Cryptography

Lecture 2

Arkady Yerukhimovich

August 28, 2024

Outline

1. Lecture 1 Review
2. Probability Review (Ch. A.3)
3. Perfectly-Secure Encryption (Ch. 2.1)
4. The One-Time Pad (Ch. 2.2)

Lecture 1 Review

- Syllabus review
- Defining Secure Encryption

Outline

Definitions

Let E_1 and E_2 be events: (e.g., a coin toss comes up HEADS)

Definitions

Let E_1 and E_2 be events: (e.g., a coin toss comes up HEADS)

- $\overline{E}$, $\neg E$ is complement of E (i.e., not E)

$$\Pr[E] = 1 - \Pr[\overline{E}]$$

Definitions

Let E_1 and E_2 be events: (e.g., a coin toss comes up HEADS)

- $\overline{E}$, $\neg E$ is complement of E (i.e., not E)

$$\Pr[E] = 1 - \Pr[\overline{E}]$$

- $E_1 \wedge E_2$ is conjunction (AND) of two events (i.e., they both occur)

$$\Pr[E_1 \wedge E_2] \leq \Pr[E_1]$$

Definitions

Let E_1 and E_2 be events: (e.g., a coin toss comes up HEADS)

- $\overline{E}$, $\neg E$ is complement of E (i.e., not E)

$$\Pr[E] = 1 - \Pr[\overline{E}]$$

- $E_1 \wedge E_2$ is conjunction (AND) of two events (i.e., they both occur)

$$\Pr[E_1 \wedge E_2] \leq \Pr[E_1]$$

- $E_1 \vee E_2$ is disjunction (OR) of two events (i.e., at least one occurs)

$$\Pr[E_1 \vee E_2] \geq \Pr[E_1]$$

Definitions

Let E_1 and E_2 be events: (e.g., a coin toss comes up HEADS)

- $\overline{E}$, $\neg E$ is complement of E (i.e., not E)

$$\Pr[E] = 1 - \Pr[\overline{E}]$$

- $E_1 \wedge E_2$ is conjunction (AND) of two events (i.e., they both occur)

$$\Pr[E_1 \wedge E_2] \leq \Pr[E_1]$$

- $E_1 \vee E_2$ is disjunction (OR) of two events (i.e., at least one occurs)

$$\Pr[E_1 \vee E_2] \geq \Pr[E_1]$$

Definition

E_1 and E_2 are *independent* if $\Pr[E_1 \wedge E_2] = \Pr[E_1] \cdot \Pr[E_2]$

Some Useful Definitions and Facts

- Conditional Probability of E_1 given E_2:

$$\Pr[E_1 \mid E_2] = \frac{\Pr[E_1 \wedge E_2]}{\Pr[E_2]}$$

Some Useful Definitions and Facts

- Conditional Probability of E_1 given E_2:

$$\Pr[E_1 \mid E_2] = \frac{\Pr[E_1 \wedge E_2]}{\Pr[E_2]}$$

- Bayes' Theorem:

$$\text{If } \Pr[E_2] \neq 0, \text{ then } \Pr[E_1 \mid E_2] = \frac{\Pr[E_2 \mid E_1] \cdot \Pr[E_1]}{\Pr[E_2]}$$

Some Useful Definitions and Facts

- Conditional Probability of E_1 given E_2:

$$\Pr[E_1 \mid E_2] = \frac{\Pr[E_1 \wedge E_2]}{\Pr[E_2]}$$

- Bayes' Theorem:

$$\text{If } \Pr[E_2] \neq 0, \text{ then } \Pr[E_1 \mid E_2] = \frac{\Pr[E_2 \mid E_1] \cdot \Pr[E_1]}{\Pr[E_2]}$$

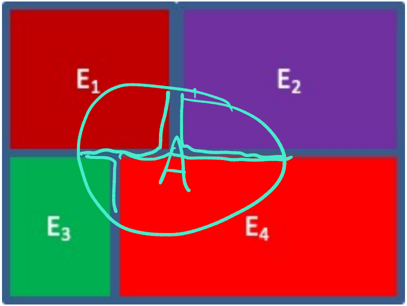
- Proof:
  By definition of conditional probability,
  $\Pr[E_1 \mid E_2] \cdot \Pr[E_2] = \Pr[E_1 \wedge E_2] = \Pr[E_2 \mid E_1] \cdot \Pr[E_1]$.
  So, $\Pr[E_1 \mid E_2] = \frac{\Pr[E_2|E_1] \cdot \Pr[E_1]}{\Pr[E_2]}$

