CSCI 1510

- Syntax of Symmetric-Key Encryption
- Kerckhoff's Principle
- Definition of Perfect Security
- One-Time Pad
- Limitations of Perfect Security

Message Secrecy

Alice

c

Bob

(plaintext)

m

Encrypt

c

(ciphertext)

Eve

$m = ?$

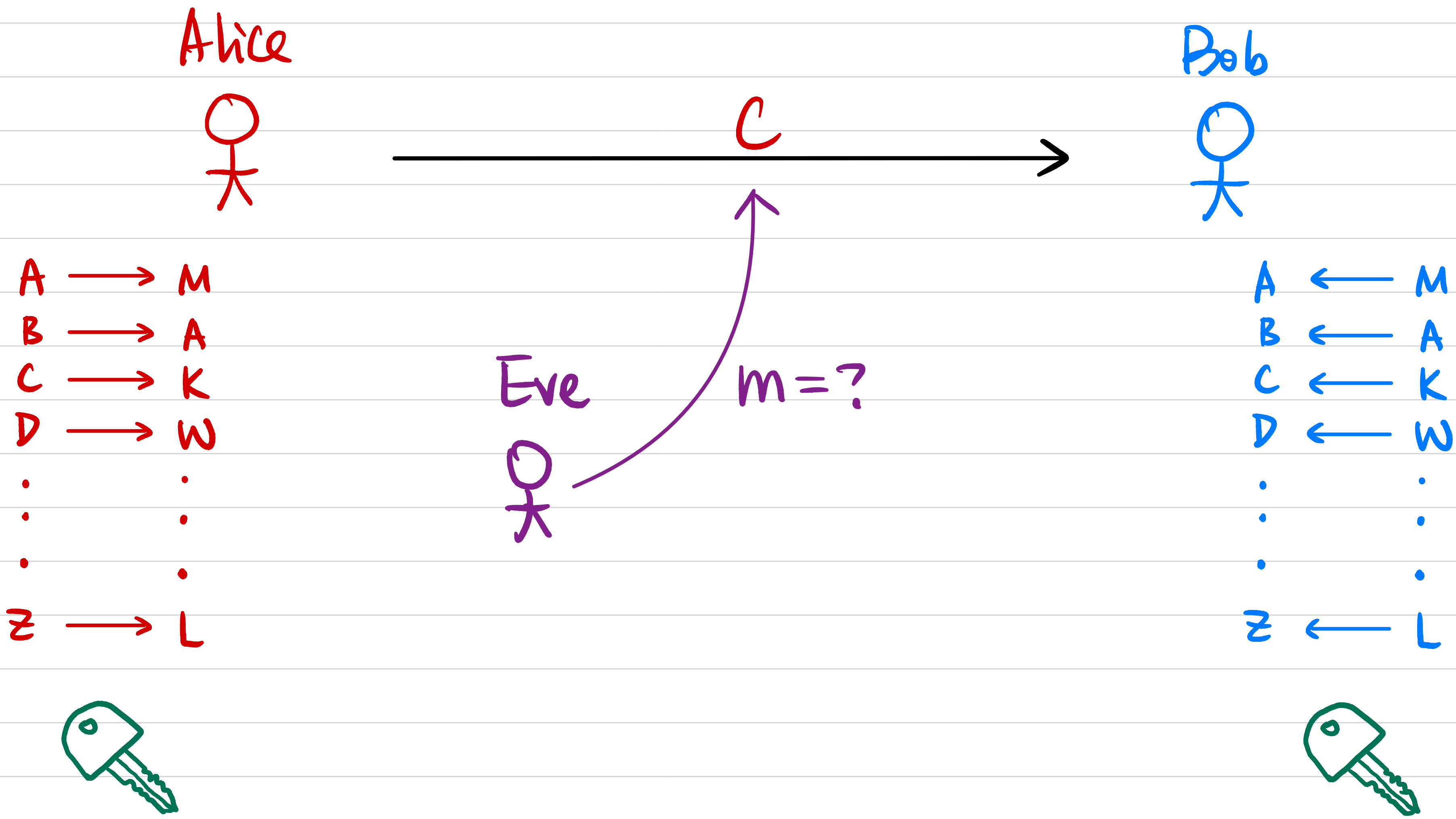
(Eavesdropper)

