When is an encryption scheme secure?

We are after a **formal** definition:

If you don't understand what you want to achieve, how can you possibly know when (or if) you have achieved it?

When is an encryption scheme secure?

We are after a **formal** definition:

If you don't understand what you want to achieve, how can you possibly know when (or if) you have achieved it?

With a definition in place, we can check if a proposed scheme meets the definition...

When is an encryption scheme secure?

We are after a **formal** definition:

If you don't understand what you want to achieve, how can you possibly know when (or if) you have achieved it?

With a definition in place, we can check if a proposed scheme meets the definition...

... and provide a formal proof!

When is an encryption scheme secure?

We are after a **formal** definition:

If you don't understand what you want to achieve, how can you possibly know when (or if) you have achieved it?

With a definition in place, we can check if a proposed scheme meets the definition...

... and provide a formal proof!

On the flip side, one can conclusively show that an encryption scheme is insecure

When is an encryption scheme secure?

We are after a **formal** definition:

If you don't understand what you want to achieve, how can you possibly know when (or if) you have achieved it?

With a definition in place, we can check if a proposed scheme meets the definition...

... and provide a formal proof!

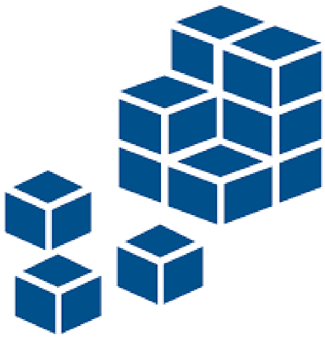
On the flip side, one can conclusively show that an encryption scheme is insecure

The historic ciphers from the previous lectures are intuitively "insecure". Can we prove that formally?

When is an encryption scheme secure?

Another benefit of formal definitions is *modularity*:

- A designer can replace an encryption scheme with another (that satisfies the same security definition)
- The security of the overall application is unaffected



When is an encryption scheme secure?

A **security definition** consists of two components:

When is an encryption scheme secure?

A **security definition** consists of two components:

- A **security guarantee**
  - What is the scheme trying to protect against?

When is an encryption scheme secure?

A **security definition** consists of two components:

- A **security guarantee**
  - What is the scheme trying to protect against?
  - From the attacker's point of view: what constitutes a successful attack?

  E.g: Should figuring out the length of the plaintext be considered a successful attack?

When is an encryption scheme secure?

A **security definition** consists of two components:

- A **security guarantee**
  - What is the scheme trying to protect against?
  - From the attacker's point of view: what constitutes a successful attack?

    E.g: Should figuring out the length of the plaintext be considered a successful attack?

- A **threat model**
  - What is the attacker allowed to do?

When is an encryption scheme secure?

A **security definition** consists of two components:

- A **security guarantee**
  - What is the scheme trying to protect against?
  - From the attacker's point of view: what constitutes a successful attack?

  E.g: Should figuring out the length of the plaintext be considered a successful attack?

- A **threat model**
  - What is the attacker allowed to do?

  E.g., can the attacker see an encrypted version of a plaintext of choice?

When is an encryption scheme secure?

A **security definition** consists of two components:

- A **security guarantee**
  - What is the scheme trying to protect against?
  - From the attacker's point of view: what constitutes a successful attack?

  E.g: Should figuring out the length of the plaintext be considered a successful attack?

- A **threat model**
  - What is the attacker allowed to do?

  E.g., can the attacker see an encrypted version of a plaintext of choice?

Threat models

One can define several different threat models depending on the environment in which the encryption scheme is going to be used

- A threat model only specifies **what** the abilities of the adversary are

- It says nothing about the *strategy* of the adversary, i.e., on **how** these abilities are used

Threat models

One can define several different threat models depending on the environment in which the encryption scheme is going to be used

- A threat model only specifies **what** the abilities of the adversary are
- It says nothing about the *strategy* of the adversary, i.e., on **how** these abilities are used

This means that an encryption scheme that is secure w.r.t. a threat model will be able to resist **all attacks** that fall within that model

Threat models

One can define several different threat models depending on the environment in which the encryption scheme is going to be used

- A threat model only specifies **what** the abilities of the adversary are
- It says nothing about the *strategy* of the adversary, i.e., on **how** these abilities are used

This means that an encryption scheme that is secure w.r.t. a threat model will be able to resist **all attacks** that fall within that model

There are several *standard* threat models:

- **Ciphertext-only attack (COA, EAV)**
- **Known-plaintext attack (KPA)**
- **Chosen-plaintext attack (CPA)**
- **Chosen-ciphertext attack (CCA)**

Threat models

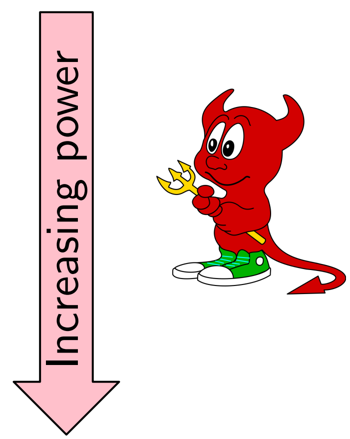
One can define several different threat models depending on the environment in which the encryption scheme is going to be used

- A threat model only specifies **what** the abilities of the adversary are
- It says nothing about the *strategy* of the adversary, i.e., on **how** these abilities are used

This means that an encryption scheme that is secure w.r.t. a threat model will be able to resist **all attacks** that fall within that model

There are several *standard* threat models:

- **Ciphertext-only attack (COA, EAV)**
- **Known-plaintext attack (KPA)**
- **Chosen-plaintext attack (CPA)**
- **Chosen-ciphertext attack (CCA)**



Threat models

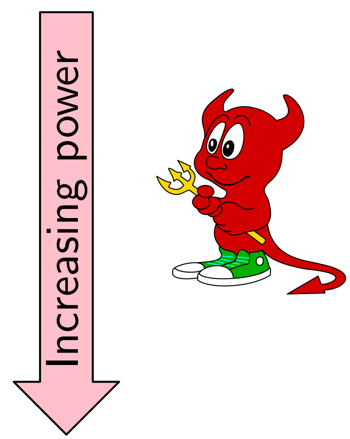
One can define several different threat models depending on the environment in which the encryption scheme is going to be used

- A threat model only specifies **what** the abilities of the adversary are
- It says nothing about the *strategy* of the adversary, i.e., on **how** these abilities are used

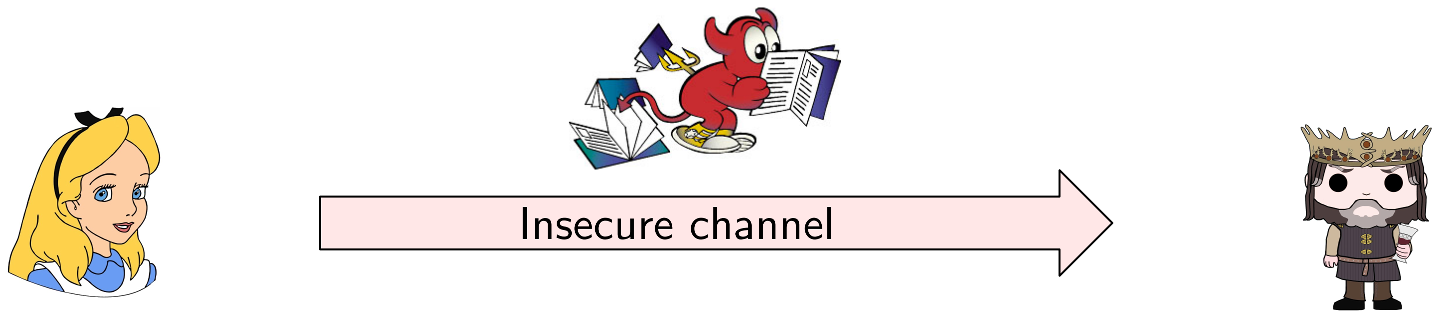
This means that an encryption scheme that is secure w.r.t. a threat model will be able to resist **all attacks** that fall within that model

There are several *standard* threat models:

- **Ciphertext-only attack (COA, EAV)**
- **Known-plaintext attack (KPA)**
- **Chosen-plaintext attack (CPA)**
- **Chosen-ciphertext attack (CCA)**



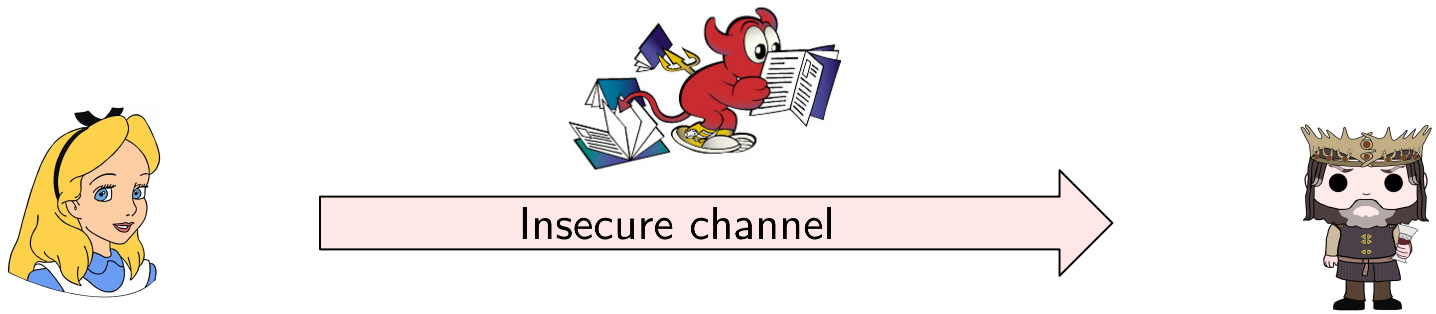
Ciphertext-only attacks



The adversary is an **eavesdropper**

- It observes a ciphertext (or multiple ciphertexts) and attempts to determine information about the underlying plaintext (or plaintexts).

Ciphertext-only attacks

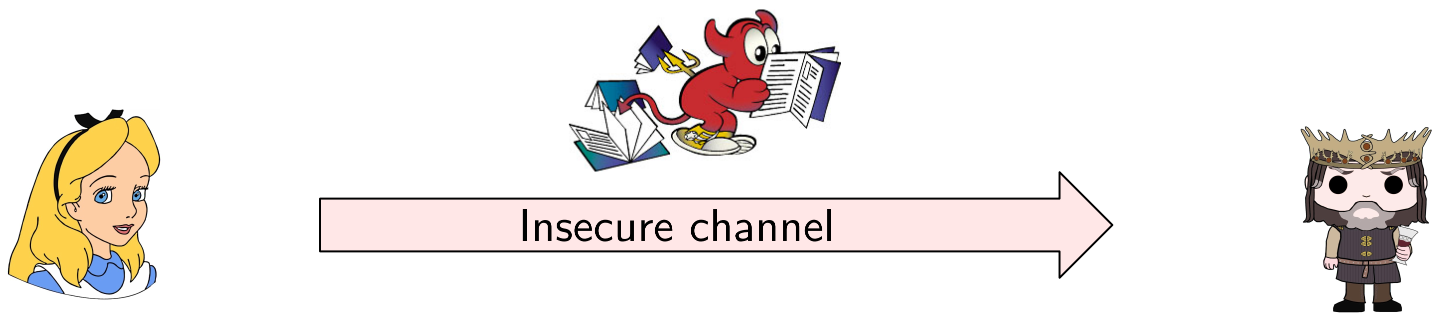


The adversary is an **eavesdropper**

- It observes a ciphertext (or multiple ciphertexts) and attempts to determine information about the underlying plaintext (or plaintexts).

Most basic type of attack (weakest threat model)

Ciphertext-only attacks



The adversary is an **eavesdropper**

- It observes a ciphertext (or multiple ciphertexts) and attempts to determine information about the underlying plaintext (or plaintexts).

Most basic type of attack (weakest threat model)

It is the attack type that we have been implicitly considering in our discussion about historic ciphers

Known-plaintext attacks

The adversary learns one or more **plaintext/ciphertext pairs (outside of the adversary's control)** generated using some key.

Known-plaintext attacks

The adversary learns one or more **plaintext/ciphertext pairs (outside of the adversary's control)** generated using some key.

The adversary wants to deduce information about the underlying plaintext of **some other ciphertext** produced using the same key

Known-plaintext attacks

The adversary learns one or more **plaintext/ciphertext pairs (outside of the adversary's control)** generated using some key.

The adversary wants to deduce information about the underlying plaintext of **some other ciphertext** produced using the same key

E.g., it is trivial to recover the key of a shift/Vigenère cipher if we know even a single plaintext-ciphertext pair (and then use the key to decrypt any other ciphertext)

Known-plaintext attacks

The adversary learns one or more **plaintext/ciphertext pairs (outside of the adversary's control)** generated using some key.

The adversary wants to deduce information about the underlying plaintext of **some other ciphertext** produced using the same key

E.g., it is trivial to recover the key of a shift/Vigenère cipher if we know even a single plaintext-ciphertext pair (and then use the key to decrypt any other ciphertext)

Is it realistic? How can the adversary learn the plaintext/ciphertext pairs?

Known-plaintext attacks

The adversary learns one or more **plaintext/ciphertext pairs (outside of the adversary's control)** generated using some key.

The adversary wants to deduce information about the underlying plaintext of **some other ciphertext** produced using the same key

E.g., it is trivial to recover the key of a shift/Vigenère cipher if we know even a single plaintext-ciphertext pair (and then use the key to decrypt any other ciphertext)

Is it realistic? How can the adversary learn the plaintext/ciphertext pairs?

- Not all encrypted messages are secret (or they are only secret for a limited amount of time)

Known-plaintext attacks

The adversary learns one or more **plaintext/ciphertext pairs (outside of the adversary's control)** generated using some key.

