CIS 5560

Cryptography
Lecture 2

Course website:

pratyushmishra.com/classes/cis-5560-s25/

Slides adapted from Dan Boneh and Vinod Vaikuntanathan

Announcements

- **HW 0 will be released tomorrow Wed Jan 22**
    - **Due Friday Jan 31** at 5PM on Gradescope
    - Recap on probability and mathematical background
    - Get started ASAP and make use of office hours!
    - Will have Homework “party” Wednesdays 4:30-6PM
- Course website is up!

Recap

An important property of XOR

Thm: Y is an RV over $\{0,1\}^n$, X is a uniform ind. RV over $\{0,1\}^n$

Then $Z := Y \oplus X$ is uniform var. on $\{0,1\}^n$

Proof: (for n=1)

Pr[Z=0] = $Pr[(x,y)=(0,0) \text{ or } (x,y)=(1,1)] =$

$= Pr[(x,y)=(0,0)] + Pr[(x,y)=(1,1)] =$

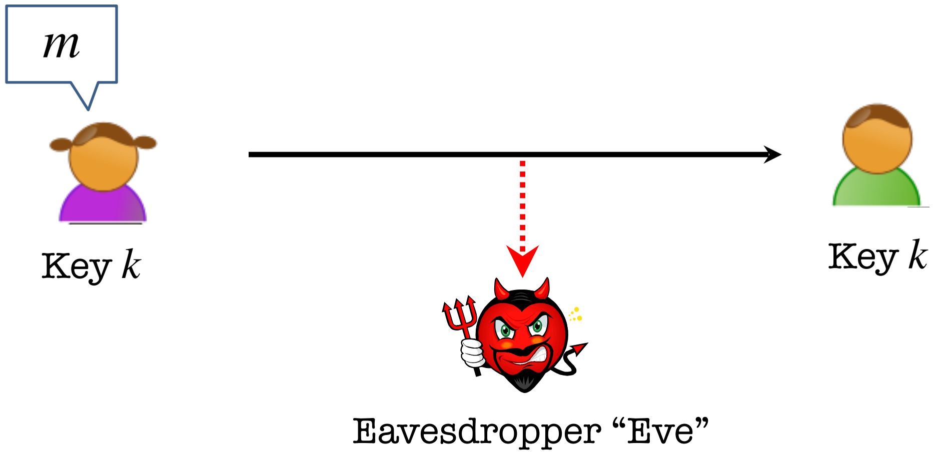
$= \frac{P_0}{2} + \frac{P_1}{2} = \frac{1}{2}$

Y	Pr
0	P_0
1	P_1

X	Pr
0	1/2
1	1/2

X	Y	Pr
0	0	$P_0/2$ ⇐
0	1	$P_1/2$
1	0	$P_0/2$
1	1	$P_1/2$ ⇐

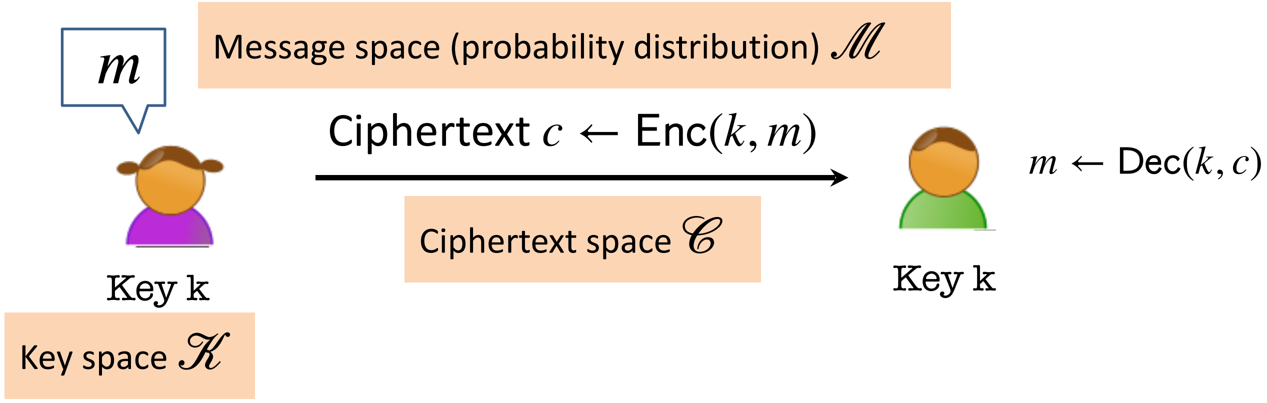
Secure Communication



Alice wants to send a message m to Bob without revealing it to Eve.