c

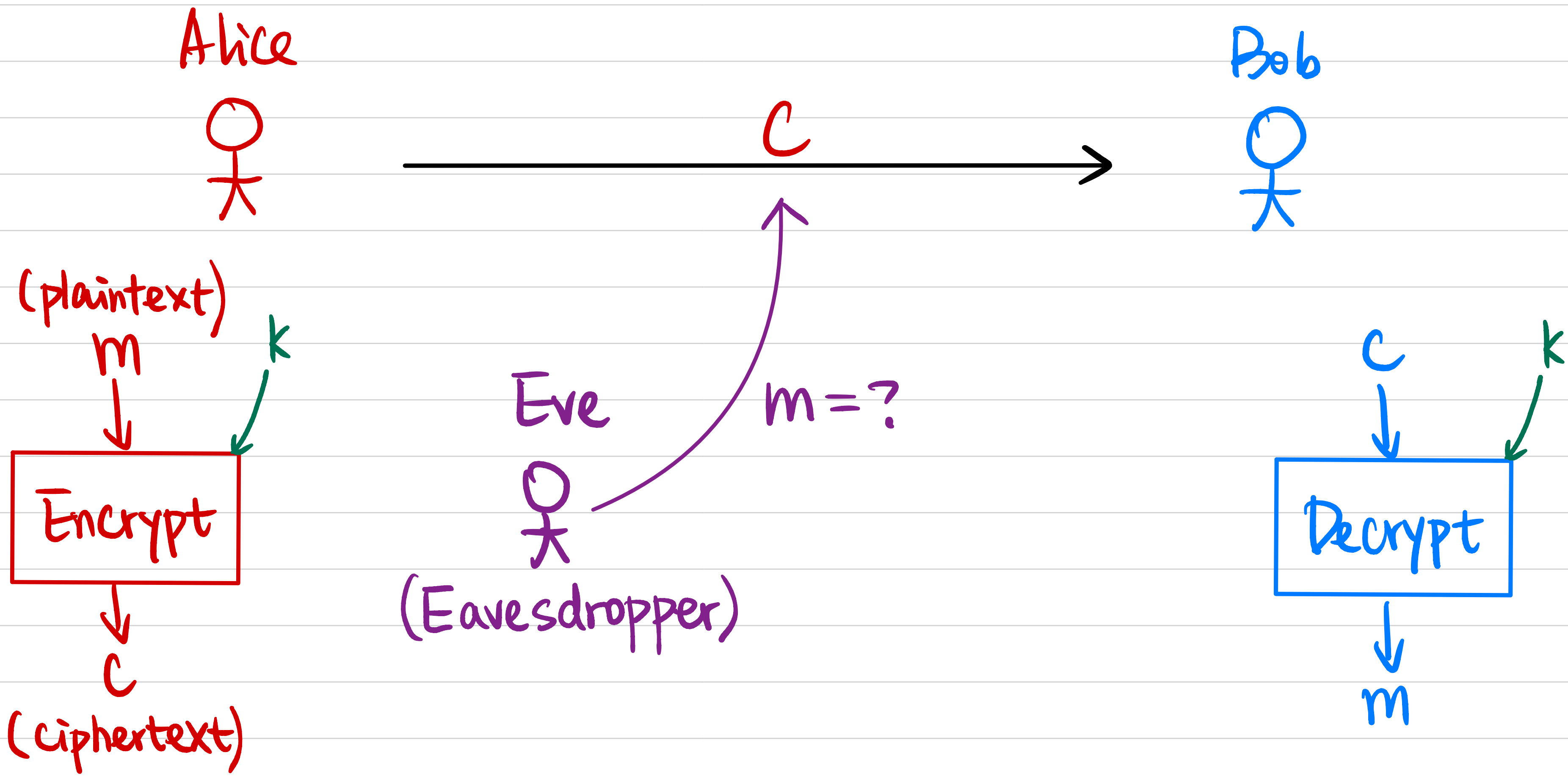
Decrypt

m

Substitution Cipher



Modern Cryptography



How to define security?

