Perfect Secrecy and One-Time Pads

CS/ECE 407

Today's objectives

Learn basic cryptographic vocabulary

Explain one-time pad encryption

Define perfect secrecy

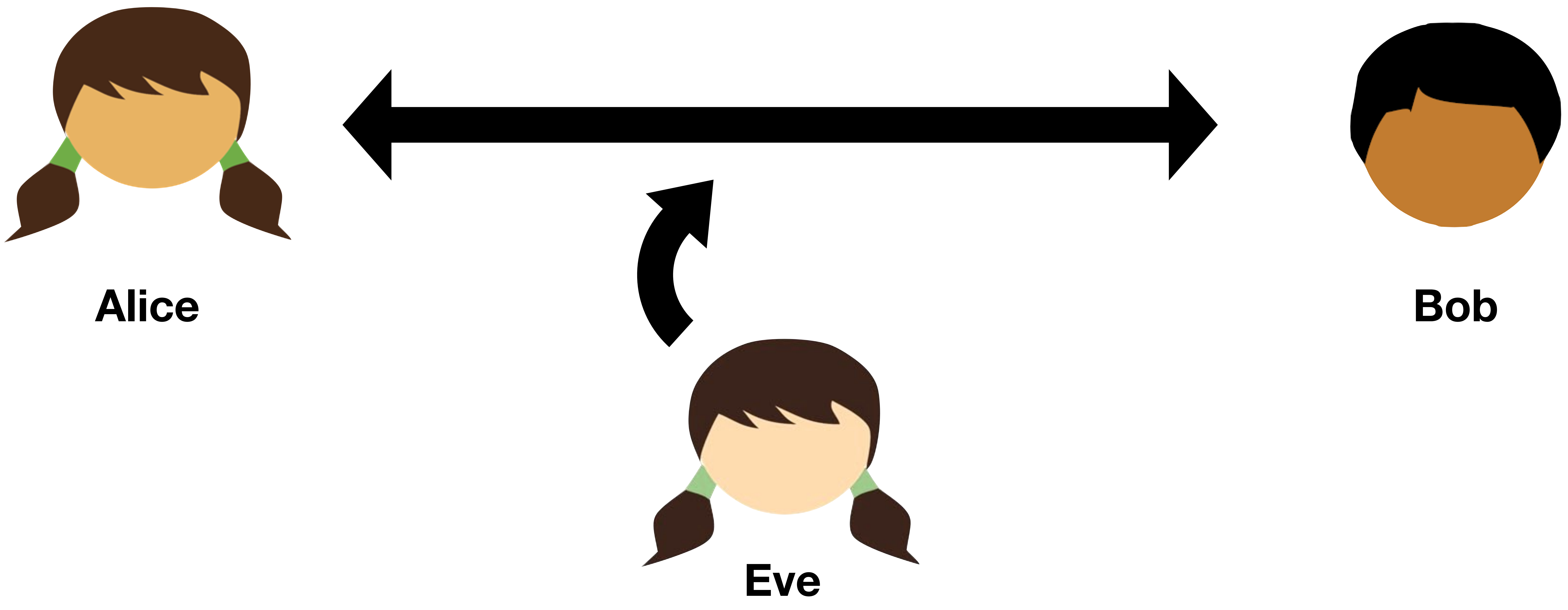
Describe limitations of perfect secrecy

Course Structure

Symmetric key cryptography
(Alice and Bob have a common key)

Public Key Cryptography
(Alice and Bob *do not* have a common key)

Beyond Secure communication
(Alice does not fully trust Bob)



Confidentiality

Can Alice and Bob prevent Eve from listening?

