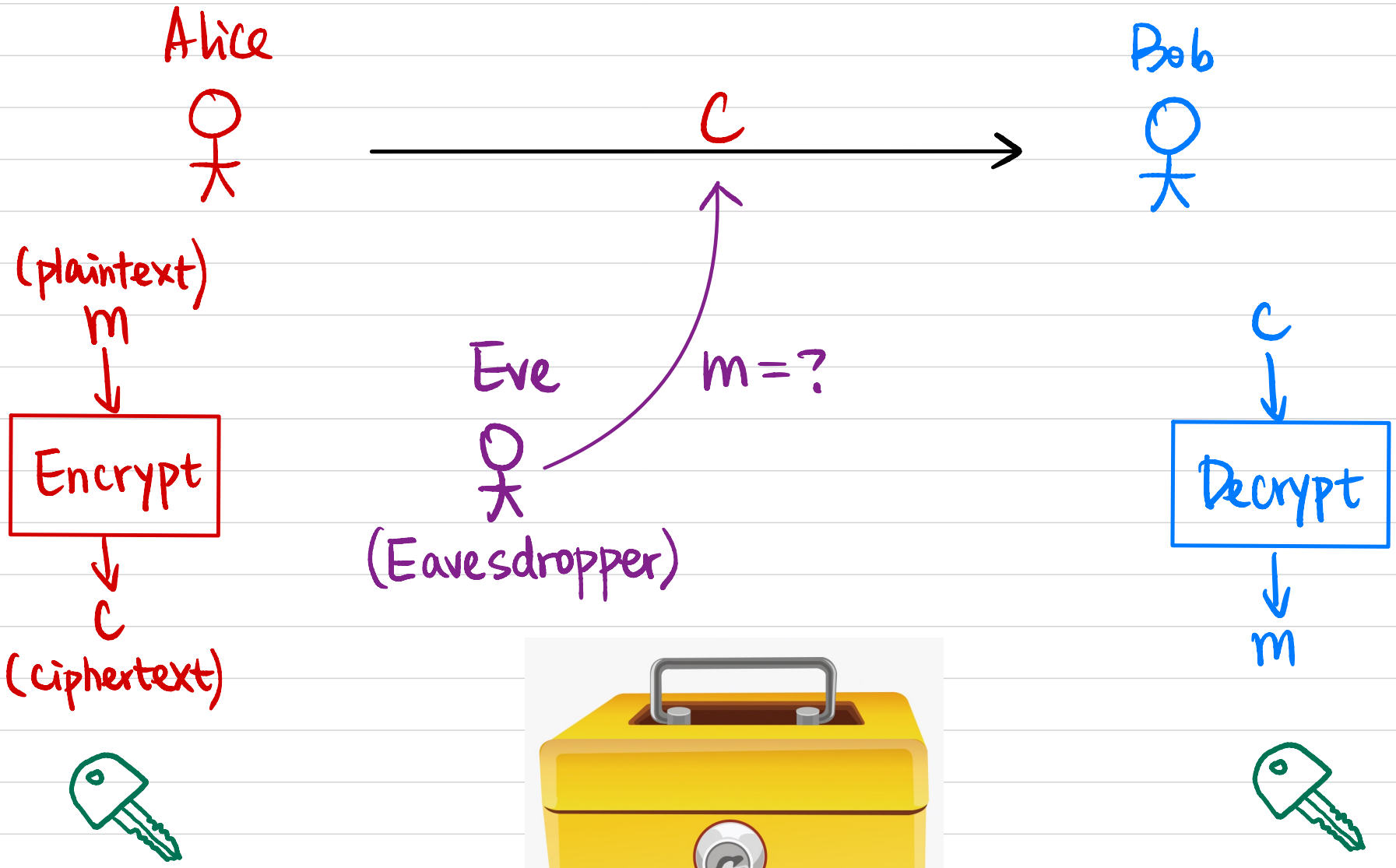
CSCI 1510

This Lecture:

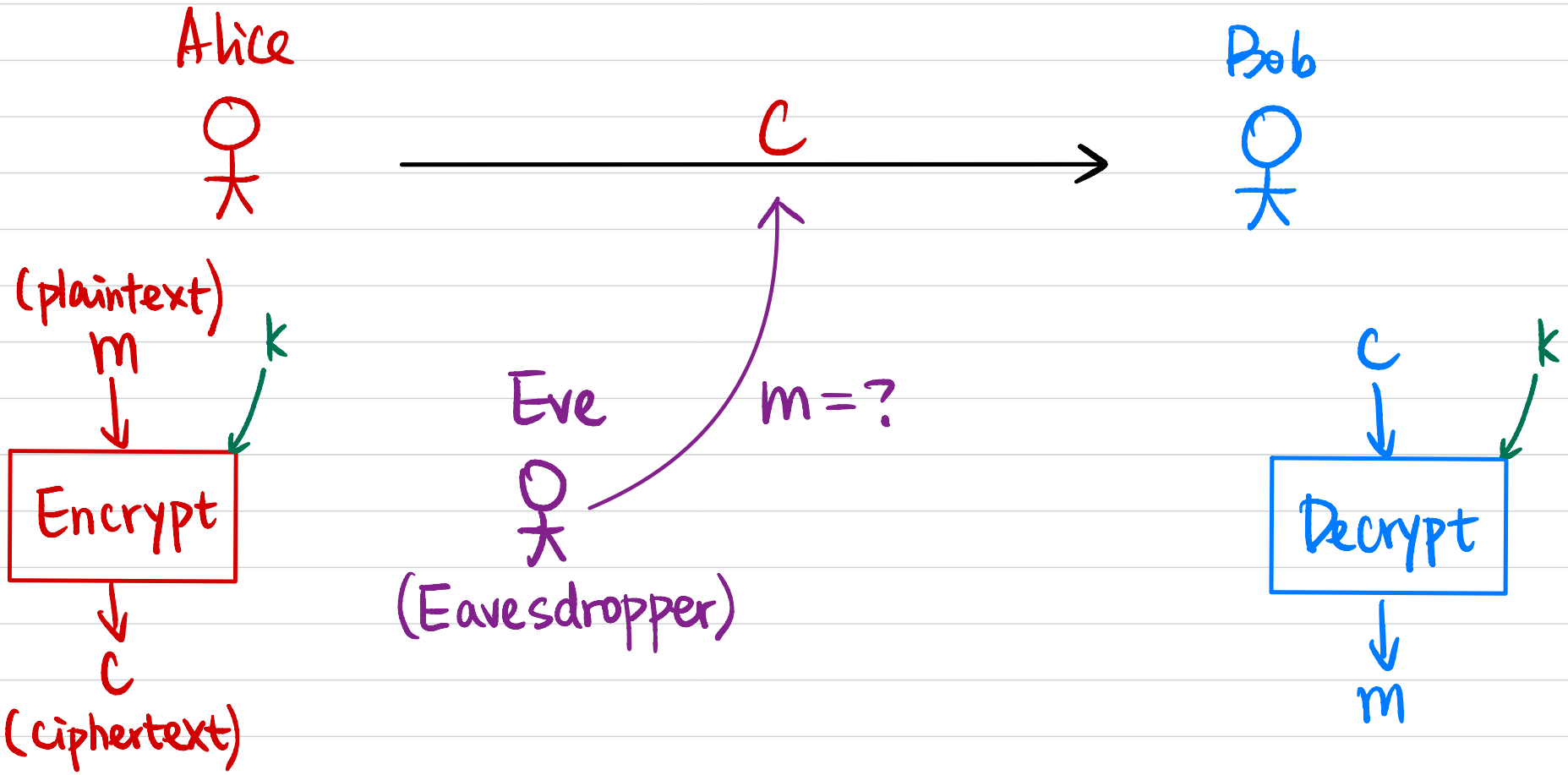
- Syntax of Symmetric-Key Encryption
- Kerckhoff's Principle
- Definition of Perfect Security
- One-Time Pad
- Limitations of Perfect Security