Symmetric-Key Encryption

Private-Key / Secret-Key

- **Syntax:**

  A symmetric-key encryption scheme is defined by a message space $\mathcal{M}$, a key space $\mathcal{K}$, and algorithms (Gen, Enc, Dec):

  $k \leftarrow \text{Gen}$

  $c \leftarrow \text{Enc}(k, m)$ $\quad$ $\text{Enc}_k(m)$

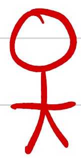
  $m/\perp := \text{Dec}(k, c)$ $\quad$ $\text{Dec}_k(c)$

- **Correctness:** $\forall m \in \mathcal{M}$, $\forall k$ output by Gen,

  $$\text{Dec}_k(\text{Enc}_k(m)) = m$$

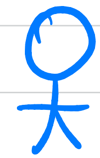
Substitution Cipher

Alice



$$\xrightarrow{\quad c \quad}$$

Bob



$A \longrightarrow M$
$B \longrightarrow A$
$C \longrightarrow K$
$D \longrightarrow W$
$\vdots \qquad \vdots$
$Z \longrightarrow L$

$M = \{\text{strings over English alphabet}\}$

$K = \{f : \{A \cdots Z\} \to \{A \cdots Z\},\ f \text{ is one-to-one}\}$

$|K| = 26!$

Gen: $f \xleftarrow{\$} K$ output f.

$\mathrm{Enc}_k(m)$: $m = m_1 m_2 \cdots m_\ell$

$\uparrow$

$f : \{A \cdots Z\} \to \{A \cdots Z\}$

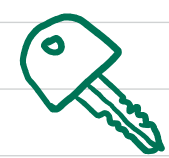
Output $c = f(m_1) f(m_2) \cdots f(m_\ell)$

$\mathrm{Dec}_k(c)$: $c = c_1 c_2 \cdots c_\ell$

$\uparrow$

$f : \{A \cdots Z\} \to \{A \cdots Z\}$ Output $m = f^{-1}(c_1) f^{-1}(c_2) \cdots f^{-1}(c_\ell)$

$A \longleftarrow M$
$B \longleftarrow A$
$C \longleftarrow K$
$D \longleftarrow W$
$\vdots \qquad \vdots$
$Z \longleftarrow L$



Private-Key / Secret-Key

Symmetric-Key Encryption

- Syntax:

A symmetric-key encryption scheme is defined by a message space $\mathcal{M}$, a key space $\mathcal{K}$, and algorithms (Gen, Enc, Dec):

$k \leftarrow \mathrm{Gen}$

$c \leftarrow \mathrm{Enc}(k, m)$ $\quad \mathrm{Enc}_k(m)$ $\quad$ k must be kept secret

$m/\perp := \mathrm{Dec}(k, c)$ $\quad \mathrm{Dec}_k(c)$ $\quad$ Keep (Gen, Enc, Dec) secret as well?

- Correctness: $\forall m \in \mathcal{M}$, $\forall k$ output by Gen,

$$\mathrm{Dec}_k(\mathrm{Enc}_k(m)) = m$$

Kerckhoff's Principle

The cipher method must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.

↑
Only the key is kept secret

Why?

① facilitates cryptanalysis
② key leakage → easy to switch to another key
③ easy to keep different keys with different people
④ easy to standardize

How to define security?

- It's impossible for Eve to recover k from c.

$$\mathrm{Enc}_k(m) = m$$

$\uparrow$

$c = m$

- It's impossible for Eve to recover m from c.

90% of m?

- It's impossible for Eve to recover any character of m from c.

distribution of m?

already knows some characters of m?

The Right Definition

Regardless of any information an attacker already has,

a ciphertext should leak no additional information about the plaintext.