Key Notion: Secret-key Encryption

(or Symmetric-key Encryption)



Three (possibly randomized) polynomial-time algorithms:

- **Key Generation Algorithm:** Gen$(1^k) \rightarrow k$
- **Encryption Algorithm:** Enc$(k, m) \rightarrow c$
- **Decryption Algorithm:** Dec$(k, c) \rightarrow m$

What is a secure encryption scheme?

Attacker's abilities: **CT only attack** (for now)

Possible security requirements:

attempt #1: **attacker cannot recover secret key**

$\text{Enc}(k, m) = m$ would be secure

attempt #2: **attacker cannot recover all of plaintext**

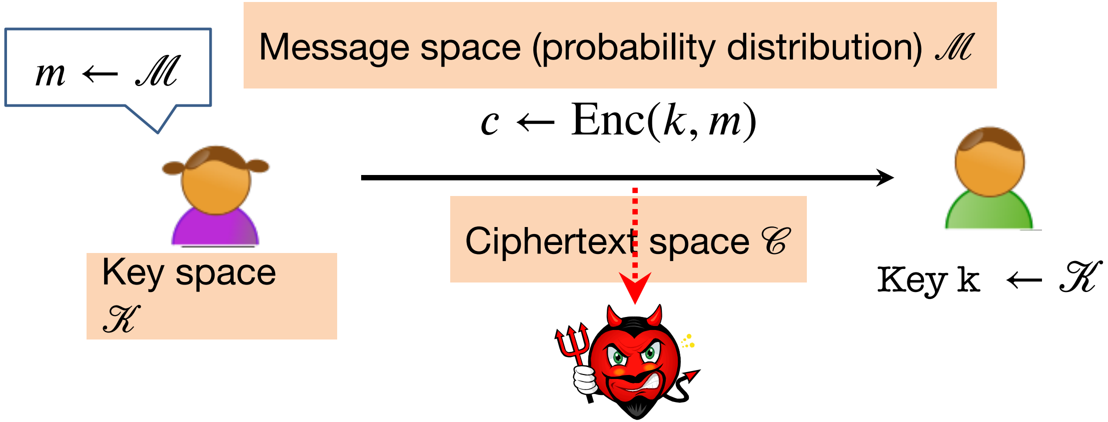
$\text{Enc}(k, (m_1, m_2)) = \text{Enc}(k, m_1) \mid\mid m_2$ would be secure

Shannon's idea: **CT should reveal no "info" about PT**

Today

- First reasonable definition of secure encryption
- First construction of “perfectly” secure encryption
- Downsides of perfect secrecy

Shannon's Perfect Secrecy Definition



What Eve knows after looking at c

=

What Eve knew before looking at c

$\forall m \in \mathscr{M}, \forall c \in \mathscr{C}, M$ is adversary's guess

$$\Pr[M = m \,|\, \text{Enc}(\mathscr{K}, m) = c] = \Pr[M = m]$$

after   before

Probability that c encrypts the particular message m

Shannon's Perfect Secrecy Definition

What Eve knows after looking at c

=

What Eve knew before looking at c

$\forall m \in \mathcal{M}, \forall c \in \mathcal{C}, M$ is adversary's guess

$$\Pr[M = m \,|\, \text{Enc}(\mathcal{K}, m) = c] = \Pr[M = m]$$

after before

✓ **CT reveals no info about PT**

But this def is difficult to work with:

How to prove that ciphertext reveals no info?

Alternate Def: Perfect Indistinguishability

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}$$
$$\Pr_{k \leftarrow \mathcal{K}}[\mathsf{Enc}(k, m) = c] = \Pr_{k \leftarrow \mathcal{K}}[\mathsf{Enc}(k, m') = c]$$

For every m, m'

Probability that c encrypts m (with random key k)

=

Probability that c encrypts m' (with diff. key k')

Hence every ciphertext is equally likely to decrypt to a given message

The Two Definitions are Equivalent

THEOREM: An encryption scheme (Gen, Enc, Dec) satisfies perfect secrecy IFF it satisfies perfect indistinguishability.

