Lecture 1: Introduction

CS 6903: Modern Cryptography
Spring 2009

Nitesh Saxena
Polytechnic University

Outline

• Administrative Stuff
• Introductory Technical Stuff
Some Pointers

• Course Web Page
  http://isis.poly.edu/courses/cs6903-s10
• Instructor: Nitesh Saxena
• Office: LC228
• Email: nsaxena@poly.edu
• Phone No: 718-260-3116
• Office Hours: Wednesday 4-5pm (or by appointment)
• MyPoly Web Page: http://my.poly.edu/

About the Instructor

• PhD from UC Irvine
• Research in computer and network security, and applied cryptography
• Web page: http://cis.poly.edu/~nsaxena
Prerequisites

1. Discrete Mathematics (MA 2312/2322)
2. Design and Analysis of Algorithms (CS603 or CS3414)
3. Data Analysis (MA2212) or equivalent

Basically, what you need is:
• Good mathematical background
• Knowledge of basic probability theory
• Knowledge of basic algorithms

• If you don’t satisfy the prerequisites as such, but are interested, I encourage you to take the course. But, do talk to me.

What to Expect

• The course would be theoretical
  – With theorems and proofs
  – No programming whatsoever
• We will have few homeworks
• We will have a project based on a relevant topic in cryptography
  – I can suggest some projects
  – You are also free to choose your own project, after discussion with me
• There will be a mid-term quiz
• Grading
  – 50% homeworks
  – 10% mid-term quiz
  – 10% notes scribing (latex)
  – 30% project (plus a class presentation of the project)
What to Expect

• Homeworks to be completed individually
  – No collaboration
• Latex scribing to be done in **groups of 3**
• Project is to be done in **groups of 3**
• Mid-term – no collaboration

What are my expectations of you

• Attend lectures
• Take notes; ask questions
• Review your notes and the scribe right after the lecture; refer to relevant material
• Use my office hrs to clear your doubts and for any help
• I’ll try to review last lecture at the beginning of every lecture
  – Ask questions then
• Turn your homeworks on time; no extensions or late submissions are allowed
• Be prompt in choosing your project topic
• Please use your Poly email id to communicate with me; I’ll be using it to communicate with you.
Today’s scribe

• Volunteer?
• Olufisan, Sarwar, and Nathan?

• I’ll bring in a sign-up sheet next time.

Other Security Courses at Poly

• Computer Security CS 392/6813
• Network Security CS 6823
• Other specialized courses
Course References

• Primary reference: some free online lecture material developed by well-known cryptographers, such as:
  – http://www-cse.ucsd.edu/users/mihir/papers/gb.html
  – http://cseweb.ucsd.edu/~mihir/cse207/index.html

• Secondary reference:
  – Introduction to Modern Cryptography, Jonathan Katz and Yehuda Lindell (available from Amazon)

Other References

• The online book on applied cryptography might be useful:
  – http://www.cacr.math.uwaterloo.ca/hac/

• Other links to be provided as we proceed
What is Cryptography

• Etymologically: secret (crypt) writing (graphy)
• Study of mathematical techniques to achieve various goals in information security, such as confidentiality, integrity, availability, non-repudiation, etc (we cover these today!)
• Not the only (and not a sufficient) means of providing information security, rather a subset of techniques
• Quite an old field!
• A cryptographer designs the code, a cryptanalyst tries to break it
• Philosophically, cryptography is a contest between the cryptographer and the cryptanalyst!

What is the course about

• Study of modern cryptography from a theoretical perspective
• Study of cryptographic primitives that are the building-blocks of various cryptographic applications
• “provable security” concept; formal analysis
How we would proceed in the course

- Study a cryptographic primitive (such as encryption)
- Study its security notions
  - What it means for a cryptographic primitive to be secure (for example, what it means for an encryption scheme to be secure)
  - What is the adversarial model
- Study its various constructions (such as symmetric key encryption DES, public key encryption RSA)
- Formally analyze the security of a particular construction based on a particular security notion
  - Theorem-Proofs (provable security)
- [Time permitting] Study how to combine various cryptographic primitives for a cryptographic application/protocol

CS 6903 vs. CS 392/6813

- Study a cryptographic primitive (such as encryption)
- Study its security notions
  - What it means for a cryptographic primitive to be secure (for example, what it means for an encryption scheme to be secure)
  - What is the adversarial model
- Study its various constructions (such as symmetric key encryption DES, public key encryption RSA)
- Formally analyze the security of a particular construction based on a particular security notion
  - Theorem-Proofs (provable security)
**Tentative Course Schedule**

- Symmetric encryption (block ciphers)
- Pseudo-random functions
- Hash functions and random oracles
- Message authentication code
- Number Theory
- Asymmetric encryption
- Digital signatures
- [Protocols for authenticated key exchange]

**Why Take this Course**

- Cryptography is HOT
- If you are “theory-inclined”, it’s an interesting course to take
- If you work in the general area of security, it’s an important course to take
- One of the mandatory course for the MS program in Cyber-Security
- According to the MS/PhD course curriculum, you are required to take at least 2 courses from the THEORY area, of which this this course is one.
  - Theory Core Area for MS
    - CS 6003 Foundations of Computer Science
    - CS 6033 Design and Analysis of Algorithms I
    - CS 6043 Design and Analysis of Algorithms II
    - CS 6753 Theory of Computation
    - **CS 6903 Modern Cryptography**
    - CS 9173 Computational Geometry
Some Basic Goals in Information Security

- Confidentiality
- Authentication
- Integrity
- Availability
- Non-repudiation
- Cryptography can be used to achieve these goals
  - Let’s see how and warm up a little bit!!
  - Please take notes

Today’s Reading