Some Useful Definitions and Facts

- Law of Total Probability: If $E_1, E_2, \ldots, E_n$ are a partition (non-overlapping) of all possibilities. Then, for any event A,

$$\Pr[A] = \sum_{i=1}^{n} \Pr[A \wedge E_i] = \sum_{i=1}^{n} \Pr[A \mid E_i] \cdot \Pr[E_i]$$

- Proof Sketch:

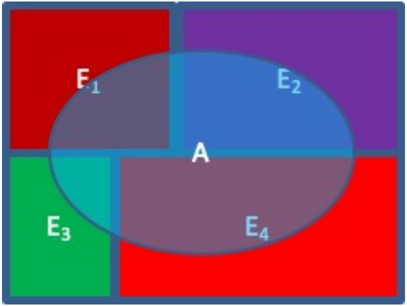


Some Useful Definitions and Facts

- Law of Total Probability: If $E_1, E_2, \ldots, E_n$ are a partition (non-overlapping) of all possibilities. Then, for any event A,

$$\Pr[A] = \sum_{i=1}^{n} \Pr[A \wedge E_i] = \sum_{i=1}^{n} \Pr[A \mid E_i] \cdot \Pr[E_i]$$

- Proof Sketch:



Some Useful Definitions and Facts

- Union Bound:

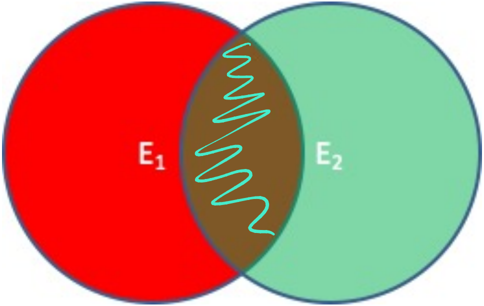
$$\Pr[E_1 \vee E_2] \leq \Pr[E_1] + \Pr[E_2]$$

Some Useful Definitions and Facts

- Union Bound:

$$\Pr[E_1 \vee E_2] \leq \Pr[E_1] + \Pr[E_2]$$

- Proof Sketch:



Outline

Private-key encryption

Eve

Alice

c

Bob

Key k
Message m
Encrypt m: $c = \mathrm{Enc}_k(m)$

Key k
Receive ciphertext c
Decrypt c: $m = \mathrm{Dec}_k(c)$

Security

Eve gets to observe c, but can not learn m

Defining Encryption Security

Security Guarantee

What is a successful attack?

- $\mathcal{A}$ learns the key k
- $\mathcal{A}$ learns the message m
- $\mathcal{A}$ learns any character of m
- Semantic security: Regardless of what $\mathcal{A}$ knows about m, she learns no new information

Threat Model

What can an adversary do?

- ciphertext-only
- known-plaintext
- chosen-plaintext
- chosen-ciphertext

Defining Encryption Security

Security Guarantee

What is a successful attack?

- $\mathcal{A}$ learns the key k
- $\mathcal{A}$ learns the message m
- $\mathcal{A}$ learns any character of m
- Semantic security:
  Regardless of what $\mathcal{A}$ knows about m, she learns no new information

Threat Model

What can an adversary do?

- ciphertext-only
- known-plaintext
- chosen-plaintext
- chosen-ciphertext

Formalizing the Definition

Probability Distributions:

- Let M be a random variable denoting value of the message
  - M ranges over plaintext space $\mathcal{M}$
  - Distribution of M reflects $\mathcal{A}$'s prior knowledge of message being sent (not all messages are equally likely)

M: 000 0000000 $\underbrace{\text{random}}$ 90-bit string

Formalizing the Definition

Probability Distributions:

- Let M be a random variable denoting value of the message
  - M ranges over plaintext space $\mathcal{M}$
  - Distribution of M reflects $\underline{\mathcal{A}\text{'s prior knowledge}}$ of message being sent (not all messages are equally likely)
- Let K be a random variable denoting the key
  - K ranges over keyspace $\mathcal{K}$
  - Distribution of K is defined by Gen