Notation

$\mathcal{K}$: key space

$\mathcal{M}$: message/plaintext space

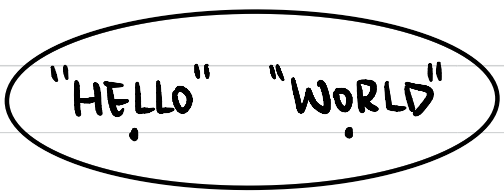
$\mathcal{C}$: ciphertext space

K: random variable denoting the output of Gen.

$$\Pr[K = k] = \Pr[\text{Gen outputs } k].$$

M: random variable denoting the message/plaintext to be encrypted.

Example: $\mathcal{M} = \{\text{"HELLO"}, \text{"WORLD"}\}$



$$\Pr[M = \text{"HELLO"}] = 0.3$$

$$\Pr[M = \text{"WORLD"}] = 0.7$$

C: random variable denoting the resulting ciphertext.

① $k \leftarrow \text{Gen}$

② $m \leftarrow \mathcal{M}$ (following a certain distribution)

③ $c \leftarrow \text{Enc}_k(m)$

Exercise: Substitution Cipher

K: $\quad \Pr[K = k] = \dfrac{1}{|\mathcal{K}|} = \dfrac{1}{26!} \quad \forall k$

M: $\quad \mathcal{M} = \{\text{"HELLO"}, \text{"WORLD"}\}$

"HELLO" "WORLD"

