

# **EECS 575: Advanced Cryptography**

## **Fall 2021**

## **Lecture 1**

1

Paul Grubbs

[paulgrub@umich.edu](mailto:paulgrub@umich.edu)

Beyster 4709

# Agenda for this lecture

- Introductions
  - Who are your course staff? Who are you all?
- Course policies and syllabus
- Motivation, course overview, and information-theoretic security

# About Me

- Just finished a postdoc at NYU
- PhD Cornell (2020), undergrad at Indiana
- Worked as a cryptography engineer
- website: <https://web.eecs.umich.edu/~paulgrub/>
- he/him/his pronouns
- Research: applied cryptography, security, systems
  - Managing encrypted data, searchable encryption, authenticated encryption, attacks, provable security, etc...
- Outside of work:
  - Reading about history, pandemics, social issues, politics...
  - watching sitcoms (currently: Brooklyn 99)
  - playing Switch



# About Our GSI

**Anthony Opipari**

topipari@umich.edu

- Born and raised in Ann Arbor
- BSE and MSE degrees in computer science from UM
- Pre-candidate in CSE PhD program
  - Research interests in probabilistic reasoning for robotics and machine learning-based perception
  - Thesis advisor: Professor Chad Jenkins
- Work experience
  - Software engineering intern at Ford Motor Company and RightHook Inc.
  - Machine-learning engineer at MIT Lincoln Laboratory
- Hobbies include gardening, running, listening and discussing ‘NPR Planet Money’



# About You!

Go around the room and introduce yourself to us:

- Name, preferred pronouns
- one thing you want to get out of this class, or a topic you're excited about
- an interesting fact about yourself

# Agenda for this lecture

- Introductions
  - Who are your course staff? Who are you all?
- Course policies and syllabus
- Motivation, course overview, and information-theoretic security

# Course Setup

- Lecture-based course. I will give lectures.
  - Monday and Wednesday, 9-10:30am DOW 1005
- One discussion per week, led by Anthony.
  - Friday 1:30-2:30pm, DOW 1005
  - I may or may not attend
- Several office hours throughout the week.
  - For now, all office hours will be via Zoom
- If you need to email the course staff, include [EECS575FA21] in the subject line

# Course Materials

- Lecture notes: <https://github.com/pag-crypto/EECS575-fall21>
  - Chris's notes from past semesters:  
<https://github.com/cpeikert/TheoryOfCryptography>
- Canvas: <https://umich.instructure.com/courses/475606>
- Piazza: <https://piazza.com/umich/fall2021/eecs575>
- No required textbook, but you'll likely find the optional textbook useful

# COVID Accommodations

- All lectures, discussions, and office hours will be recorded and made available online.
- PDFs of slides with markups will also be available on the Github.
- Students are required to wear masks in class. Make sure to complete your ResponsiBLUE screenings as well. **If you feel sick, do not come to class.**
- Anthony and I will wear masks during lectures and discussions
  - May re-evaluate if lectures are hard to understand, for accessibility, etc.

# Grading

- Your final grade will have three components:
  - 50%: homework assignments, Canvas peer review of others' solutions, and class participation
  - 25%: Take-home exam #1
  - 25%: Take-home exam #2
- All homework and exam solutions *must* be typeset in LaTeX.
- Collaboration and external sources are allowed for homeworks, with some caveats (see syllabus) but not for exams.
- Roughly six lectures are not yet typeset. You can get extra credit for writing good scribe notes for these lectures.
- Grades in grad school really don't matter, so don't worry too much about them.

# Lecture Topics Vote

- Our last few lectures don't yet have topics. We'll choose the topics by vote!
- This week: solicit topics via Canvas and Google Form (link TBA)
- Next week: Vote on topics. Top 3-4 will get a lecture at the end of the semester

# Agenda for this lecture

- Introductions
  - Who are your course staff? Who are you all?
- Course policies and syllabus
- Motivation, course overview, and information-theoretic security

# Motivating our topic of study

This class is about *cryptography*.

Anyone want to try to define cryptography, in their own words?

## Why study cryptography?

I'm going to try to answer this question two ways...

1. Standard answer I've often heard, but find incomplete
2. More satisfying answer

# Answer #1

Cryptography, an ancient discipline whose origins predate digital computers by centuries, is compelling and exciting because of how it leverages deep mathematical and complexity-theoretic insights to make computers more secure.