The adversary wants to deduce information about the underlying plaintext of **some other ciphertext** produced using the same key

E.g., it is trivial to recover the key of a shift/Vigenère cipher if we know even a single plaintext-ciphertext pair (and then use the key to decrypt any other ciphertext)

Is it realistic? How can the adversary learn the plaintext/ciphertext pairs?

- Not all encrypted messages are secret (or they are only secret for a limited amount of time)
- All "HELLO" and handshake messages of (encrypted) network protocols

Known-plaintext attacks

The adversary learns one or more **plaintext/ciphertext pairs (outside of the adversary's control)** generated using some key.

The adversary wants to deduce information about the underlying plaintext of **some other ciphertext** produced using the same key

E.g., it is trivial to recover the key of a shift/Vigenère cipher if we know even a single plaintext-ciphertext pair (and then use the key to decrypt any other ciphertext)

Is it realistic? How can the adversary learn the plaintext/ciphertext pairs?

- Not all encrypted messages are secret (or they are only secret for a limited amount of time)
- All "HELLO" and handshake messages of (encrypted) network protocols
- Embargoed documents that are published at a certain point in time (e.g., quarterly-earnings reports)

Known-plaintext attacks

The adversary learns one or more **plaintext/ciphertext pairs (outside of the adversary's control)** generated using some key.

The adversary wants to deduce information about the underlying plaintext of **some other ciphertext** produced using the same key

E.g., it is trivial to recover the key of a shift/Vigenère cipher if we know even a single plaintext-ciphertext pair (and then use the key to decrypt any other ciphertext)

Is it realistic? How can the adversary learn the plaintext/ciphertext pairs?

- Not all encrypted messages are secret (or they are only secret for a limited amount of time)
- All "HELLO" and handshake messages of (encrypted) network protocols
- Embargoed documents that are published at a certain point in time (e.g., quarterly-earnings reports)
- Most Enigma messages would start with "ANX"
  ("AN" is German for "TO" and "X" was used as a space)

Known-plaintext attacks

The adversary learns one or more **plaintext/ciphertext pairs (outside of the adversary's control)** generated using some key.

The adversary wants to deduce information about the underlying plaintext of **some other ciphertext** produced using the same key

E.g., it is trivial to recover the key of a shift/Vigenère cipher if we know even a single plaintext-ciphertext pair (and then use the key to decrypt any other ciphertext)

Is it realistic? How can the adversary learn the plaintext/ciphertext pairs?

- Not all encrypted messages are secret (or they are only secret for a limited amount of time)
- All "HELLO" and handshake messages of (encrypted) network protocols
- Embargoed documents that are published at a certain point in time (e.g., quarterly-earnings reports)
- Most Enigma messages would start with "ANX"
  ("AN" is German for "TO" and "X" was used as a space)
- Messages that were a continuation of a previous one would start with "FORT" (short for Fortsetzung)

Chosen-plaintext attack

The adversary learns the ciphertexts corresponding to one or more **plaintexts of its choice**.

Chosen-plaintext attack

The adversary learns the ciphertexts corresponding to one or more **plaintexts of its choice**.

The adversary wants to deduce information about the underlying plaintext of **some other ciphertext (outside the adversary's control)** produced using the same key

Chosen-plaintext attack

The adversary learns the ciphertexts corresponding to one or more **plaintexts of its choice**.

The adversary wants to deduce information about the underlying plaintext of **some other ciphertext (outside the adversary's control)** produced using the same key

How can the adversary learn the ciphertexts of the desired plaintexts?

Chosen-plaintext attack

The adversary learns the ciphertexts corresponding to one or more **plaintexts of its choice**.

The adversary wants to deduce information about the underlying plaintext of **some other ciphertext (outside the adversary's control)** produced using the same key

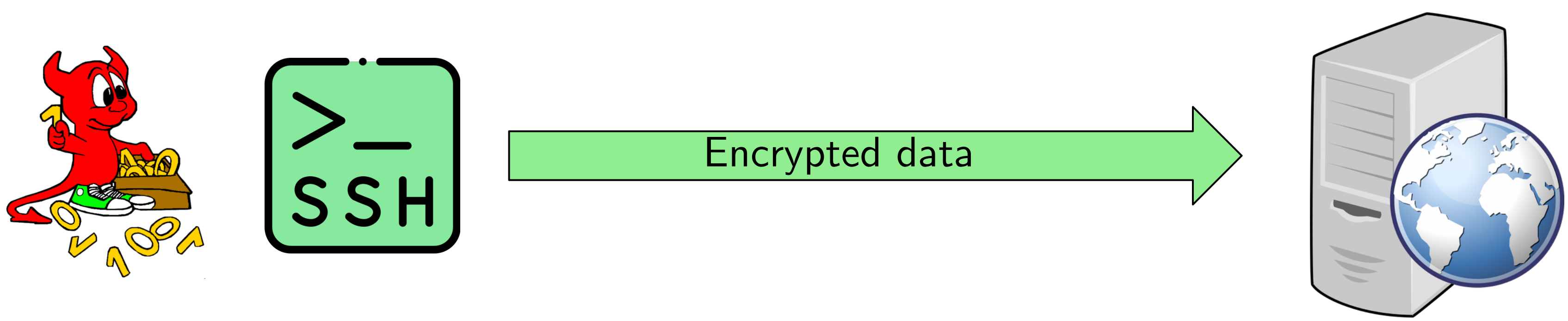
How can the adversary learn the ciphertexts of the desired plaintexts?

Chosen-plaintext attack

The adversary learns the ciphertexts corresponding to one or more **plaintexts of its choice**.

The adversary wants to deduce information about the underlying plaintext of **some other ciphertext (outside the adversary's control)** produced using the same key

How can the adversary learn the ciphertexts of the desired plaintexts?

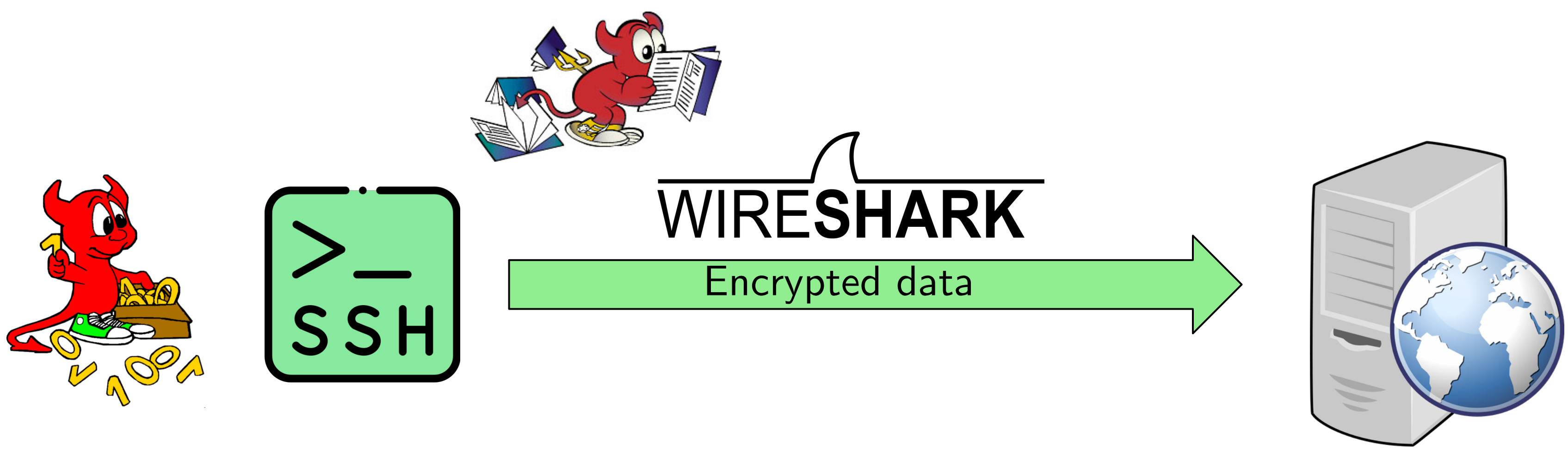


Chosen-plaintext attack

The adversary learns the ciphertexts corresponding to one or more **plaintexts of its choice**.

The adversary wants to deduce information about the underlying plaintext of **some other ciphertext (outside the adversary's control)** produced using the same key

How can the adversary learn the ciphertexts of the desired plaintexts?

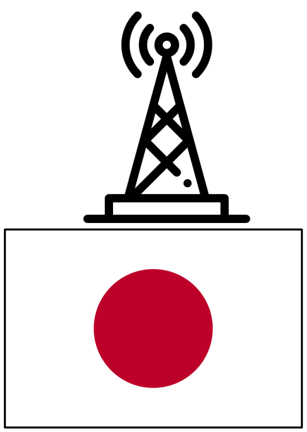


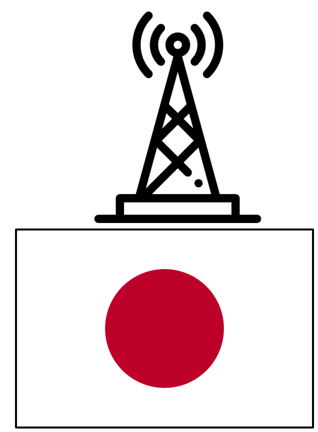
Chosen-plaintext attack

The adversary learns the ciphertexts corresponding to one or more **plaintexts of its choice**.

The adversary wants to deduce information about the underlying plaintext of **some other ciphertext (outside the adversary's control)** produced using the same key

How can the adversary learn the ciphertexts of the desired plaintexts?





Chosen-plaintext attack

The adversary learns the ciphertexts corresponding to one or more **plaintexts of its choice**.

The adversary wants to deduce information about the underlying plaintext of **some other ciphertext (outside the adversary's control)** produced using the same key

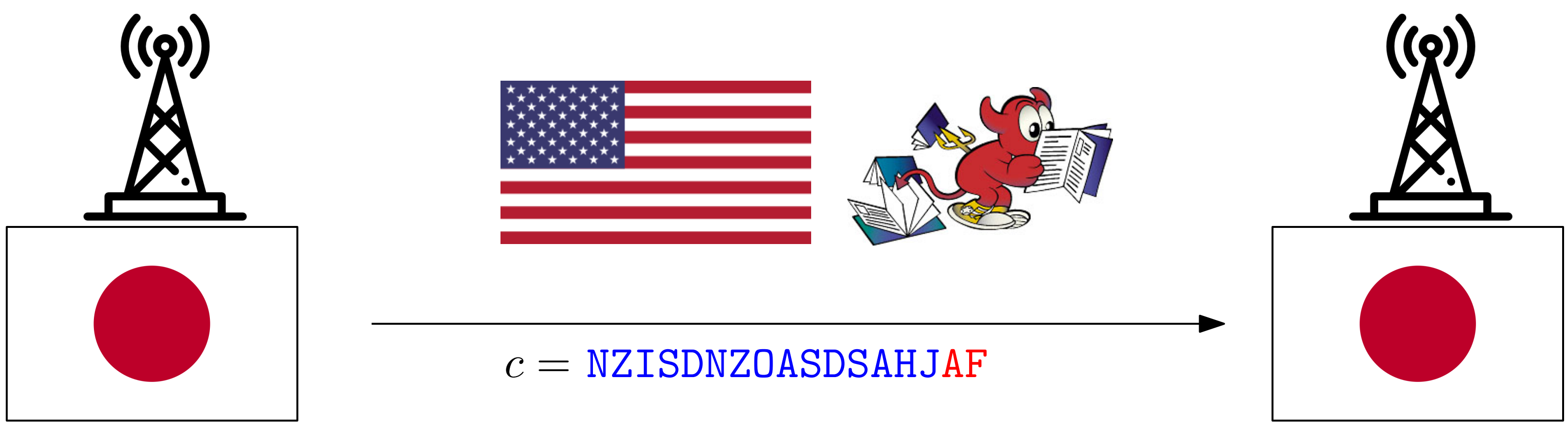
How can the adversary learn the ciphertexts of the desired plaintexts?

Chosen-plaintext attack

The adversary learns the ciphertexts corresponding to one or more **plaintexts of its choice**.

The adversary wants to deduce information about the underlying plaintext of **some other ciphertext (outside the adversary's control)** produced using the same key

How can the adversary learn the ciphertexts of the desired plaintexts?



Chosen-plaintext attack

The adversary learns the ciphertexts corresponding to one or more **plaintexts of its choice**.

The adversary wants to deduce information about the underlying plaintext of **some other ciphertext (outside the adversary's control)** produced using the same key

How can the adversary learn the ciphertexts of the desired plaintexts?

Chosen-plaintext attack

The adversary learns the ciphertexts corresponding to one or more **plaintexts of its choice**.

The adversary wants to deduce information about the underlying plaintext of **some other ciphertext (outside the adversary's control)** produced using the same key

How can the adversary learn the ciphertexts of the desired plaintexts?