Message Secrecy



Symmetric-Key Encryption

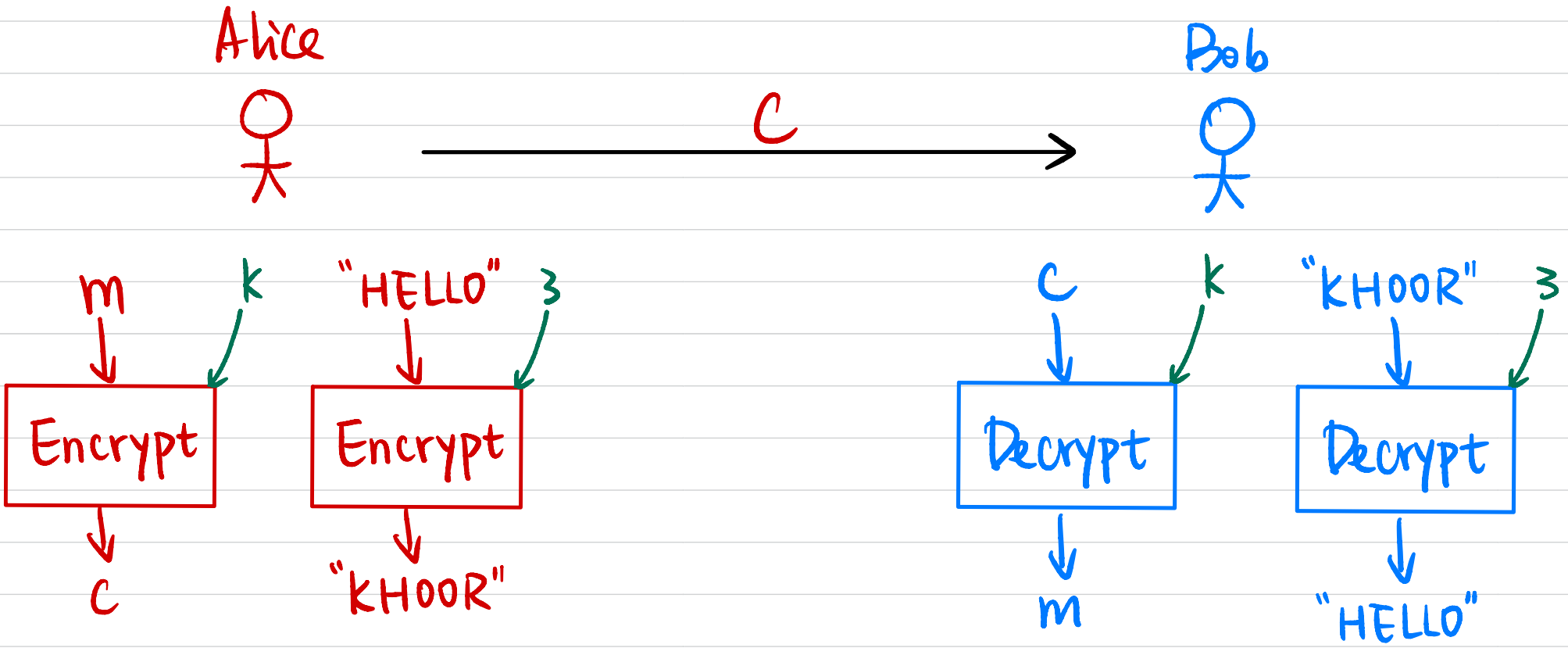
Private-Key / Secret-Key



How to define security ?

Example: Shift Cipher

$k \xleftarrow{\$} \{0, 1, \cdots, 25\}$



Shift each character forward by k.

Shift each character back by k.

