DRONACHARYA College of Engineering

KHENTAWAS, FARRUKHNAGAR, GURGAON, HR

Department:

Academic Session: 2017-18 (Jan-June 2018)

Lesson Plan for the Semester started w.e.f 08.01.2018

Subject with code: Information Security System (EC-615-F)

Name of Faculty with designation : Ms. Sameeksha Kukreti, Assistant Professor

Month	Date & Day	Sem-Class	Unit	Topic/Chapter covered	Academic activity	Test / assignment
January	08.01.2018 Monday	VI-ECS	1	Overview: Services, Mechanisms, and Attacks	………	Assignment of 02 Ques. given
	09.01.2018 Tuesday	VI-ECS	1	the OSI Security Architecture, A Model for Network, Security. Classical Encryption Techniques: Symmetric Cipher Model, Substitution Techniques, Transposition Techniques		Assignment of 02 Ques. given
	10.01.2018 Wednesday	VI-ECS	1	Rotor Machines, Stegnography,Block Ciphers And The Data Encryption Standard Simplified DES		Assignment of 02 Ques. given
	11.01.2011 Thrusday	VI-ECS	1	Block Cipher Principles, The Data Encryption Standard, The Strength of DES		Assignment of 02 Ques. given
	15.01.2018 Monday	VI-ECS	1	Differential and Linear Cryptanalysis		Assignment of 02 Ques. given
	16.01.2018 Tuesday	VI-ECS	1	Block Cipher Design Principles, Block Cipher Modes of Operation.		Assignment of 02 Ques. given
	17.01.2018 Wednesday	VI-ECS	2	Introduction To Finite Fields: Groups, Rings, and Fields		Assignment of 02 Ques. given

Month	Date & Day	Sem-Class	Unit	Topic/Chapter covered	Academic activity	Test / assignment
	18.01.2018 Thrusday	**VI-ECS**	**2**	Modular Arithmetic, Euclid’s Algorithm, Finite Fields of the Form GF(p), Polynomial Arithmetic, Finite Fields of the Form GF(2n).		**Assignment of 02 Ques. given**
	23.01.2018 Tuesday	**VI-ECS**	**2**	Advanced Encryption Standard Evaluation Criteria for AES, The AES Cipher. Contemporary Symmetric Ciphers Triple DES,		**Assignment of 02 Ques. given**
	24.01.2018 Wednesday	**VI-ECS**	**2**	Blowfish, RC5, Characteristics of Advanced Symmetric Block Ciphers, RC4 Stream Cipher		**Assignment of 02 Ques. given**
	25.01.2018 Thrusday	**VI-ECS**	**2**	Confidentiality Using Symmetric Encryption Placement of Encryption Function, Traffic Confidentiality, Key Distribution, Random Number Generation.		**Assignment of 02 Ques. given**
	29.01.2018 Monday	**VI-ECS**	**2**	Public-Key Encryption and Hash Functions: Introduction to Number Theory: Prime Numbers, Format’s and Euler's Theorems, Testing for Primality.		**Assignment of 02 Ques. given**
	30.01.2018 Tuesday	**VI-ECS**	**3**	The Chinese Remainder Theorem, Discrete Logarithms. Public-KeyCryptography and RSA: Principles of Public-Key Cryptosystems,		**Assignment of 02 Ques. given**
	01.02.2018 Thrusday	**VI-ECS**	**3**	the RSA Algorithm, Recommended Reading and Web Site, Key Terms, Review Questions, and Problems.		**Assignment of 02 Ques. given**
	05.02.2018 Monday	**VI-ECS**	**3**	Key Management and Other Public-Key Cryptosystems Key Management, Diffie-Hellman Key Exchange,		**Assignment of 02 Ques. given**

Month	Date & Day	Sem-Class	Unit	Topic/Chapter covered	Academic activity	Test / assignment
	06.02.2018 Tuesday	**VI-ECS**	**3**	Elliptic Curve Arithmetic, Elliptic Curve Cryptography.		**Assignment of 02 Ques. given**
	07.08.2018 Wednesday	**VI-ECS**	**3**	. Message Authentication and Hash Functions Authentication Requirements, Authentication Functions		**Assignment of 02 Ques. given**
	08.02.2018 Thrusday	**VI-ECS**	**3**	Message Authentication Codes, Hash Functions, Security of Hash Functions and MACs.		**Assignment of 02 Ques. given**
	19.02.2018 Monday	**VI-ECS**	3	Hash Algorithms: MD5 Message Digest Algorithm, Secure Hash Algorithm, RIPEMD-160, and HMAC.		**Assignment of 02 Ques. given**
	20.02.2018 Tuesday	**VI-ECS**	4	Digital Signatures and Authentication Protocols Digital Signatures, Authentication Protocols,		**Assignment of 02 Ques. given**
	21.02.2018 Wednesday	**VI-ECS**	4	Network Security Practice Authentication Applications: Kerberos, X.509 Authentication Service, Electronic Mail Security		**Assignment of 02 Ques. given**
	22.02.2018 Thrusday	**VI-ECS**	4	Pretty Good Privacy, S/MIME. IP Security IP Security Overview, IP Security Architecture,		**Assignment of 02 Ques. given**
	26.02.2018 Monday	**VI-ECS**	4	Authentication Header, Encapsulating Security Payload, Combining Security Associations, Key Management,		**Assignment of 02 Ques. given**
	27.02.2018 Tuesday	**VI-ECS**	4	Web Security Web Security Considerations		**Assignment of 02 Ques. given**
	28.02.2018 Wednesday	**VI-ECS**	4	Intrusion Detection Password Management,		**Assignment of 02 Ques. given**

Month	Date & Day	Sem-Class	Unit	Topic/Chapter covered	Academic activity	Test / assignment
	05.03.2018 Monday	**VI-ECS**	4	Firewalls Firewall Design Principles, Trusted Systems.		**Assignment of 02 Ques. given**
	06.03.2018 Tuesday	**VI-ECS**	4	Malicious Software Viruses and Related Threats		**Assignment of 02 Ques. given**
	07.03.2018 Wednesday	**VI-ECS**	4	Virus Countermeasures		**Assignment of 02 Ques. given**
	08.03.2018 Thrusday	**VI-ECS**	4	SecureSockets Layer and Transport Layer Security		**Assignment of 02 Ques. given**
	12.03.2018 Monday	**VI-ECS**	4	Secure Electronic Transaction		**Assignment of 02 Ques. given**