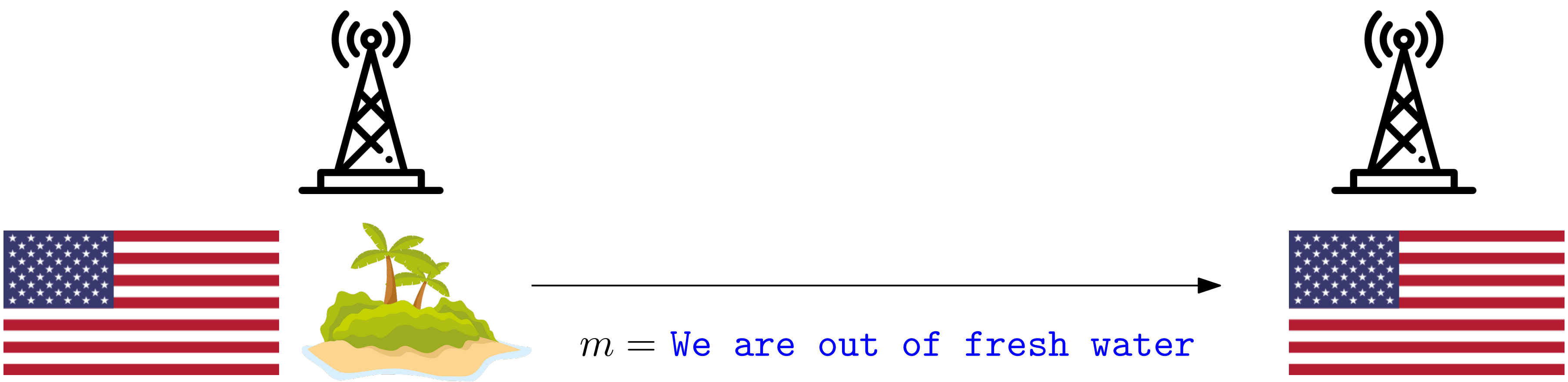
The U.S. cryptanalysts believed that AF meant Midway Island, but they were not 100% sure

Chosen-plaintext attack

The adversary learns the ciphertexts corresponding to one or more **plaintexts of its choice**.

The adversary wants to deduce information about the underlying plaintext of **some other ciphertext (outside the adversary's control)** produced using the same key

How can the adversary learn the ciphertexts of the desired plaintexts?



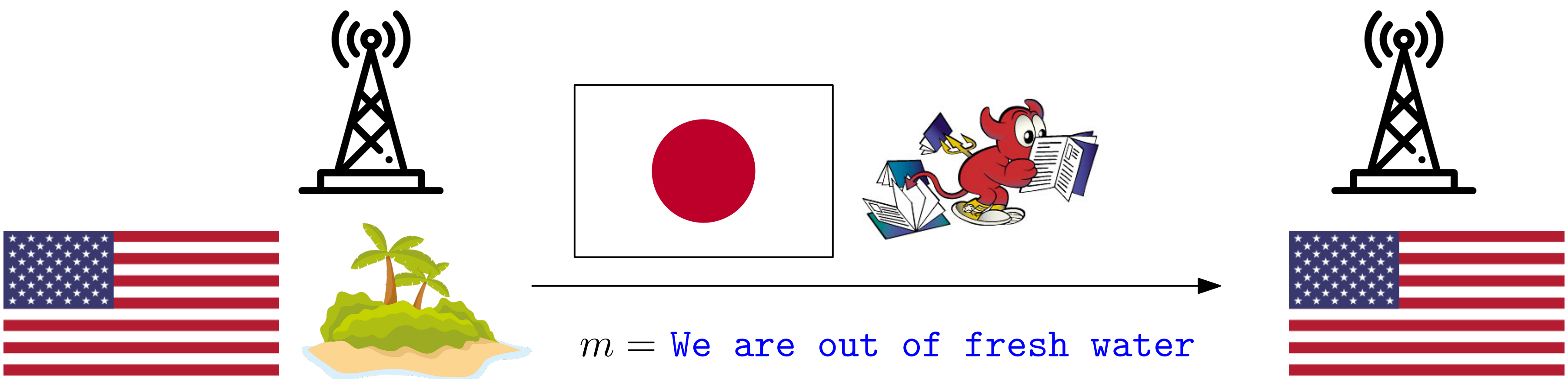
They sent a fake unencrypted message from Midway Island

Chosen-plaintext attack

The adversary learns the ciphertexts corresponding to one or more **plaintexts of its choice**.

The adversary wants to deduce information about the underlying plaintext of **some other ciphertext (outside the adversary's control)** produced using the same key

How can the adversary learn the ciphertexts of the desired plaintexts?



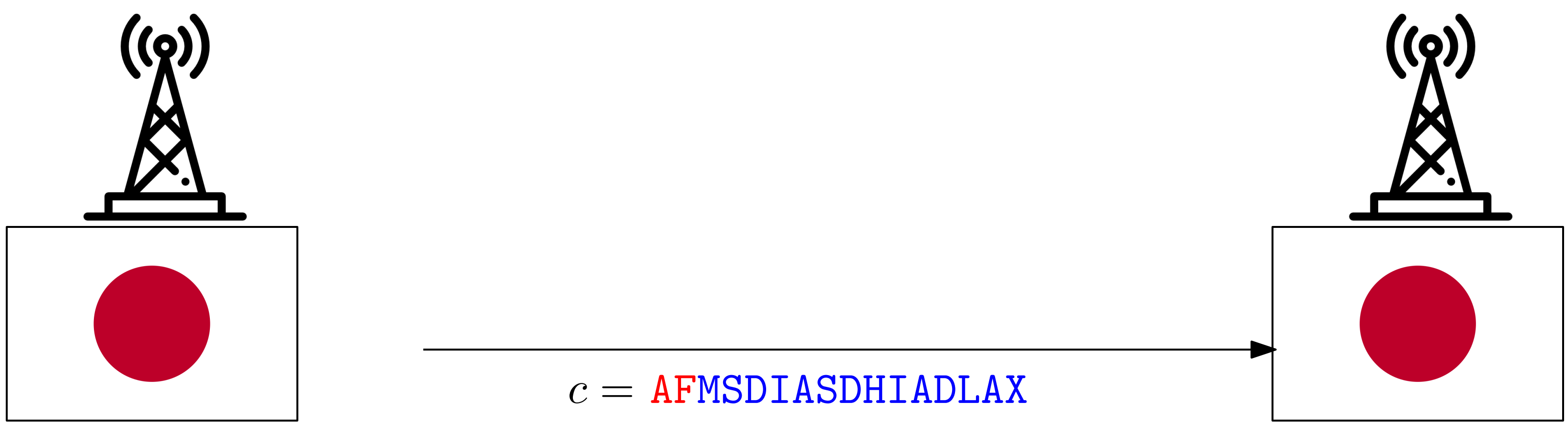
They sent a fake unencrypted message from Midway Island

Chosen-plaintext attack

The adversary learns the ciphertexts corresponding to one or more **plaintexts of its choice**.

The adversary wants to deduce information about the underlying plaintext of **some other ciphertext (outside the adversary's control)** produced using the same key

How can the adversary learn the ciphertexts of the desired plaintexts?

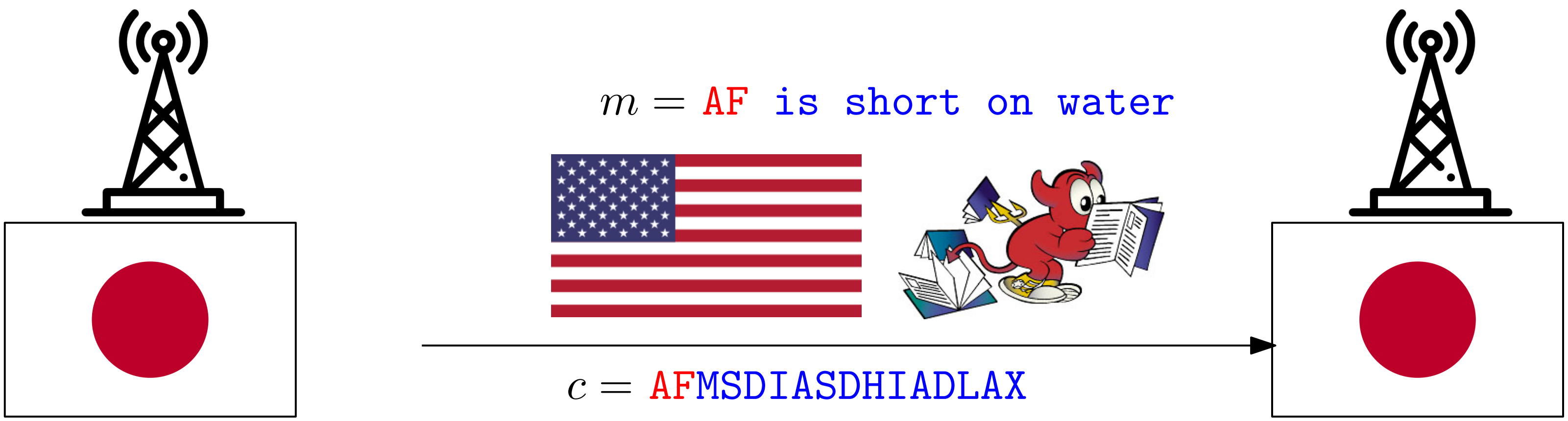


Chosen-plaintext attack

The adversary learns the ciphertexts corresponding to one or more **plaintexts of its choice**.

The adversary wants to deduce information about the underlying plaintext of **some other ciphertext (outside the adversary's control)** produced using the same key

How can the adversary learn the ciphertexts of the desired plaintexts?



Chosen-ciphertext attack

The adversary can learn the ciphertexts corresponding to one or more **plaintexts of its choice**

and

the plaintexts corresponding to one or more **ciphertexts of its choice**

Chosen-ciphertext attack

The adversary can learn the ciphertexts corresponding to one or more **plaintexts of its choice**

and

the plaintexts corresponding to one or more **ciphertexts of its choice**

The adversary wants to deduce information about the underlying plaintext of **some other ciphertext (outside its control)** produced using the same key

Chosen-ciphertext attack

The adversary can learn the ciphertexts corresponding to one or more **plaintexts of its choice**

and

the plaintexts corresponding to one or more **ciphertexts of its choice**

The adversary wants to deduce information about the underlying plaintext of **some other ciphertext (outside its control)** produced using the same key

How can the adversary learn (some information about) the plaintexts of the desired ciphertext?

Chosen-ciphertext attack

The adversary can learn the ciphertexts corresponding to one or more **plaintexts of its choice**

and

the plaintexts corresponding to one or more **ciphertexts of its choice**

The adversary wants to deduce information about the underlying plaintext of **some other ciphertext (outside its control)** produced using the same key

How can the adversary learn (some information about) the plaintexts of the desired ciphertext?

Chosen-ciphertext attack

The adversary can learn the ciphertexts corresponding to one or more **plaintexts of its choice**

and

the plaintexts corresponding to one or more **ciphertexts of its choice**

The adversary wants to deduce information about the underlying plaintext of **some other ciphertext (outside its control)** produced using the same key

How can the adversary learn (some information about) the plaintexts of the desired ciphertext?

The adversary modifies/injects traffic and observes Bob response

Chosen-ciphertext attack

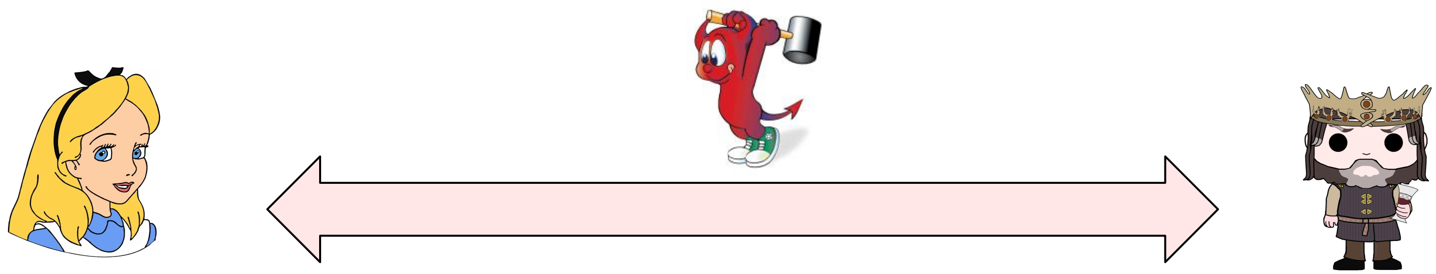
The adversary can learn the ciphertexts corresponding to one or more **plaintexts of its choice**

and

the plaintexts corresponding to one or more **ciphertexts of its choice**

The adversary wants to deduce information about the underlying plaintext of **some other ciphertext (outside its control)** produced using the same key

How can the adversary learn (some information about) the plaintexts of the desired ciphertext?



The adversary modifies/injects traffic and observes Bob response

Many protocols close a connection or request a retransmission when a bad message is received

Chosen-ciphertext attack

The adversary can learn the ciphertexts corresponding to one or more **plaintexts of its choice**

and

the plaintexts corresponding to one or more **ciphertexts of its choice**

The adversary wants to deduce information about the underlying plaintext of **some other ciphertext (outside its control)** produced using the same key

How can the adversary learn (some information about) the plaintexts of the desired ciphertext?

Being able to know whether a ciphertext is valid enables "Padding oracle" attacks:

When is an encryption scheme secure?

A **security definition** consists of two components:

- A **security guarantee**
  - What is the scheme trying to protect against?
  - From the attacker's point of view: what constitutes a successful attack?

  E.g: Should figuring out the length of the plaintext be considered a successful attack?

- A **threat model**
  - What is the attacker allowed to do?

  E.g., can the attacker see an encrypted version of a plaintext of choice?

Security guarantees

What should a secure encryption scheme guarantee?

Security guarantees

What should a secure encryption scheme guarantee?

Candidate definition 1 (inf.): *It should be impossible for an attacker to recover the key*

Security guarantees

What should a secure encryption scheme guarantee?

Candidate definition 1 (inf.): *It should be impossible for an attacker to recover the key*

Is it a "good" definition?

Security guarantees

What should a secure encryption scheme guarantee?

Candidate definition 1 (inf.): *It should be impossible for an attacker to recover the key*

Is it a "good" definition?

What about the following private-key encryption scheme?

- Gen returns a random key
- $\mathsf{Enc}_k(m) = m$
- $\mathsf{Dec}_k(c) = c$

Security guarantees

What should a secure encryption scheme guarantee?

