



Advanced Topics in Cryptography and Network Security

Breno de Medeiros

Department of Computer Science

Florida State University

Class Reference Sheet

- ⑥ Instructor's webpage: <http://www.cs.fsu.edu/~breno>
- ⑥ Course webpage:
<http://www.cs.fsu.edu/~breno/CIS-6930/advanced.html>
- ⑥ Textbook:
 - △ Modern Cryptography: Theory and Practice, by Wenbo Mao
- ⑥ Office hours: Tuesdays and Wednesdays, 3:00–5:00pm, at LOVE 269, or by appointment.
- ⑥ Phone: 645-2356
- ⑥ Electronic mail: breno [at] “cs department domain name”

Course goal

To prepare you for research in the applied cryptography and network security areas. This requires that you acquire a number of different skills: How you will be evaluated:

- ⑥ Learn how to define/understand security notions; **Midterm/ presentations/ class participation / essay**
- ⑥ Understand the structure of a security proof; **Midterm/ presentations/ class participation / essay**
- ⑥ Familiarize yourself with foundational works; **presentations/ essay**
- ⑥ Know how to organize and write a paper or technical report. **presentations/ essay**

Evaluation

⑥ Grade formula: $0.2M + 0.15C + 0.25P + 0.4E$, where M is the midterm grade, C is your class participation grade, P is the grade on presentations, and E is the grade of your essay.

⑥ What constitutes classroom participation?

- △ Attendance
- △ Questions asked in class, via e-mail, during office hours
- △ Participation in classroom discussions

The rationale of classroom participation grade is that research requires being able to communicate with colleagues and exchange ideas.

⑥ Presentations: A paper reading list will be provided, and each paper will be assigned two students, a *presenter* and a *moderator*.

- △ The presenter prepares a 45-minute slide presentation including

Course contents

- ⑥ Randomized complexity classes
- ⑥ One-way functions and complexity-based security
- ⑥ Security notions of signature schemes, public key encryption schemes, message authentication codes and symmetric encryption modes
- ⑥ Provably secure constructions of the above primitives
- ⑥ Analysis of security protocols using formal methods: formal specification, and state-system exploration.



Motivation for the use of complexity-theoretical notions in security

Breno de Medeiros

Department of Computer Science

Florida State University

Example: encryption

A typical application of cryptography in network security is to enable two parties to communicate *confidentially* over a (non-physically secured) communication means, such as radio waves, the Internet, etc.

- ⑥ Traditionally, this is achieved via *encryption*. Alice uses encryption to transform intelligible messages M (plaintext) into obscured messages C (ciphertext). Bob uses the inverse operation (decryption) to recover M from C .
 - △ Security requirement: Eavesdropper cannot figure out which message M was sent from Alice to Bob, even if it can capture the ciphertext C during transmission.

Question: How to formalize such a requirement so that it may be (mathematically, formally) proven to hold (or not to hold)?

Example: Key agreement

To communicate efficiently using encryption, Alice and Bob must have agreed on a secret value that only they know. This can be achieved using communication through a physically secure channel to exchange a common secret *directly*; or, Alice and Bob can exchange some messages through public channels and extract from these a common secret value that remains secret from eavesdroppers.

- ⑥ In either case, we would like to be able to make evaluations such as: *The key agreement protocol is secure/insecure.*

From Security to Complexity Theory

In order to formalize this, we need to understand notions such as

- ⑥ *Efficient Computability*: For e.g., an encryption scheme must be usable;
- ⑥ *Computational Infeasibility*: E.g., an eavesdropper should not be able to figure out the contents of encrypted messages.

These are notions from complexity theory.