ARSD College, University of Delhi

Model Course Handout/Lesson Plan

Course Name : B.Sc. (Honours)						
Semester	**Course Code**	**Course Title**	**Lecture (L)**	**Tutorial (T)**	**Practical (P)**	**Credit (C)**
IV	32345402	GE – Information Security and Cyber laws	4	0	4	6
Teacher/Instructor(s)		Mr. Dharmendra Singh				
Session		2022-23				

Course Objective:

- This course introduces the students to the concepts of information security and different type of attacks in the cyber space. The course also introduces countermeasures to mitigate attacks and different existing cyber laws.

Course Learning Outcomes:

On successful completion of the course, students will be able to:

1. Learn, structure, mechanics and evolution of various crime threats
2. Learn to protect information systems from external attacks by developing skills in enterprise security, wireless security and computer forensics.
3. Analyze the risks involved while sharing their information in cyber space and numerous related solutions like sending protected and digitally signed documents
4. Insights of ethical hacking and usage of password cracking tools
5. Get an overview of different ciphers used for encryption and decryption.

Lesson Plan:

Unit No.	**Learning Objective**	**Lecture No.**	**Topics to be covered**

1.	Definitions	1-8	Definitions : Protection , Security, risk, threat, vulnerability, exploit, attack, confidentiality, integrity, availability, nonrepudiation, authentication, authorization, codes, plain text, encryption, decryption, cipher text, key, ciphers, Symmetric and asymmetric cryptography
		9-12	Public key, private key, Crypt analysis, Cyber forensics. Substitution cipher (Caesar), Transposition cipher (Rail-Fence)
2.	Risk Analysis & Threats	13-16	Risk analysis, process, key principles of conventional computer security, security policies
		17-24	Data protection, access control, internal vs external threat, security assurance, Passwords, access control, computer forensics and incident response
3.	CYBER ATTACKS (definitions and examples)	25-32	Cyber-attacks, types and examples
4.	handling of attacks	33-36	Brief Introduction of handling the attacks described in UNIT 3
		37-40	Firewalls, logging and intrusion detection systems, e-mail security

		41-44	Security issues in operating systems, ethics of hacking and cracking.
5.	IT Act Provisions	45-56	Digital Signature and Electronic Signature, Digital Certificate, Penalty and compensation, Punishment for various attacks.
6.	IT Infrastructure & Handling Agencies	57-60	Brief introduction of IT security infrastructure in India. National agencies handling IT security.

Evaluation Scheme:

No.	**Component**	**Duration**	**Marks**
1.	Internal Assessment		25
	• Quiz		
	• Class Test		
	• Attendance		
	• Assignment		
2.	End Semester Examination	3 hrs	75

Details of the Course		
Unit	**Contents**	**Contact Hours**
I	Definitions: Protection, Security, risk, threat, vulnerability, exploit, attack, confidentiality, integrity, availability, non-repudiation, authentication , authorization, codes, plain text, encryption, decryption, cipher text, key,	12

	ciphers, Symmetric and asymmetric cryptography, Public key , private key ,Crypt analysis,, Cyber forensics. Substitution cipher (Caesar), Transposition cipher (Rail-Fence)	
II	Risk analysis, process, key principles of conventional computer security, security policies, data protection, access control, internal vs external threat, security assurance, passwords, access control, computer forensics and incident response.	12
III	CYBER ATTACKS (definitions and examples): Denial-of-service attacks, Man-in-themiddle attack, Phishing, spoofing and spam attacks, Drive-by attack, Password attack, SQL injection attack, Cross-site scripting attack, Eavesdropping attack, Birthday attack, Malware attacks, Social Engineering attacks	8
IV	Brief Introduction of handling the attacks described in UNIT 3. Firewalls, logging and intrusion detection systems, e-mail security, security issues in operating systems, ethics of hacking and cracking.	12
V	Definitions: Digital Signature and Electronic Signature, Digital Certificate i.[Section 43] Penalty and compensation for damage to computer etc. ii. [Section 65] Tampering with computer source documents iii. [Section 66A] Punishment for sending offensive messages through communication service etc. iv. [Section 66B] Punishment for dishonestly receiving stolen computer resource or communication device v. [Section 66C] Punishment for identity theft vi. [Section 66D] Punishment for cheating by impersonation by using computer resource vii. [Section 66E] Punishment for violation of privacy viii. [Section 66F] Punishment for cyber terrorism ix. [Section 67] Punishment for publishing or transmitting obscene material in electronic form x. [Section 67A] Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form xi.[Section 67B] Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form xii.[Section 72] Breach of confidentiality and privacy	12
VI	Brief introduction of IT infrastructure in India, National agencies handling IT.	4
	Total	**60**

Suggested Books:

Sl. No.	**Name of Authors/Books/Publishers**	**Year of Publication/Reprint**
1.	Merkow, M., & Breithaupt, J.: Information Security Principles and Practices. 5th edition. Prentice Hall.	2005
2.	Snyder, G.F.: Network Security, Cengage Learning.	2010
3.	Whitman, M. E. & Mattord, H. J.: Principles of Information Security. 6th edition. Cengage Learning.	2017

Mode of Evaluation:	Internal Assessment / End Semester Exam