Perfect Secrecy and One-Time Pads

CS/ECE 407

Today's objectives

Learn basic cryptographic vocabulary

Explain one-time pad encryption

Define perfect secrecy

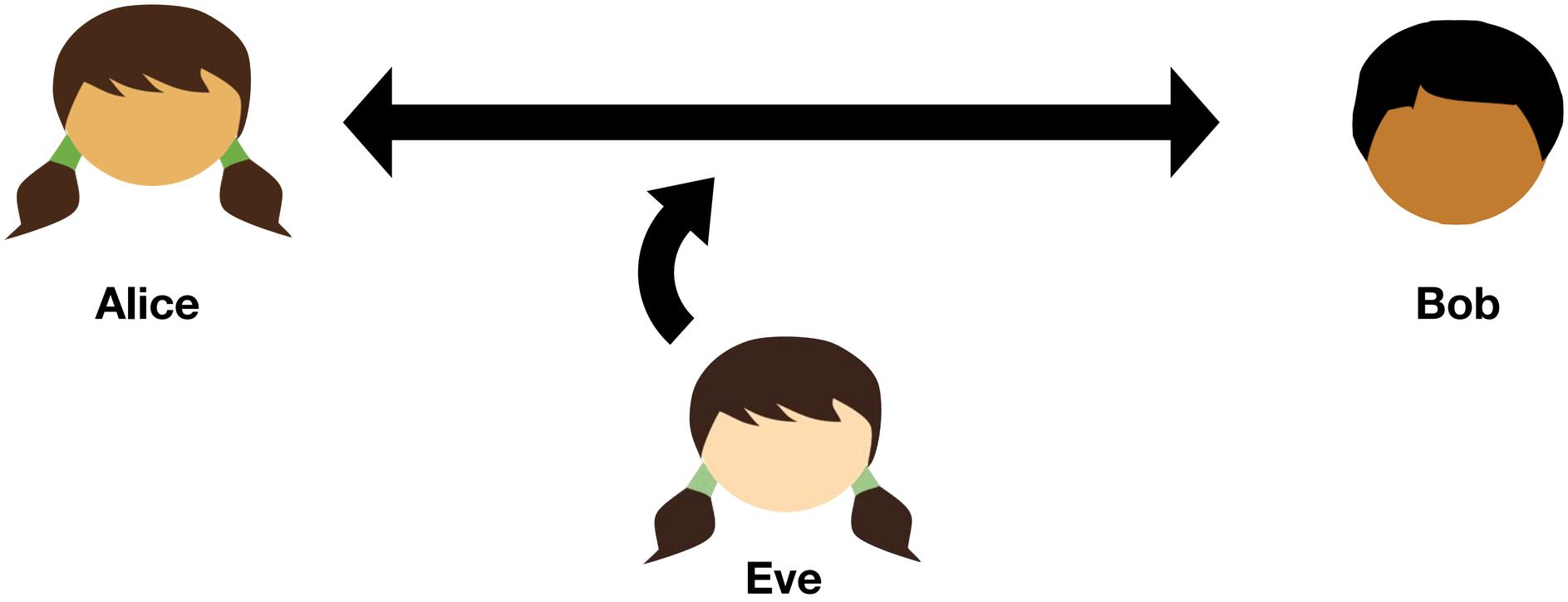
Describe limitations of perfect secrecy

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

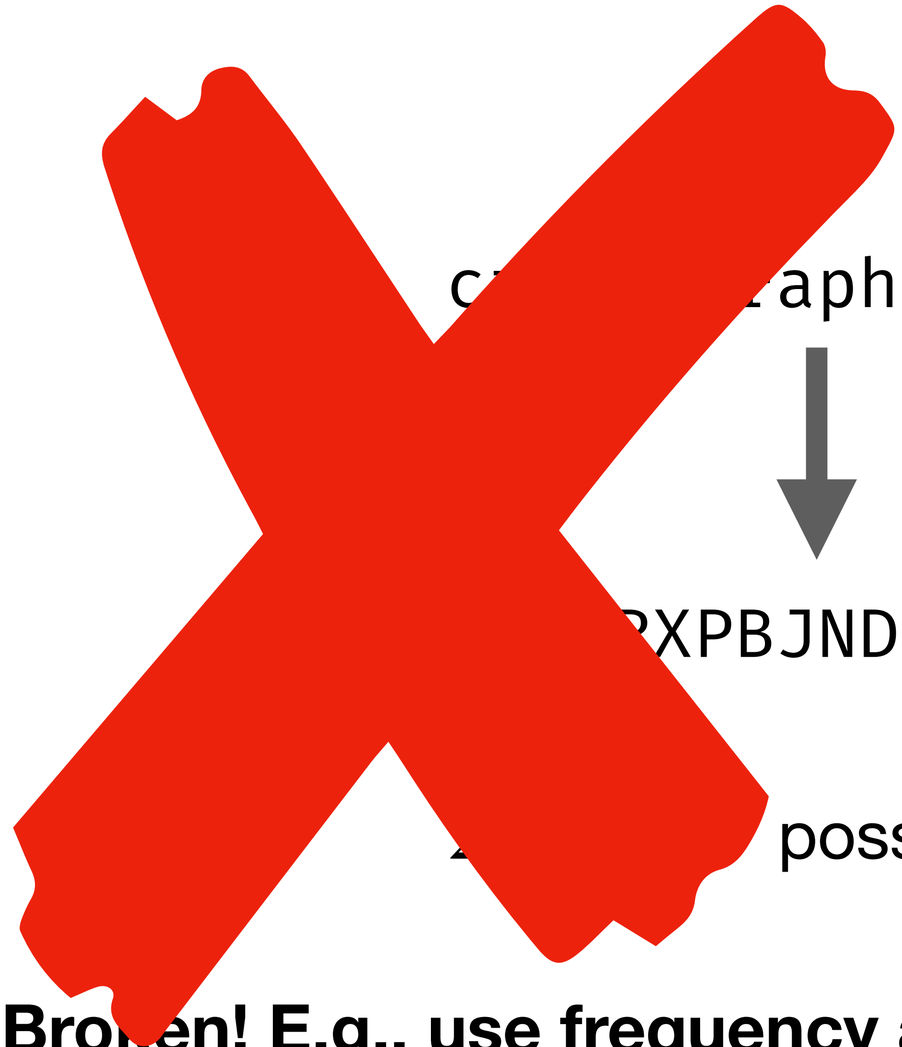
ZBGNRXPBJNDGQFZXXA

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

Broken! E.g., use frequency analysis!

Substitution Cipher

a → J
b → Y
c → Z
d → K
e → C
f → I
…



raphyiscool

RXPBJNDGQFZXXA

possible keys

Broken! E.g., use frequency analysis!

Modern Cryptography

State assumptions

Today: Understand why this is needed

Define security

Design system

Prove: if assumption holds, system meets definition

(Discrete) Probability Distribution

A **discrete probability distribution** is a map

$$X : S \to [0,1]$$

from a set of outcomes S to the probability that each outcome occurs, such that the image of X sums to 1

$$\text{fair coin} = \begin{cases} \text{heads} \mapsto \frac{1}{2} \\ \text{tails} \mapsto \frac{1}{2} \end{cases}$$

Notation:

$$x \leftarrow_{\$} X \text{ or } x \leftarrow X$$

Sample x from distribution X

(Discrete) Uniform Distribution

The **discrete uniform distribution** over a finite set S sends each element of S to probability $\frac{1}{|S|}$

$$\text{uniform coin pair} = \begin{cases} \text{HH} \mapsto \frac{1}{4} \\ \text{HT} \mapsto \frac{1}{4} \\ \text{TH} \mapsto \frac{1}{4} \\ \text{TT} \mapsto \frac{1}{4} \end{cases}$$

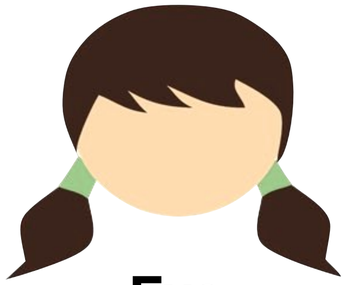
Notation:

