Sample Syllabus
CIS 525
Principles of Cryptography

Text	Cryptography and Network Security William Stallings ISBN 0136097049
	Lecture notes posted on Blackboard

Course Objective and Overview:

Course Description:

The course examines basic cryptography principles such as encryption, hashes, message authentication codes, digital signatures, digital certificates and network defense.

Course Learning Objectives:

Understand Symmetric Cipher Model
Understand Substitution Ciphers
Understand Transposition Ciphers
Understand Block Cipher Principles
Understand DES
Be able to apply Block Cipher Design Principles
Understand AES
Be able to conduct basic Block Cipher Operations
Understand Principles of Public Key Cryptosystems
Understand the RSA Algorithm
Be able to apply Hash Functions
Understand SHA and SHA-3
Be able to apply Message Authentication Codes
Understand Digital Signatures
Understand Key Management and Distribution
Be able to apply Public Key Infrastructure
Understand User Authentication Protocols
Be able to apply Remote User Authentication Principles
Understand Kerberos
Understand Federated Identity Management
Understand Transport Layer Security
Be able to apply Secure Socket Layer (SSL)
Be able to apply Transport Layer Security (TLS)
Be able to apply HTTPS
Be able to apply Secure Shell (SSH)

Understand Wireless Network Security
Be able to apply Wireless Application Protocol Overview
Be able to apply Wireless Transport Layer Security
Understand E-Mail Security and IP Security

Responsibility

The student shall be responsible for all material covered in the class lectures. Each exam will include not only the material from the assigned text chapters, but also from the readings, tours, guest lectures and any other materials covered in the class lectures.

You are also responsible for any announcements made in class. Often times I have to change the Class Schedule or I may announcements relevant for assignments. Schedule changes will be posted on my website. We will have several external speakers during the semester.

I do expect class participation from every individual in the course. Students often learn many things from student colleagues and questions in class. This participation is vital to classroom discussion. It will be a part of the evaluation of this course.

In Class Labs – We conduct some packet sniffing labs in August to illustrate how easy it is to intercept information without the use of cryptography.

Paper – Students in CIS 525 will have to write a paper (5-10) concerning some aspect of cryptography. This could be a case or a topic. This will be due on the last day of class, however, the topic must be approved by July 4.

Evaluation

The final course grade will be computed from the following inputs:

Exam 1	**30.00%**	
Final Exam	**30.00%**	**2 Tests = 60%**
Class Participation	**20.00%**	
Paper	**20.00%**	

TOTAL	**100%**	

The final course grade will be determined as follows:

90 or above	A
80-89.99	B
70-79.99	C
60-69.99	D
Less than 60%	F

Make-up Exams

There will not be any make up exams unless there are dire circumstances. It is up to the student to notify the professor under all circumstances and the student will be held accountable. Documentation for the absence will be required. A grade of 0 will be placed in place of the exam until the percentage is replaced. Under absolutely no circumstances will the final be made up.

Disabilities

Anyone with a disability that may limit participation with regular classroom activities should inform the professor at the beginning of the term. Proper adjustments will be made to compensate for limitations. **Remember that informing the professor of these disabilities is the responsibility of the student.**

Academic Integrity

I have adopted a very simple but strict policy within the overall university guidelines to maintain academic integrity. **In all cases of academic dishonesty (for example, cheating of any kind in labs, quizzes and exams or plagiarism in project reports), the involved student(s) will get the grade of Fail (F) for the whole course.** Exceptions will be made only in rare cases, in which the student makes a convincing case of the situation beyond the control of the student.

Sample Topics:

Week 1
Module 1 - Cryptography and Classical Encryption
1.1 Computer Security Concepts
1.2 OSI Security Architecture
1.3 Security Attacks
1.4 Security Mechanisms
1.5 Model for Network Security
1.6 Symmetric Cipher Model
1.7 Substitution
1.8 Transposition
1.9 Rotor Machines
1.10 Stenography

Week 2
Module 2 – Block Ciphers, DES, and AES
2.1 Block Cipher Principles
2.2 DES

2.3 Strength of DES
2.4 Differential and Linear Cryptanalysis
2.5 Block Cipher Design Principles
2.6 AES Origins
2.7 AES Structure
2.8 AES Round Functions
2.9 AES Key Expansion
2.10 AES Implementation

Week 3
Module 3 Block Cipher Operations
3.1 Multiple Encryption and Triple DES
3.2 Electronic Codebook Mode
3.3 Cipher Block Chaining Mode
3.4 Cipher Feedback Mode
3.5 Output Feedback Mode
3.6 Counter Mode
3.7 XTS Mode for Block Oriented Storage Devices

Week 4
Module 4 Public Key Encryption
4.1 Principles of Public Key Cryptosystems
4.2 RSA Algorithm
4.3 Diffie Hellman Key Exchange
4.4 ElGamal
4.5 Elliptic Curve

Week 5
Module 5 Hash Functions
5.1 Application of Hash Functions
5.2 Simple Has Functions
5.3 Requirements and Security
5.4 Cipher Block Chaining based Hash Functions
5.5 SHA
5.6 SHA-3

Week 6
Module 6 Message Authentication Codes
6.1 Message Authentication Requirements
6.2 Message Authentication Functions
6.3 Message Authentication Codes
6.4 MAC Security
6.5 Hash Function MACs - HMACs
6.6 Block Cipher MACs – DAA and CMAC
6.7 Authenticated Encryption – CCM and GCM

Week 7
Module 7 Digital Signatures
7.1 Digital Signatures
7.2 ElGamal Digital Signature Scheme
7.3 Schnorr Digital Signature Scheme
7.4 Digital Signature Standard (DSS)

Week 8
Module 8 Key Management and Distribution
8.1 Symmetric Key Distribution using Symmetric Encryption
8.2 Symmetric Key Distribution using Asymmetric Encryption
8.3 Distribution of Public Keys
8.4 X.509 Certificates
8.5 Public Key Infrastructure

Week 9
Module 9 User Authentication Protocols
9.1 Remote User Authentication Principles
9.2 Remote User Authentication Principles using Symmetric Encryption
9.3 Kerberos
9.4 Remote User Authentication Principles using Asymmetric Encryption
9.5 Federated Identity Management

Week 10
Module 10 Transport Layer Security
10.1 Web Security Issues
10.2 Secure Socket Layer (SSL)
10.3 Transport Layer Security (TLS)
10.4 HTTPS
10.5 Secure Shell (SSH)

Week 11
Module 11 Wireless Network Security
11.1 802.11 Overview
11.2 802.11 Security
11.3 Wireless Application Protocol Overview
11.4 Wireless Transport Layer Security
11.5 WAP End to End

Week 12
Module 12 E-Mail Security and IP Security
12.1 Pretty Good Privacy (PGP)
12.2 S/MIME
12.3 DomainKeys Identified Mail (DKIM)
12.4 IP Security Overview
12.5 IP Security Policy

12.6 Encapsulating Security Payload
12.7 Combining Security Associations
12.8 Internet Key Exchange
12.9 Cryptographic Suites