# Why I find it unsatisfying

This motivates cryptography, but many other things as well...

Cryptography, an ancient discipline whose origins predate digital computers by centuries, is compelling and exciting because of how it leverages deep mathematical and complexity-theoretic insights to make computers more secure.

This describes:

- number theory
- statistics (i.e., ML)
- algorithms

This describes:

- static analysis
- distributed systems
- turning the computer off
- destroying the computer

This describes:

- coding theory
- machine learning
- programming languages

# Answer #2

We live in an Information Age.  
In our world, information is...

Money



Political influence

How the Russians hacked the DNC  
and passed its emails to WikiLeaks

Weaponry



Identity



Protest



# Answer #2

Cryptography is a means to control information;  
thus, cryptography is inextricably linked to power.

We live in an Information Age.  
In our world, information is...



Power!

“Cryptography rearranges power: it configures who can do what, from what. This makes cryptography an inherently political tool, and it confers on the field an intrinsically moral dimension.”  
– Rogaway, “The Moral Character of Cryptographic Work”

# Answer #2

Governments try to subvert and/or ban strong cryptography *all the time...!*

## How Did The FBI Break Tor?

**WhatsApp Sues Indian Government Over Encryption-Breaking Surveillance Laws**

**Keeping Secrets – A History of the Birth of Non-Governmental Cryptography Research**

Henry Corrigan-Gibbs



# Answer #2

Technology

## Apple is prying into iPhones to find sexual predators, but privacy activists worry governments could weaponize the feature

The moves aimed at preventing predators and pedophiles from using Apple services raise some civil liberties concerns

# Answer #2

Cryptography is compelling, exciting, and worthwhile for all the reasons listed above, but also (especially) because in the Information Age, controlling information is exercising power.

