

# **EECS 575: Advanced Cryptography**

## **Fall 2022**

### **Lecture 2**

Paul Grubbs

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

Beyster 4709

# Agenda for this lecture

- Announcements
- Modelling secure communication
- Information-theoretic security

# Agenda for this lecture

- Announcements
- Modelling secure communication
- Information-theoretic security

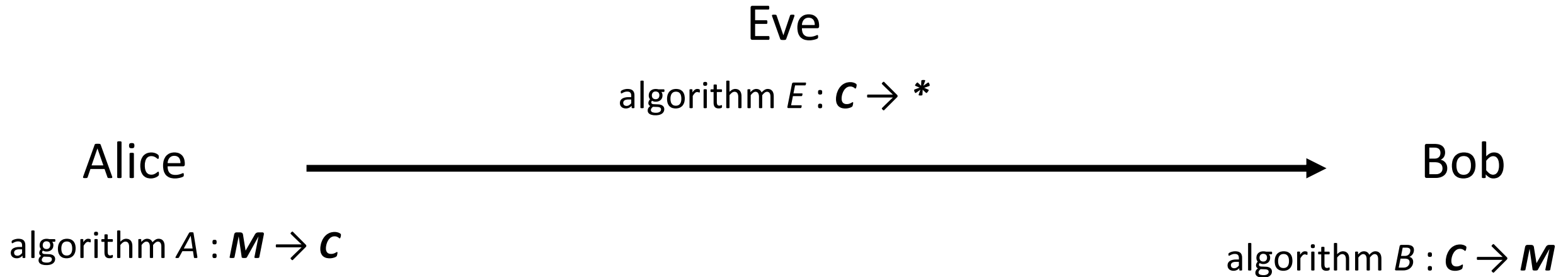
# Announcements

- Homework/exam schedule is (tentatively) done:
  - HW1: put online 9/5, due 9/16
  - HW2: put online 9/16, due 9/30
  - Take-home exam #1: put online 10/3, due 10/10
  - HW3: put online 10/7, due 10/21
  - HW4: put online 10/21, due 11/4
  - HW5: put online 11/4, due 11/18
  - HW6: put online 11/16, due 11/28\*
  - Take-home exam #2: put online 11/28, due 12/5

# Agenda for this lecture

- Announcements
- **Modelling secure communication**
- Information-theoretic security