Substitution Cipher

```
a → J
b → Y
c → Z
d → K
e → C
f → I
```

…

```
cryptographyiscool
```

↓

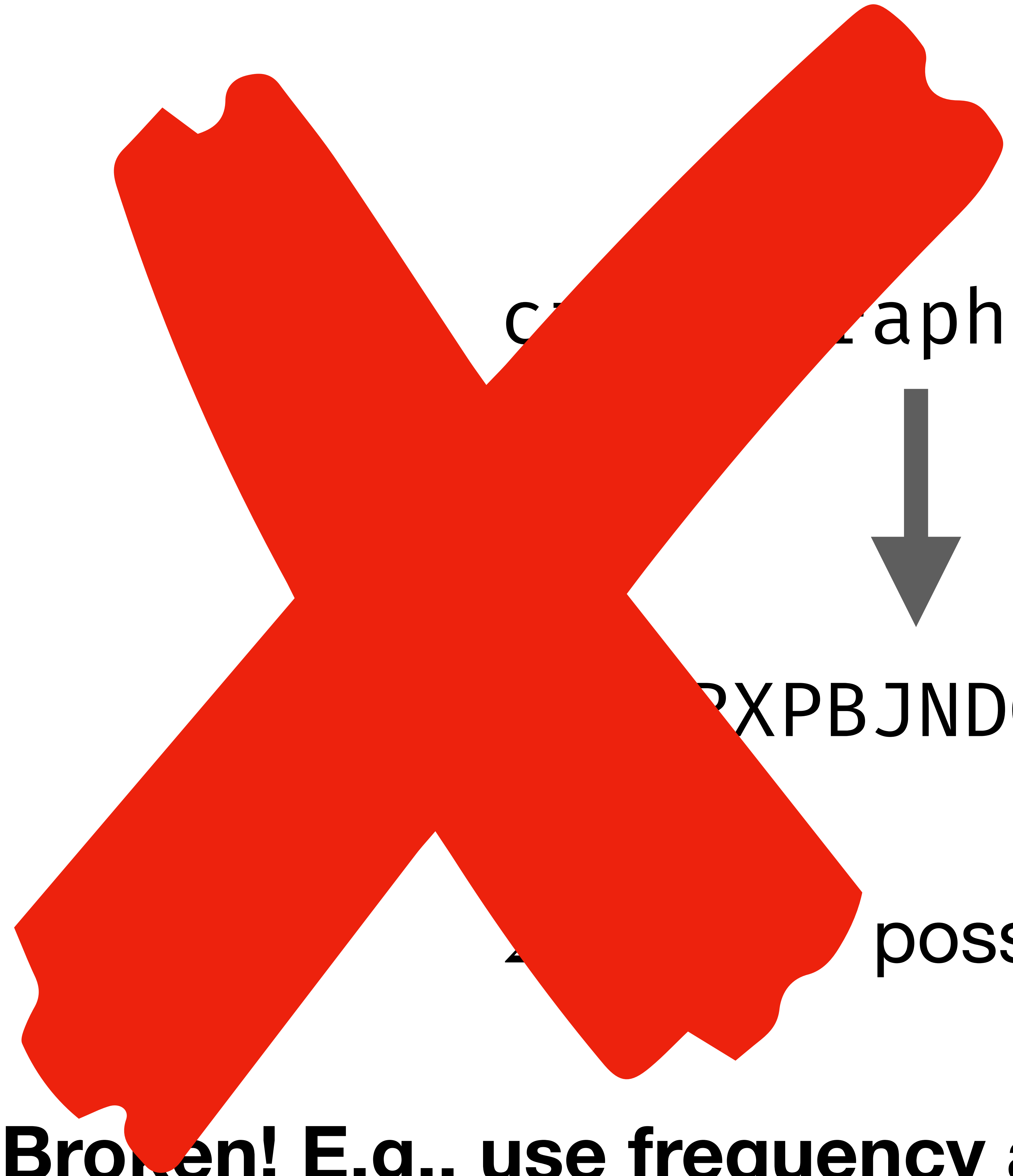
```
ZBGNRXPBJNDGQFZXXA
```

$26! \approx 2^{72}$ possible keys

Broken! E.g., use frequency analysis!

Substitution Cipher

a → J
b → Y
c → Z
d → K
e → C
f → I
…



c raphyiscool

↓

XPBJNDGQFZXXA

possible keys

Broken! E.g., use frequency analysis!