Intuition:

SEC → IND: If a ciphertext reveals no information about plaintext, it can equally likely be an encryption for m or m'

IND → SEC: If for any m, m', ciphertext is equally likely to decrypt to either m or m', then it reveals no "distinguishing" information about m or m'. Since this works for any m, m', ciphertext reveals no information about *any* message.

Perfect Secrecy is Achievable

The One-time Pad Construction:

Gen: *Choose an n-bit string k at random, i.e.* $k \leftarrow \{0,1\}^n$

Enc(k, m) *with* $\mathcal{M} = \{0,1\}^n$*: Output* $c = m \oplus k$

Dec(k, c)*: Output* $m = c \oplus k$

Perfect Secrecy is Achievable

The One-time Pad Construction:

Gen: *Choose an n-bit string k at random, i.e.* $k \leftarrow \{0,1\}^n$

Enc(k, m) *with* $\mathcal{M} = \{0,1\}^n$*: Output* $c = m \oplus k$

Dec(k, c)*: Output* $m = c \oplus k$

Correctness: $c \oplus k = m \oplus k \oplus k = m$

Perfect Secrecy is Achievable

The One-time Pad Construction:

Gen: *Choose an n-bit string k at random, i.e.* $k \leftarrow \{0,1\}^n$

Enc(k, m) *with* $\mathscr{M} = \{0,1\}^n$: *Output* $c = m \oplus k$

Dec(k, c): *Output* $m = c \oplus k$

Claim: One-time Pad achieves Perfect Indistinguishability (and therefore perfect secrecy).

Proof: For any $m, c \in \{0,1\}^n$,

$$\Pr_{k \leftarrow \mathscr{K}}[\text{Enc}(k, m) = c] = \Pr[k \oplus m = c] = \Pr[k = c \oplus m] = 1/2^n$$

Perfect Secrecy is Achievable

The One-time Pad Construction:

Gen: *Choose an n-bit string k at random, i.e.* $k \leftarrow \{0,1\}^n$

Enc(k, m) *with* $\mathscr{M} = \{0,1\}^n$: *Output* $c = m \oplus k$

Dec(k, c): *Output* $m = c \oplus k$

Claim: One-time Pad achieves Perfect Indistinguishability (and therefore perfect secrecy).

Proof: For any $m, m', c \in \{0,1\}^n$

So, $\Pr[\text{Enc}(K, m) = c] = \Pr[\text{Enc}(K, m') = c]$.

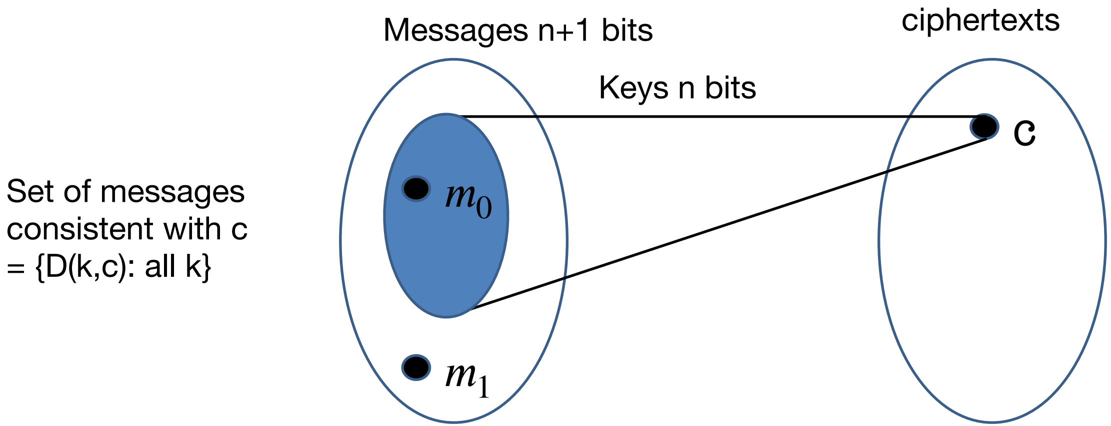
QED.