Candidate definition 2 (inf.): *It should be impossible for an attacker to recover the plaintext from the ciphertext*

Security guarantees

What should a secure encryption scheme guarantee?

Candidate definition 2 (inf.): *It should be impossible for an attacker to recover the plaintext from the ciphertext*

Is it a "good" definition?

Security guarantees

What should a secure encryption scheme guarantee?

Candidate definition 2 (inf.): *It should be impossible for an attacker to recover the plaintext from the ciphertext*

Is it a “good” definition?

What about an encryption scheme that only changes the last character of the plaintext?

Security guarantees

What should a secure encryption scheme guarantee?

Candidate definition 3 (inf.): *It should be impossible for an attacker to recover* <u>*any character*</u> *of the plaintext from the ciphertext*

Security guarantees

What should a secure encryption scheme guarantee?

Candidate definition 3 (inf.): *It should be impossible for an attacker to recover any character of the plaintext from the ciphertext*

Is it a "good" definition?

Security guarantees

What should a secure encryption scheme guarantee?

Candidate definition 3 (inf.): *It should be impossible for an attacker to recover any character of the plaintext from the ciphertext*

Is it a "good" definition?

What about an encryption scheme where:

- $\mathcal{M} \subset \{A, \ldots, Z, -\}^*$ is the set of all "spelled-out" natural numbers, in English

  $\texttt{FORTY-TWO} \in \mathcal{M}$, $\texttt{KITTEN} \notin \mathcal{M}$

Security guarantees

What should a secure encryption scheme guarantee?

Candidate definition 3 (inf.): *It should be impossible for an attacker to recover <u>any character</u> of the plaintext from the ciphertext*

Is it a "good" definition?

What about an encryption scheme where:

- $\mathcal{M} \subset \{A, \dots, Z, -\}^*$ is the set of all "spelled-out" natural numbers, in English

  $\texttt{FORTY-TWO} \in \mathcal{M}$, $\texttt{KITTEN} \notin \mathcal{M}$

- $\mathsf{Enc}_k(m) = \begin{cases} \texttt{A} \| f_k(m) & \text{if } m \geq 100 \\ \texttt{B} \| f_k(m) & \text{if } m < 100 \end{cases}$, for some $f_k(\cdot)$?

Security guarantees

What should a secure encryption scheme guarantee?

Candidate definition 4 (inf.): *It should be impossible for an attacker to compute <u>any function</u> of the plaintext from the ciphertext*

Security guarantees

What should a secure encryption scheme guarantee?

Candidate definition 4 (inf.): *It should be impossible for an attacker to compute any function of the plaintext from the ciphertext*

Is it a "good" definition?

Security guarantees

What should a secure encryption scheme guarantee?

Candidate definition 4 (inf.): *It should be impossible for an attacker to compute any function of the plaintext from the ciphertext*

Is it a "good" definition?

What about $f(m) = |m|$?

Security guarantees

What should a secure encryption scheme guarantee?

Candidate definition 4 (inf.): *It should be impossible for an attacker to compute any function of the plaintext from the ciphertext*

Is it a "good" definition?

What about $f(m) = |m|$?

What about $f(m) = 42$?

Security guarantees

What should a secure encryption scheme guarantee?

Candidate definition 5 (inf.): *Regardless of any information an attacker already has, a ciphertext should leak* <u>*no additional information*</u> *about the underlying plaintext.*

Security guarantees

What should a secure encryption scheme guarantee?

Candidate definition 5 (inf.): *Regardless of any information an attacker already has, a ciphertext should leak <u>no additional information</u> about the underlying plaintext.*

Is it a "good" definition?

Security guarantees

What should a secure encryption scheme guarantee?

Candidate definition 5 (inf.): *Regardless of any information an attacker already has, a ciphertext should leak <u>no additional information</u> about the underlying plaintext.*

Is it a "good" definition? Maybe...

Security guarantees

What should a secure encryption scheme guarantee?

Candidate definition 5 (inf.): *Regardless of any information an attacker already has, a ciphertext should leak <u>no additional information</u> about the underlying plaintext.*

Is it a "good" definition? Maybe...

- What do we mean by information?

Security guarantees

What should a secure encryption scheme guarantee?

Candidate definition 5 (inf.): *Regardless of any information an attacker already has, a ciphertext should leak no additional information about the underlying plaintext.*

Is it a "good" definition?   Maybe...

- What do we mean by information?
- What does it mean to leak additional information?

Security guarantees

What should a secure encryption scheme guarantee?

Candidate definition 5 (inf.): *Regardless of any information an attacker already has, a ciphertext should leak no additional information about the underlying plaintext.*

Is it a "good" definition? Maybe...

- What do we mean by information?
- What does it mean to leak additional information?
- How do we capture the attacker's prior knowledge about the plaintext?

Security guarantees

What should a secure encryption scheme guarantee?

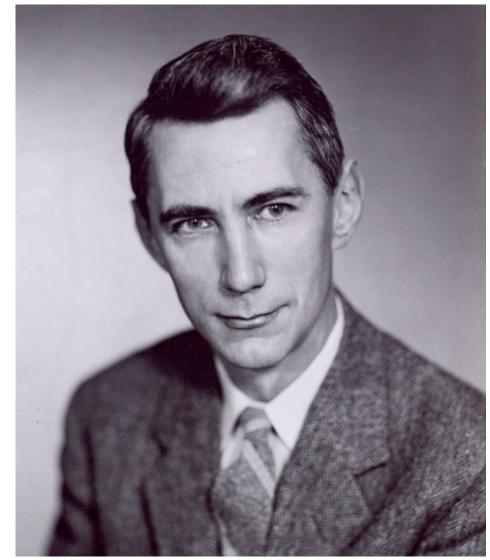
> **Candidate definition 5 (inf.):** *Regardless of any information an attacker already has, a ciphertext should leak <u>no additional information</u> about the underlying plaintext.*

Is it a "good" definition?   Maybe...

- What do we mean by information?
- What does it mean to leak <u>additional</u> information?
- How do we capture the attacker's prior knowledge about the plaintext?

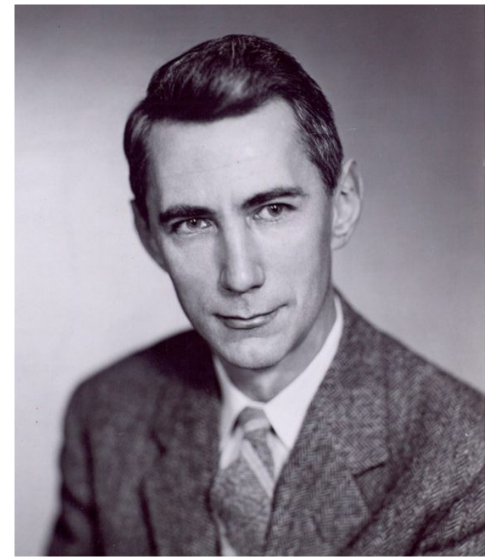
Shannon's Treatment

Messages come from a probability distribution over the message space $\mathcal{M}$



Shannon's Treatment

Messages come from a probability distribution over the message space $\mathcal{M}$

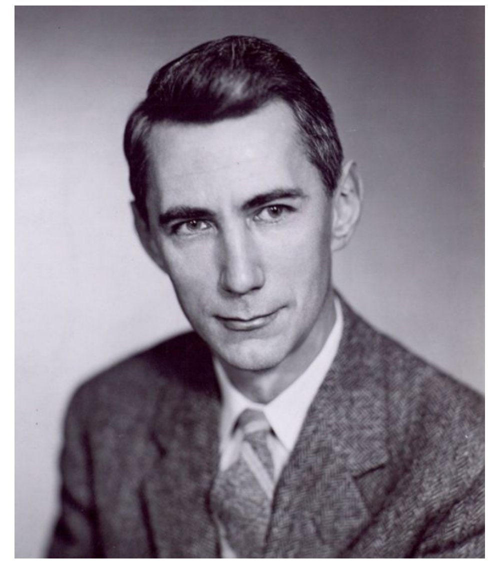


The distribution is known to the adversary and captures all the information the adversary has about the possible messages that can be sent

Shannon's Treatment

Messages come from a probability distribution over the message space $\mathcal{M}$

The distribution is known to the adversary and captures all the information the adversary has about the possible messages that can be sent

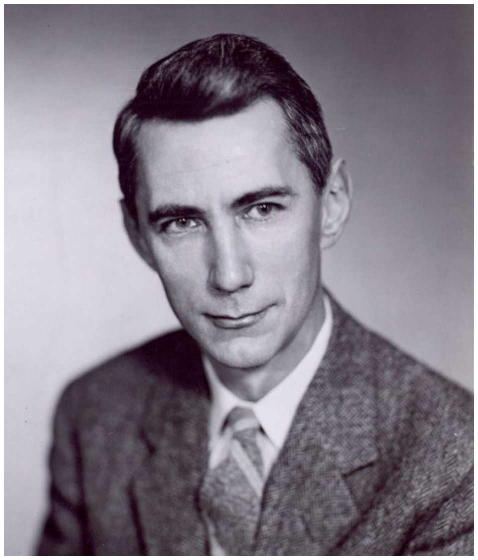


M is a random variable over $\mathcal{M}$

$\Pr[M = m]$ probability that the plaintext is m

Shannon's Treatment

Messages come from a probability distribution over the message space $\mathcal{M}$



The distribution is known to the adversary and captures all the information the adversary has about the possible messages that can be sent

M is a random variable over $\mathcal{M}$

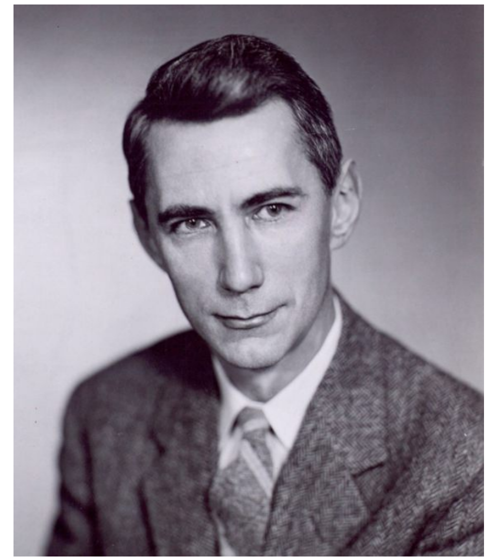
$\Pr[M = m]$ probability that the plaintext is m

K is a random variable over the key space $\mathcal{K}$ and is distributed according to the output distribution of `Gen`

Shannon's Treatment

Messages come from a probability distribution over the message space $\mathcal{M}$

The distribution is known to the adversary and captures all the information the adversary has about the possible messages that can be sent



M is a random variable over $\mathcal{M}$

$\Pr[M = m]$ probability that the plaintext is m

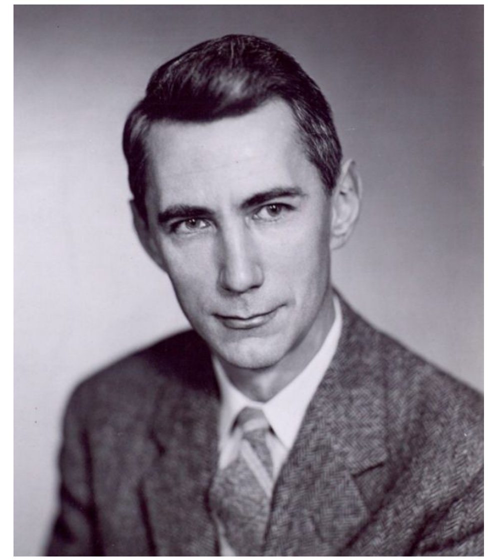
K is a random variable over the key space $\mathcal{K}$ and is distributed according to the output distribution of `Gen`

A message m and a key k are chosen *independently* from $\mathcal{M}$ and $\mathcal{K}$, respectively, and $c \leftarrow \mathsf{Enc}_k(m)$ is computed.

Shannon's Treatment

Messages come from a probability distribution over the message space $\mathcal{M}$

The distribution is known to the adversary and captures all the information the adversary has about the possible messages that can be sent



M is a random variable over $\mathcal{M}$

$\Pr[M = m]$ probability that the plaintext is m

K is a random variable over the key space $\mathcal{K}$ and is distributed according to the output distribution of `Gen`

A message m and a key k are chosen *independently* from $\mathcal{M}$ and $\mathcal{K}$, respectively, and $c \leftarrow \mathsf{Enc}_k(m)$ is computed.

C is a random variable (over $\mathcal{C}$) denoting the resulting ciphertext.