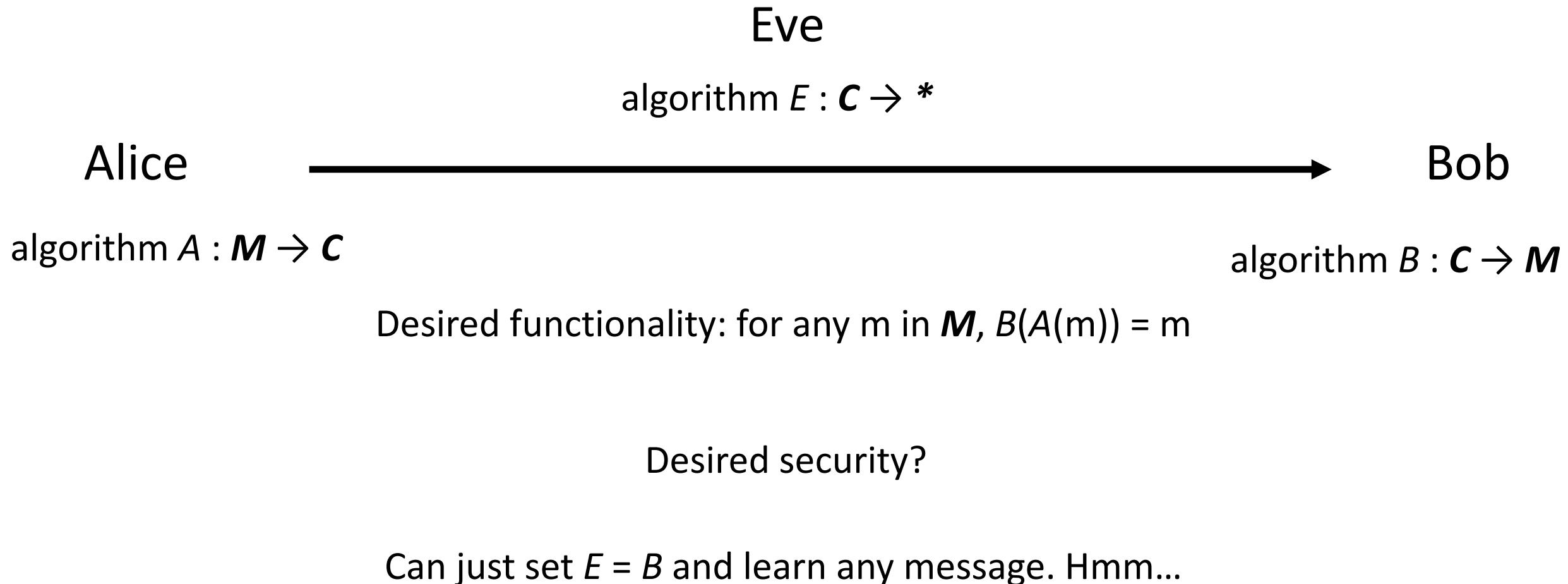
# Course Overview

- **Information-theoretic security:** Perfect secrecy. The one-time pad.
- **Symmetric cryptography:** one-way functions, computational security, pseudorandomness, encryption, message authentication, authenticated encryption, hash functions
- **Asymmetric cryptography:** Number-theoretic background. Public-key encryption. Digital signatures. Identity-based encryption.
- **Protocols:** Commitment, identification schemes, secret sharing, zero-knowledge proofs.
- **Applications/Special Topics:** chosen by vote

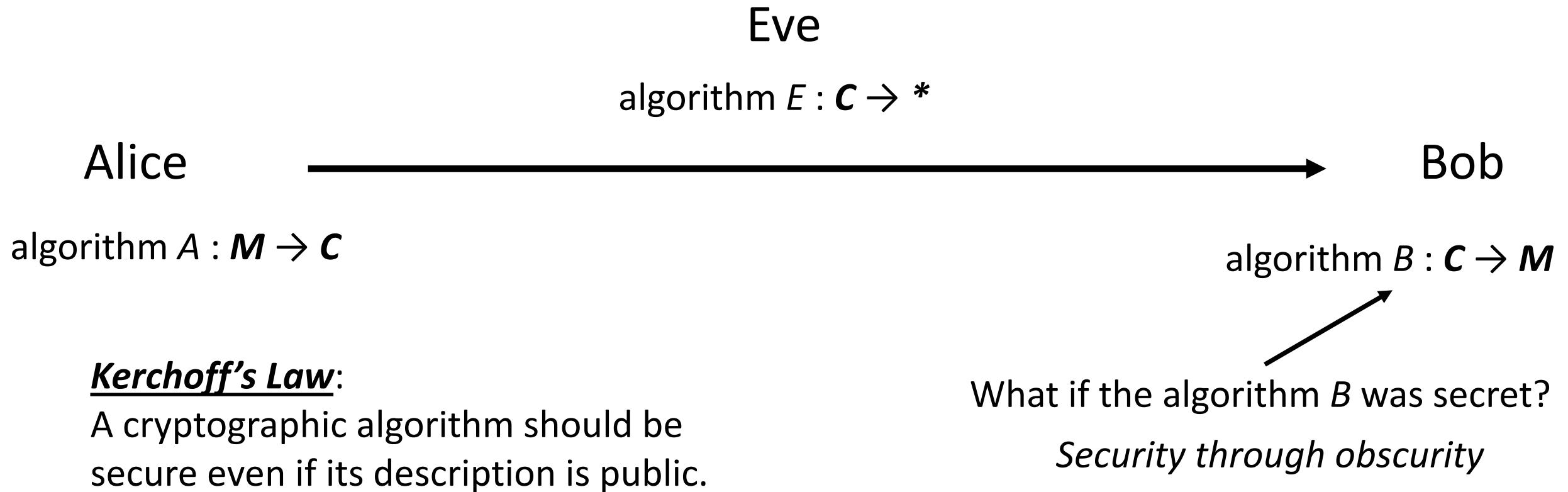
In studying these, we'll follow the *cryptographic methodology*:

1. Form a precise mathematical model of the problem
2. Define the desired functionality and security properties of a solution
3. Construct a candidate solution with the desired functionality
4. Analyze the solution and rigorously prove it satisfies the security properties

