CSE1011	Cryptography Fundamentals	L	T	P	J	C
		2	0	2	4	4
Objectives	1. To learn the fundamental concepts of cryptography 2. To defend the security attacks on information systems with secure algorithms					
Expected Outcome	At the end of the course, the students will be able to 3. Learn to analyse the security of the in-built cryptosystems 4. Develop cryptographic algorithms for information security 5. Develop authentication schemes for identity and membership authorization					
Student Learning Outcome	1) Having an ability to apply mathematics and science in engineering applications 5) Having design thinking capability 6) Having an ability to design a component or a product applying all the relevant standards and with realistic constraints 9) Having problem solving ability- solving social issues and engineering problems 12) Having adaptive thinking and adaptability 14) Having an ability to design and conduct experiments, as well as to analyse and interpret data 18) Having critical thinking and innovative skills					

Modules	Topics	L hrs	SLO
1	**INTRODUCTION TO SECURITY** Information Security - Confidentiality, Integrity & Availability – Authentication, Authorization & Non-Repudiation – Introduction to Plain Text, Cipher Text, Encryption and Decryption Techniques, Secure Key, Hashing, Digital signature	4	1
2	**SYMMETRIC ENCRYPTION** Block cipher, Stream Cipher - Data Encryption Standard (DES) - Cipher Block Chaining (CBC) - Multiple Encryption DES - International Data Encryption Algorithm (IDEA) - Advanced Encryption Standard (AES)	4	1,9,14

3	**ASYMMETRIC ENCRYPTION** Asymmetric key generation techniques – Applications of Asymmetric encryption methods – RSA- Elliptic Curve Cryptography	4	5,9
4	**DIGITAL SIGNATURES** Digital signature standards - Secure One-time Signatures - Application of Digital Signatures - Diffie-Hellman Key Exchange - Elliptic Curve Digital Signature algorithm	3	12
5	**HASHING AND MESSAGE DIGESTS** Cryptographic Hash Functions- Applications- Simple hash functions and features for ensuring security - Hash functions based on Cipher Block Chaining- Secure Hash Algorithm (SHA) - Message Digest - MD5	4	14
6	**MESSAGE AUTHENTICATION** Authentication Systems – Password and Address - Security Handshake Drawbacks - Authentication Standards – Kerberos- PKI Trust Models -Message Authentication Codes (MAC) – Security features- MAC based on Hash Functions - MAC based on Block Ciphers	5	9
7	**APPLICATIONS OF CRYPTOGRAPHIC ALGORITHMS** Applying cryptography algorithms - Smart cards-Mobile phone security - Electronic passports and ID cards - SDA/DDA/CDA Bank Cards - Financial Cryptography – Secure Payment Systems - Crypto currencies - Bitcoin	4	6,18
8	**Contemporary Issues (To be handled by experts from industry)**	2	2
	Indicative List of lab experiments 1. Demonstration of Symmetric conventional cryptographic techniques 2. Demonstration of Symmetric classic cryptographic techniques 3. Demonstration of Asymmetric cryptographic techniques 4. Demonstration of Hashing and Message digest techniques 5. Design and implementation of new cryptographic algorithms 6. Demonstration and implementation of secure communication using standard crypto libraries 7. Implementation of smart card based server/client applications 8. Demonstration of authentication techniques		

	9. Developing cryptographic algorithms for industrial applications 10. Developing cryptographic algorithms for innovative applications		
	Projects 1. Developing highly secure banking application for credit/debit card transactions 2. Developing new pseudorandom number generation for Bitcoin like secure application 3. Developing new key generation algorithm for symmetric and asymmetric encryption methods 4. Implementing new secure communication platforms or protocols for TCP/UDP 5. Developing security analysis techniques for various applications 6. Developing alarming or notification techniques for attack detections in applications	**60** [Non Contact]	

Reference Books

1. D. R. Stinson, *Cryptography: Theory and Practice*, 3rd ed. Boca Raton, FL: Chapman & Hall/CRC, 2005. (ISBN No.: 978-1-58-488508-5)
2. W. Stallings, *Cryptography and Network Security: Principles and Practice*, 5th Ed. Boston: Prentice Hall, 2010. (ISBN No.: 978-0-13-609704-4)
3. J. H. Silverman, *A Friendly Introduction to Number Theory*, 4th Ed. Boston: Pearson, 2012. (ISBN No.: 978-0-321-81619-1)
4. C. Kaufman, R. Perlman, and M. Speciner, *Network Security: Private Communication in a Public World*, 2nd Ed. United States: Prentice Hall PTR, 2002. (ISBN No.: 978-0-13-046019-6)

Knowledge Areas that contain topics and learning outcomes covered in the course

Knowledge Area	Total Hours of Coverage
CS: Cryptography (CG)	14
CS : Network Security (NS)	4
CS : Foundational Concepts in Security (FCS)	12