Example 0

The adversary knows that the message is going to be either `ATTACK` or `RETREAT`

Moreover, he believes that the probability of `ATTACK` is 70%

Example 0

The adversary knows that the message is going to be either `ATTACK` or `RETREAT`

Moreover, he believes that the probability of `ATTACK` is 70%

$\Pr[M = \texttt{ATTACK}] = 0.7$

$\Pr[M = \texttt{RETREAT}] = 0.3$

Example 0

The adversary knows that the message is going to be either `ATTACK` or `RETREAT`

Moreover, he believes that the probability of `ATTACK` is 70%

$\Pr[M = \texttt{ATTACK}] = 0.7$ $\qquad$ $\Pr[M = \texttt{RETREAT}] = 0.3$

a priori probability

Example 0

The adversary knows that the message is going to be either `ATTACK` or `RETREAT`

Moreover, he believes that the probability of `ATTACK` is 70%

$\Pr[M = \texttt{ATTACK}] = 0.7$ $\qquad$ $\Pr[M = \texttt{RETREAT}] = 0.3$

a priori probability

Gen outputs a binary string of length 3 chosen uniformly at random (u.a.r.):

$\Pr[K = \texttt{011}] = \frac{1}{8}$

Example 1

Consider a shift cipher:

$\mathcal{M} = \{\texttt{a}, \ldots, \texttt{z}\}^*$ $\mathcal{C} = \{\texttt{A}, \ldots, \texttt{Z}\}^*$ $\mathcal{K} = \{0, \ldots, 25\}$

Example 1

Consider a shift cipher:

$\mathcal{M} = \{\texttt{a}, \ldots, \texttt{z}\}^*$ $\qquad$ $\mathcal{C} = \{\texttt{A}, \ldots, \texttt{Z}\}^*$ $\qquad$ $\mathcal{K} = \{0, \ldots, 25\}$

Lower-case for plaintexts $\qquad$ Upper-case for ciphertexts

Example 1

Consider a shift cipher:

$\mathcal{M} = \{\mathtt{a}, \ldots, \mathtt{z}\}^*$ $\qquad$ $\mathcal{C} = \{\mathtt{A}, \ldots, \mathtt{Z}\}^*$ $\qquad$ $\mathcal{K} = \{0, \ldots, 25\}$

K is distributed uniformly over $\mathcal{K}$

Example 1

Consider a shift cipher:

$\mathcal{M} = \{\mathtt{a}, \ldots, \mathtt{z}\}^*$ $\qquad$ $\mathcal{C} = \{\mathtt{A}, \ldots, \mathtt{Z}\}^*$ $\qquad$ $\mathcal{K} = \{0, \ldots, 25\}$

K is distributed uniformly over $\mathcal{K}$

The adversary has the following a priori distribution over $\mathcal{M}$:

$\Pr[M = \mathtt{a}] = 0.7$ $\qquad$ $\Pr[M = \mathtt{b}] = 0.3$

Example 1

Consider a shift cipher:

$\mathcal{M} = \{\mathtt{a}, \ldots, \mathtt{z}\}^*$ $\qquad$ $\mathcal{C} = \{\mathtt{A}, \ldots, \mathtt{Z}\}^*$ $\qquad$ $\mathcal{K} = \{0, \ldots, 25\}$

K is distributed uniformly over $\mathcal{K}$

The adversary has the following a priori distribution over $\mathcal{M}$:

$$\Pr[M = \mathtt{a}] = 0.7 \qquad \Pr[M = \mathtt{b}] = 0.3$$

What is the probability that the ciphertext is $\mathtt{B}$?

Example 1

Consider a shift cipher:

$\mathcal{M} = \{\texttt{a}, \ldots, \texttt{z}\}^*$ $\qquad$ $\mathcal{C} = \{\texttt{A}, \ldots, \texttt{Z}\}^*$ $\qquad$ $\mathcal{K} = \{0, \ldots, 25\}$

K is distributed uniformly over $\mathcal{K}$

The adversary has the following a priori distribution over $\mathcal{M}$:

$$\Pr[M = \texttt{a}] = 0.7 \qquad \Pr[M = \texttt{b}] = 0.3$$

What is the probability that the ciphertext is B?

$\Pr[C = \texttt{B}]$

Example 1

Consider a shift cipher:

$\mathcal{M} = \{\mathtt{a}, \ldots, \mathtt{z}\}^*$ $\qquad$ $\mathcal{C} = \{\mathtt{A}, \ldots, \mathtt{Z}\}^*$ $\qquad$ $\mathcal{K} = \{0, \ldots, 25\}$

K is distributed uniformly over $\mathcal{K}$

The adversary has the following a priori distribution over $\mathcal{M}$:

$$\Pr[M = \mathtt{a}] = 0.7 \qquad \Pr[M = \mathtt{b}] = 0.3$$

What is the probability that the ciphertext is $\mathtt{B}$?

$$\Pr[C = \mathtt{B}] \quad = \sum_{m \in \mathcal{M}} \Pr[C = \mathtt{B} \wedge M = m]$$

Example 1

Consider a shift cipher:

$\mathcal{M} = \{\mathtt{a}, \ldots, \mathtt{z}\}^*$ $\qquad$ $\mathcal{C} = \{\mathtt{A}, \ldots, \mathtt{Z}\}^*$ $\qquad$ $\mathcal{K} = \{0, \ldots, 25\}$

K is distributed uniformly over $\mathcal{K}$

The adversary has the following a priori distribution over $\mathcal{M}$:

$$\Pr[M = \mathtt{a}] = 0.7 \qquad \Pr[M = \mathtt{b}] = 0.3$$

What is the probability that the ciphertext is $\mathtt{B}$?

$$\Pr[C = \mathtt{B}] \;= \sum_{m \in \mathcal{M}} \Pr[C = \mathtt{B} \wedge M = m] \;= \Pr[C = \mathtt{B} \wedge M = \mathtt{a}] + \Pr[C = \mathtt{B} \wedge M = \mathtt{b}]$$

Example 1

Consider a shift cipher:

$\mathcal{M} = \{\mathtt{a}, \ldots, \mathtt{z}\}^*$ $\qquad$ $\mathcal{C} = \{\mathtt{A}, \ldots, \mathtt{Z}\}^*$ $\qquad$ $\mathcal{K} = \{0, \ldots, 25\}$

K is distributed uniformly over $\mathcal{K}$

The adversary has the following a priori distribution over $\mathcal{M}$:

$\Pr[M = \mathtt{a}] = 0.7$ $\qquad$ $\Pr[M = \mathtt{b}] = 0.3$

What is the probability that the ciphertext is $\mathtt{B}$?

$$\begin{aligned}\Pr[C = \mathtt{B}] &= \textstyle\sum_{m \in \mathcal{M}} \Pr[C = \mathtt{B} \wedge M = m] = \Pr[C = \mathtt{B} \wedge M = \mathtt{a}] + \Pr[C = \mathtt{B} \wedge M = \mathtt{b}] \\ &= \Pr[C = \mathtt{B} \mid M = \mathtt{a}] \cdot \Pr[M = \mathtt{a}] \;+\; \Pr[C = \mathtt{B} \mid M = \mathtt{b}] \cdot \Pr[M = \mathtt{b}]\end{aligned}$$

Example 1

Consider a shift cipher:

$\mathcal{M} = \{\mathtt{a}, \ldots, \mathtt{z}\}^*$ $\qquad$ $\mathcal{C} = \{\mathtt{A}, \ldots, \mathtt{Z}\}^*$ $\qquad$ $\mathcal{K} = \{0, \ldots, 25\}$

K is distributed uniformly over $\mathcal{K}$

The adversary has the following a priori distribution over $\mathcal{M}$:

$\Pr[M = \mathtt{a}] = 0.7$ $\qquad$ $\Pr[M = \mathtt{b}] = 0.3$

What is the probability that the ciphertext is B?

$$\begin{aligned}
\Pr[C = \mathtt{B}] &= \textstyle\sum_{m \in \mathcal{M}} \Pr[C = \mathtt{B} \wedge M = m] \ = \Pr[C = \mathtt{B} \wedge M = \mathtt{a}] + \Pr[C = \mathtt{B} \wedge M = \mathtt{b}] \\
&= \Pr[C = \mathtt{B} \mid M = \mathtt{a}] \cdot \Pr[M = \mathtt{a}] \ + \ \Pr[C = \mathtt{B} \mid M = \mathtt{b}] \cdot \Pr[M = \mathtt{b}] \\
&= \Pr[K = 1] \cdot \Pr[M = \mathtt{a}] \ + \ \Pr[K = 0] \cdot \Pr[M = \mathtt{b}]
\end{aligned}$$

Example 1

Consider a shift cipher:

$\mathcal{M} = \{\mathtt{a}, \ldots, \mathtt{z}\}^*$ $\qquad$ $\mathcal{C} = \{\mathtt{A}, \ldots, \mathtt{Z}\}^*$ $\qquad$ $\mathcal{K} = \{0, \ldots, 25\}$

K is distributed uniformly over $\mathcal{K}$

The adversary has the following a priori distribution over $\mathcal{M}$:

$$\Pr[M = \mathtt{a}] = 0.7 \qquad \Pr[M = \mathtt{b}] = 0.3$$

What is the probability that the ciphertext is $\mathtt{B}$?

$$\begin{aligned}
\Pr[C = \mathtt{B}] &= \textstyle\sum_{m \in \mathcal{M}} \Pr[C = \mathtt{B} \wedge M = m] \ = \Pr[C = \mathtt{B} \wedge M = \mathtt{a}] + \Pr[C = \mathtt{B} \wedge M = \mathtt{b}] \\
&= \Pr[C = \mathtt{B} \mid M = \mathtt{a}] \cdot \Pr[M = \mathtt{a}] \ + \ \Pr[C = \mathtt{B} \mid M = \mathtt{b}] \cdot \Pr[M = \mathtt{b}] \\
&= \Pr[K = 1] \cdot \Pr[M = \mathtt{a}] \ + \ \Pr[K = 0] \cdot \Pr[M = \mathtt{b}] \ = \tfrac{1}{26} \cdot \tfrac{7}{10} \ + \ \tfrac{1}{26} \cdot \tfrac{3}{10}
\end{aligned}$$

Example 1

Consider a shift cipher:

$\mathcal{M} = \{\texttt{a}, \dots, \texttt{z}\}^*$ $\qquad$ $\mathcal{C} = \{\texttt{A}, \dots, \texttt{Z}\}^*$ $\qquad$ $\mathcal{K} = \{0, \dots, 25\}$

K is distributed uniformly over $\mathcal{K}$

The adversary has the following a priori distribution over $\mathcal{M}$:

$$\Pr[M = \texttt{a}] = 0.7 \qquad \Pr[M = \texttt{b}] = 0.3$$

What is the probability that the ciphertext is B?

$$\begin{aligned}
\Pr[C = \texttt{B}] &= \textstyle\sum_{m \in \mathcal{M}} \Pr[C = \texttt{B} \wedge M = m] \;= \Pr[C = \texttt{B} \wedge M = \texttt{a}] + \Pr[C = \texttt{B} \wedge M = \texttt{b}] \\
&= \Pr[C = \texttt{B} \mid M = \texttt{a}] \cdot \Pr[M = \texttt{a}] \;+\; \Pr[C = \texttt{B} \mid M = \texttt{b}] \cdot \Pr[M = \texttt{b}] \\
&= \Pr[K = 1] \cdot \Pr[M = \texttt{a}] \;+\; \Pr[K = 0] \cdot \Pr[M = \texttt{b}] \;= \tfrac{1}{26} \cdot \tfrac{7}{10} \;+\; \tfrac{1}{26} \cdot \tfrac{3}{10} \;= \tfrac{1}{26}
\end{aligned}$$

Example 1

Consider a shift cipher:

$\mathcal{M} = \{\mathtt{a}, \ldots, \mathtt{z}\}^*$ $\qquad$ $\mathcal{C} = \{\mathtt{A}, \ldots, \mathtt{Z}\}^*$ $\qquad$ $\mathcal{K} = \{0, \ldots, 25\}$

K is distributed uniformly over $\mathcal{K}$

The adversary has the following a priori distribution over $\mathcal{M}$:

$$\Pr[M = \mathtt{a}] = 0.7 \qquad \Pr[M = \mathtt{b}] = 0.3$$

What is the probability that the plaintext is $\mathtt{a}$ if the adversary has observed the ciphertext $\mathtt{B}$?

Example 1

Consider a shift cipher:

$\mathcal{M} = \{\mathtt{a}, \ldots, \mathtt{z}\}^*$ $\qquad$ $\mathcal{C} = \{\mathtt{A}, \ldots, \mathtt{Z}\}^*$ $\qquad$ $\mathcal{K} = \{0, \ldots, 25\}$

K is distributed uniformly over $\mathcal{K}$

The adversary has the following a priori distribution over $\mathcal{M}$:

$$\Pr[M = \mathtt{a}] = 0.7 \qquad\qquad \Pr[M = \mathtt{b}] = 0.3$$

What is the probability that the plaintext is a if the adversary has observed the ciphertext B?

