Lecture 1

COSC-260 Codes and Ciphers
Adam O’Neill
Instructor: Adam O’Neill; adam@cs.georgetown.edu  
Office Hours: Tues & Thurs 2-3:30pm

TA: Mohammad Zaheri; mz394@georgetown.edu  
Office Hours: Mon & Weds 1-2:30pm

Grades are based on 50% problem sets, 25% midterm, 25% final

For problem sets, you can work together but must list your collaborators. Turn them in before class on the due date.
What’s Cryptography?
What’s Cryptography?

Broadly, how to communicate in the presence of an adversary.
What’s Cryptography?

Broadly, how to communicate in the presence of an adversary.

You may also think of a storage medium (e.g. Gmail server) as the communication channel.
What’s Cryptography?

Broadly, how to communicate in the presence of an adversary.

You may also think of a storage medium (e.g. Gmail server) as the communication channel.

Cryptography is full of counter-intuitive solutions to seemingly impossible problems!
Who Cares about Crypto?
Who Uses Crypto?
Who Uses Crypto?

You probably did, today!
Who Uses Crypto?

You probably did, today!

- **TLS/SSL** protocol (used for Gmail, Facebook, YouTube, etc.)
Who Uses Crypto?

You probably did, today!

- **TLS/SSL** protocol (used for Gmail, Facebook, YouTube, etc.)
- Tens of **thousands of apps** use crypto (many incorrectly...)
Basic Task: Secure Channels
Desired Properties
Desired Properties

**Privacy:** Adversary does not learn anything about the message.
Desired Properties

**Privacy:** Adversary does not learn anything about the message.

**Authenticity:** Bob is assured the message “really came from” Alice and was not modified.
Desired Properties

**Privacy:** Adversary does not learn anything about the message.

**Authenticity:** Bob is assured the message “really came from” Alice and was not modified.

But what do these *really mean*?
Modern Cryptography
Modern Cryptography

Modern cryptography deals with how to formalize and provably achieve such properties.
Modern Cryptography

Modern cryptography deals with how to formalize and provably achieve such properties.

Grew out of theoretical computer science in the 1980s, and has seen a surge of interest due to the Internet.
Provable Security

Lower-Level Primitive

Higher-Level Primitive

construction

reduction
Why is this the Right Approach?
Why is this the Right Approach?

Ad-hoc design is subject to **bug-then-patch** cycle. Very **dangerous** and costly.
Why is this the Right Approach?

Ad-hoc design is subject to bug-then-patch cycle. Very dangerous and costly.

Doesn’t make sense to try to design a secure encryption scheme without first asking what “secure” means.
Security Mindset
Security Mindset

Put on your adversary hat!
Security Mindset

Put on your adversary hat!
Ask what the risks and threats are. How might the system be attacked?
Security Mindset

Put on your adversary hat!
Ask what the risks and threats are. How might the system be attacked?
Be critical of security claims.
Security Mindset

Put on your adversary hat!
Ask what the risks and threats are. How might the system be attacked?
Be critical of security claims.

Our system is secure because it uses 128-bit keys!

How are they being used? What is the threat model? Do you have a security proof?
Beware of Human Fallibility
Beware of Human Fallibility

Edgar Allen Poe (an amateur cryptographer!) said “human ingenuity cannot concoct a cipher which human ingenuity cannot resolve.”
Beware of Human Fallibility

Edgar Allen Poe (an amateur cryptographer!) said “human ingenuity cannot concoct a cipher which human ingenuity cannot resolve.”

As famous physicist Richard Feynman said, “the first principle is to not fool yourself – And you are the easiest person to fool.”
Probability Quiz!
Probability Quiz!

We’ll experiment with Socrative.com for (ungraded) in-class quizzes and responses.
Probability Quiz!

We’ll experiment with Socrative.com for (ungraded) in-class quizzes and responses.

Let’s warm up with some timely probability questions...
Probability Quiz!
Rest of the Lecture
Rest of the Lecture

A taste of crypto beyond secure channels:

– Coin flipping over the telephone.
– The dating game.
Coin Flipping
Coin Flipping

Alice and Bob are getting divorced 😞 They only speak to each other over the telephone.
Coin Flipping

Alice and Bob are getting divorced 😞 They only speak to each other over the telephone.

They want to flip a coin to decide who gets to keep the car. Is this possible?
Coin Flipping
The Dating Game
The Dating Game

Alice and Bob have been friends and want to determine if they both want to go on a date.
The Dating Game

Alice and Bob have been friends and want to determine if they both want to go on a date.

Can they do this in such a way that they only learn if they are both interested?
The Dating Game