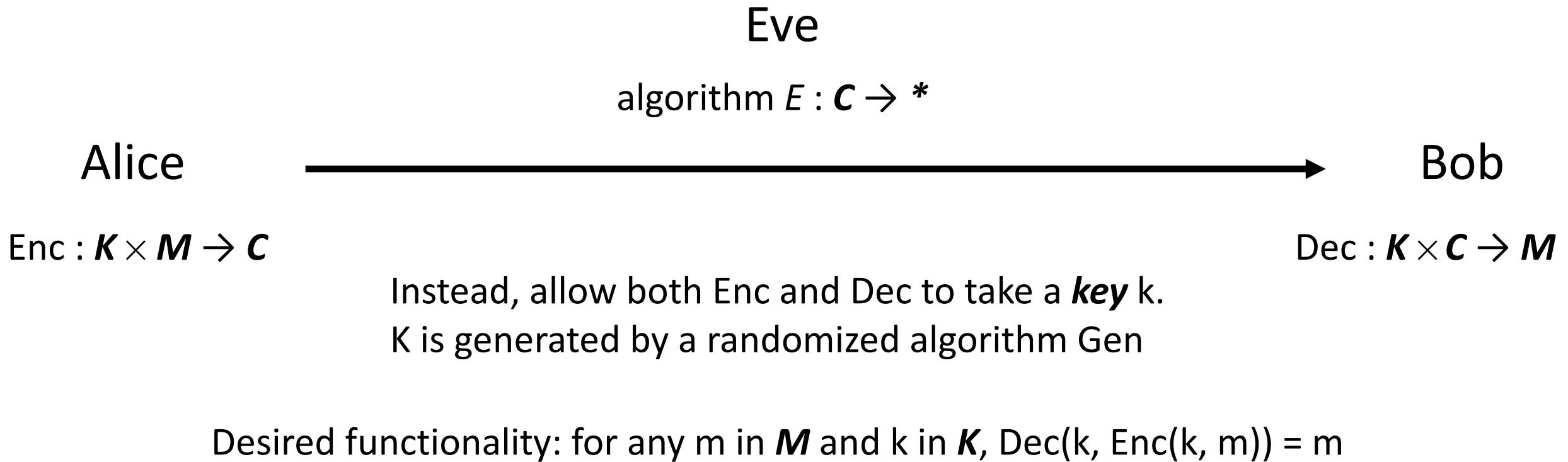
# Modelling Secure Communication



# Fixing the Model



# Symmetric-Key Encryption

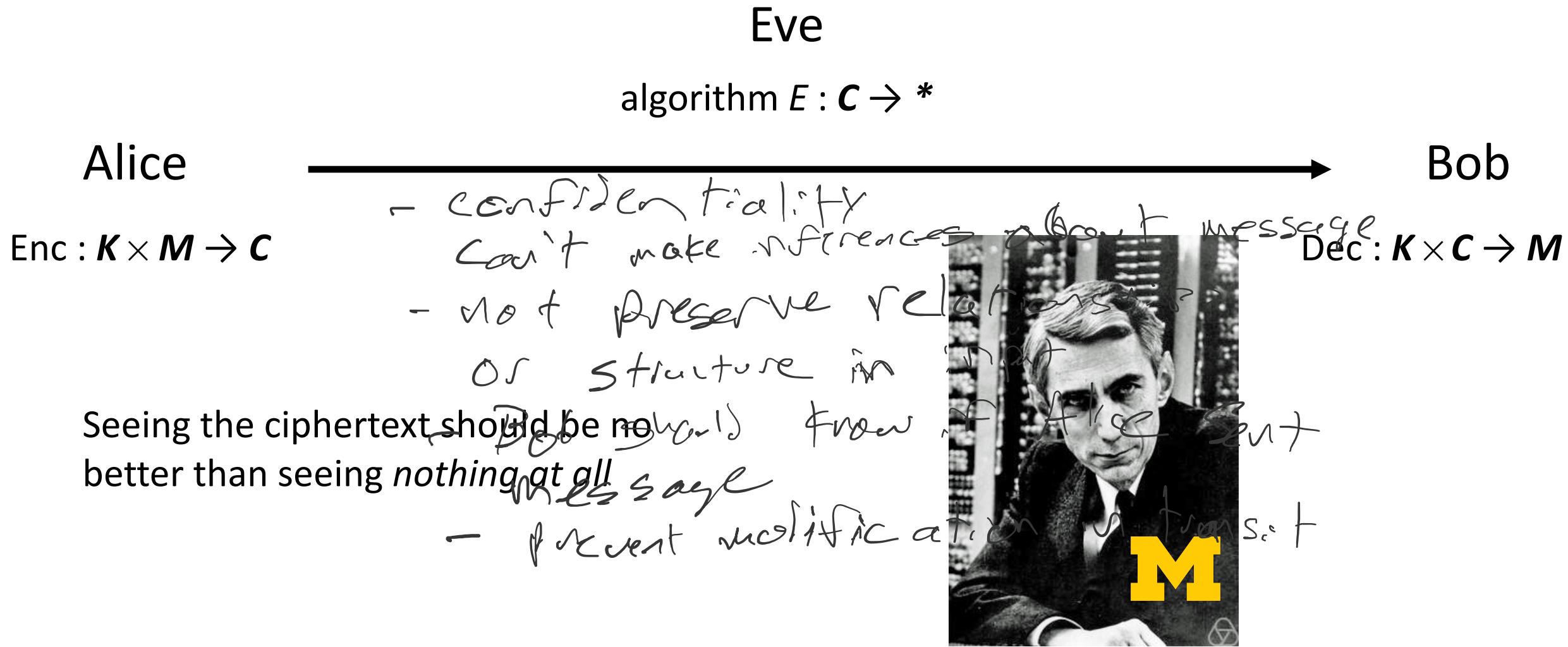


Questions:

- In this model, how must  $|M|$  and  $|C|$  be related?
- Can we infer anything about  $|K|$  in relation to  $|M|$  or  $|C|$  ?

# Security of Symmetric-Key Encryption

What security properties might we want here?



# Shannon Secrecy

**Definition 2.1** (Shannon secrecy). A symmetric-key encryption scheme  $(\text{Gen}, \text{Enc}, \text{Dec})$  with message space  $\mathcal{M}$  and ciphertext space  $\mathcal{C}$  is *Shannon secret with respect to a probability distribution  $D$*  over  $\mathcal{M}$  if for all  $\bar{m} \in \mathcal{M}$  and all  $\bar{c} \in \mathcal{C}$ ,

$$\Pr_{m \leftarrow D, k \leftarrow \text{Gen}} [m = \bar{m} \mid \text{Enc}_k(m) = \bar{c}] = \Pr_{m \leftarrow D} [m = \bar{m}].$$

The scheme is *Shannon secret* if it is Shannon secret with respect to every distribution  $D$  over  $\mathcal{M}$ .

# Rewriting Shannon Secrecy

**Definition 2.1** (Shannon secrecy). A symmetric-key encryption scheme  $(\text{Gen}, \text{Enc}, \text{Dec})$  with message space  $\mathcal{M}$  and ciphertext space  $\mathcal{C}$  is *Shannon secret with respect to a probability distribution  $D$*  over  $\mathcal{M}$  if for all  $\bar{m} \in \mathcal{M}$  and all  $\bar{c} \in \mathcal{C}$ ,

$$\Pr_{m \leftarrow D, k \leftarrow \text{Gen}}[m = \bar{m} \mid \text{Enc}_k(m) = \bar{c}] = \Pr_{m \leftarrow D}[m = \bar{m}].$$