Perfect Secrecy has its Price

THEOREM: For any perfectly secure encryption scheme,

$$|\mathscr{K}| \geq |\mathscr{M}|$$

Shannon's impossibility!



Each cipher text can correspond to at most 2^n messages, but message space contains 2^{n+1} possible messages!

So it is possible (and likely!) that a given cipher text can *never* decrypt to m_1!

$$\Pr[\text{Enc}(\mathcal{K}, m_1) = c] = 0$$

Why is this bad?

- Exchanging large keys is difficult
- Need to keep large keys secure for a long time
- Generating truly random bits is kinda expensive!

So what can we do?

Let’s look at our definition in more detail…

Why Perfect Indistinguishability?

For all m_0, m_1, c: $\Pr[E(\mathscr{K}, m_0) = c] = \Pr[E(\mathscr{K}, m_1) = c]$

Why do we call it indistinguishability?

World 0:

$k \leftarrow \mathscr{K}$

$c = \text{Enc}(k, m_0)$

World 1:

$k \leftarrow \mathscr{K}$

$c = \text{Enc}(k, m_1)$

For all m_0, m_1, c : $\Pr[\text{world 0}] = \Pr[\text{world 1}]$

Ok, but why do we care? What does it matter whether we are in world 0 or world 1?

Perfect Indistinguishability from Eve's POV

Let's bring introduce Eve into this definition. Now we don't care whether or not we are in world 0 or world 1, but rather whether *Eve* can tell whether we are in world 0 or world 1

World 0:

$k \leftarrow \mathcal{K}$

$c = \mathsf{Enc}(k, m_0)$

World 1:

$k \leftarrow \mathcal{K}$

$c = \mathsf{Enc}(k, m_1)$

Eve is an **all-powerful distinguisher**.

She needs to decide whether c came from World 0 or World 1.

For every Eve and all m_0, m_1,

$$\Pr\left[\text{Eve says that we are in world 0}\right]$$

$$= \Pr\left[\text{Eve says that we are in world 1}\right]$$

Perfect Indistinguishability from Eve's POV

Let's formalize what it means for Eve to guess correctly:

World 0:

$k \leftarrow \mathcal{K}$

$c = \mathsf{Enc}(k, m_0)$

World 1:

$k \leftarrow \mathcal{K}$

$c = \mathsf{Enc}(k, m_1)$

Eve is an **all-powerful distinguisher**.

She needs to decide whether c came from World 0 or World 1.

For every Eve and all m_0, m_1,

$$\Pr\left[\mathsf{Eve}(c) = 0 \,\middle|\, \begin{array}{r} k \leftarrow \mathcal{K} \\ c = \mathsf{Enc}(k, m_0) \end{array}\right] = \Pr\left[\mathsf{Eve}(c) = 1 \,\middle|\, \begin{array}{r} k \leftarrow \mathcal{K} \\ c = \mathsf{Enc}(k, m_1) \end{array}\right]$$

Perfect Indistinguishability from Eve's POV

Equivalently,

World 0:	World 1:
$k \leftarrow \mathscr{K}$	$k \leftarrow \mathscr{K}$
$c = \mathsf{Enc}(k, m_0)$	$c = \mathsf{Enc}(k, m_1)$

Eve is an **all-powerful distinguisher**.

She needs to decide whether c came from World 0 or World

For every Eve and all m_0, m_1,

$$\left| \Pr\left[\mathsf{Eve}(c) = 0 \,\middle|\, \begin{array}{c} k \leftarrow \mathscr{K} \\ c = \mathsf{Enc}(k, m_0) \end{array} \right] - \Pr\left[\mathsf{Eve}(c) = 1 \,\middle|\, \begin{array}{c} k \leftarrow \mathscr{K} \\ c = \mathsf{Enc}(k, m_1) \end{array} \right] \right| = 0$$

Called adversary's "advantage"

Perfect Indistinguishability from Eve's POV, Take 2

We can rewrite this into an equivalent form with just one probability. Essentially, if Eve can't distinguish between either world, it means that she is right half the time, and wrong half the time.

