Foundations of Cryptography

CS668A
Fall 2003
Prof. Rebecca N. Wright

Syllabus
4 September, 2003

Note: This class was previously called CyberSecurity Techniques and Mechanisms, and has also been listed by CpE as Computer & Telecomm Security. Foundations of Cryptography is a more accurate name than either of these.

Location, etc:

Place:	Pierce 120
Time:	6:15pm–8:45pm Thursdays
Professor:	Rebecca Wright, `rwright@cs.stevens-tech.edu`
Office hours:	2-4pm Tuesdays, 216 Lieb

Description:

This course provides a broad introduction to cornerstones of security (authenticity, confidentiality, message integrity, and non-repudiation) and the mechanisms to achieve them, as well as the underlying mathematical basics. Topics include: block and stream ciphers, public-key systems, key management, certificates, public-key infrastructure (PKI), digital signatures, non-repudiation, and message authentication. Various security standards and protocols such as DES, AES, PGP, and Kerberos, are studied.

Prerequisites: MA 502 (Mathematical Foundations of Computer Science) and CS 590 (Introduction to Data Structures and Algorithms), or permission of the instructor.

Textbooks:

Douglas Stinson, *Cryptography: Theory and Practice*, second edition, CRC Press. (Required).

Alfred Menezes, Paul van Oorschot, and Scott Vanstone, *Handbook of Applied Cryptography*, CRC Press. (Optional).

I think you will find the Handbook a useful supplement to the main text. It is accessible on the web, at `http://www.cacr.math.uwaterloo.ca/hac/`.

Syllabus:

September 4 — Introduction, Classical Cryptography
Reading: ch. 1

September 11 — Information Theory
Reading: ch. 2

September 18	HOMEWORK 1 DUE Block Ciphers, AES **Reading: ch. 3**
September 25	Hash Functions **Reading: ch. 4**
October 2	Message Authentication Codes
October 9	HOMEWORK 2 DUE Public Key Encryption: intro, RSA **Reading: ch. 5**
October 16	MIDTERM EXAM
October 23	Public Key Encryption: Diffie-Hellman, ElGamal **Reading: ch. 6**
October 30	Public Key Encryption: additional topics
November 6	HOMEWORK 3 DUE Digital Signatures **Reading: ch. 7**
November 13	Digital Signatures, cont'd
November 20	Additional Topics
November 27	THANKSGIVING RECESS: NO CLASS
December 4	HOMEWORK 4 DUE Additional Topics
December 11	FINAL EXAM

Grading:

Homework Assignments	40%	(lowest score dropped)
Midterm Exam	25%	
Final Exam	25%	
Class Participation	10%	

Late policy:

Assigments are due at the *start* of class on their due dates. Late assignments will not be accepted. All exceptions must be cleared in advance, and will only be granted in extreme circumstances.