Body of Knowledge coverage

KA	Knowledge Unit	Topics Covered	Hours
CS: FCS	Security	Information Security - Confidentiality, Integrity & Availability – Authentication, Authorization & Non-Repudiation – Introduction to Plain Text, Cipher Text, Encryption and Decryption Techniques, Secure Key, Hashing, Digital signature	4
CS: FCS	Symmetric Encryption	Symmetric Algorithms- Block cipher, Stream Cipher	1
CS: CG	Symmetric Encryption	Data Encryption Standard (DES) - International Data Encryption Algorithm (IDEA) - Advanced Encryption Standard (AES) - Cipher Block Chaining (CBC) - Multiple Encryption DES	3
CS: FCS	Asymmetric Encryption	Computational aspects, finite fields, primes and unique factorization of integers, computing discrete logarithms	2
CS: CG	Asymmetric Encryption	Asymmetric Algorithms - Public key encryption – RSA - Applications of Public Key cryptography	2
CS:FCS	Digital Signature	Digital signature standards - Secure One-time Signatures -	1
CS:CG	Digital Signature	Diffie-Hellman Key Exchange - Elliptic Curve Cryptography - Elliptic Curve Digital Signature algorithm	2
CS: FCS	Hashing and Message Digests	Cryptographic Hash Functions- Applications- Simple hash functions and features for ensuring security	2
CS: NS	Hashing and Message Digests	Hash functions based on Cipher Block Chaining- Secure Hash Algorithm (SHA) - Message Digest - MD5	2
CS: FCS	Message Authentication	Authentication Systems – Password and Address - Security Handshake Drawbacks - Authentication Standards	2
CS: CG	Message Authentication	Kerberos- PKI Trust Models -Message Authentication Codes (MAC) – Security features- MAC based on Hash Functions - MAC based on Block Ciphers	3

CS: CG	Application of Cryptographic algorithms	Applying cryptography algorithms - Smart cards- Mobile phone security- Applications of digital signatures - Electronic passports and ID cards - SDA/DDA/CDA Bank Cards - Financial Cryptography – Secure Payment Systems - Crypto currencies – Bitcoin	4
CS:NS	Information Security	**Contemporary Issues (To be handled by experts from industry)**	2
		Total hours	**30**

Where does the course fit in the curriculum?

This course is a

- Core Course.
- Suitable from 2nd semester onwards.
- Programming knowledge in C/ Java

What is covered in the course?

Part I: Security Fundamentals

This section introduces the basic concepts of security and briefs the encryption techniques and algorithms. This section also discusses the various characteristic requirements for the security measures.

Part II: Symmetric and Asymmetric Cryptographic Algorithms

This section briefs about the various types of symmetric and asymmetric cryptographic algorithms. The classical and conventional cryptographic algorithms based on the secret keys and cipher types used in the encryption mechanisms are detailed in the section.

Part III: Digital Signature

This section details the digital signature, its need, standard and application. This section also discusses authentication techniques such as, Elliptic Curve Cryptography and Elliptic Curve Digital Signature algorithm.

Part IV: Message Authentication

This section briefs about the various message authentication mechanisms. The applications based on hashing and message digest are also discussed. This section also discusses Message Authentication Code (MAC), Hash functions, Secure Hash Algorithm (SHA-1), Message Digest (MD5).

Part V: Application of Cryptographic Algorithms

This section deals with various cryptographic implementations and recently developed security features embedded in critical applications.

What is the format of the course?

This Course is designed with 2 hours of lecture every week, 60 minutes of video/reading instructional material per week. Generally this course should have the combination of lectures, in-class discussion, case studies, guest-lectures, mandatory off-class reading material, quizzes.

How are students assessed?

- Students are assessed on a combination group activities, classroom discussion, projects, and continuous, final assessment tests.
- Additional weightage will be given based on their rank in developing applications during lab.
- Students can earn additional weightage based on certificate of completion of a related MOOC course.

Session Wise Plan

S.No.	Topics Covered	Class Hour	Lab Hour	Levels of mastery	Ref Book
1.	Information Security and features	2		Familiarity	2
2.	Basics of encryption and decryption techniques	2	1	Familiarity	2
3.	Symmetric Encryption Techniques, Block Cipher and Stream Cipher	1	1	Familiarity	1,2
4.	Encryption Algorithms: DES	1	1	Usage	1,2
5.	Encryption Algorithms: AES	1	1	Usage	1,2
6.	Encryption Algorithms: IDEA, CBC, Multiple Encryption DES.	2	1	Usage	1,2
7.	Asymmetric Encryption-RSA algorithm	2	1	Usage	1,2
8.	Number Theory	2	1	Assessment	3
9.	Digital Signature standards and application	1		Usage	2
10.	Diffie Hellmann Key Agreement	1	1	Usage	1,2
11.	Elliptic Curve Cryptography - Elliptic Curve Digital Signature algorithm	2	1	Familiarity	2
12.	Hash functions, Secure Hash Algorithm: SHA-1	1	2	Usage	1,2
13.	Message Digest , MD5	2	1	Usage	1,2
14.	Message Authentication Mechanism	1		Familiarity	2
15.	Kerberos- PKI Trust Models	1		Usage	2
16.	Message Authentication Codes (MAC), MAC based on Hash Functions and Block Ciphers	2	1	Usage	2
17.	Application of Cryptographic Algorithms	1	2	Usage	4
18.	Application of Digital Signatures	1		Usage	4
19.	Secure Systems	2		Familiarity	4