

Spring 2008
CSC/ECE574 Intro to Computer and Network Security

Calendar

[Calendar](#) · [Syllabus](#) · [Message Board](#) · [Exams](#) · [Project](#) · [Links](#)

Week	Day	Topic	Due	Reading
Jan 07-11	Monday	(no class)		
	Wednesday	Introduction [1c , 6c , 6bw]		Text Ch. 1
Jan 14-18	Monday	Basic Cryptographic Schemes [1c , 6c , 6bw]		Text Ch. 2
	Wednesday	Secret Key Crypto (DES) [1c , 6c , 6bw]	HW1 (due Sat. 1/19) Solutions Zip file of Java program for computing letter, digram, and trigram frequencies, provided by TJ O'Connor	Text Ch. 3
Jan 21-25	Monday	(no class, university holiday)		
	Wednesday	Secret Key Crypto (AES) [see lecture notes above]		Text Ch. 3
Jan 28-Feb 01	Monday	Block Chaining Modes and Message Authentication Codes [1c , 6c , 6bw]		Text Ch. 4
	Wednesday	Hash Functions and Message Digests [1c , 6c , 6bw]	HW2 (due Thursday, 1/31 at noon) Solutions [PDF] AES calculator DES calculator	Text Ch. 5
Feb 04-08	Monday	Hash Functions and Message Digests (cont'd)		Text Ch. 5
	Wednesday	Number Theory for Crypto [1c , 6c , 6bw]		Text Ch. 7
Feb 11-15	Monday	Exam #1		
	Wednesday	Number Theory for Crypto (cont'd)		Text Ch. 7
Feb 18-22	Monday	Public Key Cryptography [1c , 6c , 6bw]	HW3 (due Tues. 2/19 at 11:45pm) Solutions [PDF]	Text Ch. 6
	Wednesday	Public Key Cryptography (cont'd)		Text Ch. 6
Feb 25-29	Monday	User Authentication [1c , 6c , 6bw]		Text Ch. 9, 10
	Wednesday	Analysis of Security Protocols [1c , 6c , 6bw]		Text Ch. 11
Mar 03-07	Monday	(spring break, no class)		
	Wednesday	(spring break, no class)		
Mar 10-14	Monday	Analysis of Security Protocols (cont'd)	HW4 (due Tuesday 3/11 at 11:45pm) Solutions	Text Ch. 11
	Wednesday	Protocol Example: Kerberos [1c , 6c , 6bw]		Text Ch. 13, 14
Mar 17-21	Monday	<i>Class Cancelled</i>		
	Wednesday	Exam #2		
Mar 24-28	Monday	Certificates and PKI [1c , 6c , 6bw]		Text Ch. 15
	Wednesday	The Project		
Mar 31-Apr 04	Monday	Protocol Example: IPSec and IKE [1c , 6c , 6bw]		Text Ch. 17, 18
	Wednesday	Protocol Example: SSL/TLS [1c , 6c , 6bw]		Text Ch. 19
	Monday	Access Control, Operating Systems Security [1c , 6c , 6bw]	HW5 (Solutions)	Security Eng., 2nd ed., by R. Anderson Chapters 4 (Access Control) and 7 (Multilevel Security)

07-11	Wednesday	Firewalls and Intrusion Detection Systems [Lc. 6c. 6bw]		IDS FAQ (sections on The Basics and Terms, Theory, and Research), Security Engineering , Ch. 18 (Network Attack and Defense)
Apr 14-18	Monday	Firewalls and Intrusion Detection Systems		TBD
	Wednesday	Project Status Meetings (3:30-7:30pm)	HW6 (due Friday April 18, 11:45pm) (Solutions)	
Apr 21-25	Monday	(no class)		
	Wednesday	Exam #3 (Solutions)		
Apr 28-May 02	Monday	(no class, finals week)		
	Wednesday	(no class, finals week)	Project Papers (due Friday May 02 at 11:45pm)	
May 05	Monday, 1-5pm	Project Presentations (submit online by 12:00 noon)		

Notes:

- Classes held Mon/Wed 3:50-5:05
- January 15 Tuesday: Last day to add a course without permission of instructor.
- January 23 Wednesday: Last day to enroll (register) or to add a course.
- March 19 Wednesday: Last day to withdraw or drop a course without a grade, or to change from credit to audit.

[Douglas S. Reeves](#)

[Computer Science Department](#)

[N.C. State University](#)

Last modified on January 02, 2008
 Send comments to: [web page maintainer](#)

designed with 