The scheme is *Shannon secret* if it is Shannon secret with respect to every distribution  $D$  over  $\mathcal{M}$ .

$$\Pr_{m, k}[\bar{m} \mid \text{Enc}_k(\bar{m}) = \bar{c}]$$

$$= \frac{\Pr_{m, k}[\bar{m} \wedge \text{Enc}_k(\bar{m}) = \bar{c}]}{\Pr_{m, k}[\text{Enc}_k(\bar{m}) = \bar{c}]} =$$

$$\Pr_{m, k}[\bar{m}] \Pr_{k}[\text{Enc}_k(\bar{m}) = \bar{c}]$$

$$\Pr_k[\text{Enc}_k(\bar{m}) = \bar{c}] = \Pr_{m, k}[\text{Enc}(m) = \bar{c}]$$

# Perfect Secrecy

**Definition 2.2** (Perfect secrecy). A symmetric-key encryption scheme  $(\text{Gen}, \text{Enc}, \text{Dec})$  with message space  $\mathcal{M}$  and ciphertext space  $\mathcal{C}$  is *perfectly secret* if for all  $m_0, m_1 \in \mathcal{M}$  and all  $\bar{c} \in \mathcal{C}$ ,

$$\Pr_{k \leftarrow \text{Gen}} [\text{Enc}_k(m_0) = \bar{c}] = \Pr_{k \leftarrow \text{Gen}} [\text{Enc}_k(m_1) = \bar{c}].$$

# The One-Time Pad

# Perfect Secrecy of the One-Time Pad

**Theorem 2.4.** *The one-time pad is a perfectly secret symmetric-key encryption scheme.*

**Proof:**

# Questions to think about

If we replaced XOR with AND in the one-time pad, would it still be a valid encryption scheme? Would it be perfectly secret?

Can you think of some other ways cryptography is related to power? Do you agree that cryptography is *inherently* political?