MANIPAL UNIVERSITY JAIPUR

School of Information Technology

Department of Information Technology

Course Hand-out

Cryptography & Information Security |IT 3203| [4 Credits] [3104]

Session: Jan' 24 – May' 24 | Faculty: Dr. Lokesh Sharma, Dr. Vivek Kumar Verma, Dr. Ashish Jain, Mr. Ankit Mundra, Ms. Vineeta Soni | Class: B.Tech. VI Semester

Introduction: The course is offered to Information Technology Engineering students to understand the principles and practices of Cryptography and Information Security. To acquire knowledge on standard algorithms used to provide confidentiality, integrity, and authentication. It allows the students to learn that the sensitive information is to be passed through network safely.

A. Course Objectives: At the end of the course, students will be able to

[3203.1] Define the fundamentals of Number Theory used in Cryptography. (Remembering)
[3203.2] Explain the standard cipher algorithms in transit across data networks. (Understanding)
[3203.3] Identify Security attacks and select its identification mechanism. (Applying)
[3203.4] Apply various key distribution and management schemes. (Applying)
[3203.5] Evaluate authentication mechanisms. (Evaluating)

B. Program Outcomes and Program Specific Outcomes

PROGRAM OUTCOMES

[PO.1]. **Engineering knowledge**: Demonstrate and apply knowledge of Mathematics, Science and Engineering to classical and recent problems of electronic design & communication system.

[PO.2]. **Problem analysis**: Identify, formulate, research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences

[PO.3]. **Design/development of solutions**: Design a component system, or process to meet desired needs within realistic constraints such as economic, environmental, social, political, ethical, health and safety, manufacturability, and sustainability.

[PO.4]. **Conduct investigations of complex problems**: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions

[PO.5]. **Modern tool usage**: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations

[PO.6]. **The engineer and society**: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal, and cultural issues and the consequent responsibilities relevant to the professional engineering practice

[PO.7]. **Environment and sustainability**: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development

[PO.8]. **Ethics**: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practices

[PO.9]. **Individual and team work**: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings

[PO.10]. **Communication**: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions

[PO.11]. **Project management and finance:** Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environment.

[PO.12]. **Life-long learning**: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change

PROGRAM SPECIFIC OUTCOMES

[PSO.1]. To apply creativity in support of the design, simulation, implementation, and inference of existing and advanced technologies.

[PSO.2]. To participate & succeed in IT oriented jobs/competitive examinations that offer inspiring & gratifying careers.

[PSO.3]. To recognize the importance of professional developments by pursuing postgraduate studies and positions.

C. Assessment Plan:

Criteria	Description	Maximum Marks
Internal Assessment (Summative)	Sessional Exam (Close Book)	30
	In class Quizzes and Assignments, Activity feedbacks (Accumulated and Averaged)	30
End Term Exam (Summative)	End Term Exam (Close Book)	40
	Total	100
Attendance (Formative)	A minimum of 75% Attendance is required to be maintained by a student to be qualified for taking up the End Semester examination. The allowance of 25% includes all types of leaves including medical leaves.	
Make up Assignments (Formative)	Students who miss a class will have to report to the teacher about the absence. A makeup assignment on the topic taught on the day of absence will be given which has to be submitted within a week from the date of absence. No extensions will be given on this. The attendance for that day of absence will be marked blank, so that the student is not accounted for absence. These assignments are limited to a maximum of 5 throughout the entire semester.	
Homework/ Home Assignment/ Activity Assignment (Formative)	There are situations where a student may have to work in home, especially before a flipped classroom. Although these works are not graded with marks. However, a student is expected to participate and perform these assignments with full zeal since the activity/ flipped classroom participation by a student will be assessed and marks will be awarded.	

D. Syllabus:

Introduction: Computer and Network Security Concepts, Number Theory and Finite Fields; Symmetric Ciphers: Classical Encryption Techniques, Block Ciphers – DES and AES, Block Cipher Operation, Pseudorandom Number Generators and Stream Ciphers; Asymmetric Ciphers: Principles of Public Key Cryptography, RSA, Elliptic Curve Cryptography; Cryptographic Data Integrity Algorithms: Cryptographic Hash Functions, Message Authentication Codes, Digital Signatures; Mutual Trust: Key Distribution, PKI, User Authentication, Kerberos; Network and Internet Security: Transport Level Security, Wireless Network Security, Email Security, IP Security.

References:

1. Stallings W, Cryptography and Network Security: Principles and Practice, (7e), Pearson Education India, ISBN 978-1-292-15858-7, 2017.

2. Katz J, Menezes A J, Van Oorschot PC, Vanstone S A, Handbook of Applied Cryptography, (2e), CRC press, ISBN 0849385237, 2010.