Modern Cryptography

State assumptions

Define security

Design system

Prove: if assumption holds, system meets definition

Modern Cryptography

State assumptions

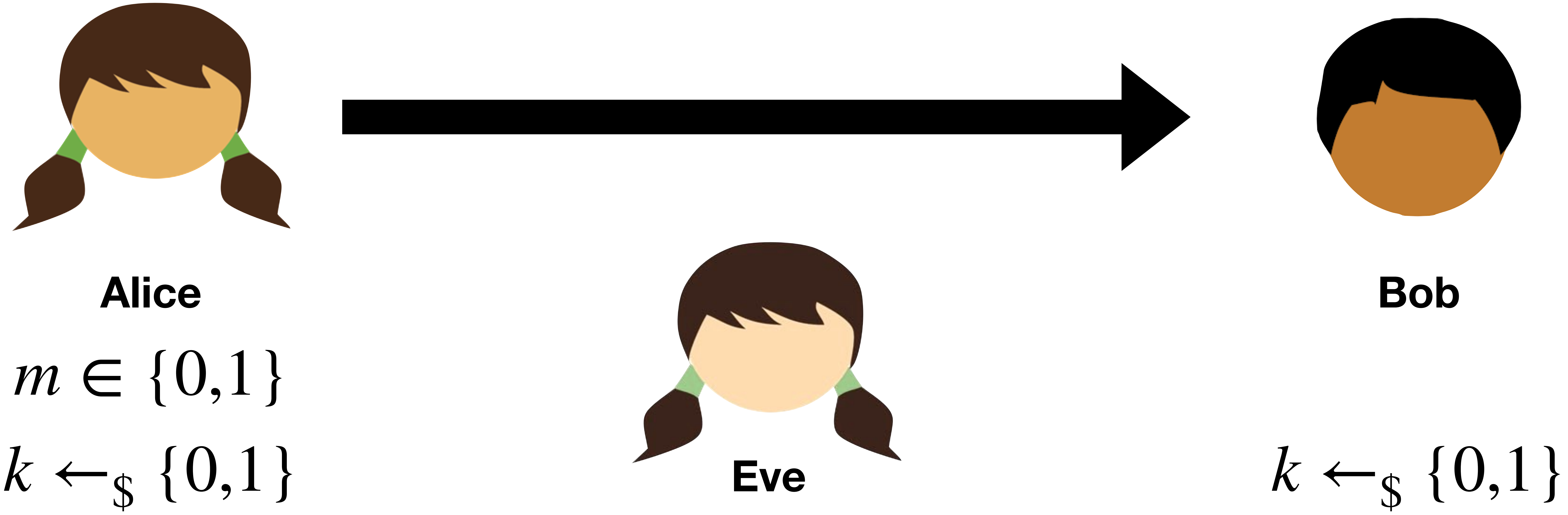
Today: Understand why this is needed

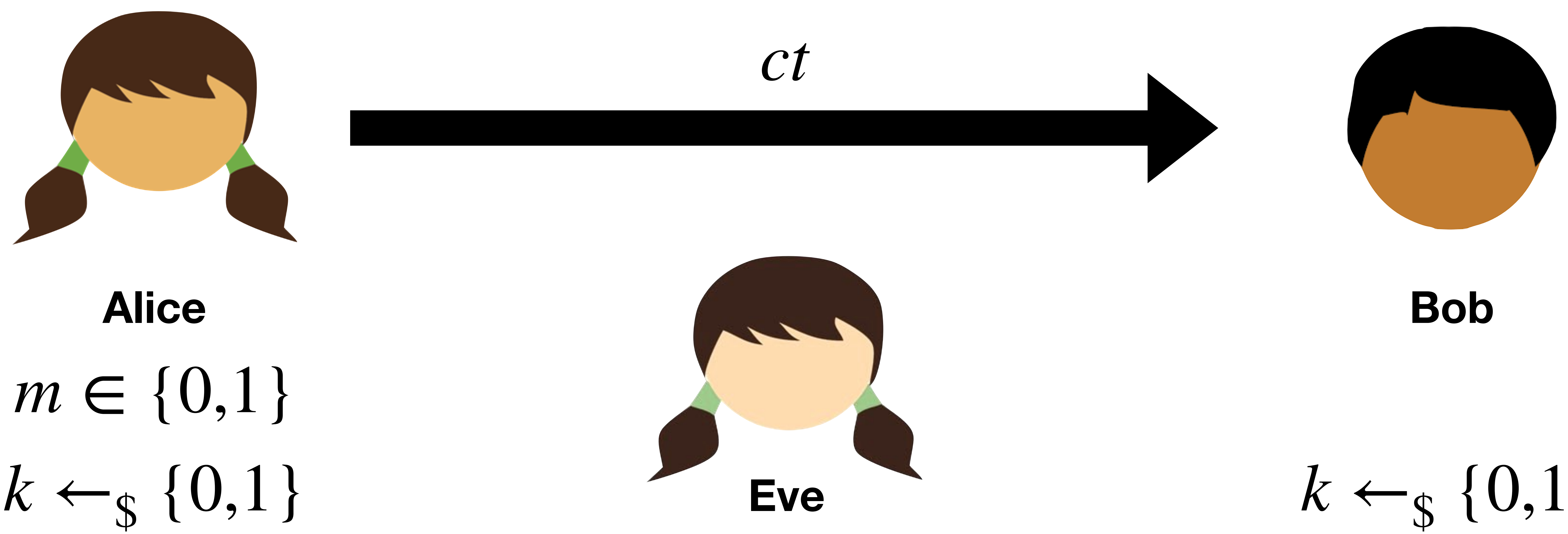
Define security

Design system

Prove: if assumption holds, system meets definition


Alice
$m \in \{0,1\}$
Bob
Eve


Alice
$m \in \{0,1\}$
$k \leftarrow_\$ \{0,1\}$
Eve
Bob
$k \leftarrow_\$ \{0,1\}$



