CO-5
	Week 12	**System Level Security:** Intrusion detection, Viruses and related Threats, Firewall Design Principles, Trusted Systems.	CO-6

LIST OF PRACTICALS

Practical No.	Title	Learning Outcomes
1	To implement Caesar Cipher Encryption - Decryption.	Encryption - Decryption
2	To implement Mono-alphabetic Cipher Encryption – Decryption.	Encryption - Decryption
3	To implement Hill Cipher Encryption	Encryption
4	To implement Poly-alphabetic Cipher (Vigener Cipher) Technique	Vigener CipherTechnique
5	To implement Play-Fair Cipher Technique.	Play-Fair CipherTechnique
6	Write a program to implement Rail-Fence Encryption Technique.	Rail-Fence Encryption Technique.
7	To implement S-DES algorithm for data encryption.	S-DES algorithm
8	Write a program to implement RSA asymmetric (public key and private key)-Encryption.	RSA asymmetric
9	Write a program to generate digital signature using Hash code.	Hash code.
10	Case Study on Kerberos.	Case Study
11	Case Study on Firewalls.	Case Study
12	Study of MD5 hash function and implement the hash code using MD5.	MD5 hash function
13	Study of SHA-1 hash function and implement the hash code using SHA-1.	SHA-1 hash function
14	Write a program to implement transposition Encryption Technique	Transposition Encryption Technique


Subject Mind Mapping
Semester1&2
Semester 3
Semester 4
Semester 5
Semester 6
Semester 7
Semester 8
Programming and Software Development
System tools and Technology
System Architecture and design
Networking
Mathematics
Advanced Learning
Principles of Programming
Object Orieneted concepts and Programming
Web Design
Core Java Prog
Object Orieneted Design and Analysis
Web technology
Advanced java Technology
Software Engineering
Python Programming
Android
Web data Management
Advanced .Net
Principle of Database Management System
Operating System
Computer Graphics
Mobile Computing
Digital Logic Design
Computer Organization and Architecture
Microprocessor
Formal language and Automata Theory
System Programming
Compiler Design
Data Communication and Engineering
Computer Networks
Cryptography & Network Security
ICLA
DCMA
DEIT
CANM
Design and Analysis of Algorithms
Parallel Computing
Soft Computing
Data warehousing
Distributed OS
Big Data
Iot & Application
High Performance Computing
Project