$\Pr[M = \mathtt{a} \mid C = \mathtt{B}]$

Example 1

Consider a shift cipher:

$\mathcal{M} = \{\texttt{a}, \dots, \texttt{z}\}^*$ $\mathcal{C} = \{\texttt{A}, \dots, \texttt{Z}\}^*$ $\mathcal{K} = \{0, \dots, 25\}$

K is distributed uniformly over $\mathcal{K}$

The adversary has the following a priori distribution over $\mathcal{M}$:

$\Pr[M = \texttt{a}] = 0.7$ $\Pr[M = \texttt{b}] = 0.3$

What is the probability that the plaintext is a if the adversary has observed the ciphertext B?

$$\Pr[M = \texttt{a} \mid C = \texttt{B}] = \Pr[C = \texttt{B} \mid M = \texttt{a}] \cdot \frac{\Pr[M=\texttt{a}]}{\Pr[C=\texttt{B}]}$$

Example 1

Consider a shift cipher:

$\mathcal{M} = \{\texttt{a}, \ldots, \texttt{z}\}^*$ $\qquad$ $\mathcal{C} = \{\texttt{A}, \ldots, \texttt{Z}\}^*$ $\qquad$ $\mathcal{K} = \{0, \ldots, 25\}$

K is distributed uniformly over $\mathcal{K}$

The adversary has the following a priori distribution over $\mathcal{M}$:

$$\Pr[M = \texttt{a}] = 0.7 \qquad \Pr[M = \texttt{b}] = 0.3$$

What is the probability that the plaintext is a if the adversary has observed the ciphertext B?

$$\begin{aligned}\Pr[M = \texttt{a} \mid C = \texttt{B}] &= \Pr[C = \texttt{B} \mid M = \texttt{a}] \cdot \tfrac{\Pr[M=\texttt{a}]}{\Pr[C=\texttt{B}]} \\ &= \Pr[C = \texttt{B} \mid M = \texttt{a}] \cdot \tfrac{7/10}{1/26}\end{aligned}$$

Example 1

Consider a shift cipher:

$\mathcal{M} = \{\mathtt{a}, \ldots, \mathtt{z}\}^*$ $\qquad$ $\mathcal{C} = \{\mathtt{A}, \ldots, \mathtt{Z}\}^*$ $\qquad$ $\mathcal{K} = \{0, \ldots, 25\}$

K is distributed uniformly over $\mathcal{K}$

The adversary has the following a priori distribution over $\mathcal{M}$:

$$\Pr[M = \mathtt{a}] = 0.7 \qquad \Pr[M = \mathtt{b}] = 0.3$$

What is the probability that the plaintext is $\mathtt{a}$ if the adversary has observed the ciphertext $\mathtt{B}$?

$$\begin{aligned}
\Pr[M = \mathtt{a} \mid C = \mathtt{B}] &= \Pr[C = \mathtt{B} \mid M = \mathtt{a}] \cdot \tfrac{\Pr[M=\mathtt{a}]}{\Pr[C=\mathtt{B}]} \\
&= \Pr[C = \mathtt{B} \mid M = \mathtt{a}] \cdot \tfrac{7/10}{1/26} \\
&= \Pr[K = 1] \cdot \tfrac{7/10}{1/26}
\end{aligned}$$

Example 1

Consider a shift cipher:

$\mathcal{M} = \{\mathtt{a}, \ldots, \mathtt{z}\}^*$ $\qquad$ $\mathcal{C} = \{\mathtt{A}, \ldots, \mathtt{Z}\}^*$ $\qquad$ $\mathcal{K} = \{0, \ldots, 25\}$

K is distributed uniformly over $\mathcal{K}$

The adversary has the following a priori distribution over $\mathcal{M}$:

$$\Pr[M = \mathtt{a}] = 0.7 \qquad \Pr[M = \mathtt{b}] = 0.3$$

What is the probability that the plaintext is a if the adversary has observed the ciphertext B?

$$\begin{aligned}
\Pr[M = \mathtt{a} \mid C = \mathtt{B}] &= \Pr[C = \mathtt{B} \mid M = \mathtt{a}] \cdot \tfrac{\Pr[M=\mathtt{a}]}{\Pr[C=\mathtt{B}]} \\
&= \Pr[C = \mathtt{B} \mid M = \mathtt{a}] \cdot \tfrac{7/10}{1/26} \\
&= \Pr[K = 1] \cdot \tfrac{7/10}{1/26} \;\; = \tfrac{1}{26} \cdot \tfrac{7/10}{1/26}
\end{aligned}$$

Example 1

Consider a shift cipher:

$\mathcal{M} = \{\mathtt{a}, \ldots, \mathtt{z}\}^*$ $\qquad$ $\mathcal{C} = \{\mathtt{A}, \ldots, \mathtt{Z}\}^*$ $\qquad$ $\mathcal{K} = \{0, \ldots, 25\}$

K is distributed uniformly over $\mathcal{K}$

The adversary has the following a priori distribution over $\mathcal{M}$:

$$\Pr[M = \mathtt{a}] = 0.7 \qquad \Pr[M = \mathtt{b}] = 0.3$$

What is the probability that the plaintext is a if the adversary has observed the ciphertext B?

$$\begin{aligned}
\Pr[M = \mathtt{a} \mid C = \mathtt{B}] &= \Pr[C = \mathtt{B} \mid M = \mathtt{a}] \cdot \tfrac{\Pr[M=\mathtt{a}]}{\Pr[C=\mathtt{B}]} \\
&= \Pr[C = \mathtt{B} \mid M = \mathtt{a}] \cdot \tfrac{7/10}{1/26} \\
&= \Pr[K = 1] \cdot \tfrac{7/10}{1/26} = \tfrac{1}{26} \cdot \tfrac{7/10}{1/26} = \tfrac{7}{10}
\end{aligned}$$

Example 1

Consider a shift cipher:

$\mathcal{M} = \{\mathtt{a}, \ldots, \mathtt{z}\}^*$ $\qquad$ $\mathcal{C} = \{\mathtt{A}, \ldots, \mathtt{Z}\}^*$ $\qquad$ $\mathcal{K} = \{0, \ldots, 25\}$

K is distributed uniformly over $\mathcal{K}$

The adversary has the following a priori distribution over $\mathcal{M}$:

$$\Pr[M = \mathtt{a}] = 0.7 \qquad \Pr[M = \mathtt{b}] = 0.3$$

What is the probability that the plaintext is a if the adversary has observed the ciphertext B?

$$\begin{aligned}
\Pr[M = \mathtt{a} \mid C = \mathtt{B}] &= \Pr[C = \mathtt{B} \mid M = \mathtt{a}] \cdot \tfrac{\Pr[M=\mathtt{a}]}{\Pr[C=\mathtt{B}]} \\
&= \Pr[C = \mathtt{B} \mid M = \mathtt{a}] \cdot \tfrac{7/10}{1/26} \\
&= \Pr[K = 1] \cdot \tfrac{7/10}{1/26} = \tfrac{1}{26} \cdot \tfrac{7/10}{1/26} = \tfrac{7}{10}
\end{aligned}$$

a posteriori probability

Example 2

Consider a shift cipher:

$\mathcal{M} = \{\mathtt{a}, \dots, \mathtt{z}\}^*$ $\quad$ $\mathcal{C} = \{\mathtt{A}, \dots, \mathtt{Z}\}^*$ $\quad$ $\mathcal{K} = \{0, \dots, 25\}$

K is distributed uniformly over $\mathcal{K}$

The adversary has the following a priori distribution over $\mathcal{M}$:

$\Pr[M = \mathtt{kim}] = 0.5$ $\quad$ $\Pr[M = \mathtt{ann}] = 0.2$ $\quad$ $\Pr[M = \mathtt{boo}] = 0.3$

Example 2

Consider a shift cipher:

$\mathcal{M} = \{\texttt{a}, \dots, \texttt{z}\}^*$ $\qquad$ $\mathcal{C} = \{\texttt{A}, \dots, \texttt{Z}\}^*$ $\qquad$ $\mathcal{K} = \{0, \dots, 25\}$

K is distributed uniformly over $\mathcal{K}$

The adversary has the following a priori distribution over $\mathcal{M}$:

$$\Pr[M = \texttt{kim}] = 0.5 \qquad \Pr[M = \texttt{ann}] = 0.2 \qquad \Pr[M = \texttt{boo}] = 0.3$$

What is the probability that the ciphertext is DQQ?

Example 2

Consider a shift cipher:

$\mathcal{M} = \{\mathtt{a}, \dots, \mathtt{z}\}^*$ $\qquad$ $\mathcal{C} = \{\mathtt{A}, \dots, \mathtt{Z}\}^*$ $\qquad$ $\mathcal{K} = \{0, \dots, 25\}$

K is distributed uniformly over $\mathcal{K}$

The adversary has the following a priori distribution over $\mathcal{M}$:

$$\Pr[M = \mathtt{kim}] = 0.5 \qquad \Pr[M = \mathtt{ann}] = 0.2 \qquad \Pr[M = \mathtt{boo}] = 0.3$$

What is the probability that the ciphertext is DQQ?

$\Pr[C = \mathtt{DQQ}] =$

Example 2

Consider a shift cipher:

$\mathcal{M} = \{\texttt{a}, \ldots, \texttt{z}\}^*$ $\qquad$ $\mathcal{C} = \{\texttt{A}, \ldots, \texttt{Z}\}^*$ $\qquad$ $\mathcal{K} = \{0, \ldots, 25\}$

K is distributed uniformly over $\mathcal{K}$

The adversary has the following a priori distribution over $\mathcal{M}$:

$$\Pr[M = \texttt{kim}] = 0.5 \qquad \Pr[M = \texttt{ann}] = 0.2 \qquad \Pr[M = \texttt{boo}] = 0.3$$

What is the probability that the ciphertext is DQQ?

$$\begin{aligned}\Pr[C = \texttt{DQQ}] = \quad & \Pr[C = \texttt{DQQ} \mid M = \texttt{kim}] \Pr[M = \texttt{kim}] \\ & + \Pr[C = \texttt{DQQ} \mid M = \texttt{ann}] \Pr[M = \texttt{ann}] \\ & + \Pr[C = \texttt{DQQ} \mid M = \texttt{boo}] \Pr[M = \texttt{boo}]\end{aligned}$$

Example 2

Consider a shift cipher:

$\mathcal{M} = \{\texttt{a}, \ldots, \texttt{z}\}^*$ $\quad\quad$ $\mathcal{C} = \{\texttt{A}, \ldots, \texttt{Z}\}^*$ $\quad\quad$ $\mathcal{K} = \{0, \ldots, 25\}$

K is distributed uniformly over $\mathcal{K}$

The adversary has the following a priori distribution over $\mathcal{M}$:

$$\Pr[M = \texttt{kim}] = 0.5 \qquad \Pr[M = \texttt{ann}] = 0.2 \qquad \Pr[M = \texttt{boo}] = 0.3$$

What is the probability that the ciphertext is $\texttt{DQQ}$?

$$\begin{aligned}
\Pr[C = \texttt{DQQ}] = \quad & \cancel{\Pr[C = \texttt{DQQ} \mid M = \texttt{kim}] \Pr[M = \texttt{kim}]} \\
& + \Pr[C = \texttt{DQQ} \mid M = \texttt{ann}] \Pr[M = \texttt{ann}] \\
& + \Pr[C = \texttt{DQQ} \mid M = \texttt{boo}] \Pr[M = \texttt{boo}]
\end{aligned}$$

Example 2

Consider a shift cipher:

$\mathcal{M} = \{\mathtt{a}, \dots, \mathtt{z}\}^*$ $\qquad$ $\mathcal{C} = \{\mathtt{A}, \dots, \mathtt{Z}\}^*$ $\qquad$ $\mathcal{K} = \{0, \dots, 25\}$

K is distributed uniformly over $\mathcal{K}$

The adversary has the following a priori distribution over $\mathcal{M}$:

$$\Pr[M = \mathtt{kim}] = 0.5 \qquad \Pr[M = \mathtt{ann}] = 0.2 \qquad \Pr[M = \mathtt{boo}] = 0.3$$

What is the probability that the ciphertext is $\mathtt{DQQ}$?

$$\Pr[C = \mathtt{DQQ}] = \Pr[C = \mathtt{DQQ} \mid M = \mathtt{ann}] \Pr[M = \mathtt{ann}] + \Pr[C = \mathtt{DQQ} \mid M = \mathtt{boo}] \Pr[M = \mathtt{boo}]$$

Example 2

Consider a shift cipher:

$\mathcal{M} = \{\mathtt{a}, \dots, \mathtt{z}\}^*$ $\qquad$ $\mathcal{C} = \{\mathtt{A}, \dots, \mathtt{Z}\}^*$ $\qquad$ $\mathcal{K} = \{0, \dots, 25\}$

K is distributed uniformly over $\mathcal{K}$

The adversary has the following a priori distribution over $\mathcal{M}$:

$\Pr[M = \mathtt{kim}] = 0.5$ $\qquad$ $\Pr[M = \mathtt{ann}] = 0.2$ $\qquad$ $\Pr[M = \mathtt{boo}] = 0.3$

What is the probability that the ciphertext is DQQ?

$$\begin{aligned}
\Pr[C = \mathtt{DQQ}] = & \Pr[C = \mathtt{DQQ} \mid M = \mathtt{ann}] \Pr[M = \mathtt{ann}] + \Pr[C = \mathtt{DQQ} \mid M = \mathtt{boo}] \Pr[M = \mathtt{boo}] \\
= & \Pr[K = 3] \cdot 0.2 + \Pr[K = 2] \cdot 0.3
\end{aligned}$$

Example 2

Consider a shift cipher:

$\mathcal{M} = \{\texttt{a}, \ldots, \texttt{z}\}^*$ $\qquad$ $\mathcal{C} = \{\texttt{A}, \ldots, \texttt{Z}\}^*$ $\qquad$ $\mathcal{K} = \{0, \ldots, 25\}$

K is distributed uniformly over $\mathcal{K}$

The adversary has the following a priori distribution over $\mathcal{M}$:

$$\Pr[M = \texttt{kim}] = 0.5 \qquad \Pr[M = \texttt{ann}] = 0.2 \qquad \Pr[M = \texttt{boo}] = 0.3$$

What is the probability that the ciphertext is DQQ?

$$\begin{aligned}
\Pr[C = \texttt{DQQ}] &= \Pr[C = \texttt{DQQ} \mid M = \texttt{ann}] \Pr[M = \texttt{ann}] + \Pr[C = \texttt{DQQ} \mid M = \texttt{boo}] \Pr[M = \texttt{boo}] \\
&= \Pr[K = 3] \cdot 0.2 + \Pr[K = 2] \cdot 0.3 \\
&= \tfrac{1}{26} \cdot 0.2 + \tfrac{1}{26} \cdot 0.3 = \tfrac{1}{52}
\end{aligned}$$

Perfect secrecy

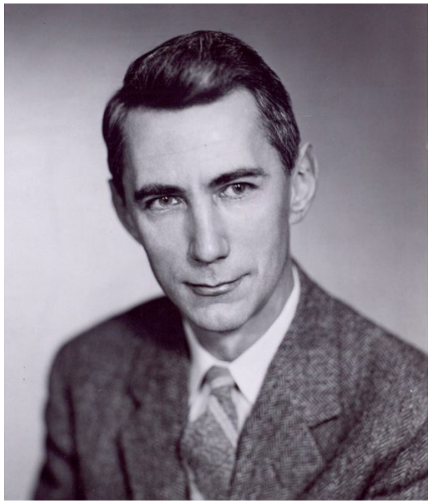
Candidate definition 5 (inf.): *Regardless of any information an attacker already has, a ciphertext should leak <u>no additional information</u> about the underlying plaintext.*