$x \leftarrow_{\$} S$ or $x \leftarrow S$

Sample x from uniform distribution over S

Alice

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



Eve

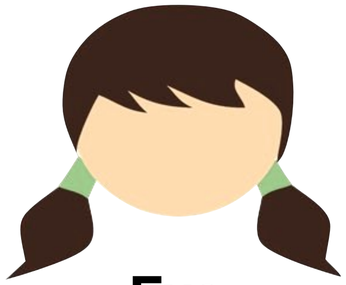
Bob

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

Alice

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

k



Eve

Bob

k

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

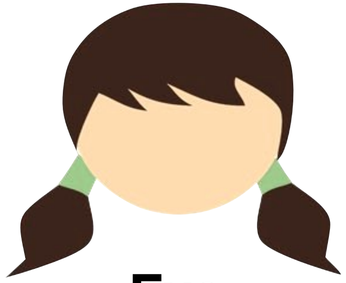
ct

Alice

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

k

$ct = m \oplus k$



Eve

Bob

k

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

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

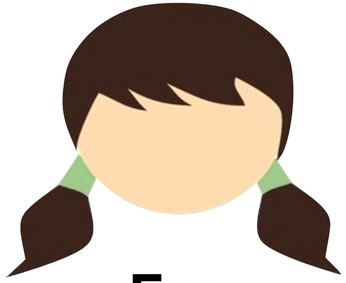
ct

Alice

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

k

$ct = m \oplus k$



Eve

Bob

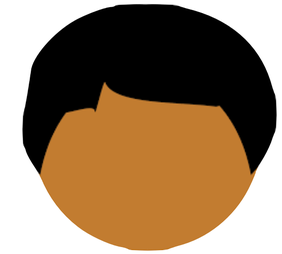
k

$m' = ct \oplus k$

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

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

ct

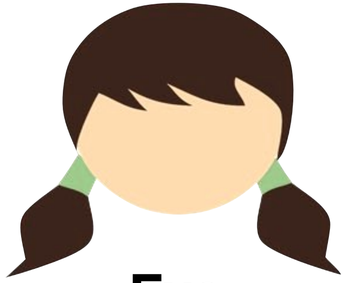


Alice

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

k

$ct = m \oplus k$



Eve

Bob

k

$m' = ct \oplus k$

What are we *not* hiding?

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

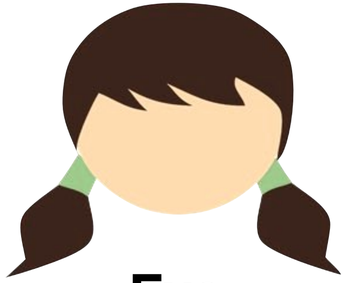
ct

Alice

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

k

$ct = m \oplus k$



Eve

Bob

k

$m' = ct \oplus k$

What are we *not* hiding?

We do not hide that a message *exists*

We are cryptographers, not steganographers

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

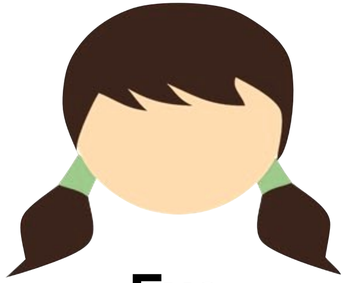
ct

Alice

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

k

$ct = m \oplus k$



Eve

Bob

k

$m' = ct \oplus k$

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

Kerckhoffs's Principle

Security Through Obscurity — Conceal details of the system in the hopes that it will protect you

Kerckhoff’s Principle: “[A cipher’s design] should not require secrecy, and it should not be a problem be a problem if it falls into enemy hands.”

Claude Shannon’s phrasing: “The enemy knows the system.”

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*:

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

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

Enc can be probabilistic

Dec is deterministic

Symmetric Cipher

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

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

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

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:

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:

For every message $m \in \mathrm{M}$:

$$\Pr\left[Dec(k, c) = m \;\middle|\; \begin{array}{l} k \leftarrow_{\$} K \\ c \leftarrow Enc(k, m) \end{array} \right] = 1$$

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:

For every message $m \in \mathrm{M}$:

$$\Pr\left[Dec(k, c) = m \;\middle|\; \begin{array}{l} k \leftarrow_{\$} K \\ c \leftarrow Enc(k, m) \end{array} \right] = 1$$

$$k \oplus (k \oplus m) = m$$

Symmetric Cipher

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

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

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

Correctness:

For every message $m \in \mathrm{M}$:

$$\Pr\left[Dec(k, c) = m \;\middle|\; \begin{array}{l} k \leftarrow_{\$} K \\ c \leftarrow Enc(k, m) \end{array} \right] = 1$$

$$k \oplus (k \oplus m) = m$$

Confidentiality:

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:

For every message $m \in \mathrm{M}$:

$$\Pr\left[Dec(k, c) = m \;\middle|\; \begin{array}{l} k \leftarrow_{\$} K \\ c \leftarrow Enc(k, m) \end{array} \right] = 1$$

$$k \oplus (k \oplus m) = m$$

Perfect Secrecy:

Symmetric Cipher

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

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

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

Correctness:

For every message $m \in \mathrm{M}$:

$$\Pr\left[Dec(k, c) = m \;\middle|\; \begin{array}{l} k \leftarrow_{\$} K \\ c \leftarrow Enc(k, m) \end{array} \right] = 1$$

$$k \oplus (k \oplus m) = m$$

Perfect Secrecy:

For every message $m \in \mathrm{M}$:

$$\left\{ c \;\middle|\; \begin{array}{l} k \leftarrow_{\$} K \\ c = Enc(k, m) \end{array} \right\} \equiv \left\{ c \;\middle|\; c \leftarrow_{\$} C \right\}$$

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:

For every message $m \in \mathrm{M}$:

$$\Pr\left[Dec(k, c) = m \;\middle|\; \begin{array}{l} k \leftarrow_{\$} K \\ c \leftarrow Enc(k, m) \end{array} \right] = 1$$

$$k \oplus (k \oplus m) = m$$ ✓

Perfect Secrecy:

For every message $m \in \mathrm{M}$:

$$\left\{ c \;\middle|\; \begin{array}{l} k \leftarrow_{\$} K \\ c = Enc(k, m) \end{array} \right\} \equiv \left\{ c \;\middle|\; c \leftarrow_{\$} C \right\}$$ ✓

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

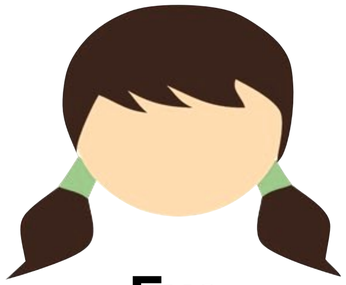
ct

Alice

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

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

$ct \leftarrow m \oplus k$



Eve

Bob

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

$m' \leftarrow ct \oplus k$

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

Alice

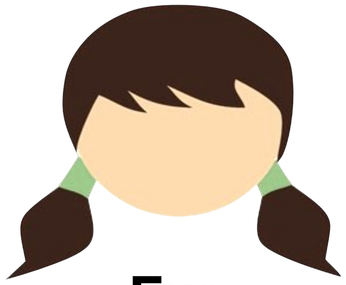
$m \in \{0,1\}^2$

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

$ct \leftarrow m \oplus k$

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

ct



Eve

Bob

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

$m' \leftarrow ct \oplus k$

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

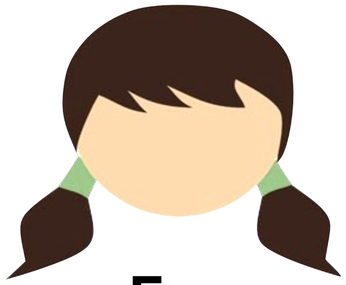
ct

Alice

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

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

$ct \leftarrow m \oplus k$



Eve

Bob

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

$m' \leftarrow ct \oplus k$

Key k is a one-time pad

Perfect Secrecy:

For every message $m \in \mathrm{M}$, the following are identically distributed:

$$\left\{ c \;\middle|\; \begin{array}{l} k \leftarrow_{\$} K \\ c = Enc(k, m) \end{array} \right\} \equiv \left\{ c \;\middle|\; c \leftarrow_{\$} C \right\}$$

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 message $m \in \mathrm{M}$, the following are identically distributed:

$$\left\{ c \;\middle|\; \begin{array}{l} k \leftarrow_{\$} K \\ c = Enc(k, m) \end{array} \right\} \equiv \left\{ c \;\middle|\; c \leftarrow_{\$} C \right\}$$

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