$\Pr[M = \text{"HELLO"}] = 0.3$

$\Pr[M = \text{"WORLD"}] = 0.7$

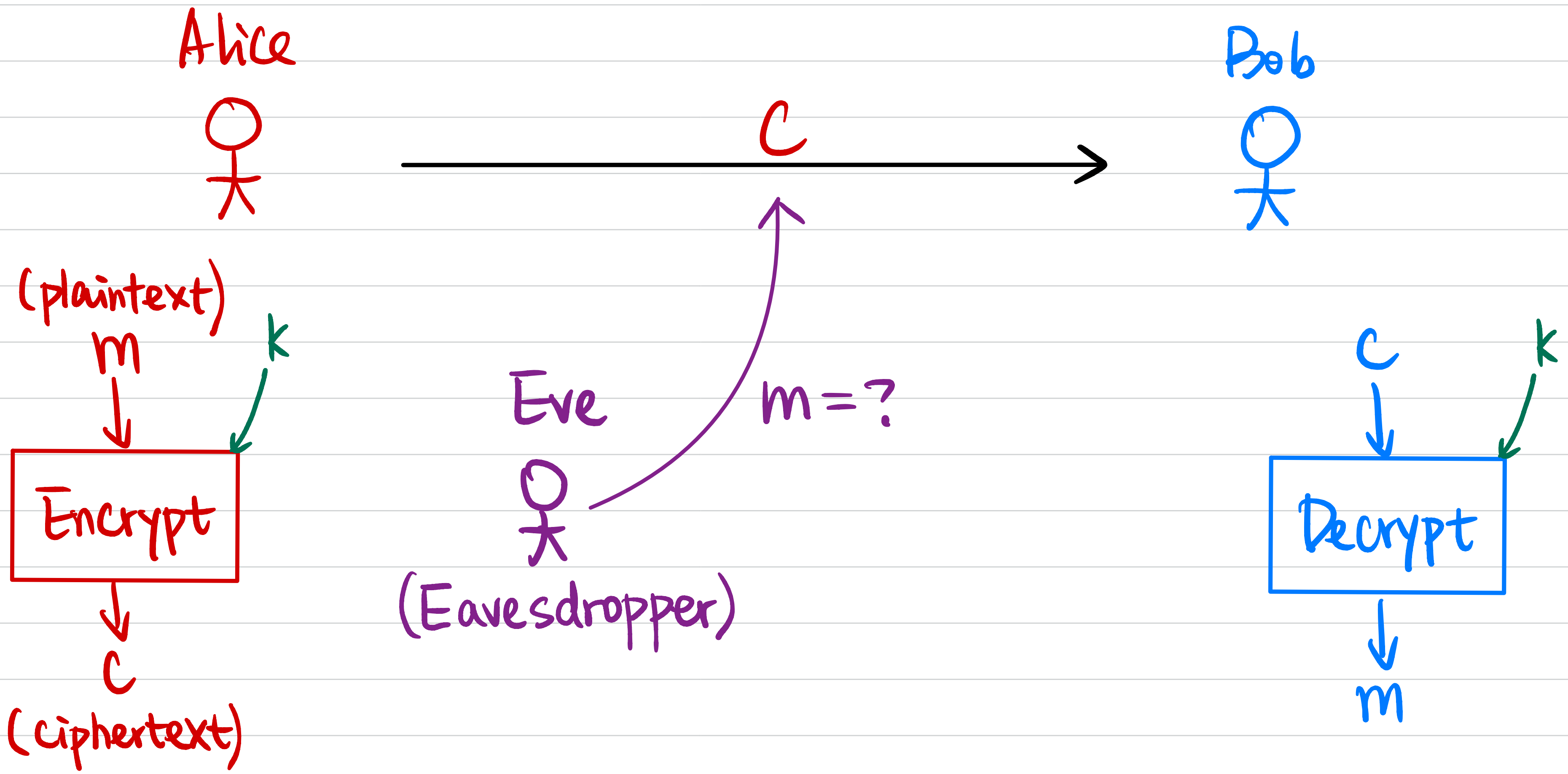
C: $\quad \Pr[C = c] = ?$

$$\Pr[C = \text{"ABCDE"}] = \Pr[M = \text{"WORLD"} \wedge \mathrm{Enc}_K(\text{"WORLD"}) = \text{"ABCDE"}]$$

$$= \Pr[M = \text{"WORLD"}] \cdot \Pr\left[f: \begin{array}{l} W \to A \\ O \to B \\ R \to C \\ L \to D \\ D \to E \end{array}\right]$$

$$= 0.7 \cdot \frac{1}{26 \cdot 25 \cdot 24 \cdot 23 \cdot 22}$$

Symmetric-Key Encryption



Eve Knows: ① $\mathcal{K}, \mathcal{M}, \mathcal{C}$, (Gen, Enc, Dec)

② distribution over $\mathcal{M}$

③ ciphertext c

Perfect Security

Def 1 A symmetric-key encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secure if

$\forall$ probability distribution over $\mathcal{M}$,

$\forall m \in \mathcal{M}$,

$\forall c \in \mathcal{C}$ for which $\Pr[C=c]>0$:

$$\Pr[M=m \mid C=c] = \Pr[M=m].$$

Exercise: Substitution Cipher

$$\Pr[M = m \mid C = c] \stackrel{?}{=} \Pr[M = m].$$

K: $\Pr[K = k] = \dfrac{1}{26!} \quad \forall k$

M: $\mathcal{M} = \{\text{"HELLO"}, \text{"WORLD"}\}$

"HELLO" "WORLD"

$\Pr[M = \text{"HELLO"}] = 0.3$

$\Pr[M = \text{"WORLD"}] = 0.7$

C: $\Pr[C = \text{"ABCDE"}] = 0.7 \cdot \dfrac{1}{26 \cdot 25 \cdot 24 \cdot 23 \cdot 22}$

$$\Pr[M = \text{"HELLO"} \mid C = \text{"ABCDE"}] = 0$$

Exercise: Substitution Cipher

$$\Pr[M=m \mid C=c] \stackrel{?}{=} \Pr[M=m].$$

K: $\Pr[K=k] = \frac{1}{26!} \quad \forall k$

M: $\mathcal{M} = \{\text{"CRYPT"}, \text{"WORLD"}\}$

"CRYPT" "WORLD"

