CS 600.442: Modern Cryptography

Instructor: Abhishek Jain

Fall 2016

What is Cryptography?

- **Controlling access to information**

What is Cryptography?

- **Controlling access to information**
    - “Who” learns “what?”

What is Cryptography?

- **Controlling access to information**
    - "Who" learns "what?"
    - "Who" can influence?

What is Cryptography?

- **Controlling access to information**
    - "Who" learns "what?"
    - "Who" can influence?
- **Relation to other areas**

What is Cryptography?

- **Controlling access to information**
  - “Who” learns “what?”
  - “Who” can influence?
- **Relation to other areas**
  - Mathematical foundation of Information Security

What is Cryptography?

- **Controlling access to information**
  - “Who” learns “what?”
  - “Who” can influence?
- **Relation to other areas**
  - Mathematical foundation of Information Security
  - Large intersection with: complexity theory, information theory, number theory, linear algebra, combinatorics...

Course Objectives

Course Objectives

- Learn the modern, reduction based, approach to Cryptography

Course Objectives

- Learn the modern, reduction based, approach to Cryptography
- Introduce some of the latest topics in this area

Course Objectives

- Learn the modern, reduction based, approach to Cryptography
- Introduce some of the latest topics in this area
- Learn the mathematical language used to express cryptographic concepts and **speak** this language

Course Objectives

- Learn the modern, reduction based, approach to Cryptography
- Introduce some of the latest topics in this area
- Learn the mathematical language used to express cryptographic concepts and **speak** this language
- Think intuitively but write rigorous proofs

Course Objectives

- Learn the modern, reduction based, approach to Cryptography
- Introduce some of the latest topics in this area
- Learn the mathematical language used to express cryptographic concepts and **speak** this language
- Think intuitively but write rigorous proofs
- Students encouraged to conjecture

Course Objectives

- Learn the modern, reduction based, approach to Cryptography
- Introduce some of the latest topics in this area
- Learn the mathematical language used to express cryptographic concepts and **speak** this language
- Think intuitively but write rigorous proofs
- Students encouraged to conjecture

Grand aim: Initiate into state-of-the-art research in Cryptography

Pre-requisites

No background in Cryptography is necessary. However, the following are expected:

- Basic mathematical maturity, e.g., comfortable with "Definitions" and "Proofs"
- Basic familiarity with **probability**
- Basic familiarity with asymptotic notation, **P** & **NP** complexity classes, Turing machines, Circuits
- If you have taken undergraduate algorithms/theory of computation and basic math courses involving proofs, you will do just fine. Otherwise, this is NOT the course for you.

General Information

- **Course website:** Link on my homepage http://www.cs.jhu.edu/∼abhishek
- **Office Hours:** Drop by Malone 315 or email `abhishek@cs.jhu.edu`
- **Teaching Assistant:** Gijs Van Laer, `gijs.vanlaer@jhu.edu`
- **Review Session:** Fridays, 3-4pm, Malone 228

Grading

- **Homeworks:** 3 HW assignments, each counts 10%, total 30%, towards your final grade.

Grading

- **Homeworks:** 3 HW assignments, each counts 10%, total 30%, towards your final grade.

— Late homework submission: HWs that are 0-24 hours late will lose **HALF** of their value. HWs submitted more than 24 hours late carry no value at all.

Grading

- **Homeworks:** 3 HW assignments, each counts 10%, total 30%, towards your final grade.

— Late homework submission: HWs that are 0-24 hours late will lose **HALF** of their value. HWs submitted more than 24 hours late carry no value at all.

- **Mid-term:** 20% (Date: Oct 19, 2016)

Grading

- **Homeworks:** 3 HW assignments, each counts 10%, total 30%, towards your final grade.

— Late homework submission: HWs that are 0-24 hours late will lose **HALF** of their value. HWs submitted more than 24 hours late carry no value at all.

- **Mid-term:** 20% (Date: Oct 19, 2016)
- **Final:** 40% (Date: Dec 19, 2016)

Grading

- **Homeworks:** 3 HW assignments, each counts 10%, total 30%, towards your final grade.

— Late homework submission: HWs that are 0-24 hours late will lose **HALF** of their value. HWs submitted more than 24 hours late carry no value at all.

- **Mid-term:** 20% (Date: Oct 19, 2016)
- **Final:** 40% (Date: Dec 19, 2016)
- **Scribes:** 10% of your grade. Use template available on class website.

Scribes

- **Due date:** DUE in 1 week from lecture date.

Scribes

- **Due date:** DUE in 1 week from lecture date.

— Late Scribe submission: Scribes submitted 0-24 hours late will lose **HALF** of their value. Scribes submitted more than 24 hours late carry no value at all.

Scribes

- **Due date:** DUE in 1 week from lecture date.

— Late Scribe submission: Scribes submitted 0-24 hours late will lose **HALF** of their value. Scribes submitted more than 24 hours late carry no value at all.

- Must meet with TA or instructor 2-3 days before the due date for feedback on scribe quality. Its up to you to setup meeting by email.

Scribes

- **Due date:** DUE in 1 week from lecture date.

— Late Scribe submission: Scribes submitted 0-24 hours late will lose **HALF** of their value. Scribes submitted more than 24 hours late carry no value at all.

- Must meet with TA or instructor 2-3 days before the due date for feedback on scribe quality. Its up to you to setup meeting by email.
- Do not just copy-paste from class presentations. Scribes must include formal definitions and proofs with detailed explanations. Scribes are meant to supplement class presentations.

Collaboration

- You can collaborate with other students on homework problems

Collaboration

- You can collaborate with other students on homework problems
- However: you must write the solutions in your own words

Collaboration

- You can collaborate with other students on homework problems
- However: you must write the solutions in your own words
- You must also list the names of students you collaborated with for each problem

Collaboration

- You can collaborate with other students on homework problems
- However: you must write the solutions in your own words
- You must also list the names of students you collaborated with for each problem
- Do not collaborate with more than 2 students.

Plagiarism

Plagiarism will be dealt with strictly. You will be IMMEDIATELY reported.

If you have a problem, come and talk to me. Do NOT cheat!

How to use the course

- **Grades:** Do well in homeworks & exams
- **Research:**
  - Solve extra-credit questions
  - Read additional prescribed material
  - Discuss with me
  - Target: find a topic you are interested in

Syllabus

The main (basic & advanced) topics we will cover:

- Modern approach based on reduction to hard problems
- One way functions
- Pseudo-randomness
- Symmetric Encryption
- Public-Key Encryption
- Hash Functions & Digital Signatures
- Zero-Knowledge Proofs
- Secure Multiparty Computation

Syllabus continued . . .

Some not-so-basic topics we will discuss (time permitting):

- Identity-based Encryption
- Attribute-based Encryption
- Fully Homomorphic Encryption
- Functional Encryption
- Program Obfuscation

Textbook

- No required or prescribed textbook.

Textbook

- No required or prescribed textbook.
- Class lectures and scribes will serve as main study material

Textbook

- No required or prescribed textbook.
- Class lectures and scribes will serve as main study material
- Look for suggestions on class website for supplementary online reading material and books.

Important Note

- This is NOT a computer security course.
- We will never talk about topics such as:
  - Memory overflow
  - SQL Injection
  - Viruses and Worms
  - Malware Protection
  - Phishing attacks
  - ...