Perfect secrecy

Candidate definition 5 (inf.): *Regardless of any information an attacker already has, a ciphertext should leak* <u>*no additional information*</u> *about the underlying plaintext.*

Definition: *An encryption scheme* $(\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** *probability distribution over* $\mathcal{M}$, **every** *message* $m \in \mathcal{M}$, *and* **every** *ciphertext* $c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$:

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



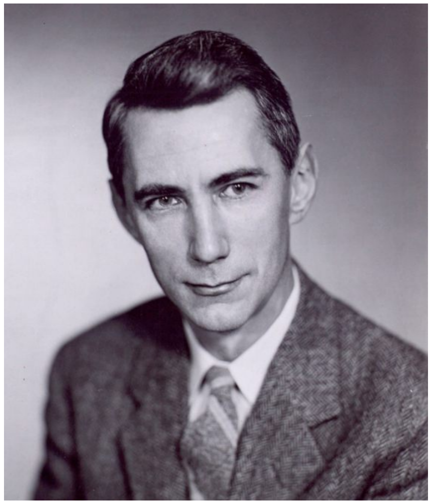
Perfect secrecy

Candidate definition 5 (inf.): *Regardless of any information an attacker already has, a ciphertext should leak* *no additional information* *about the underlying plaintext.*

Definition: *An encryption scheme* (Gen, Enc, Dec) *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** *probability distribution over* $\mathcal{M}$, **every** *message* $m \in \mathcal{M}$, *and* **every** *ciphertext* $c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$*:*

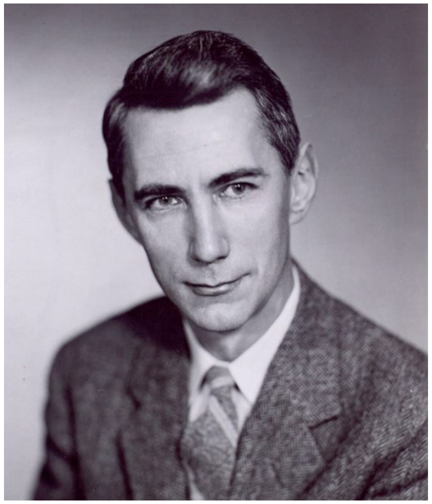
$$\Pr[M = m \mid C = c] = \Pr[M = m]$$

All the a priori information known by the adversary about the plaintexts



Perfect secrecy

Candidate definition 5 (inf.): *Regardless of any information an attacker already has, a ciphertext should leak <u>no additional information</u> about the underlying plaintext.*



Definition: *An encryption scheme* (*Gen*, *Enc*, *Dec*) *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** *probability distribution over* $\mathcal{M}$, **every** *message* $m \in \mathcal{M}$, *and* **every** *ciphertext* $c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$:

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

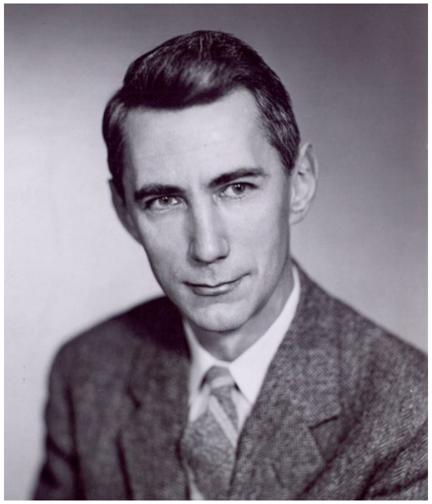
A posteriori probability

The knowledge the adversary has about m after observing c

All the a priori information known by the adversary about the plaintexts

Perfect secrecy

Candidate definition 5 (inf.): *Regardless of any information an attacker already has, a ciphertext should leak no additional information about the underlying plaintext.*



Definition: *An encryption scheme* $(\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** *probability distribution over* $\mathcal{M}$, **every** *message* $m \in \mathcal{M}$, *and* **every** *ciphertext* $c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$:

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

The adversary learns nothing **new**

Example

Are shift ciphers perfectly secret?

Our intuition says "no"... can we prove that formally?

Example

Are shift ciphers perfectly secret?

Our intuition says “no”… can we prove that formally?

- We need to prove that shift ciphers do not satisfy Shannon’s definition

Example

Are shift ciphers perfectly secret?

Our intuition says “no”… can we prove that formally?

- We need to prove that shift ciphers do not satisfy Shannon's definition
- We need to find a probability distribution over $\mathcal{M}$, a plaintext m, and a ciphertext c such that:

$$\Pr[C = c] \neq 0 \quad \text{and} \quad \Pr[M = m \mid C = c] \neq \Pr[M = m]$$

Example

Are shift ciphers perfectly secret?

Our intuition says "no"... can we prove that formally?

- We need to prove that shift ciphers do not satisfy Shannon's definition
- We need to find a probability distribution over $\mathcal{M}$, a plaintext m, and a ciphertext c such that:

$$\Pr[C = c] \neq 0 \quad \text{and} \quad \Pr[M = m \mid C = c] \neq \Pr[M = m]$$

Idea: Two occurrences of the same characters in the plaintext must produce the same characters in the ciphertext

Example

Are shift ciphers perfectly secret?

Our intuition says "no"... can we prove that formally?

- We need to prove that shift ciphers do not satisfy Shannon's definition
- We need to find a probability distribution over $\mathcal{M}$, a plaintext m, and a ciphertext c such that:

$$\Pr[C = c] \neq 0 \quad \text{and} \quad \Pr[M = m \mid C = c] \neq \Pr[M = m]$$

Probability distribution: $\Pr[M = \texttt{aa}] = \Pr[M = \texttt{ab}] = \frac{1}{2}$

Example

Are shift ciphers perfectly secret?

Our intuition says "no"... can we prove that formally?

- We need to prove that shift ciphers do not satisfy Shannon's definition
- We need to find a probability distribution over $\mathcal{M}$, a plaintext m, and a ciphertext c such that:

$$\Pr[C = c] \neq 0 \quad \text{and} \quad \Pr[M = m \mid C = c] \neq \Pr[M = m]$$

Probability distribution: $\Pr[M = \texttt{aa}] = \Pr[M = \texttt{ab}] = \frac{1}{2}$

Plaintext: $m = \texttt{ab}$

Example

Are shift ciphers perfectly secret?

Our intuition says "no"... can we prove that formally?

- We need to prove that shift ciphers do not satisfy Shannon's definition
- We need to find a probability distribution over $\mathcal{M}$, a plaintext m, and a ciphertext c such that:

$$\Pr[C = c] \neq 0 \quad \text{and} \quad \Pr[M = m \mid C = c] \neq \Pr[M = m]$$

Probability distribution: $\Pr[M = \texttt{aa}] = \Pr[M = \texttt{ab}] = \frac{1}{2}$

Plaintext: $m = \texttt{ab}$

Ciphertext: $c = \texttt{XX}$

Example

Are shift ciphers perfectly secret?

Our intuition says "no"... can we prove that formally?

- We need to prove that shift ciphers do not satisfy Shannon's definition
- We need to find a probability distribution over $\mathcal{M}$, a plaintext m, and a ciphertext c such that:

$$\Pr[C = c] \neq 0 \quad \text{and} \quad \Pr[M = m \mid C = c] \neq \Pr[M = m]$$

Probability distribution: $\Pr[M = \mathtt{aa}] = \Pr[M = \mathtt{ab}] = \frac{1}{2}$

Plaintext: $m = \mathtt{ab}$

Ciphertext: $c = \mathtt{XX}$

This is a valid choice since:

$$\begin{aligned}\Pr[C = \mathtt{XX}] &\geq \Pr[C = \mathtt{XX} \wedge M = \mathtt{aa}] \\ &= \Pr[C = \mathtt{XX} \mid M = \mathtt{aa}] \Pr[M = \mathtt{aa}] \\ &= \Pr[K = 23] \Pr[M = \mathtt{aa}] > 0\end{aligned}$$

Example

Are shift ciphers perfectly secret?

Our intuition says "no"... can we prove that formally?

- We need to prove that shift ciphers do not satisfy Shannon's definition
- We need to find a probability distribution over $\mathcal{M}$, a plaintext m, and a ciphertext c such that:

$$\Pr[C = c] \neq 0 \quad \text{and} \quad \Pr[M = m \mid C = c] \neq \Pr[M = m]$$

Probability distribution: $\Pr[M = \texttt{aa}] = \Pr[M = \texttt{ab}] = \frac{1}{2}$

Plaintext: $m = \texttt{ab}$

Ciphertext: $c = \texttt{XX}$

$$\Pr[M = \texttt{ab} \mid C = \texttt{XX}] \qquad\qquad \Pr[M = \texttt{ab}]$$

Example

Are shift ciphers perfectly secret?

Our intuition says "no"… can we prove that formally?

- We need to prove that shift ciphers do not satisfy Shannon's definition
- We need to find a probability distribution over $\mathcal{M}$, a plaintext m, and a ciphertext c such that:

$$\Pr[C = c] \neq 0 \quad \text{and} \quad \Pr[M = m \mid C = c] \neq \Pr[M = m]$$

Probability distribution: $\Pr[M = \texttt{aa}] = \Pr[M = \texttt{ab}] = \frac{1}{2}$

Plaintext: $m = \texttt{ab}$

Ciphertext: $c = \texttt{XX}$

$$\Pr[M = \texttt{ab} \mid C = \texttt{XX}] \qquad\qquad \Pr[M = \texttt{ab}] = \frac{1}{2}$$

Example

Are shift ciphers perfectly secret?

Our intuition says "no"... can we prove that formally?

- We need to prove that shift ciphers do not satisfy Shannon's definition
- We need to find a probability distribution over $\mathcal{M}$, a plaintext m, and a ciphertext c such that:

$$\Pr[C = c] \neq 0 \quad \text{and} \quad \Pr[M = m \mid C = c] \neq \Pr[M = m]$$

Probability distribution: $\Pr[M = \texttt{aa}] = \Pr[M = \texttt{ab}] = \frac{1}{2}$

Plaintext: $m = \texttt{ab}$

Ciphertext: $c = \texttt{XX}$

$$0 = \Pr[M = \texttt{ab} \mid C = \texttt{XX}] \qquad \Pr[M = \texttt{ab}] = \frac{1}{2}$$

Example

Are shift ciphers perfectly secret?

Our intuition says "no"... can we prove that formally?

- We need to prove that shift ciphers do not satisfy Shannon's definition
- We need to find a probability distribution over $\mathcal{M}$, a plaintext m, and a ciphertext c such that:

$$\Pr[C = c] \neq 0 \quad \text{and} \quad \Pr[M = m \mid C = c] \neq \Pr[M = m]$$

Probability distribution: $\Pr[M = \mathtt{aa}] = \Pr[M = \mathtt{ab}] = \frac{1}{2}$

Plaintext: $m = \mathtt{ab}$

Ciphertext: $c = \mathtt{XX}$

$$0 = \Pr[M = \mathtt{ab} \mid C = \mathtt{XX}] \quad \neq \quad \Pr[M = \mathtt{ab}] = \frac{1}{2}$$

$\square$

Another definition

What about the following definition of *perfect secrecy*?

Definition: *An encryption scheme* (Gen, Enc, Dec) *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** $m, m' \in \mathcal{M}$*, and* **every** $c \in \mathcal{C}$*:*

$$\Pr[Enc_K(m) = c] = \Pr[Enc_K(m') = c]$$

Another definition

What about the following definition of *perfect secrecy*?

> **Definition:** *An encryption scheme* $(\textit{Gen}, \textit{Enc}, \textit{Dec})$ *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** $m, m' \in \mathcal{M}$*, and* **every** $c \in \mathcal{C}$*:*
>
> $$\Pr[\textit{Enc}_K(m) = c] = \Pr[\textit{Enc}_K(m') = c]$$

Random key!

The probability is taken over the possible choices of K

Another definition

What about the following definition of *perfect secrecy*?

Definition: *An encryption scheme* $(\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** $m, m' \in \mathcal{M}$*, and* **every** $c \in \mathcal{C}$*:*

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

Random key!

The probability is taken over the possible choices of K

The above definition requires no underlying distribution over the message space $\mathcal{M}$

Another definition

What about the following definition of *perfect secrecy*?

> **Definition:** *An encryption scheme* $(\textit{Gen}, \textit{Enc}, \textit{Dec})$ *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** $m, m' \in \mathcal{M}$, *and* **every** $c \in \mathcal{C}$*:*
>
> $$\Pr[\textit{Enc}_K(m) = c] = \Pr[\textit{Enc}_K(m') = c]$$

Random key!

The probability is taken over the possible choices of K

The above definition requires no underlying distribution over the message space $\mathcal{M}$

Intuition: the distribution of the ciphertexts does not depend on the plaintext

Another definition

What about the following definition of *perfect secrecy*?

> **Definition:** *An encryption scheme* $(\textit{Gen}, \textit{Enc}, \textit{Dec})$ *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** $m, m' \in \mathcal{M}$*, and* **every** $c \in \mathcal{C}$*:*
>
> $$\Pr[\textit{Enc}_K(m) = c] = \Pr[\textit{Enc}_K(m') = c]$$

Random key!

The probability is taken over the possible choices of K

The above definition requires no underlying distribution over the message space $\mathcal{M}$

Intuition: the distribution of the ciphertexts does not depend on the plaintext

- If the distribution of the ciphertexts obtained when m is encrypted is identical to the distribution obtained when m' is encrypted, then it is impossible to tell m and m' apart when observing c

Another definition: Example

Are shift ciphers perfectly secure according to this new definition?