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):

  $k \leftarrow Gen$

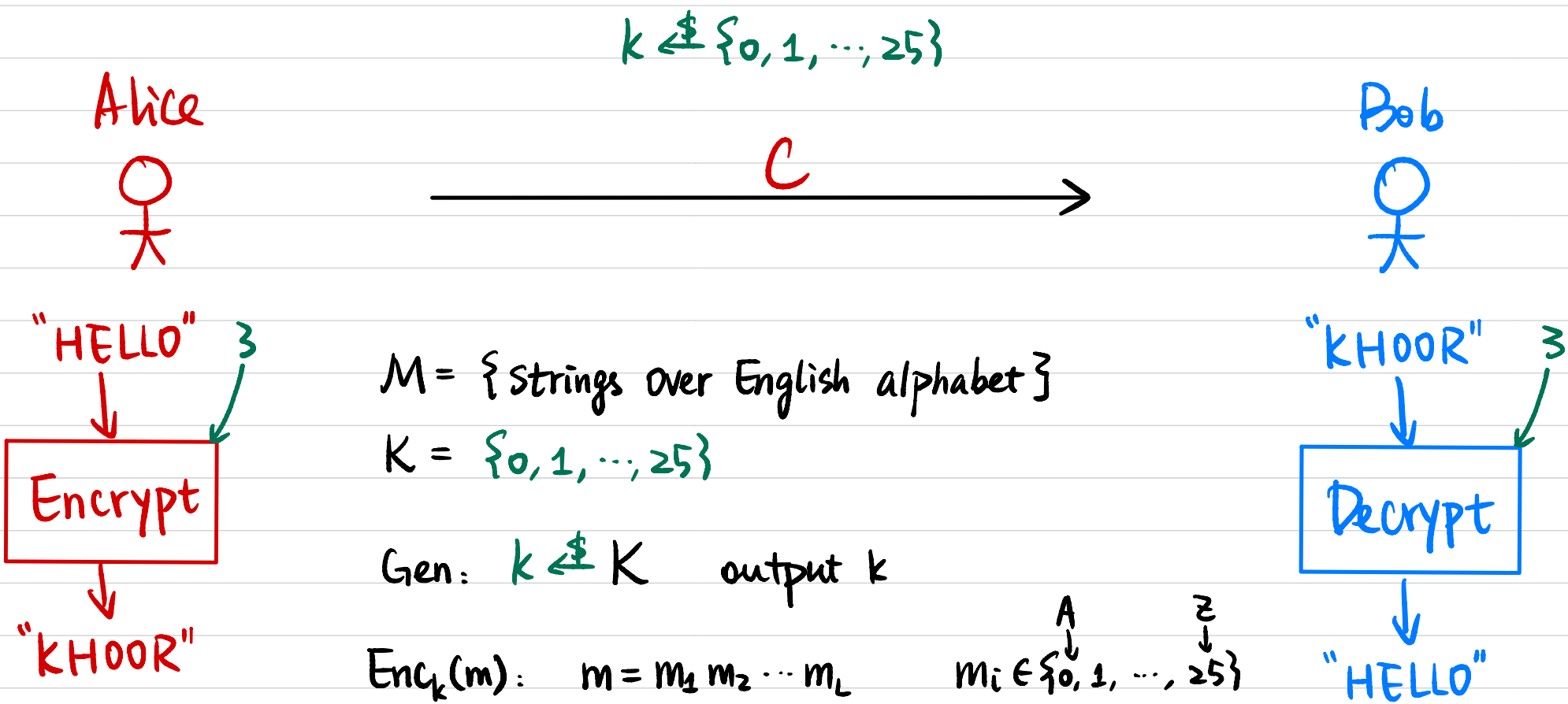
  $c \leftarrow Enc(k, m)$ $\quad Enc_k(m)$

  $m/\perp := Dec(k, c)$ $\quad Dec_k(c)$

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

  $$Dec_k(Enc_k(m)) = m$$

Example: Shift Cipher



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

$K = \{0, 1, \cdots, 25\}$

Gen: $k \xleftarrow{\$} K$ output k

$\text{Enc}_k(m)$: $m = m_1 m_2 \cdots m_L$ $\quad m_i \in \{0, 1, \cdots, 25\}$ (A ↓, Z ↓)