Formalizing the Definition

Probability Distributions: $m \leftarrow \mathcal{M}$

- Let M be a random variable denoting value of the message
  - M ranges over plaintext space $\mathcal{M}$
  - Distribution of M reflects $\mathcal{A}$'s prior knowledge of message being sent (not all messages are equally likely)
- Let K be a random variable denoting the key
  - K ranges over keyspace $\mathcal{K}$
  - Distribution of K is defined by Gen
- Let C be a random variable (ranging over ciphertext space $\mathcal{C}$) denoting the ciphertext. It's distribution is defined by the following experiment:
  - A key k is chosen using Gen
  - A message m is chosen according to distribution over $\mathcal{M}$
  - Compute $c \leftarrow \mathsf{Enc}_k(m)$

Formalizing the Definition

Probability Distributions:

- Let M be a random variable denoting value of the message
  - M ranges over plaintext space $\mathcal{M}$
  - Distribution of M reflects $\mathcal{A}$'s prior knowledge of message being sent (not all messages are equally likely)
- Let K be a random variable denoting the key
  - K ranges over keyspace $\mathcal{K}$
  - Distribution of K is defined by Gen
- Let C be a random variable (ranging over ciphertext space $\mathcal{C}$) denoting the ciphertext. It's distribution is defined by the following experiment:
  - A key k is chosen using Gen
  - A message m is chosen according to distribution over $\mathcal{M}$
  - Compute $c \leftarrow \mathsf{Enc}_k(m)$

Remember

$\mathcal{M}$ is a space, M is a random variable, m is a value taken on by M
We will often look at $\Pr[M = m]$

Formalizing the Definition

Informal Definition

$\mathcal{A}$ knows the distribution M over $\mathcal{M}$. After seeing one ciphertext c, she should learn no additional info about m.

Formalizing the Definition

Informal Definition

$\mathcal{A}$ knows the distribution M over $\mathcal{M}$. After seeing one ciphertext c, she should learn no additional info about m.

Encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$ is *perfectly secret* if

Formalizing the Definition

Informal Definition

$\mathcal{A}$ knows the distribution M over $\mathcal{M}$. After seeing one ciphertext c, she should learn no additional info about m.

Encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$ is *perfectly secret* if

- For all distributions over $\mathcal{M}$

Formalizing the Definition

Informal Definition

$\mathcal{A}$ knows the distribution M over $\mathcal{M}$. After seeing one ciphertext c, she should learn no additional info about m.

Encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$ is *perfectly secret* if

- For all distributions over $\mathcal{M}$, for all $m \in \mathcal{M}$

Formalizing the Definition

Informal Definition

$\mathcal{A}$ knows the distribution M over $\mathcal{M}$. After seeing one ciphertext c, she should learn no additional info about m.

Encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$ is *perfectly secret* if

- For all distributions over $\mathcal{M}$, for all $m \in \mathcal{M}$, for all $c \in \mathcal{C}$ with $\Pr[C = c] > 0$

Formalizing the Definition

Informal Definition

$\mathcal{A}$ knows the distribution M over $\mathcal{M}$. After seeing one ciphertext c, she should learn no additional info about m.

Encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$ is *perfectly secret* if

- For all distributions over $\mathcal{M}$, for all $m \in \mathcal{M}$, for all $c \in \mathcal{C}$ with $\Pr[C = c] > 0$

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

00 = 1/2
01 1/2
10 0
11 0

$\mathcal{M} =$
00 $\frac{1}{7}$
01 $\frac{1}{7}$
10 1/7
11 4/7

$c = 0^*$

Formalizing the Definition

Informal Definition

$\mathcal{A}$ knows the distribution M over $\mathcal{M}$. After seeing one ciphertext c, she should learn no additional info about m.

Encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$ is *perfectly secret* if

- For all distributions over $\mathcal{M}$, for all $m \in \mathcal{M}$, for all $c \in \mathcal{C}$ with $\Pr[C = c] > 0$

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

- For all pairs $m, m' \in \mathcal{M}$, for all $c \in \mathcal{C}$

$$\Pr[\mathsf{Enc}_K(m) = c] = \Pr[\mathsf{Enc}_K(m') = c]$$

A Game-Based Definition

Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme. Consider the following game between an adversary $\mathcal{A}$ and a challenger:

A Game-Based Definition

Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme. Consider the following game between an adversary $\mathcal{A}$ and a challenger:

$\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi}$

- $\mathcal{A}$ outputs two messages $m_0, m_1 \in \mathcal{M}$, s.t. $|m_0| = |m_1|$
- The challenger chooses $k \leftarrow \mathsf{Gen}$, $b \leftarrow \{0,1\}$, computes $c \leftarrow \mathsf{Enc}_k(m_b)$ and gives c to $\mathcal{A}$
- $\mathcal{A}$ outputs a guess bit b'
- We say that $\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi} = 1$ (i.e., $\mathcal{A}$ wins) if $b' = b$.

A Game-Based Definition

Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme. Consider the following game between an adversary $\mathcal{A}$ and a challenger:

$\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi}$

- $\mathcal{A}$ outputs two messages $m_0, m_1 \in \mathcal{M}$, s.t. $|m_0| = |m_1|$
- The challenger chooses $k \leftarrow \mathsf{Gen}$, $b \leftarrow \{0,1\}$, computes $c \leftarrow \mathsf{Enc}_k(m_b)$ and gives c to $\mathcal{A}$
- $\mathcal{A}$ outputs a guess bit b'
- We say that $\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi} = 1$ (i.e., $\mathcal{A}$ wins) if $b' = b$.

Definition: An encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$ is *perfectly indistinguishable* if for all $\mathcal{A}$ it holds that

$$\Pr[\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi} = 1] = 1/2$$

A Game-Based Definition

$\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi}$

- $\mathcal{A}$ outputs two messages $m_0, m_1 \in \mathcal{M}$, s.t. $|m_0| = |m_1|$
- The challenger chooses $k \leftarrow \mathsf{Gen}$, $b \leftarrow \{0,1\}$, computes $c \leftarrow \mathsf{Enc}_k(m_b)$ and gives c to $\mathcal{A}$
- $\mathcal{A}$ outputs a guess bit b'
- We say that $\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi} = 1$ (i.e., $\mathcal{A}$ wins) if $b' = b$.

Definition: An encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$ is *perfectly indistinguishable* if for all $\mathcal{A}$ it holds that

$$\Pr[\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi} = 1] = 1/2$$

Observation

Note that $\mathcal{A}$ can win with probability $1/2$ by just guessing b' at random. This definition says that this is the best she can do.

Outline

Perfectly Secure Encryption Definition

Informal Definition

$\mathcal{A}$ knows the distribution of M over $\mathcal{M}$. After seeing one ciphertext c, she should learn no additional info about m.

Encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$ is *perfectly secret* if

- For all distributions over $\mathcal{M}$, for all $m \in \mathcal{M}$, for all $c \in \mathcal{C}$ with $\Pr[C = c] > 0$

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

The One-Time Pad

XOR

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

One-Time Pad Encryption Scheme

- Let $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^{\ell}$

The One-Time Pad

XOR

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

One-Time Pad Encryption Scheme

- Let $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^\ell$
- Gen: $k \leftarrow \mathcal{K}$

The One-Time Pad

XOR

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

One-Time Pad Encryption Scheme

- Let $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^\ell$
- Gen: $k \leftarrow \mathcal{K}$
- Enc: $c = k \oplus m$ ($\oplus$ denotes bitwise exclusive-OR)

The One-Time Pad

XOR

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

One-Time Pad Encryption Scheme

- Let $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^\ell$
- Gen: $k \leftarrow \mathcal{K}$
- Enc: $c = k \oplus m$ ($\oplus$ denotes bitwise exclusive-OR)
- Dec: $m = k \oplus c$

The One-Time Pad

XOR

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

One-Time Pad Encryption Scheme

- Let $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^\ell$
- Gen: $k \leftarrow \mathcal{K}$
- Enc: $c = k \oplus m$ ($\oplus$ denotes bitwise exclusive-OR)
- Dec: $m = k \oplus c$

Correctness: For all $k \in \mathcal{K}$ and all $m \in \mathcal{M}$,

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

The One-Time Pad

XOR

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

One-Time Pad Encryption Scheme

- Let $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^\ell$
- Gen: $k \leftarrow \mathcal{K}$
- Enc: $c = k \oplus m$ ($\oplus$ denotes bitwise exclusive-OR)
- Dec: $m = k \oplus c$