Alice

$m \in \{0,1\}$

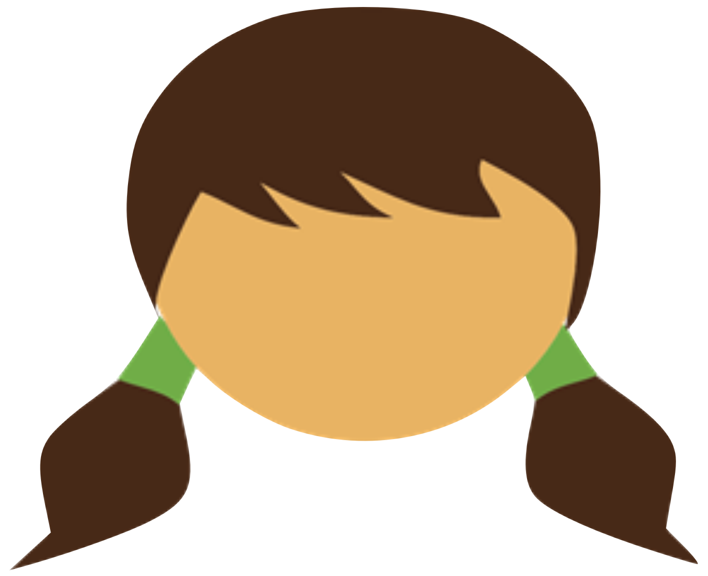
$k \leftarrow_{\$} \{0,1\}$

$ct \leftarrow m \oplus k$

Bob

$k \leftarrow_{\$} \{0,1\}$

$\oplus$	0	1
0	0	1
1	1	0



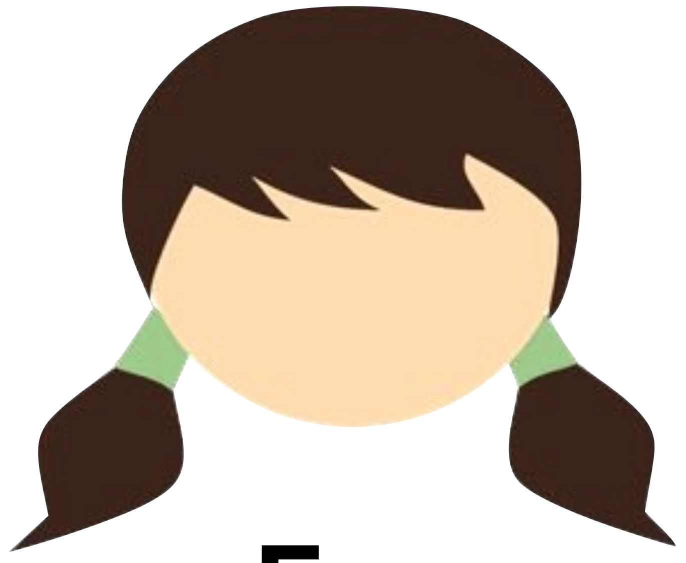
Alice

$m \in \{0,1\}$

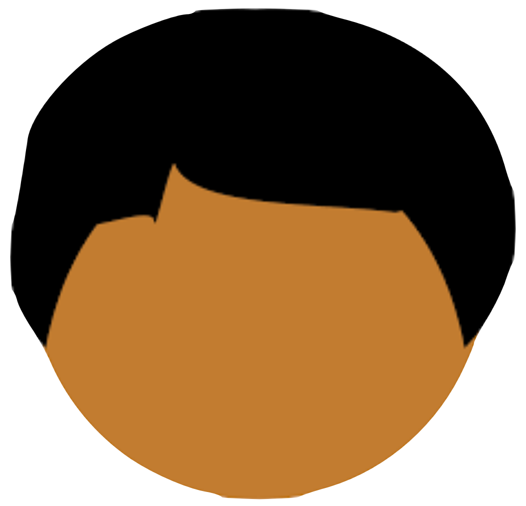
$k \leftarrow_{\$} \{0,1\}$

$ct \leftarrow m \oplus k$

$\xrightarrow{\quad ct \quad}$



Eve

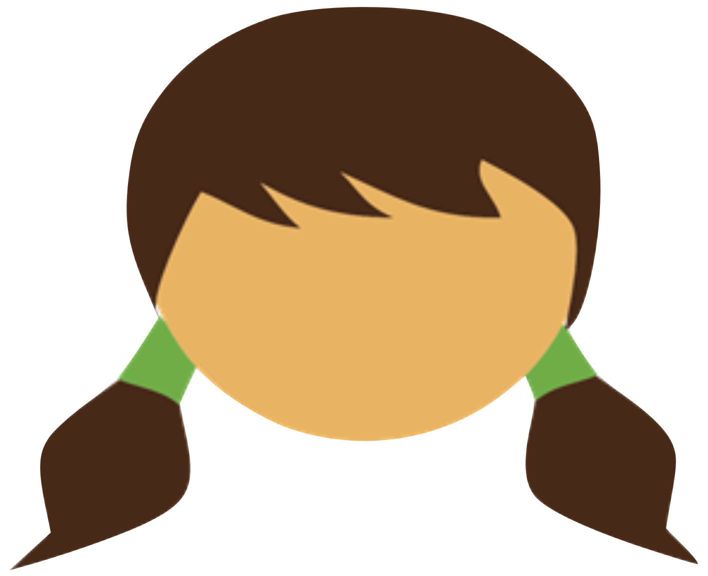


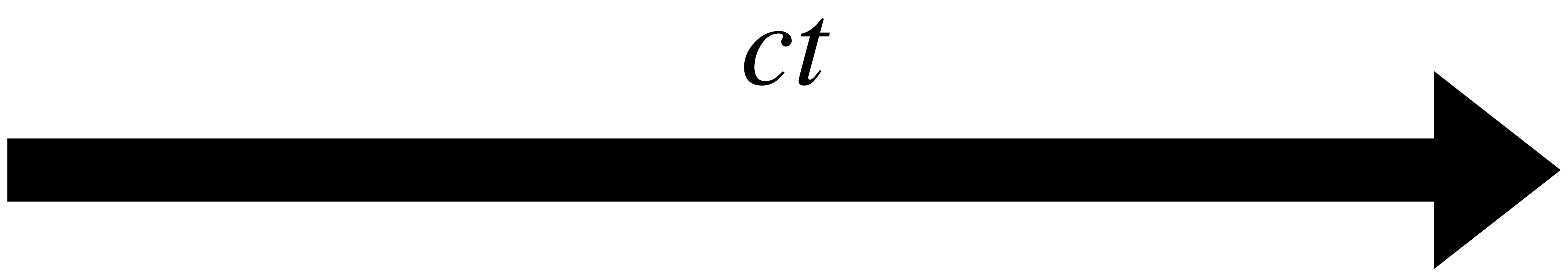
Bob

$k \leftarrow_{\$} \{0,1\}$

$m' \leftarrow ct \oplus k$

$\oplus$	0	1
0	0	1
1	1	0



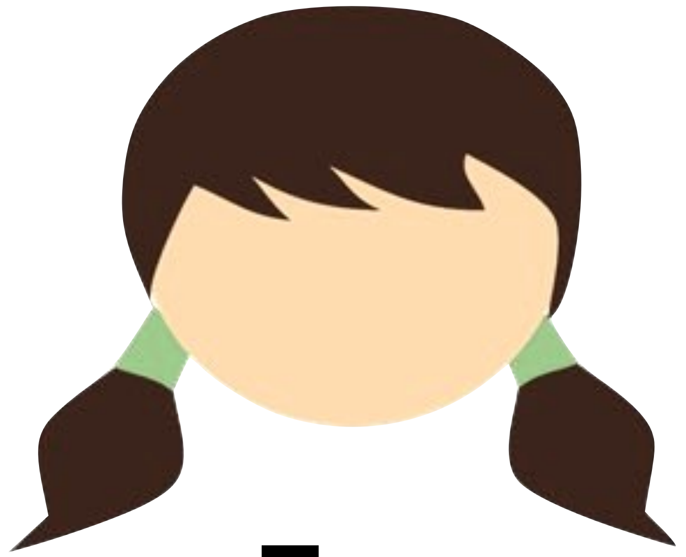


Alice

$$m \in \{0,1\}$$

$$k \leftarrow_\$ \{0,1\}$$

$$ct \leftarrow m \oplus k$$



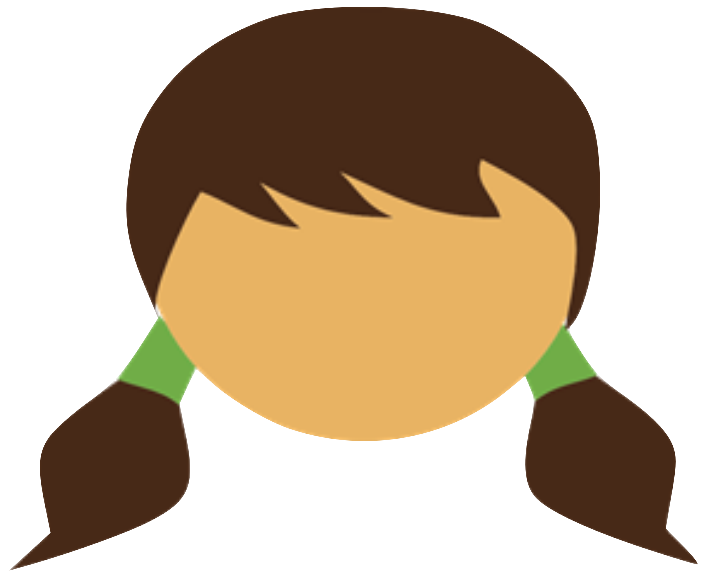
Eve

Bob

$$k \leftarrow_\$ \{0,1\}$$

$$m' \leftarrow ct \oplus k$$

What are we *not* hiding?



