



Lecture 1: Introduction

CS996: Modern Cryptography **Spring 2007**

Nitesh Saxena



Outline

- Administrative Staff
- Introductory Technical Staff



Some Pointers

- Course Web Page
<http://isis.poly.edu/courses/cs996-s2007>
- Instructor: Nitesh Saxena
 - Office: LC 228
 - Email: nsaxena@poly.edu
 - Phone No: 718-260-3116
 - Office Hours: Wednesday 3-4pm (or by appointment)
- MyPoly Web Page: <http://my.poly.edu/>



About the Instructor

- A recent PhD graduate 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 cool projects
 - You are also free to choose your own project, after discussion with me

- **There will be no exam; no programming**

- **Grading**
 - **60% homeworks**
 - **40% project (plus a class presentation of the project)**

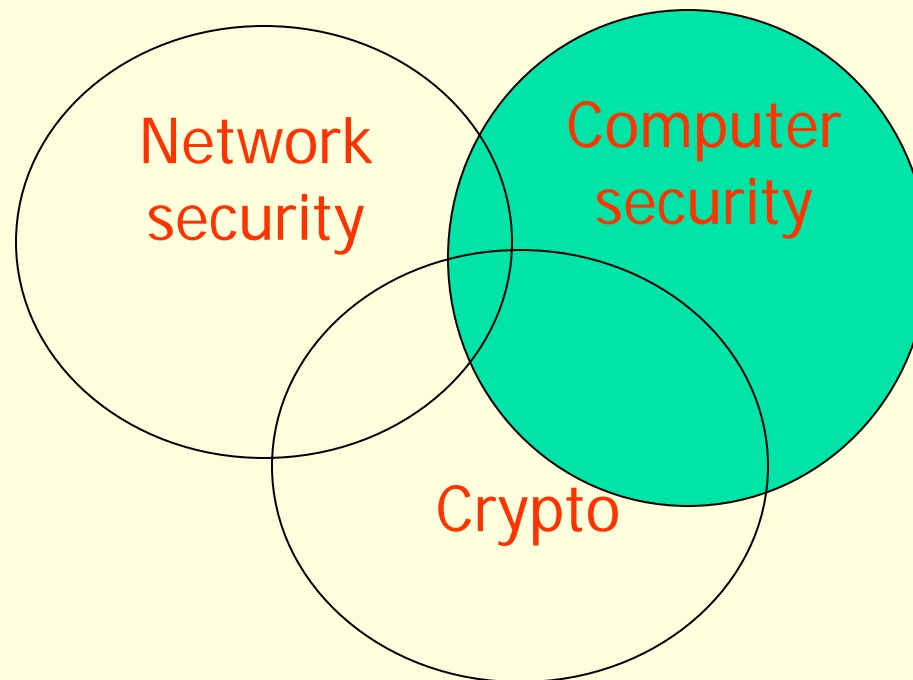
- I might/will make mistakes
 - Please point them out
 - Talk to me if you have any complaints (or send me an anonymous email ☺)

- **I guarantee that**
 - you'll have fun and you'll learn
 - you won't become experts, but you will learn enough to move on!
 - you'll hopefully get motivated to pursue research in this area, ultimately



Other Security Courses at Poly

- Computer Security 392/681
- Network Security 682
- Other specialized courses





Course References

- No textbook – no \$\$ to be spent by you 😊
- Mostly some free online lecture material developed by well-known cryptographers, such as:

<http://www-cse.ucsd.edu/users/mihir/papers/gb.html>

- Other links to be provided as we proceed



Grading

- 60% - Homeworks (probably 6 in #)
- 40% - Project (and presentation)



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 crypto primitives for a cryptographic application/protocol



CS996 vs CS681

- 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,
- 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
- According to the new 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

- CS 600 Foundations of Computer Science
- CS 603 Design and Analysis of Algorithms I
- CS 604 Design and Analysis of Algorithms II
 - CS 675 Theory of Computation
 - **CS 996 Cryptography**
 - CS 917 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

- <http://www-cse.ucsd.edu/users/mihir/cse207/w-intro.pdf>