Correctness: For all $k \in \mathcal{K}$ and all $m \in \mathcal{M}$,

$$\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = k \oplus (k \oplus m) = (k \oplus k) \oplus m = 0^\ell \oplus m = m$$

The One-Time Pad

One-Time Pad Encryption Scheme

Gen: $k \leftarrow \mathcal{K}$ Enc: $c = k \oplus m$

Theorem: The OTP is perfectly secret ($\Pr[M = m \mid C = c] = \Pr[M = m]$)

One-Time Pad Encryption Scheme

Gen: $k \leftarrow \mathcal{K}$

Enc: $c = k \oplus m$

Theorem: The OTP is perfectly secret ($\Pr[M = m \mid C = c] = \Pr[M = m]$)

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

The One-Time Pad

One-Time Pad Encryption Scheme

Gen: $k \leftarrow \mathcal{K}$ Enc: $c = k \oplus m$

Theorem: The OTP is perfectly secret ($\Pr[M = m \mid C = c] = \Pr[M = m]$)

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

The One-Time Pad

One-Time Pad Encryption Scheme

Gen: $k \leftarrow \mathcal{K}$ Enc: $c = k \oplus m$

Theorem: The OTP is perfectly secret ($\Pr[M = m \mid C = c] = \Pr[M = m]$)

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

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

The One-Time Pad

One-Time Pad Encryption Scheme

Gen: $k \leftarrow \mathcal{K}$ Enc: $c = k \oplus m$

Theorem: The OTP is perfectly secret ($\Pr[M = m \mid C = c] = \Pr[M = m]$)

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

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

The One-Time Pad

One-Time Pad Encryption Scheme

Gen: $k \leftarrow \mathcal{K}$ Enc: $c = k \oplus m$

Theorem: The OTP is perfectly secret ($\Pr[M = m \mid C = c] = \Pr[M = m]$)

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

$$\Pr[C = c \mid M = m] \;=\; \Pr[\mathrm{Enc}_K(m) = c] = \Pr[m \oplus K = c]$$

The One-Time Pad

One-Time Pad Encryption Scheme

Gen: $k \leftarrow \mathcal{K}$ Enc: $c = k \oplus m$

Theorem: The OTP is perfectly secret ($\Pr[M = m \mid C = c] = \Pr[M = m]$)

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

$$\begin{aligned}\Pr[C = c \mid M = m] &= \Pr[\mathrm{Enc}_K(m) = c] = \Pr[m \oplus K = c] \\ &= \Pr[K = m \oplus c] = 2^{-\ell}\end{aligned}$$

The One-Time Pad

One-Time Pad Encryption Scheme

Gen: $k \leftarrow \mathcal{K}$ Enc: $c = k \oplus m$

Theorem: The OTP is perfectly secret ($\Pr[M = m \mid C = c] = \Pr[M = m]$)

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

$$\begin{aligned} \Pr[C = c \mid M = m] &= \Pr[\mathrm{Enc}_K(m) = c] = \Pr[m \oplus K = c] \\ &= \Pr[K = m \oplus c] = 2^{-\ell} \end{aligned}$$

$$\Pr[C = c]$$

The One-Time Pad

One-Time Pad Encryption Scheme

Gen: $k \leftarrow \mathcal{K}$ Enc: $c = k \oplus m$

Theorem: The OTP is perfectly secret ($\Pr[M = m \mid C = c] = \Pr[M = m]$)

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

$$\begin{aligned}
\Pr[C = c \mid M = m] &= \Pr[\mathsf{Enc}_K(m) = c] = \Pr[m \oplus K = c] \\
&= \Pr[K = m \oplus c] = 2^{-\ell} \\
\Pr[C = c] &= \sum_{m' \in \mathcal{M}} \Pr[C = c \mid M = m'] \cdot \Pr[M = m']
\end{aligned}$$

The One-Time Pad

One-Time Pad Encryption Scheme

Gen: $k \leftarrow \mathcal{K}$ Enc: $c = k \oplus m$

Theorem: The OTP is perfectly secret ($\Pr[M = m \mid C = c] = \Pr[M = m]$)

