

# LESSON PLAN

Period	Date (Tentative)	Topic	Unit No.	Teaching Methodology	Remarks	Corrective Action Upon Review
1	10-6-13	Introduction To Network Security	I	CR		
1	<del>10-6-13</del>	Security Attacks (Interception)				
4	11-6-13	Security Attack Interruption,	I	CR		
		Fabrication, Modification				
3	13-6-13	Security Services	I	CR		
3	14-6-13	Security Mechanisms	I	CR		
4	16-6-13	Model for Network Security	I	CR		
1	17-6-13	Vulnerabilities - Dos, DDOS,	I	CR		
<del>4</del>	<del>18-6-13</del>	session hijacking				
4	18-6-13	spoofing,	I	CR		
		Buffer overflows				
3	20-6-13	Denial of Service Vulnerabilities	I	CR		
		SQL Injection				
3	21-6-13	Symmetric Cipher Model	I	CR		
4	22-6-13	Substitution and	I	CR		
		Transposition Techniques				
1	24-6-13	Block and Stream	I	CR		
		Cipher Techniques				
4	25-6-13	Data Encryption	II	CR		
		Standard (DES)				

# LESSON PLAN

Period	Date (Tentative)	Topic	Unit No.	Teaching Methodology	Remarks	Corrective Action Upon Review
3	27-6-13	Basic Cipher Design	<u>I</u>	CR		
		Principles				
3	28-6-13	Cipher Modes	<u>I</u>	CR		
		of operations				
4	29-6-13	Double DES	<u>I</u>	CR		
		and Triple DES				
4	2-7-13	International Data Encryption Algorithm	<u>I</u>	CR		
3	4-7-13	Blowfish	<u>I</u>	CR		
3	5-7-13	CAST-128	<u>I</u>	CR		
4	6-7-13	AES	<u>I</u>	CR		
4	9-7-13	Prime and	<u>III</u>	CR		
		Relative primeness - mbr				
3	11-7-13	Modern Arithmetic	<u>II</u>	CR		
3	12-7-13	Euler's Theorem	<u>II</u>	CR		
4	16-7-13	Chinese Remainder	<u>III</u>	CR		
		Theorem				
3	18-7-13	Discrete Algorithm	<u>III</u>	CR		
3	19-7-13	Discrete Algorithm	<u>III</u>	CR		
4	20-7-13	Discrete Algorithm	<u>III</u>	CR		

# LESSON PLAN

Period	Date (Tentative)	Topic	Unit No.	Teaching Methodology	Remarks	Corrective Action Upon Review
4	23-7-13	Principle of Public Key Cryptography	IV	CL		
3	25-7-13	about Public Key Cryptography Algorithm	IV	CL		
3	26-7-13	RSA Algorithm	IV	CL		
4	27-7-13	RSA Algorithm	IV	CL		
4	30-7-13	Diffie-Hellman Key exchange Algorithm	IV	CL		
3	1-8-13	Example in Diffie-Hellman Key exchange Algorithm	IV	CL		
3	2-8-13	Introduction to Elliptic Curve Cryptography	IV	CL		
4	3-8-13	elliptic curve Cryptography Algorithm	IV	CL		
4	13-8-13	Application of Cryptographic Hashing functions	V	CL		
3	16-8-13	Secure Hashing Algorithm	V	CL		
4	17-8-13	Message Authentication Code	V	CL		



# LESSON PLAN

Period	Date (Month)	Topic	Unit No.	Teaching Methodology	Remarks	Correction/Action Taken
3	18-4-13	Digital Signatures	2	ca		
3	19-4-13	Digital Signature Schemes	2	ca		
4	24-4-13	Authentication Protocols	2	ca		
4	28-4-13	Authentication Functions and Experiment	2	ca		
3	29-4-13	Digital Signature Standards	2	ca		
3	30-4-13	Verifiers	2	ca		
4	1-5-13	Key Management and Distribution	2	ca		
4	3-5-13	Key Diversity Authentication Schemes	2	ca		
3	5-5-13	Public Key Infrastructure	2	ca		
3	6-5-13	E-mail Security	2	ca		
4	7-5-13	Privacy	2	ca		
		Privacy				
4	10-5-13	M I M E	2	ca		
3	12-5-13	S/M I M E	2	ca		

# LESSON PLAN

Period	Date (Tentative)	Topic	Unit No.	Teaching Methodology	Remarks	Corrective Action Upon Review
3	13-9-13	IP Security Overview	<u>VII</u>	ce		
		And Architecture				
4	17-9-13	Authentication Header (AH)	<u>VII</u>	ce		
3	19-9-13	Encapsulating	<u>VII</u>	ce		
		Security Payload				
3	20-9-13	Combining Security Associations	<u>VII</u>	ce		
4	21-9-13	Introduction TO	<u>VII</u>	ce		
		IPsec Security				
4	24-9-13	about Security Protocol Layer	<u>VII</u>	ce		
3	26-9-13	Transport Layer Level Security	<u>VII</u>	ce		
3	27-9-13	Electronic Payload	<u>VII</u>	ce		
4	28-9-13	Introducers	<u>VIII</u>	ce		
		Introducers detection				
4	1-9-13	Pass Word Management	<u>VIII</u>	ce		
1	2-9-13	Malicious Software	<u>VIII</u>	ce		
3	3-9-13	Viruses and	<u>VIII</u>	ce		
		Types of Viruses				

## LESSON PLAN

[illegible]