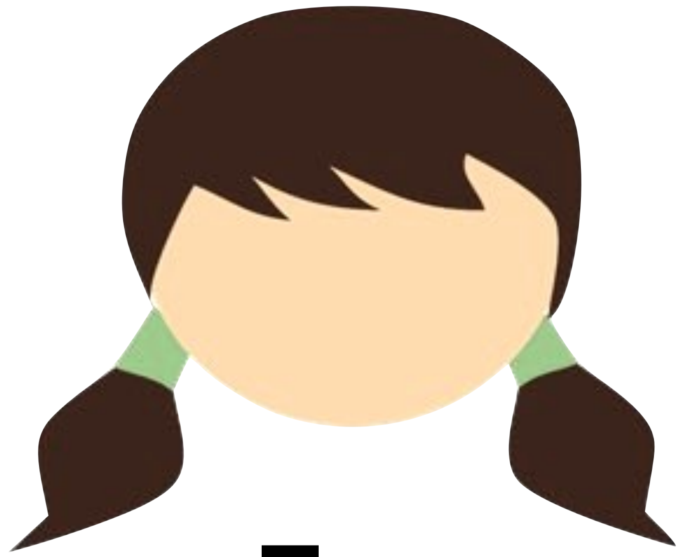
Alice

$m \in \{0,1\}$

$k \leftarrow_\$ \{0,1\}$

$ct \leftarrow m \oplus k$

$\xrightarrow{\quad ct \quad}$



Eve

Bob

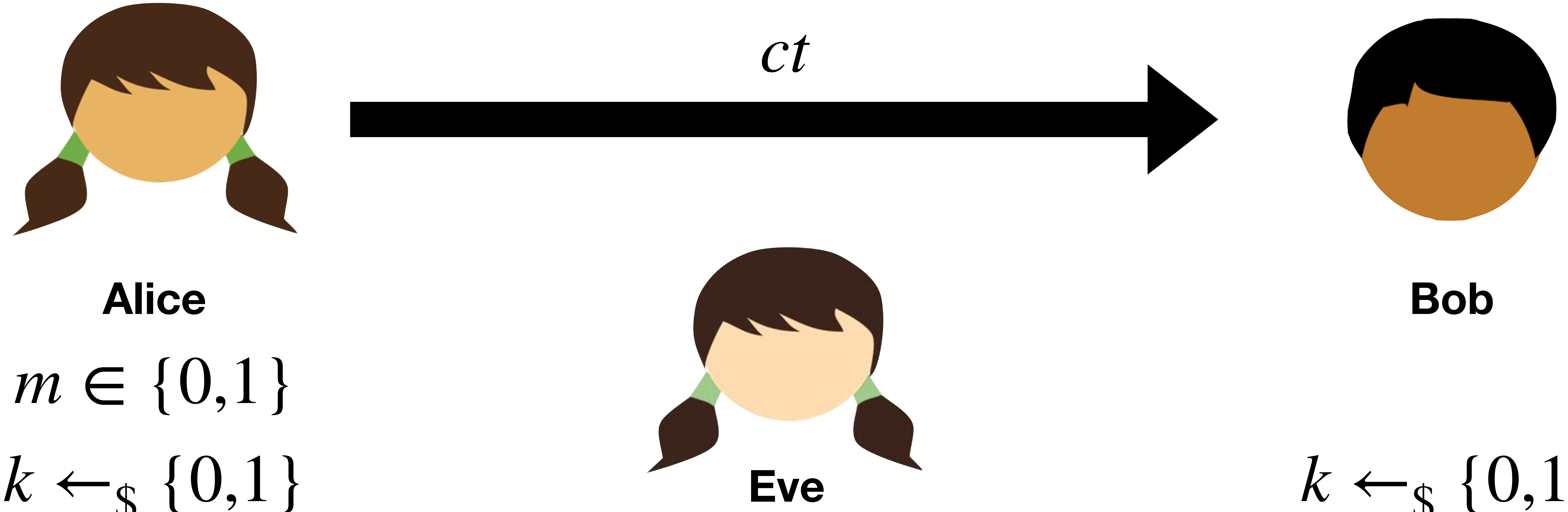
$k \leftarrow_\$ \{0,1\}$

$m' \leftarrow ct \oplus k$

What are we *not* hiding?

We do not hide that a message *exists*

We are cryptographers, not steganographers



Alice

$m \in \{0,1\}$

$k \leftarrow_\$ \{0,1\}$

$ct \leftarrow m \oplus k$

Bob

$k \leftarrow_\$ \{0,1\}$

$m' \leftarrow ct \oplus k$

What are we *not* hiding?

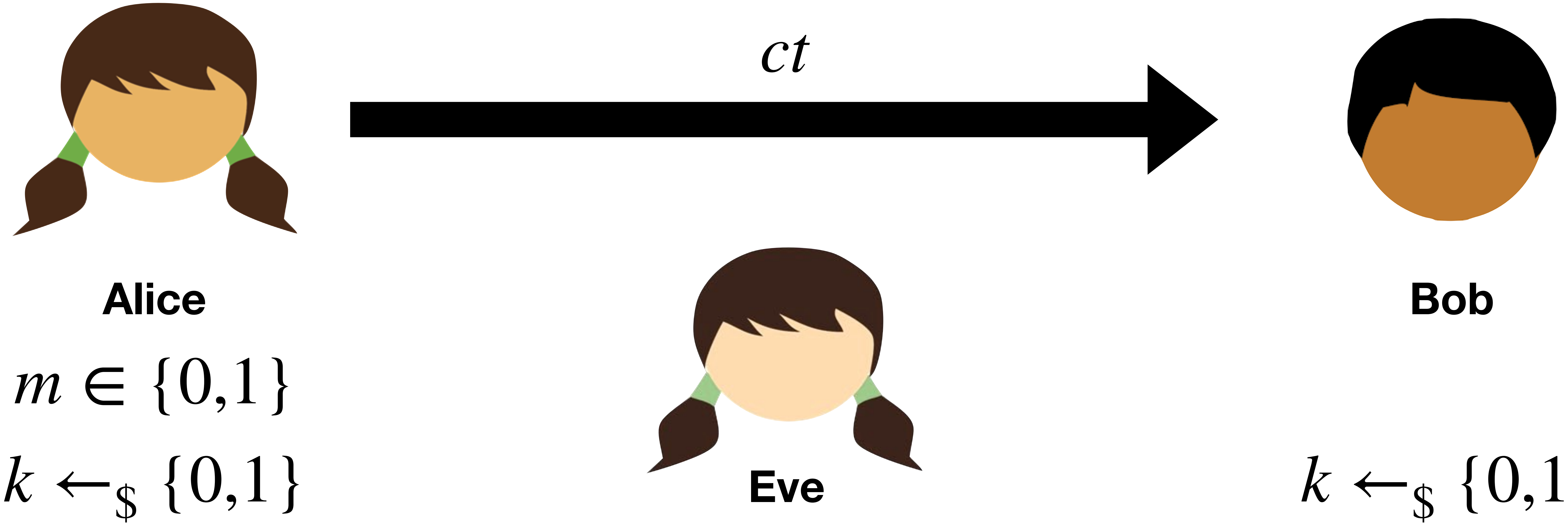
We do not hide that a message *exists*

We do not hide *message length*

We do not hide *the protocol*

We are cryptographers, not steganographers

Kerckhoffs's principle



Alice

$m \in \{0,1\}$

$k \leftarrow_{\$} \{0,1\}$

$ct \leftarrow m \oplus k$

Bob

$k \leftarrow_{\$} \{0,1\}$

$m' \leftarrow ct \oplus k$

Question: Is it possible to achieve encryption without a key?