$c_i := (m_i + k) \bmod 26 \quad \forall i \in [L]$

output $c = c_1 c_2 \cdots c_L$

$\text{Dec}_k(c)$: $c = c_1 c_2 \cdots c_L$

$m_i := (c_i - k) \bmod 26 \quad \forall i \in [L]$

output $m = m_1 m_2 \cdots m_L$

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):

$k \leftarrow Gen$

$c \leftarrow Enc(k, m)$ $\quad Enc_k(m)$

$m/\perp := Dec(k, c)$ $\quad Dec_k(c)$

k must be kept secret

Keep (Gen, Enc, Dec) secret as well?

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

$$Dec_k(Enc_k(m)) = m$$

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 In case of key leakage → easy to switch to another key

② Facilitates cryptanalysis

③ More scalable: easy to use different keys with different people

④ Easier for standardization

How to define security?

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

$Enc_k(m) = m$

- 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?

Perfect Security

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

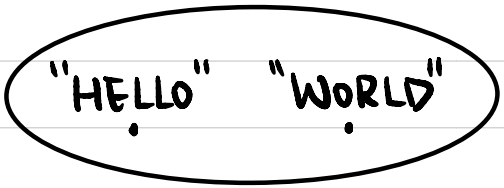
$\mathcal{C}$: ciphertext space

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 $k \leftarrow \text{Gen}$

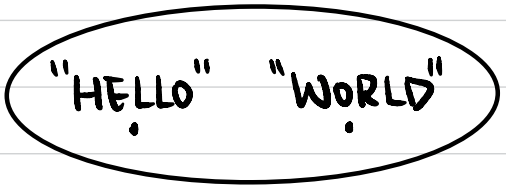
② $m \leftarrow \mathcal{M}$ (following a certain distribution)