World 0:

$k \leftarrow \mathcal{K}$

$c = \mathsf{Enc}(k, m_0)$

World 1:

$k \leftarrow \mathcal{K}$

$c = \mathsf{Enc}(k, m_1)$

Eve is an **all-powerful distinguisher**.

She needs to decide whether c came from World 0 or World 1.

For every Eve and m_0, m_1, $\Pr\left[\mathsf{Eve}(c) = b \;\middle|\; \begin{array}{r} k \leftarrow \mathcal{K} \\ b \leftarrow \{0,1\} \\ c = \mathsf{Enc}(k, m_b) \end{array}\right] = \frac{1}{2}$

So what can we do with this framing?

The Key Idea:

Computationally Bounded Adversaries

Life
The Axiom of ~~Modern Crypto~~

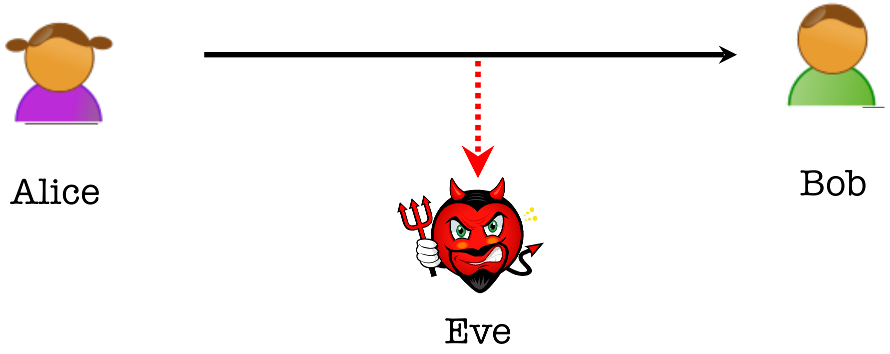
Feasible Computation = randomized polynomial-time* algorithms

(**p.p.t.** = Probabilistic polynomial-time)

(polynomial in a security parameter n)

* in recent years, quantum polynomial-time

Secure Communication



Running time of Alice and Bob?

Fixed p.p.t. (e.g., run in time $O(n^2)$)

Running time of Eve?

Arbitrary p.p.t. (e.g., run in time $O(n^2)$ or $O(n^4)$ or $O(n^{1000})$)

Computational Indistinguishability (take 1)

World 0:

$k \leftarrow \mathscr{K}$

$c = \text{Enc}(k, m_0)$

World 1:

$k \leftarrow \mathscr{K}$

$c = \text{Enc}(k, m_1)$

Eve is a **PPT distinguisher**.

She needs to decide whether c came from World 0 or World 1.

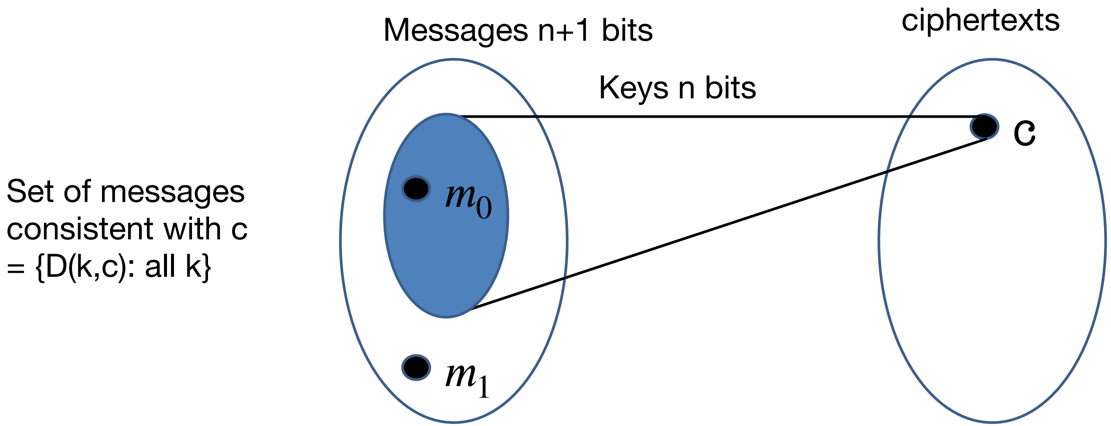
For every **PPT** Eve and m_0, m_1,

$$\left| \Pr\left[\text{Eve}(c) = 0 \,\middle|\, \begin{array}{c} k \leftarrow \mathscr{K} \\ c = \text{Enc}(k, m_0) \end{array} \right] - \Pr\left[\text{Eve}(c) = 1 \,\middle|\, \begin{array}{c} k \leftarrow \mathscr{K} \\ c = \text{Enc}(k, m_1) \end{array} \right] \right| = 0$$

Is this enough?