$\Pr[M=\text{"CRYPT"}] = 0.3$

$\Pr[M=\text{"WORLD"}] = 0.7$

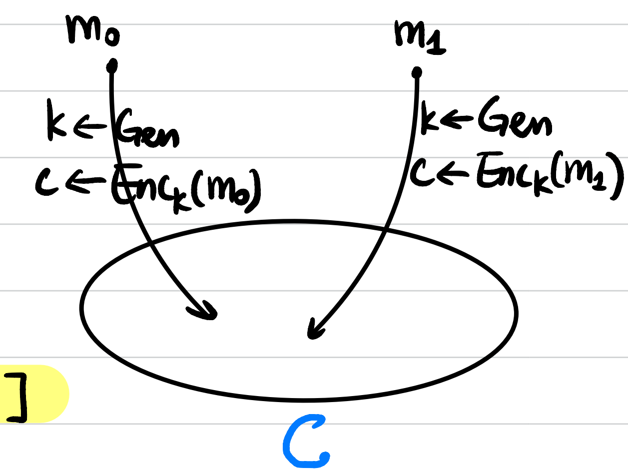
C:
$$\begin{aligned}\Pr[C=\text{"ABCDE"}] &= \Pr[M=\text{"WORLD"} \wedge \mathrm{Enc}_K(\text{"WORLD"}) = \text{"ABCDE"}] \\ &\quad + \Pr[M=\text{"CRYPT"} \wedge \mathrm{Enc}_K(\text{"CRYPT"}) = \text{"ABCDE"}] \\ &= 0.7 \cdot \frac{1}{26\cdot 25\cdot 24\cdot 23\cdot 22} + 0.3 \cdot \frac{1}{26\cdot 25\cdot 24\cdot 23\cdot 22} \\ &= \frac{1}{26\cdot 25\cdot 24\cdot 23\cdot 22}\end{aligned}$$

Bayes' Rule

$$\begin{aligned}\Pr[M=\text{"CRYPT"} \mid C=\text{"ABCDE"}] &= \frac{\Pr[M=\text{"CRYPT"} \wedge C=\text{"ABCDE"}]}{\Pr[C=\text{"ABCDE"}]} \\ &= \frac{0.3 \cdot \frac{1}{26\cdot 25\cdot 24\cdot 23\cdot 22}}{\frac{1}{26\cdot 25\cdot 24\cdot 23\cdot 22}} = 0.3\end{aligned}$$

Perfect Security

Def 2 A symmetric-key encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secure if



$\forall\, m_0, m_1 \in \mathcal{M}$,

$\forall\, c \in \mathcal{C}$:

$$\Pr[\,Enc_K(m_0) = c\,] = \Pr[\,Enc_K(m_1) = c\,]$$

over choice of K & randomness of Enc

Def 1 $\forall$ probability distribution over $\mathcal{M}$,

$\forall\, m \in \mathcal{M}$,

$\forall\, c \in \mathcal{C}$ for which $\Pr[C = c] > 0$:

$$\Pr[\,M = m \mid C = c\,] = \Pr[\,M = m\,].$$

Def 1 $\Leftrightarrow$ Def 2

"$\Rightarrow$": If $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ is secure under Def 1, then Π is also secure under Def 2.

Proof: $\forall\, m_0, m_1 \in \mathcal{M}$, $\forall\, c \in \mathcal{C}$:

$$\Pr[\mathrm{Enc}_K(m_0) = c] = \Pr[C = c \mid M = m_0]$$

$$(\text{Bayes' Rule}) = \frac{\Pr[C=c] \cdot \Pr[M = m_0 \mid C = c]}{\Pr[M = m_0]}$$

$$(\text{Def } 1) = \frac{\Pr[C=c] \cdot \Pr[M = m_0]}{\Pr[M = m_0]}$$

$$= \Pr[C = c]$$

Similarly, $\Pr[\mathrm{Enc}_K(m_1) = c] = \Pr[C = c]$

$$\Pr[\mathrm{Enc}_K(m_0) = c] = \Pr[\mathrm{Enc}_K(m_1) = c]$$

Def 1 $\Leftrightarrow$ Def 2

"$\Leftarrow$": If $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ is secure under Def 2, then Π is also secure under Def 1.