③ $c \leftarrow \text{Enc}_k(m)$

Example: Shift Cipher

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

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



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

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

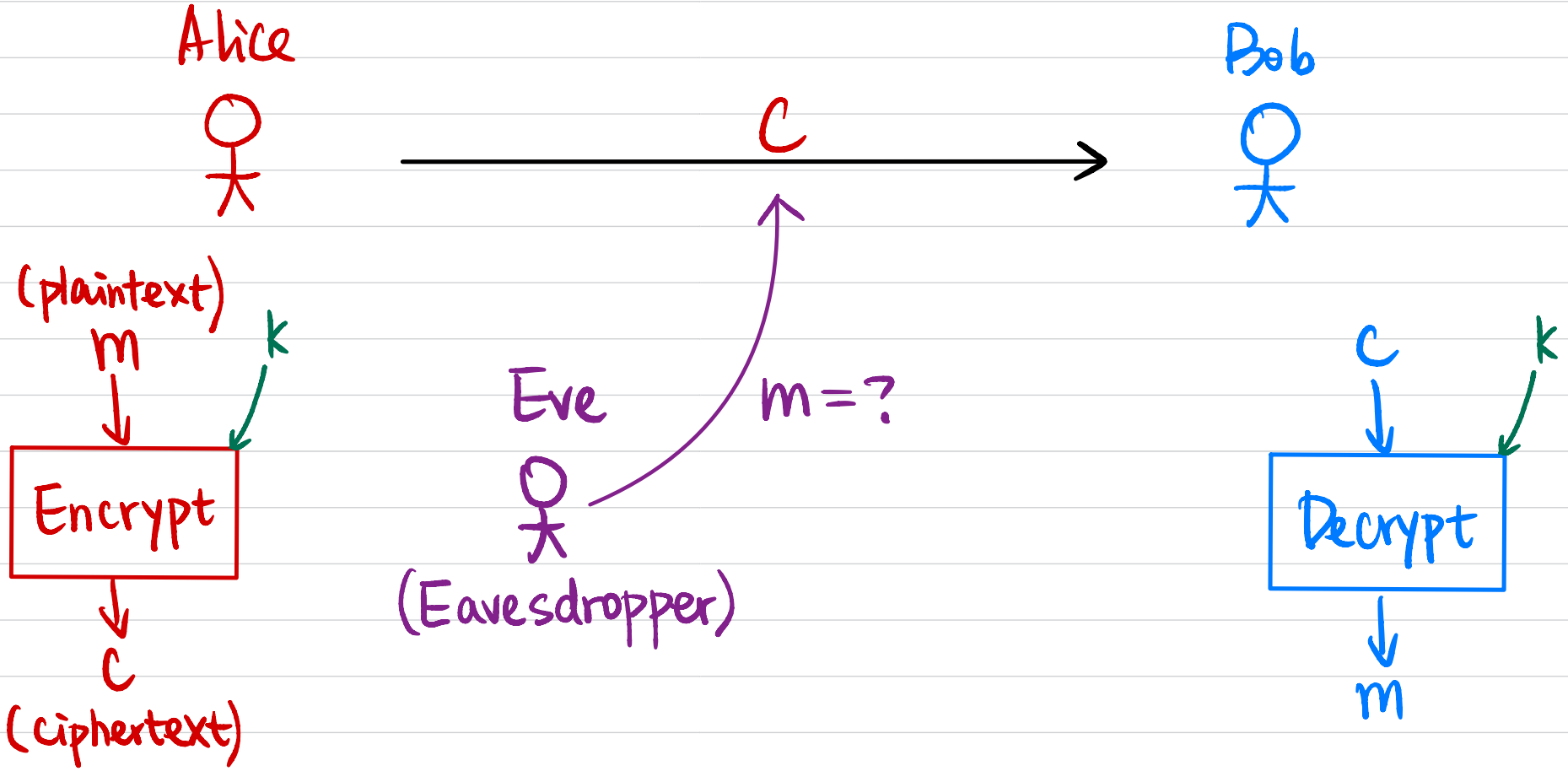
C: $\Pr[C = c] = ?$

$$\Pr[C = \text{"KHOOR"}] = \Pr[M = \text{"HELLO"} \wedge K = 3]$$

$$= \Pr[M = \text{"HELLO"}] \cdot \Pr[K = 3]$$

$$= 0.3 \cdot \frac{1}{26}$$

Symmetric-Key Encryption



Eve knows: ① K, M, C, (Gen, Enc, Dec)

② distribution over 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 $\Pr[C=c] > 0$:

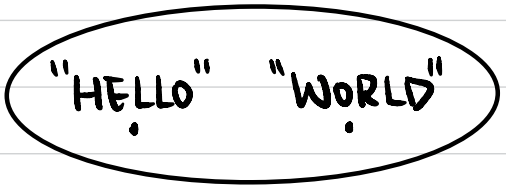
$$\Pr[M=m \mid C=c] = \Pr[M=m].$$

Example: Shift Cipher

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

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

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



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

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

$\Pr[M = \text{"HELLO"} \mid C = \text{"KHOOR"}] = 1$

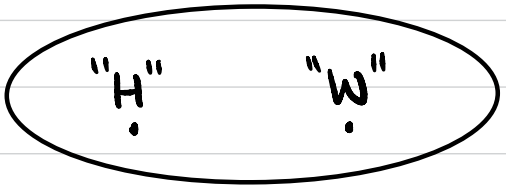
$\Pr[M = \text{"HELLO"}] = 0.3$ ≠

Example: Shift Cipher

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

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

M: $M = \{\text{"H"}, \text{"W"}\}$



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

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

Bayes' Rule

$K=3$

$$\Pr[M=\text{"H"} \mid C=\text{"k"}] = \frac{\Pr[M=\text{"H"}] \cdot \Pr[C=\text{"k"} \mid M=\text{"H"}]}{\Pr[C=\text{"k"}]}$$

$$= \frac{0.3 \cdot \frac{1}{26}}{\Pr[M=\text{"H"} \wedge C=\text{"k"}] + \Pr[M=\text{"W"} \wedge C=\text{"k"}]}$$

$$= \frac{0.3 \cdot \frac{1}{26}}{0.3 \cdot \frac{1}{26} + 0.7 \cdot \frac{1}{26}}$$

