Introduction

Chanathip Namprempre

Computer Science
Reed College

What crypto was and what it has become

PAST	**PRESENT**
secret communication	data integrity authentication of people etc.
military use only	e-commerce (ATM withdrawals, bill payments, etc) conversations (phone, Internet chat, etc) broadcasts (cable TV, etc)
art	science (based on many disciplines, e.g. number theory, complexity theory, communication theory, probability theory, etc)

Most well-known goal

Sender (Alice) and receiver (Bob) talking over an **ideal channel**, i.e.

- dedicated
- untappable
- impenetrable

in the presence of an adversary EVE.

Such a channel doesn't exist in the real world!

- In the real world, we use public channel, e.g. the Internet.
- Crypto tries to provide something as close to the ideal channel as possible.
- Approach: distill goals and try to achieve them.

What cryptography is about

Definition

Cryptography = Communication in the presence of adversaries

There must be

- good parties,
- something distinguishing good parties from bad parties, and
- a goal for each of the good parties.

Some examples: people trying to talk in private, an ATM talking to the bank server, etc.

What cryptography is not about

- social engineering
- dumpster diving
- shoulder surfing
- skimming scams

Setup assumptions

- **Symmetric Setting**: good parties share secret key *before* they start talking.
- **Asymmetric setting**: every one has a pair of key, one public, the other private.

Basic terminology

- cryptographer
- cryptanalyst

Approach taken in this course

abstraction, abstraction, abstraction, ...

We separate things into layers.

- low-level building blocks
- primitives
- high-level protocols

	Symmetric setting	Asymmetric setting
Low-level tools	block ciphers pseudorandom function families	one-way functions (OWF) trapdoor OWF
Primitives	symmetric encryption message authentication codes	asymmetric encryption digital signatures
High-level protocols	key exchange	key exchange electronic voting payment