Foundations of Cryptography

CS668A  Syllabus  Fall 2004
Prof. Rebecca N. Wright

Location, etc:
Place: Burchard 124
Time: 6:15pm–8:45pm Thursdays
Professor: Rebecca Wright, rwright@cs.stevens.edu
Office hours: 3–5pm Tuesdays, 216 Lieb
Teaching Assisant Sun Qi (River), sunq@cs.stevens-tech.edu
Office hours: 3–5pm Thursdays, 101 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. Topics include: block and stream ciphers, public key cryptosystems, 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 SSL are also discussed.

Prerequisites: CS/MA 503 (Discrete Mathematics for Cryptography) and either CS 600 (Data Structures and Algorithms) or CS 434 Theory of Computation, or permission of the instructor.

Textbooks:

Syllabus:
September 2  Introduction, Classical Cryptography
  Reading: ch. 1

September 9  Classical Cryptography, cont’d; Information Theory
  Reading: ch. 2

September 16  HOMEWORK 1 DUE
  Block Ciphers
  Reading: ch. 3

September 23  Advanced Encryption Standard (AES)
September 30  Hash Functions
\textbf{Reading: ch. 4}

October 7  \textbf{Homework 2 DUE}
Message Authentication Codes

October 14  \textbf{Midterm Exam}

October 21  Public Key Encryption: intro, RSA
\textbf{Reading: ch. 5}

October 28  Public Key Encryption: Diffie-Hellman, ElGamal
\textbf{Reading: ch. 6}

November 4  \textbf{Homework 3 DUE}
Public Key Encryption: additional topics

November 11  Digital Signatures
\textbf{Reading: ch. 7}

November 18  Digital Signatures, cont’d

November 25  \textbf{Thanksgiving Recess: No Class}

December 2  \textbf{Homework 4 DUE}
Key Management

December 9  \textbf{Final Exam}

\textbf{Grading:}

\begin{itemize}
  \item Homework Assignments 40%  (lowest score dropped)
  \item Midterm Exam 25%
  \item Final Exam 25%
  \item Class Participation 10%
\end{itemize}

\textbf{Late policy:}

Assignments are due at the \textit{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. This somewhat strict policy is intended to be balanced by the dropping of the lowest homework score.