$$= 0.3$$

Perfect Security

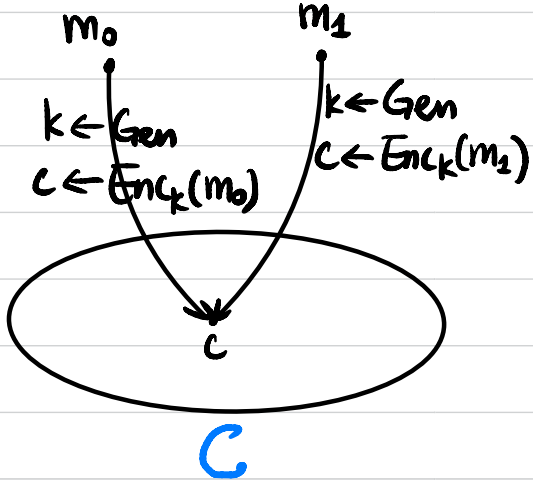
Def 2 A symmetric-key encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secure if

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

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

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

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 $\Pi = (Gen, Enc, Dec)$ is secure under Def 1, then Π is also secure under Def 2.

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

$$\Pr[Enc_K(m_0) = c] = \Pr[C = c \mid M = m_0]$$

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

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

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

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

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

Def 1 $\Leftrightarrow$ Def 2

"$\Leftarrow$": If $\Pi = (Gen, Enc, Dec)$ 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 $Pr[C=c] > 0$:

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

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

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

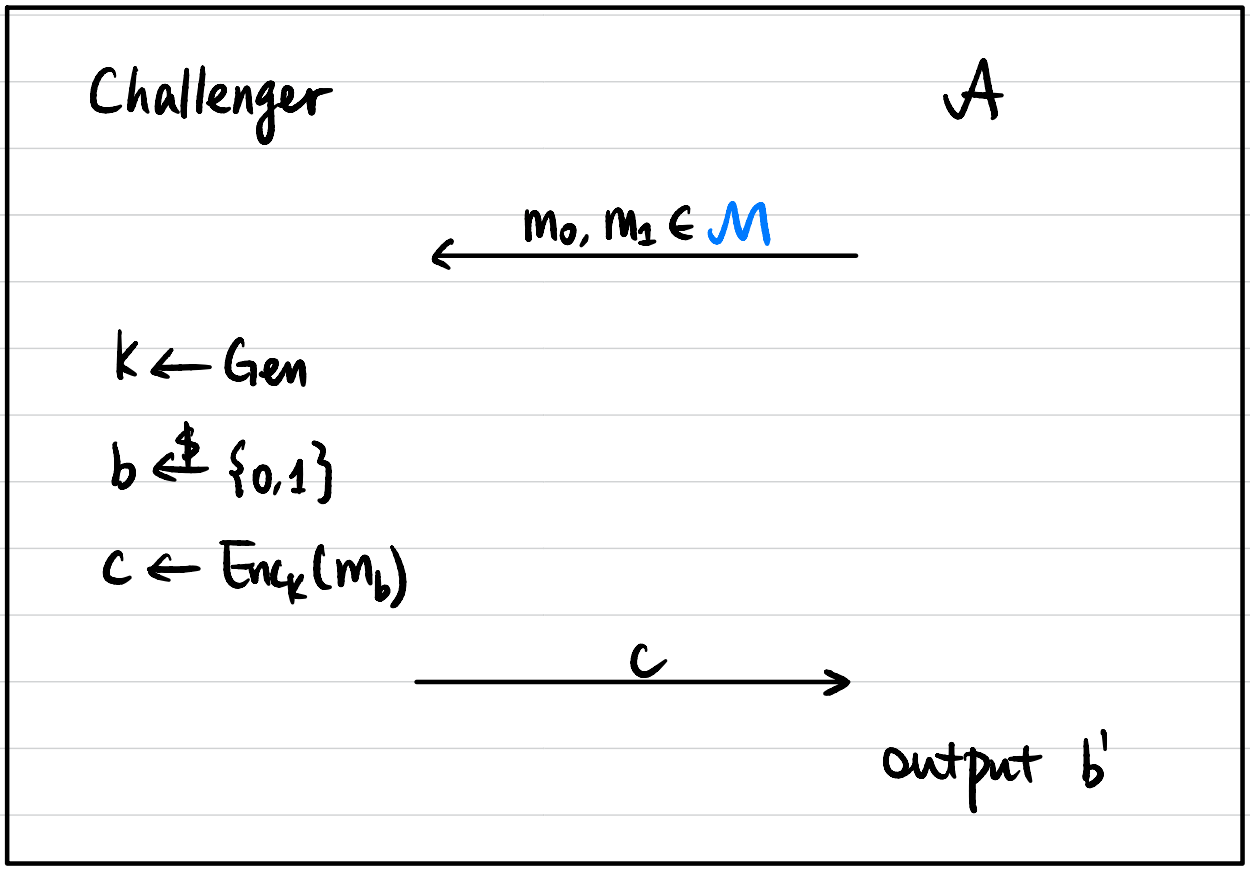
$$\overset{(Def\,2)}{=} \frac{Pr[M=m] \cdot Pr[C=c \mid M=m]}{\sum_{m' \in \mathcal{M}} Pr[M=m'] \cdot Pr[C=c \mid M=m]}$$