Modern Cryptography

State assumptions

Define security

Design system

Prove: if assumption holds, system meets definition

Symmetric Cipher

A **cipher** over $(\mathrm{K}, \mathrm{M}, \mathrm{C})$ is two *algorithms*:

$$Enc : \mathrm{K} \times \mathrm{M} \to \mathrm{C}$$

$$Dec : \mathrm{K} \times \mathrm{C} \to \mathrm{M}$$

Symmetric Cipher

A **cipher** over $(\mathrm{K}, \mathrm{M}, \mathrm{C})$ is two *algorithms*:

$$Enc : \mathrm{K} \times \mathrm{M} \rightarrow \mathrm{C} \qquad Enc(k, m) := k \oplus m$$

$$Dec : \mathrm{K} \times \mathrm{C} \rightarrow \mathrm{M} \qquad Dec(k, ct) := k \oplus ct$$

Symmetric Cipher

A **cipher** over $(\mathrm{K}, \mathrm{M}, \mathrm{C})$ is two *algorithms*:

$$Enc : \mathrm{K} \times \mathrm{M} \rightarrow \mathrm{C} \qquad Enc(k, m) := k \oplus m$$

$$Dec : \mathrm{K} \times \mathrm{C} \rightarrow \mathrm{M} \qquad Dec(k, ct) := k \oplus ct$$

Correctness:

Symmetric Cipher

A **cipher** over $(\mathrm{K}, \mathrm{M}, \mathrm{C})$ is two *algorithms*:

$$Enc : \mathrm{K} \times \mathrm{M} \to \mathrm{C} \qquad Enc(k, m) := k \oplus m$$

$$Dec : \mathrm{K} \times \mathrm{C} \to \mathrm{M} \qquad Dec(k, ct) := k \oplus ct$$

Correctness:

$$Dec(k, Enc(k, m)) = m$$

Symmetric Cipher

A **cipher** over $(\mathrm{K}, \mathrm{M}, \mathrm{C})$ is two *algorithms*:

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

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

$$Enc(k, m) := k \oplus m$$

$$Dec(k, ct) := k \oplus ct$$

Correctness:

$$Dec(k, Enc(k, m)) = m$$

$$Dec(k, Enc(k, m))$$

Symmetric Cipher

A **cipher** over $(\mathrm{K}, \mathrm{M}, \mathrm{C})$ is two *algorithms*:

$$Enc : \mathrm{K} \times \mathrm{M} \to \mathrm{C} \qquad Enc(k, m) := k \oplus m$$

$$Dec : \mathrm{K} \times \mathrm{C} \to \mathrm{M} \qquad Dec(k, ct) := k \oplus ct$$

Correctness:

$$k \oplus (k \oplus m) = m$$ ✓

Symmetric Cipher

A **cipher** over $(\mathrm{K}, \mathrm{M}, \mathrm{C})$ is two *algorithms*:

$$Enc : \mathrm{K} \times \mathrm{M} \rightarrow \mathrm{C} \qquad Enc(k, m) := k \oplus m$$

$$Dec : \mathrm{K} \times \mathrm{C} \rightarrow \mathrm{M} \qquad Dec(k, ct) := k \oplus ct$$

Correctness:

$$Dec(k, Enc(k, m)) = m \qquad k \oplus (k \oplus m) = m \checkmark$$

Confidentiality

Symmetric Cipher

A **cipher** over $(\mathrm{K}, \mathrm{M}, \mathrm{C})$ is two *algorithms*:

$$Enc : \mathrm{K} \times \mathrm{M} \rightarrow \mathrm{C} \qquad Enc(k, m) := k \oplus m$$

$$Dec : \mathrm{K} \times \mathrm{C} \rightarrow \mathrm{M} \qquad Dec(k, ct) := k \oplus ct$$

Correctness:

$$Dec(k, Enc(k, m)) = m \qquad k \oplus (k \oplus m) = m \checkmark$$

Perfect Secrecy:

Symmetric Cipher

A **cipher** over $(\mathrm{K}, \mathrm{M}, \mathrm{C})$ is two *algorithms*:

$$Enc : \mathrm{K} \times \mathrm{M} \to \mathrm{C} \qquad\qquad Enc(k, m) := k \oplus m$$

$$Dec : \mathrm{K} \times \mathrm{C} \to \mathrm{M} \qquad\qquad Dec(k, ct) := k \oplus ct$$

Correctness:

$$Dec(k, Enc(k, m)) = m \qquad\qquad k \oplus (k \oplus m) = m \;\checkmark$$

Perfect Secrecy:

For every pair of messages $m_0, m_1 \in \mathrm{M}$ and every cipher text $c \in \mathrm{C}$:

$$\Pr_{k \leftarrow \mathrm{K}} [\ Enc(k, m_0) = c\ ] = \Pr_{k \leftarrow \mathrm{K}} [\ Enc(k, m_1) = c\ ]$$

Symmetric Cipher

A **cipher** over $(\mathrm{K}, \mathrm{M}, \mathrm{C})$ is two *algorithms*:

$$Enc : \mathrm{K} \times \mathrm{M} \to \mathrm{C} \qquad Enc(k, m) := k \oplus m$$

$$Dec : \mathrm{K} \times \mathrm{C} \to \mathrm{M} \qquad Dec(k, ct) := k \oplus ct$$

Correctness:

$$Dec(k, Enc(k, m)) = m \qquad k \oplus (k \oplus m) = m \checkmark$$

Perfect Secrecy:

For every pair of messages $m_0, m_1 \in \{0,1\}$ and every cipher text $c \in \{0,1\}$:

$$\Pr_{k \leftarrow \{0,1\}} [\ Enc(k, m_0) = c\ ] = \Pr_{k \leftarrow \{0,1\}} [\ Enc(k, m_1) = c\ ]$$