# Modelling Secure Communication

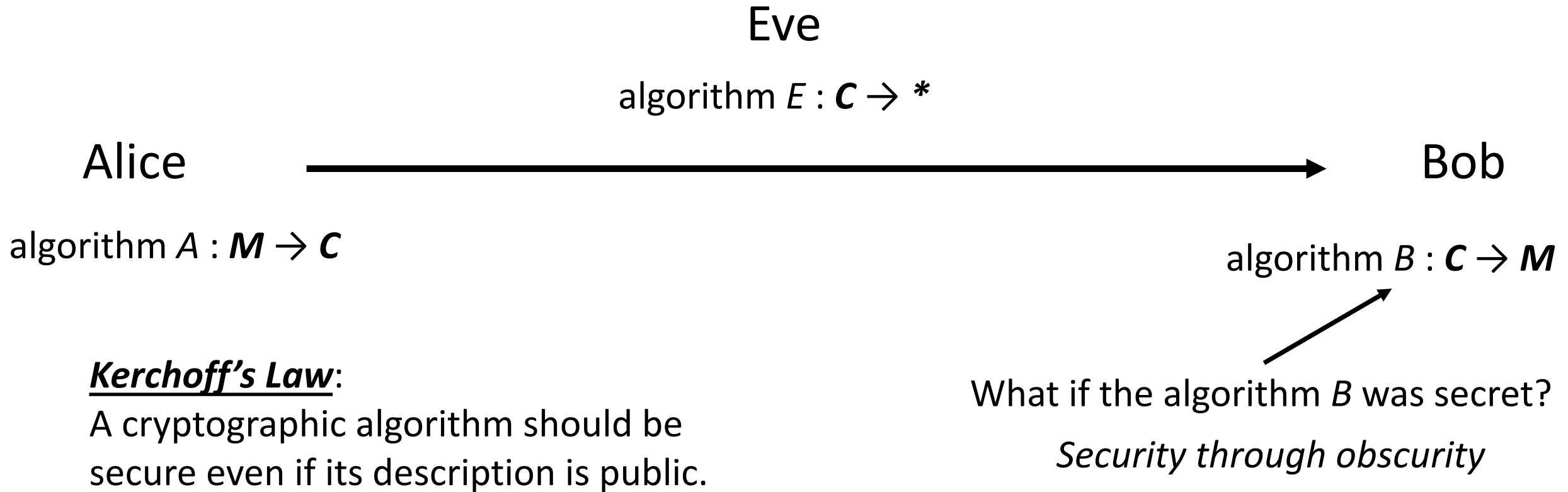


Desired functionality: for any  $m$  in  $\mathcal{M}$ ,  $B(A(m)) = m$

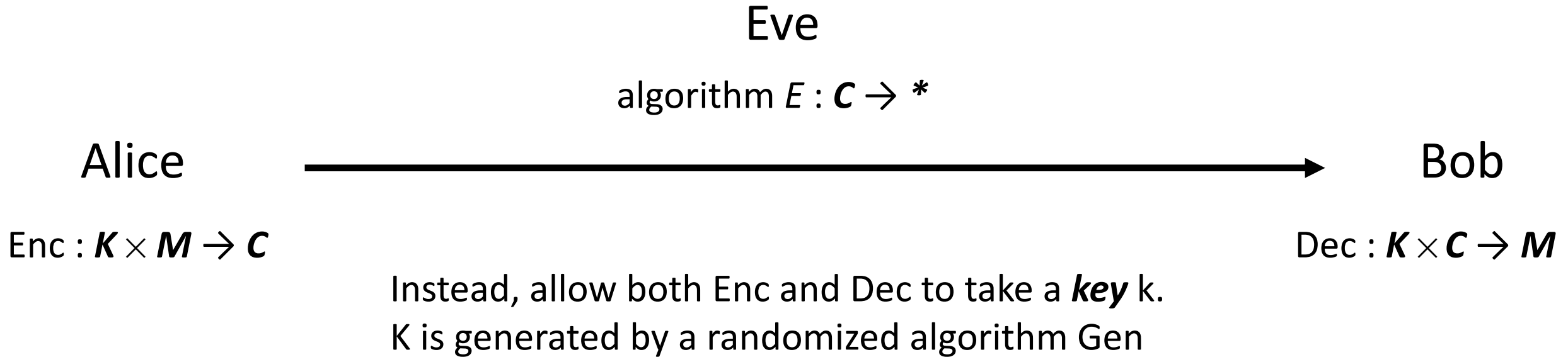
Desired security?

Can just set  $E = B$  and learn any message. Hmm...

# Fixing the Model



# Symmetric-Key Encryption



Desired functionality: for any  $m$  in  $\mathbf{M}$  and  $k$  in  $\mathbf{K}$ ,  $\text{Dec}(k, \text{Enc}(k, m)) = m$

Questions:

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



# Security of Symmetric-Key Encryption

What security properties might we want here?

Eve

algorithm  $E : \mathcal{C} \rightarrow *$

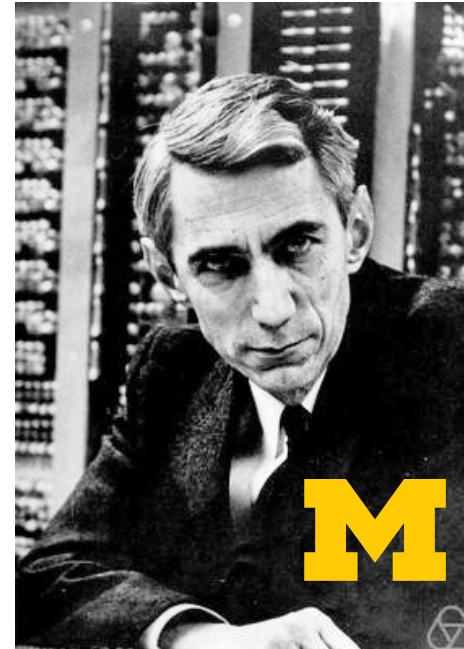
Alice



Bob

Enc :  $K \times M \rightarrow \mathcal{C}$

Dec :  $K \times \mathcal{C} \rightarrow M$



Seeing the ciphertext should be no better than seeing *nothing at all*

# Agenda for this lecture

- Announcements
- Modelling secure communication
- Information-theoretic security

# 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  $\mathcal{M}$ .

# 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?