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?”
What is Cryptography?

- Controlling access to information
  - “Who” learns “what?”
  - “Who” can influence “what?”

- Relation to other areas

Instructor: Abhishek Jain
CS 601.642/442: Modern Cryptography
Fall 2019
What is Cryptography?

- Controlling access to information
  - “Who” learns “what?”
  - “Who” can influence “what?”

- Relation to other areas
  - Mathematical foundation of Information Security
What is Cryptography?

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

- **Relation to other areas**
  - Mathematical foundation of Information Security
  - Large intersection with: complexity theory, information theory, number theory, linear algebra, combinatorics...
Course Objectives

Learn the modern, provable-security 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
Course Objectives

- Learn the modern, provable-security based approach to Cryptography
Course Objectives

- Learn the modern, provable-security based approach to Cryptography
- Introduce some of the latest topics in this area
Course Objectives

- Learn the modern, provable-security 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, provable-security 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, provable-security 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, provable-security 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
No background in Cryptography is necessary. However, the following are expected:

- Basic mathematical maturity, e.g., comfort with “Definitions” and “Proofs”
- Basic familiarity with probability, e.g., Random Variables, Expectation, Union Bound, Conditional Probability
- When and how to use tail bounds (Markov, Chebyshev, Chernoff)
- Basic familiarity with asymptotic (Big-O) notation,
- $P$ & $NP$ complexity classes, Turing machines
- If you have taken undergraduate theory of computation/algorithms and basic math courses involving proofs, you will do just fine.
- For a refresh: Review notes on course website.
Pre-requisites

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

- Basic mathematical maturity, e.g., comfort with “Definitions” and “Proofs”
Pre-requisites

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

- Basic mathematical maturity, e.g., comfort with “Definitions” and “Proofs”
- Basic familiarity with probability

For a refresh: Review notes on course website.

Required reading before next class.

Instructor: Abhishek Jain
Pre-requisites

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

- Basic mathematical maturity, e.g., comfort with “Definitions” and “Proofs”
- Basic familiarity with **probability**
  - E.g., Random Variables, Expectation, Union Bound, Conditional Probability
Pre-requisites

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

- Basic mathematical maturity, e.g., comfort with “Definitions” and “Proofs”
- Basic familiarity with **probability**
  - E.g., Random Variables, Expectation, Union Bound, Conditional Probability
  - When and how to use tail bounds (Markov, Chebyshev, Chernoff)
Pre-requisites

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

- Basic mathematical maturity, e.g., comfort with “Definitions” and “Proofs”
- Basic familiarity with **probability**
  - E.g., Random Variables, Expectation, Union Bound, Conditional Probability
  - When and how to use tail bounds (Markov, Chebyshev, Chernoff)
- Basic familiarity with asymptotic (Big-O) notation, **P & NP** complexity classes, Turing machines
Pre-requisites

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

- Basic mathematical maturity, e.g., comfort with “Definitions” and “Proofs”
- Basic familiarity with **probability**
  - E.g., Random Variables, Expectation, Union Bound, Conditional Probability
  - When and how to use tail bounds (Markov, Chebyshev, Chernoff)
- Basic familiarity with asymptotic (Big-O) notation, **P & NP** complexity classes, Turing machines
- If you have taken undergraduate theory of computation/algorithms and basic math courses involving proofs, you will do just fine.
Pre-requisites

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

- Basic mathematical maturity, e.g., comfort with “Definitions” and “Proofs”
- Basic familiarity with **probability**
  - E.g., Random Variables, Expectation, Union Bound, Conditional Probability
  - When and how to use tail bounds (Markov, Chebyshev, Chernoff)
- Basic familiarity with asymptotic (Big-O) notation, **P & NP** complexity classes, Turing machines
- If you have taken undergraduate theory of computation/algorithms and basic math courses involving proofs, you will do just fine.
- **For a refresh**: Review notes on course website. *Required reading before next class.*
General Information

- **Course website:** Link on my homepage
  http://www.cs.jhu.edu/~abhishek

- **Office Hours:** Tuesdays 3:30-4:30pm, Malone 315

- **Teaching Assistant:** Arka Rai Choudhuri, achoud@cs.jhu.edu

- **Review Session:** Regular hours and locations TBA. (Optional, but strongly recommended.)
Grading

- **Homeworks**: 5 HW assignments, each counts 9%, total 45%.

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

- **Mid-term**: 15% (In Class. Tentative Date: Oct 30; may be changed.)

- **Final**: 30% (Take Home)

- **Class participation**: 10%

Instructor: Abhishek Jain
CS 601.642/442: Modern Cryptography
Fall 2019
**Grading**

- **Homeworks**: 5 HW assignments, each counts 9%, total 45%.
  - 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:** 5 HW assignments, each counts 9%, total 45%.
  - **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:** 15% (In Class. Tentative Date: Oct 30; may be changed.)
Grading

- **Homeworks**: 5 HW assignments, each counts 9%, total 45%.
  - **Late homework submission**: HWs that are 0-24 hours late will lose \textbf{HALF} of their value. HWs submitted more than 24 hours late carry no value at all.

- **Mid-term**: 15% (In Class. Tentative Date: Oct 30; may be changed.)

- **Final**: 30% (Take Home)
Grading

- **Homeworks**: 5 HW assignments, each counts 9%, total 45%.
  - 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**: 15% (In Class. Tentative Date: Oct 30; may be changed.)

- **Final**: 30% (Take Home)

- **Class participation**: 10%
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.
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 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
No required or prescribed textbook.
No required or prescribed textbook.

Class lectures and notes will serve as main study material. Will be available on class website.
No required or prescribed textbook.

Class lectures and notes will serve as main study material. Will be available on class website.

Look for suggestions on class website for supplementary online reading material and books.
The main (basic & advanced) topics we will cover:

- Modern provable-security approach based on reduction to hard problems
- One way functions
- Pseudo-randomness
- Key Agreement
- Symmetric Encryption
- Public-Key Encryption
- Hash Functions & Digital Signatures
- Zero-Knowledge Proofs
- Secure Multiparty Computation
Some not-so-basic topics we will discuss (time permitting):

- Identity-based Encryption
- Fully Homomorphic Encryption
- Functional Encryption
- Program Obfuscation
- Blockchains and Cryptocurrencies