Proof: $\forall m \in \mathcal{M}$, $\forall c \in \mathcal{C}$ for which $\Pr[C=c]>0$:

$$\Pr[M=m \mid C=c] = \frac{\Pr[M=m]\cdot\Pr[C=c \mid M=m]}{\Pr[C=c]}$$

$$= \frac{\Pr[M=m]\cdot\Pr[C=c \mid M=m]}{\sum_{m'\in\mathcal{M}} \Pr[M=m' \wedge C=c]}$$

$$= \frac{\Pr[M=m]\cdot\Pr[C=c \mid M=m]}{\sum_{m'\in\mathcal{M}} \Pr[M=m']\cdot\Pr[C=c \mid M=m']}$$

$$\text{(Def 2)} = \frac{\Pr[M=m]\cdot\Pr[C=c \mid M=m]}{\sum_{m'\in\mathcal{M}} \Pr[M=m']\cdot\Pr[C=c \mid M=m]}$$

$$= \frac{\Pr[M=m]}{\sum_{m'\in\mathcal{M}} \Pr[M=m']} = \Pr[M=m]$$

Perfect Security

Def 3 A symmetric-key encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly indistinguishable if $\forall \mathcal{A}$:

(Game-based)

$$\Pr[b = b'] = \frac{1}{2}$$

Challenger		$\mathcal{A}$
	$\xleftarrow{m_0, m_1 \in \mathcal{M}}$	
$k \leftarrow \text{Gen}$		
$b \xleftarrow{\$} \{0,1\}$		
$c \leftarrow \text{Enc}_k(m_b)$		
	$\xrightarrow{c}$	
		output b'

One-Time Pad (OTP)

Fix an integer $\ell > 0$.

$\mathcal{K}, \mathcal{M}, \mathcal{C} = \{0,1\}^\ell$ all ℓ-bit strings

- Gen: $k \xleftarrow{\$} \{0,1\}^\ell$, output k.
- $\text{Enc}_k(m)$: output $c := m \oplus k$
- $\text{Dec}_k(c)$: output $m := c \oplus k$

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

Example: $\ell = 5$.

$k = 01101$

Enc: $m = 00110$

$c = 01011$

Dec: $k = 01101$

$m = 00110$

- Correctness? $(k \oplus m) \oplus k = m \oplus (k \oplus k) = m$

- Security? $\forall m_0, m_1 \in \mathcal{M}, \forall c \in \mathcal{C}$:

$$\Pr[\text{Enc}_K(m_0) = c] = \Pr[C = c \mid M = m_0] = \Pr[K = m_0 \oplus c] = 2^{-\ell}$$

$$\Pr[\text{Enc}_K(m_1) = c] = 2^{-\ell}$$

One-Time Pad (OTP)

Limitations:

① key is as long as the plaintext

② Cannot reuse the key ← why?

$$\left.\begin{aligned} Enc_k(m_1) &= c_1 \\ Enc_k(m_2) &= c_2 \end{aligned}\right\} \rightarrow c_1 \oplus c_2 = (m_1 \oplus \cancel{k}) \oplus (m_2 \oplus \cancel{k}) = m_1 \oplus m_2$$

Can we make $|M| > |K|$?

Limitations of Perfect Security

Thm If $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ is a perfectly secure encryption scheme with message space $\mathcal{M}$ & key space $\mathcal{K}$, then $|\mathcal{M}| \le |\mathcal{K}|$.

Proof: Assume $|\mathcal{K}| < |\mathcal{M}|$.

Pick an arbitrary $c \in \mathcal{C}$ where $\Pr[C=c] > 0$.

$\mathcal{M}(c) := \{ m \mid m = \mathrm{Dec}_k(c) \text{ for some } k \in \mathcal{K} \}$.

$|\mathcal{M}(c)| \le |\mathcal{K}| < |\mathcal{M}|$.

$\exists m' \in \mathcal{M}$ s.t. $m' \notin \mathcal{M}(c)$.

$\Pr[M=m' \mid C=c] = 0 \ne \Pr[M=m']$.