No!

Still subject to Shannon's impossibility!



Consider Eve that picks a random key k and

outputs 0 if $\mathrm{Dec}(k,c) = m_0$ **w.p** $\geq 1/2^n$

outputs 1 if $\mathrm{Dec}(k,c) = m_1$ **w.p = 0**

and a random bit if neither holds.

Bottomline: Pr[EVE succeeds] $\geq$ 1/2 + $1/2^n$

What do we do?

Relax guarantees further!

Computational Indistinguishability (take 2)

World 0:

$k \leftarrow \mathcal{K}$

$c = \mathsf{Enc}(k, m_0)$

World 1:

$k \leftarrow \mathcal{K}$

$c = \mathsf{Enc}(k, m_1)$

Eve is arbitrary **PPT distinguisher**.

She needs to decide whether c came from World 0 or World 1.

For every **PPT** Eve and m_0, m_1,

$$\left| \Pr\left[\mathsf{Eve}(c) = 0 \,\middle|\, \begin{array}{c} k \leftarrow \mathcal{K} \\ c = \mathsf{Enc}(k, m_0) \end{array} \right] - \Pr\left[\mathsf{Eve}(c) = 1 \,\middle|\, \begin{array}{c} k \leftarrow \mathcal{K} \\ c = \mathsf{Enc}(k, m_1) \end{array} \right] \right| = \varepsilon$$

Idea: Eve can only do ε better than random guessing.

How small should ε be?

- In practice:
  - Non-negligible (too large): $1/2^{30}$
  - Negligible: $1/2^{128}$

- In theory, we care about asymptotics:
  - Non-negligible: $\varepsilon > 1/n^2$
  - Negligible: $\varepsilon < 1/p(n)$ for every poly p

New Notion: Negligible Functions

Functions that grow slower than $1/p(n)$ for any polynomial p.

Definition: A function $\varepsilon : \mathbb{N} \to \mathbb{R}$ is **negligible** if

for every polynomial function p,

there exists an n_0 s.t.

for all $n > n_0$:

$$\varepsilon(n) < \frac{1}{p(n)}$$

Key property: Events that occur with negligible probability look ***to poly-time algorithms*** like they ***never*** occur.

Why is this the right notion?

Let Eve's ε be non-negligible $1/n^2$

(i.e. distinguishes wp $1/2 + 1/n^2$)

Eve can distinguish for $1/n^2$ fraction of keys!

Formalization: Negligible Functions

Functions that grow slower than 1/p(n) for any polynomial p.

Definition: A function $\varepsilon : \mathbb{N} \to \mathbb{R}$ is **negligible** if
for every polynomial function p,
there exists an n_0 s.t.
for all $n > n_0$:

$$\varepsilon(n) < \frac{1}{p(n)}$$

Question: Let $\varepsilon(n) = 1/n^{\log n}$. Is ε negligible?

New Notion: Negligible Functions

Functions that grow slower than 1/p(n) for any polynomial p.

Definition: A function $\varepsilon : \mathbb{N} \to \mathbb{R}$ is **negligible** if
for every polynomial function p,
there exists an n_0 s.t.
for all $n > n_0$:

$$\varepsilon(n) < \frac{1}{p(n)}$$

Security Parameter: n *(sometimes λ)*

Definition: A function $\varepsilon : \mathbb{N} \to \mathbb{R}$ is **negligible** if
for every polynomial function p,
there exists an n_0 s.t.
for all $n > n_0$:

$$\varepsilon(n) < \frac{1}{p(n)}$$

- Runtimes & success probabilities are measured as a function of n.
- ***Want***: Honest parties run in time (fixed) polynomial in $\underline{n}$.
- ***Allow***: Adversaries to run in time (arbitrary) polynomial in $\underline{n}$,
- ***Require***: adversaries to have success probability negligible in $\underline{n}$.