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

$$\begin{aligned}
\Pr[C = c \mid M = m] &= \Pr[\mathrm{Enc}_K(m) = c] = \Pr[m \oplus K = c] \\
&= \Pr[K = m \oplus c] = 2^{-\ell} \\
\Pr[C = c] &= \sum_{m' \in \mathcal{M}} \Pr[C = c \mid M = m'] \cdot \Pr[M = m'] \\
&= 2^{-\ell} \cdot \sum_{m' \in \mathcal{M}} \Pr[M = m']
\end{aligned}$$

The One-Time Pad

One-Time Pad Encryption Scheme

Gen: $k \leftarrow \mathcal{K}$ Enc: $c = k \oplus m$

Theorem: The OTP is perfectly secret ($\Pr[M = m \mid C = c] = \Pr[M = m]$)

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

$$\begin{aligned}
\Pr[C = c \mid M = m] &= \Pr[\mathsf{Enc}_K(m) = c] = \Pr[m \oplus K = c] \\
&= \Pr[K = m \oplus c] = 2^{-\ell} \\
\Pr[C = c] &= \sum_{m' \in \mathcal{M}} \Pr[C = c \mid M = m'] \cdot \Pr[M = m'] \\
&= 2^{-\ell} \cdot \sum_{m' \in \mathcal{M}} \Pr[M = m'] = 2^{-\ell}
\end{aligned}$$

The One-Time Pad

One-Time Pad Encryption Scheme

Gen: $k \leftarrow \mathcal{K}$ Enc: $c = k \oplus m$

Theorem: The OTP is perfectly secret $(\Pr[M = m \mid C = c] = \Pr[M = m])$

$$\begin{aligned}
\Pr[M = m \mid C = c] &= \frac{\Pr[C = c \mid M = m] \cdot \Pr[M = m]}{\Pr[C = c]} \\
&= \frac{2^{-\ell} \cdot \Pr[M = m]}{2^{-\ell}} \\
\Pr[C = c \mid M = m] &= \Pr[\mathsf{Enc}_K(m) = c] = \Pr[m \oplus K = c] \\
&= \Pr[K = m \oplus c] = 2^{-\ell} \\
\Pr[C = c] &= \sum_{m' \in \mathcal{M}} \Pr[C = c \mid M = m'] \cdot \Pr[M = m'] \\
&= 2^{-\ell} \cdot \sum_{m' \in \mathcal{M}} \Pr[M = m'] = 2^{-\ell}
\end{aligned}$$

The One-Time Pad

One-Time Pad Encryption Scheme

Gen: $k \leftarrow \mathcal{K}$ Enc: $c = k \oplus m$

Theorem: The OTP is perfectly secret ($\Pr[M = m \mid C = c] = \Pr[M = m]$)

$$
\begin{aligned}
\Pr[M = m \mid C = c] &= \frac{\Pr[C = c \mid M = m] \cdot \Pr[M = m]}{\Pr[C = c]} \\
&= \frac{2^{-\ell} \cdot \Pr[M = m]}{2^{-\ell}} = \Pr[M = m] \\
\Pr[C = c \mid M = m] &= \Pr[\mathsf{Enc}_K(m) = c] = \Pr[m \oplus K = c] \\
&= \Pr[K = m \oplus c] = 2^{-\ell} \\
\Pr[C = c] &= \sum_{m' \in \mathcal{M}} \Pr[C = c \mid M = m'] \cdot \Pr[M = m'] \\
&= 2^{-\ell} \cdot \sum_{m' \in \mathcal{M}} \Pr[M = m'] = 2^{-\ell}
\end{aligned}
$$

Limitations of the One-Time Pad

The one-time pad has some critical limitations that make it not ideal for real-world use.

- Can only use a key k to encrypt at most one message

Limitations of the One-Time Pad

The one-time pad has some critical limitations that make it not ideal for real-world use.

- Can only use a key k to encrypt at most one message
- Need the length of the key to be as long as the message (i.e., $|k| \geq |m|$)

Limitations of the One-Time Pad

The one-time pad has some critical limitations that make it not ideal for real-world use.

- Can only use a key k to encrypt at most one message
- Need the length of the key to be as long as the message (i.e., $|k| \geq |m|$)

Why?