3. Stinson Douglas R., Cryptography: Theory and Practice, (3e), Chapman and Hall / CRC Press, 2005.

F. Lecture Plan:

Lec No	Major Topics	Topics	Corresponding CO	Mode of Delivery	Mode of Assessing CO
1.	Elements of Number Theory	Introduction to Number Theory	CO1	Lecture	In class Quiz Mid Term I End Term Exam
2.		Prime Number Concept Euclid Algorithm	CO1	Lecture	In class Quiz Mid Term I End Term Exam
3.		Fermat's Little Theorem Entropy	CO1	Lecture	In Class Quiz, Mid Term I End Term
4.	Classical Cipher Techniques	Classical Cipher Technique Introduction to Cryptography	CO2	Lecture	In Class Quiz Mid Term I End Term
5.		Substitution Cipher (Mono & Poly Alphabetic)	CO2	Flipped Class	In Class Quiz Mid Term I End Term
6.		Caesar Cipher & Affine Cipher	CO2	Flipped Class	Class Quiz, Mid Term I End Term
7.		Play Fair & Hill Cipher	CO2	Lecture	Class Quiz Mid Term I End Term
8.		Transposition Techniques and Rail Fence Cipher	CO2	Flipped Class	Class Quiz, Mid Term I End Term
9.	Security Attacks	Security Attack Active & Passive Attack	CO3	Lecture	Class Quiz Mid Term I End Term
10.		Security Services (ITU-T X.800)	CO3	Lecture	Class Quiz, Mid Term I End Term
11.		Introduction to Encryption Techniques Stream Cipher and Block Cipher	CO3	Tutorial	Class Quiz Mid Term I End Term
12.		Symmetric Encryption Feistel Cipher	CO2	Tutorial	Class Quiz Mid Term I

	Symmetric Encryption				End Term
13.		Confusion and Diffusion	CO2, CO4	Lecture	Class Quiz Mid Term I End Term
14.		DES Algorithm	CO2, CO4	Lecture	Class Quiz Mid Term I End Term
15.		Analysis of DES Algorithm	CO2, CO4	Lecture	Class Quiz Mid Term I End Term
16.		2-DES & 3-DES	CO2, CO4	Lecture	Class Quiz Mid Term I End Term
17-18		AES Algorithm	CO3, CO4	Lecture	Class Quiz Mid Term I End Term
19-20.		Modes of Operation (Block)	CO4	Lecture	Class Quiz Mid Term I End Term
21.	**Asymmetric Encryption**	Asymmetric Encryption	CO4	Lecture	Class Quiz Mid Term II End Term
22.		Public Key Cryptosystem	CO4	Lecture	Class Quiz Mid Term II End Term
23.		RSA Algorithm	CO4	Lecture	Class Quiz Mid Term II End Term
24.		Security Analysis of RSA Algorithm	CO4	Flipped Class	Class Quiz Mid Term II End Term
25.		ElGamal Cryptosystem & Security Analysis	CO3, CO4	Lecture	Class Quiz Mid Term II End Term
26.		Introduction to MAC, HMAC & CMAC	CO4	Lecture	Class Quiz Mid Term II End Term

27.		Introduction to Hashing Properties of Hash	CO4	Tutorial	Class Quiz Mid Term II End Term
28.		MD-5, SHA-1	CO2, CO4	Lecture	Class Quiz Mid Term II End Term
29.		SHA-128, SHA-2	CO2, CO4	Lecture	Class Quiz Mid Term II End Term
30.	**Digital Signatures**	Digital Signature Scheme	CO5	Lecture	Class Quiz Mid Term II End Term
31.		RSA Based	CO5	Lecture	Class Quiz Mid Term II End Term
32.		EL-Gamal	CO4, CO5	Lecture	Class Quiz Mid Term II End Term
33.		Problem of Key Sharing & Diffie Hellman	CO4, CO5	Lecture	Class Quiz Mid Term II End Term
34.	**User Authentication Protocols**	Key Distribution Scheme, Symmetric Key Distribution	CO4, CO5	Lecture	Class Quiz Mid Term II End Term
35.		Kerberos Authentication	CO5	Lecture	Class Quiz Mid Term II End Term
36.		Symmetric Key Agreement	CO4, CO5	Lecture	Class Quiz Mid Term II End Term
37.		Public Key Distribution	CO4	Lecture	Class Quiz End Term
38.	**User Authentication Protocols**	User Authentication Protocols	CO5	Flipped Class	Class Quiz End Term
39.		IP Security Introduction		Tutorial	Class Quiz End Term

40.	**IP Sec**	AH & ESP Schemes	CO5	Tutorial	Class Quiz End Term
41.		Introduction to SSL	CO5	Lecture	Class Quiz End Term
42.		OPEN SSL	CO5	Lecture	Class Quiz End Term
43.		Transport Layer Security	CO2, CO5	Lecture	Class Quiz End Term
44.	**Intrusion Detection**	Intrusion: Introduction	CO3, CO5	Tutorial	Class Quiz End Term
45.		Statistical Anomaly Detection	CO3, CO5	Tutorial	Class Quiz End Term
46.		Rule Based Detection	CO3, CO5	Flipped Class	Class Quiz End Term
47.		Honeypots	CO3, CO5	Lecture	Class Quiz End Term
48.	**Password Protection & Firewalls**	Password Protection	CO5	Lecture	End Term
49.		Password Protection Schemes & Policies	CO5	Lecture	End Term
50.		Firewalls: Definition & Construction	CO3, CO5	Lecture	End Term
51.		Working Principle of Firewalls	CO3, CO5	Lecture	End Term

Course Articulation Matrix: (Mapping of COs with POs)

CO	STATEMENT	CORRELATION WITH PROGRAM OUTCOMES												CORRELATION WITH PROGRAM SPECIFIC OUTCOMES		
		PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
3203.1	Define the fundamentals of Number Theory used in Cryptography.	3	2	1	1		1				1		1	1	1	1
3203.2	Explain the standard cipher algorithms in transit across data networks.	2		2	1	1	1				1		1	1	1	1
3203.3	Identify Security attacks and select its identification mechanism.	2		1	1		1		2		1		1	1	1	1
3203.4	Apply various key distribution and management schemes.	2		2	1	1	1				1		1	1	1	1
3203.5	Evaluate authentication mechanisms.	2		2	1		1				1		1	1	1	1

I- Low Correlation; 2- Moderate Correlation; 3- Substantial Correlation