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

Perfect Security

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

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



One-Time Pad (OTP)

Fix an integer $\ell > 0$.

$K, M, C = \{0,1\}^\ell$ 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? $\text{Dec}_k(\text{Enc}_k(m)) = k \oplus (k \oplus m) = 0^\ell \oplus m = m$

- Security? $\forall\, m_0, m_1 \in M,\ \forall\, c \in C$: $k = m_0 \oplus c$

$$\Pr[\text{Enc}_K(m_0) = c] = \Pr[C = c \mid M = m_0] = \Pr[K = m_0 \oplus c] = \frac{1}{2^\ell}$$

$$\Pr[\text{Enc}_K(m_1) = c] = \Pr[C = c \mid M = m_1] = \Pr[K = m_1 \oplus c] = \frac{1}{2^\ell}$$

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

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

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

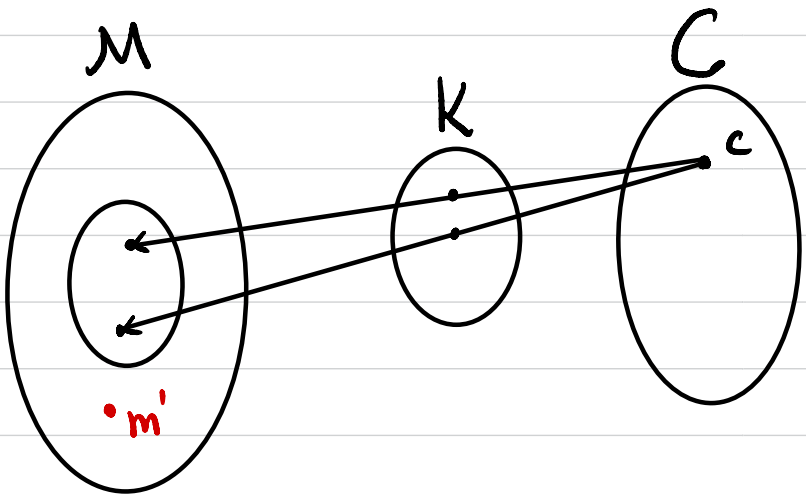
$\mathcal{M}(c) := \{m \mid m = Dec_k(c) \text{ for some } k \in K\}$.

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

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

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

↑ possible for some distribution over $\mathcal{M}$



Computational Security

Perfect Security:

① Absolutely no information is leaked

② $\mathcal{A}$ has unlimited computational power

Relaxation (Practical Purpose):

① "Tiny" information can be leaked

② $\mathcal{A}$ has limited computational power

How to formalize?