Symmetric Cipher

A **cipher** over $(\mathrm{K}, \mathrm{M}, \mathrm{C})$ is two *algorithms*:

$$Enc : \mathrm{K} \times \mathrm{M} \to \mathrm{C} \qquad Enc(k, m) := k \oplus m$$

$$Dec : \mathrm{K} \times \mathrm{C} \to \mathrm{M} \qquad Dec(k, ct) := k \oplus ct$$

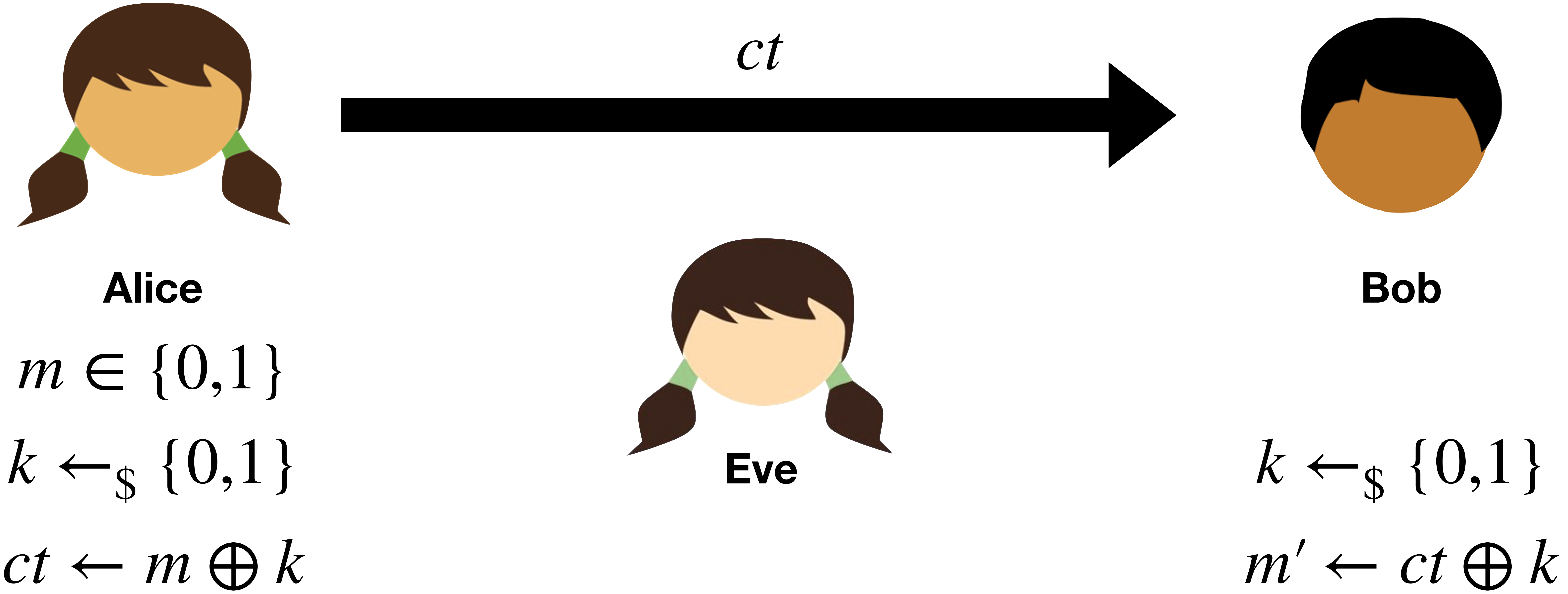
Correctness:

$$Dec(k, Enc(k, m)) = m \qquad k \oplus (k \oplus m) = m \ ✓$$

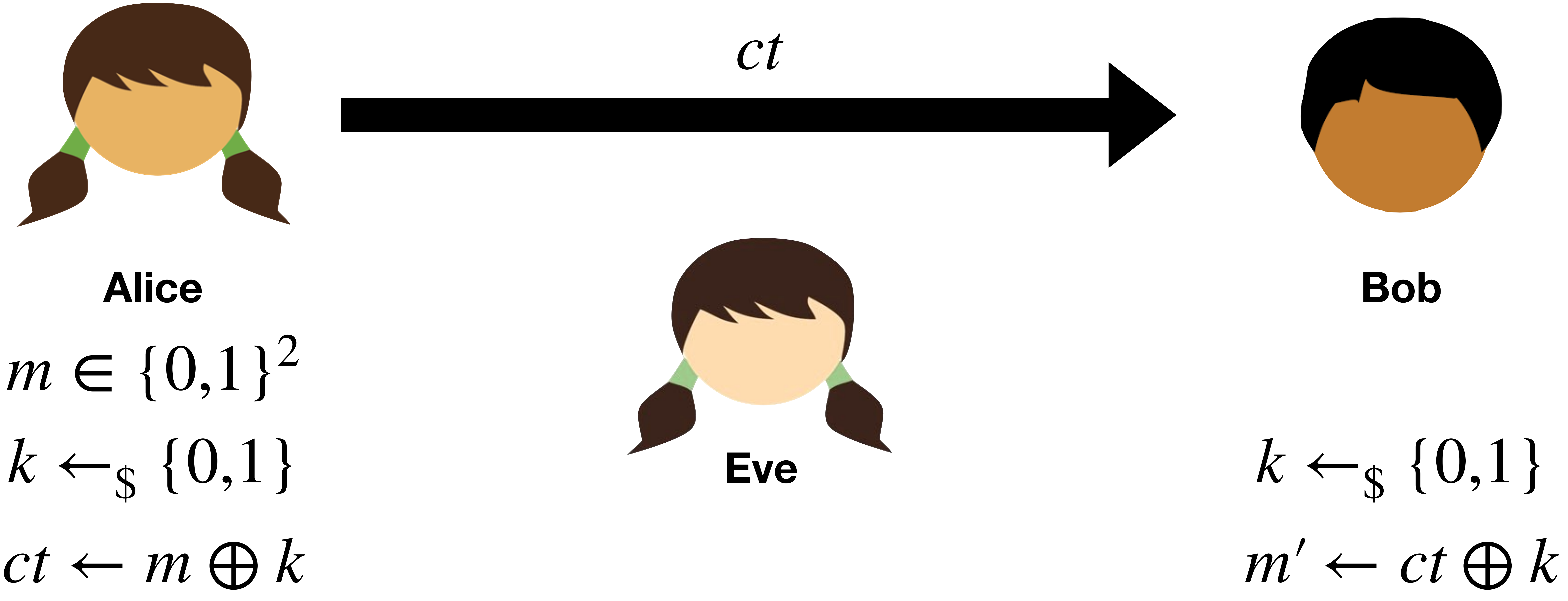
Perfect Secrecy:

For every pair of messages $m_0, m_1 \in \{0,1\}$ and every cipher text $c \in \{0,1\}$:

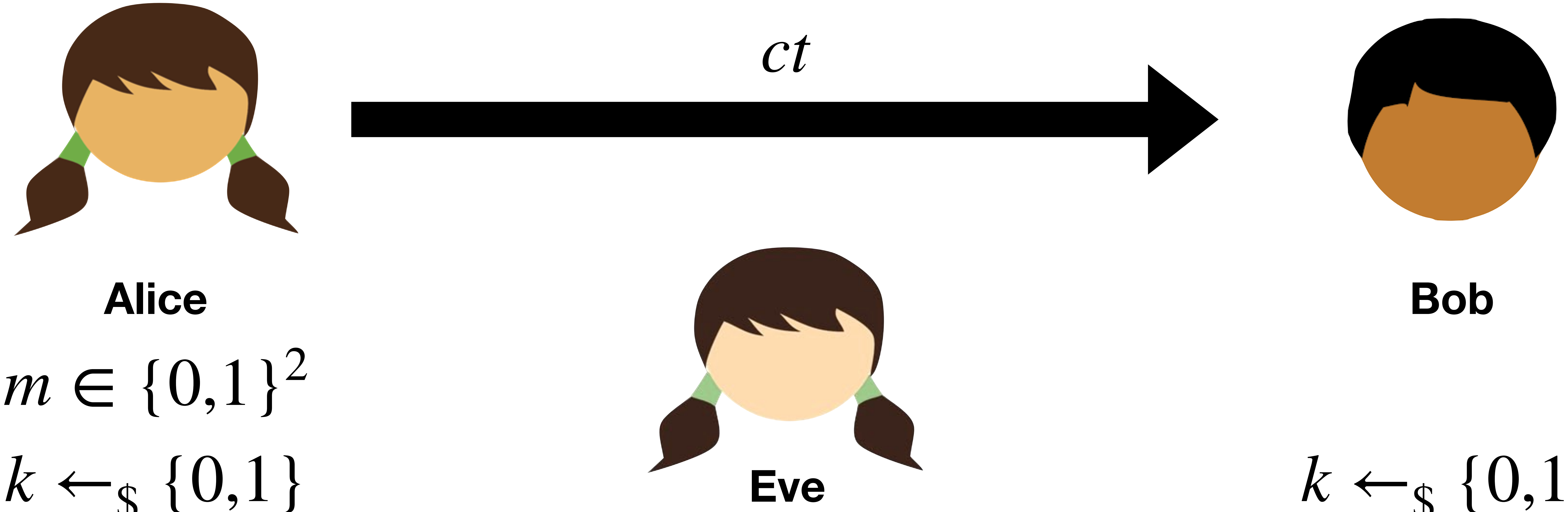
$$\Pr_{k \leftarrow \{0,1\}} [\ k \oplus m_0 = c\ ] = \Pr_{k \leftarrow \{0,1\}} [\ k \oplus m_1 = c\ ]$$



Question: *what if Alice wants to send more than one bit?*



ct
Alice
$m \in \{0,1\}^2$
$k \leftarrow_\$ \{0,1\}$
$ct \leftarrow m \oplus k$
Eve
Bob
$k \leftarrow_\$ \{0,1\}$
$m' \leftarrow ct \oplus k$



Alice:

$m \in \{0,1\}^2$

$k \leftarrow_\$ \{0,1\}$

$ct \leftarrow m \oplus k$

Bob:

$k \leftarrow_\$ \{0,1\}$

$m' \leftarrow ct \oplus k$

Key k is a one-time pad

Perfect Secrecy:

For every pair of messages $m_0, m_1 \in \mathrm{M}$ and every cipher text $c \in \mathrm{C}$:

$$\Pr_{k \leftarrow \mathrm{K}} [\ Enc(k, m_0) = c\ ] = \Pr_{k \leftarrow \mathrm{K}} [\ Enc(k, m_1) = c\ ]$$

Theorem [Shannon 1949]: *Any cipher achieving perfect secrecy requires that* $|\mathrm{K}| \geq |\mathrm{M}|$.

Perfect Secrecy:

For every pair of messages $m_0, m_1 \in \mathrm{M}$ and every cipher text $c \in \mathrm{C}$:

$$\Pr_{k \leftarrow \mathrm{K}} [\ Enc(k, m_0) = c\ ] = \Pr_{k \leftarrow \mathrm{K}} [\ Enc(k, m_1) = c\ ]$$

Theorem [Shannon 1949]: *Any cipher achieving perfect secrecy requires that* $|\mathrm{K}| \geq |\mathrm{M}|$*.*

Bad News! We will need another approach!

Perfect Secrecy:

For every pair of messages $m_0, m_1 \in \mathrm{M}$ and every cipher text $c \in \mathrm{C}$:

$$\Pr_{k \leftarrow \mathrm{K}} [\ Enc(k, m_0) = c\ ] = \Pr_{k \leftarrow \mathrm{K}} [\ Enc(k, m_1) = c\ ]$$

Theorem [Shannon 1949]: *Any cipher achieving perfect secrecy requires that* $|\mathrm{K}| \geq |\mathrm{M}|$*.*

Bad News! We will need another approach!

Key idea: what if we can make something that *looks* random, but actually isn't

Modern Cryptography

State assumptions

Today: Understand why this is needed

Define security

Design system

Prove: if assumption holds, system meets definition

Today's objectives

Learn basic cryptographic vocabulary

Explain one-time pad encryption

Define perfect secrecy

Describe limitations of perfect secrecy