Another definition: Example

Are shift ciphers perfectly secure according to this new definition?

Hopefully they are not...

Another definition: Example

Are shift ciphers perfectly secure according to this new definition?

Hopefully they are not...

We would like to find two messages m, m' and a ciphertext c such that:

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

Another definition: Example

Are shift ciphers perfectly secure according to this new definition?

Hopefully they are not...

We would like to find two messages m, m' and a ciphertext c such that:

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

Choose: $m = \texttt{aa}$ $m' = \texttt{ab}$ $c = \texttt{CC}$

Another definition: Example

Are shift ciphers perfectly secure according to this new definition?

Hopefully they are not...

We would like to find two messages m, m' and a ciphertext c such that:

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

Choose: $m = \texttt{aa}$ $m' = \texttt{ab}$ $c = \texttt{CC}$

$$\Pr[\mathsf{Enc}_K(\texttt{aa}) = \texttt{CC}]$$

$$\Pr[Enc_K(\texttt{ab}) = \texttt{CC}]$$

Another definition: Example

Are shift ciphers perfectly secure according to this new definition?

Hopefully they are not...

We would like to find two messages m, m' and a ciphertext c such that:

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

Choose: $m = \mathtt{aa}$ $m' = \mathtt{ab}$ $c = \mathtt{CC}$

$$\Pr[\mathsf{Enc}_K(\mathtt{aa}) = \mathtt{CC}] = \Pr[K = 2] = \tfrac{1}{26}$$

$$\Pr[Enc_K(\mathtt{ab}) = \mathtt{CC}]$$

Another definition: Example

Are shift ciphers perfectly secure according to this new definition?

Hopefully they are not...

We would like to find two messages m, m' and a ciphertext c such that:

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

Choose: $m = \mathtt{aa}$ $m' = \mathtt{ab}$ $c = \mathtt{CC}$

$$\Pr[\mathsf{Enc}_K(\mathtt{aa}) = \mathtt{CC}] = \Pr[K = 2] = \frac{1}{26}$$

$$\Pr[Enc_K(\mathtt{ab}) = \mathtt{CC}] = 0$$

Another definition: Example

Are shift ciphers perfectly secure according to this new definition?

Hopefully they are not...

We would like to find two messages m, m' and a ciphertext c such that:

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

Choose: $m = \mathtt{aa}$ $m' = \mathtt{ab}$ $c = \mathtt{CC}$

$$\Pr[\mathsf{Enc}_K(\mathtt{aa}) = \mathtt{CC}] = \Pr[K = 2] = \frac{1}{26}$$

$$\nparallel$$

$$\Pr[Enc_K(\mathtt{ab}) = \mathtt{CC}] = 0$$

$\square$

Relating the two definitions

Definition: *An encryption scheme* $(\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** *probability distribution over* $\mathcal{M}$, **every** *message* $m \in \mathcal{M}$, *and* **every** *ciphertext* $c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$*:*

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

Definition: *An encryption scheme* $(\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** $m, m' \in \mathcal{M}$, *and* **every** $c \in \mathcal{C}$*:*

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

Relating the two definitions

Definition: *An encryption scheme* $(\textit{Gen}, \textit{Enc}, \textit{Dec})$ *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** *probability distribution over* $\mathcal{M}$*,* **every** *message* $m \in \mathcal{M}$*, and* **every** *ciphertext* $c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$*:*

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

Definition: *An encryption scheme* $(\textit{Gen}, \textit{Enc}, \textit{Dec})$ *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** $m, m' \in \mathcal{M}$*, and* **every** $c \in \mathcal{C}$*:*

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

How do the two definitions compare?

Relating the two definitions

Definition: *An encryption scheme* $(\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** *probability distribution over* $\mathcal{M}$, **every** *message* $m \in \mathcal{M}$, *and* **every** *ciphertext* $c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$*:*

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

Definition: *An encryption scheme* $(\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** $m, m' \in \mathcal{M}$, *and* **every** $c \in \mathcal{C}$*:*

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

How do the two definitions compare?

Which one is “better”?

Relating the two definitions

Definition: *An encryption scheme* $(\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** *probability distribution over* $\mathcal{M}$, **every** *message* $m \in \mathcal{M}$, *and* **every** *ciphertext* $c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$:

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

$$\Updownarrow$$

Definition: *An encryption scheme* $(\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** $m, m' \in \mathcal{M}$, *and* **every** $c \in \mathcal{C}$:

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

How do the two definitions compare?

Which one is "better"?

They are equivalent!

Proof of equivalence

$\forall$ *probability distribution over* $\mathcal{M}$, $\forall m \in \mathcal{M}, c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$:

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

$$\Downarrow$$

$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}$:

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

Proof of equivalence

$\forall$ *probability distribution over* $\mathcal{M}$*,* $\forall m \in \mathcal{M}, c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$*:*

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

$$\Downarrow$$

$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}$*:*

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

Pick the uniform distribution over $\mathcal{M}$ and any c s.t. $\Pr[C = c] \neq 0$. For an arbitrary m:

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

Proof of equivalence

$\forall$ *probability distribution over* $\mathcal{M}$*,* $\forall m \in \mathcal{M}, c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$*:*

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

$$\Downarrow$$

$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}$*:*

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

Pick the uniform distribution over $\mathcal{M}$ and any c s.t. $\Pr[C = c] \neq 0$. For an arbitrary m:

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

Proof of equivalence

$\forall$ *probability distribution over* $\mathcal{M}$*,* $\forall m \in \mathcal{M}, c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$*:*

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

$$\Downarrow$$

$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}$*:*

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

Pick the uniform distribution over $\mathcal{M}$ and any c s.t. $\Pr[C = c] \neq 0$. For an arbitrary m:

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

Proof of equivalence

> $\forall$ *probability distribution over* $\mathcal{M}$*,* $\forall m \in \mathcal{M}, c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$*:*
>
> $$\Pr[M = m \mid C = c] = \Pr[M = m]$$

$$\Downarrow$$

> $\forall m, m' \in \mathcal{M}, c \in \mathcal{C}$*:*
>
> $$\Pr[\mathit{Enc}_K(m) = c] = \Pr[\mathit{Enc}_K(m') = c]$$

Pick the uniform distribution over $\mathcal{M}$ and any c s.t. $\Pr[C = c] \neq 0$. For an arbitrary m:

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

Proof of equivalence

$\forall$ *probability distribution over* $\mathcal{M}$, $\forall m \in \mathcal{M}, c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$*:*

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

$$\Downarrow$$

$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}$*:*

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

Pick the uniform distribution over $\mathcal{M}$ and any c s.t. $\Pr[C = c] \neq 0$. For an arbitrary m:

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

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

Proof of equivalence

$\forall$ *probability distribution over* $\mathcal{M}$*,* $\forall m \in \mathcal{M}, c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$*:*

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

$$\Downarrow$$

$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}$*:*

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

Pick the uniform distribution over $\mathcal{M}$ and any c s.t. $\Pr[C = c] \neq 0$. For an arbitrary m:

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

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

This does not depend on the choice of m!

Proof of equivalence

$\forall$ *probability distribution over* $\mathcal{M}$*,* $\forall m \in \mathcal{M}, c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$*:*

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

$$\Downarrow$$

$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}$*:*

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

Pick the uniform distribution over $\mathcal{M}$ and any c s.t. $\Pr[C = c] \neq 0$. For an arbitrary m:

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

$$\Pr[\mathsf{Enc}_K(m) = c] = \Pr[C = c] = \Pr[\mathsf{Enc}_K(m') = c] \qquad \text{(repeating the same argument for } m'\text{)}$$

This does not depend on the choice of m!

Proof of equivalence

$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}$:

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

$$\Downarrow$$

$\forall$ *probability distribution over* $\mathcal{M}$, $\forall m \in \mathcal{M}, c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$:

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

Consider an *arbitrary* distribution over $\mathcal{M}$, any $m \in \mathcal{M}$, and any c s.t. $\Pr[C = c] \neq 0$.

We only need to consider $\Pr[M = m] > 0$ (otherwise the thesis is trivially true)

Proof of equivalence

$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}$:

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

$$\Downarrow$$

$\forall$ *probability distribution over* $\mathcal{M}$*,* $\forall m \in \mathcal{M}, c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$*:*

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

Consider an *arbitrary* distribution over $\mathcal{M}$, any $m \in \mathcal{M}$, and any c s.t. $\Pr[C = c] \neq 0$.

We only need to consider $\Pr[M = m] > 0$ (otherwise the thesis is trivially true)

We start by showing that $\Pr[C = c] = \Pr[C = c \mid M = m]$

Proof of equivalence

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}\text{:}$$
$$\Pr[\mathit{Enc}_K(m) = c] = \Pr[\mathit{Enc}_K(m') = c]$$

$$\Downarrow$$

$\forall$ *probability distribution over* $\mathcal{M}$*,* $\forall m \in \mathcal{M}, c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$*:*

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

Consider an *arbitrary* distribution over $\mathcal{M}$, any $m \in \mathcal{M}$, and any c s.t. $\Pr[C = c] \neq 0$.

We only need to consider $\Pr[M = m] > 0$ (otherwise the thesis is trivially true)

We start by showing that $\Pr[C = c] = \Pr[C = c \mid M = m]$

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

Proof of equivalence

$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}$:

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

$$\Downarrow$$

$\forall$ *probability distribution over* $\mathcal{M}$, $\forall m \in \mathcal{M}, c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$:

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

Consider an *arbitrary* distribution over $\mathcal{M}$, any $m \in \mathcal{M}$, and any c s.t. $\Pr[C = c] \neq 0$.

We only need to consider $\Pr[M = m] > 0$ (otherwise the thesis is trivially true)

We start by showing that $\Pr[C = c] = \Pr[C = c \mid M = m]$

$$\Pr[C = c] = \sum_{m' \in \mathcal{M}} \Pr[C = c \mid M = m'] \cdot \Pr[M = m'] \quad = \sum_{m' \in \mathcal{M}} \Pr[\mathsf{Enc}_K(m') = c] \cdot \Pr[M = m']$$

Proof of equivalence

$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}$:

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

$$\Downarrow$$

$\forall$ *probability distribution over* $\mathcal{M}$, $\forall m \in \mathcal{M}, c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$:

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

Consider an *arbitrary* distribution over $\mathcal{M}$, any $m \in \mathcal{M}$, and any c s.t. $\Pr[C = c] \neq 0$.

We only need to consider $\Pr[M = m] > 0$ (otherwise the thesis is trivially true)

We start by showing that $\Pr[C = c] = \Pr[C = c \mid M = m]$

$$\Pr[C = c] = \sum_{m' \in \mathcal{M}} \Pr[C = c \mid M = m'] \cdot \Pr[M = m'] = \sum_{m' \in \mathcal{M}} \Pr[\mathsf{Enc}_K(m') = c] \cdot \Pr[M = m']$$

$$= \Pr[\mathsf{Enc}_K(m) = c] \cdot \sum_{m' \in \mathcal{M}} \Pr[M = m']$$

Proof of equivalence

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}\textit{:}$$
$$\Pr[\textit{Enc}_K(m) = c] = \Pr[\textit{Enc}_K(m') = c]$$

$$\Downarrow$$

$\forall$ *probability distribution over* $\mathcal{M}$*,* $\forall m \in \mathcal{M}, c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$*:*
$$\Pr[M = m \mid C = c] = \Pr[M = m]$$

Consider an *arbitrary* distribution over $\mathcal{M}$, any $m \in \mathcal{M}$, and any c s.t. $\Pr[C = c] \neq 0$.

We only need to consider $\Pr[M = m] > 0$ (otherwise the thesis is trivially true)

We start by showing that $\Pr[C = c] = \Pr[C = c \mid M = m]$

$$\Pr[C = c] = \sum_{m' \in \mathcal{M}} \Pr[C = c \mid M = m'] \cdot \Pr[M = m'] \quad = \sum_{m' \in \mathcal{M}} \Pr[\mathsf{Enc}_K(m') = c] \cdot \Pr[M = m']$$

$$= \Pr[\mathsf{Enc}_K(m) = c] \cdot \sum_{m' \in \mathcal{M}} \Pr[M = m'] \quad = \Pr[\mathsf{Enc}_K(m) = c]$$

Proof of equivalence

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}\text{:}$$
$$\Pr[\mathit{Enc}_K(m) = c] = \Pr[\mathit{Enc}_K(m') = c]$$

$$\Downarrow$$

$\forall$ *probability distribution over* $\mathcal{M}$, $\forall m \in \mathcal{M}, c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$*:*

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

Consider an *arbitrary* distribution over $\mathcal{M}$, any $m \in \mathcal{M}$, and any c s.t. $\Pr[C = c] \neq 0$.

We only need to consider $\Pr[M = m] > 0$ (otherwise the thesis is trivially true)

We start by showing that $\Pr[C = c] = \Pr[C = c \mid M = m]$

$$\Pr[C = c] = \sum_{m' \in \mathcal{M}} \Pr[C = c \mid M = m'] \cdot \Pr[M = m'] = \sum_{m' \in \mathcal{M}} \Pr[\mathsf{Enc}_K(m') = c] \cdot \Pr[M = m']$$
$$= \Pr[\mathsf{Enc}_K(m) = c] \cdot \sum_{m' \in \mathcal{M}} \Pr[M = m'] = \Pr[\mathsf{Enc}_K(m) = c] = \Pr[C = c \mid M = m]$$

Proof of equivalence

$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}$:

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

$$\Downarrow$$

$\forall$ *probability distribution over* $\mathcal{M}$*,* $\forall m \in \mathcal{M}, c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$*:*

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

Consider an *arbitrary* distribution over $\mathcal{M}$, any $m \in \mathcal{M}$, and any c s.t. $\Pr[C = c] \neq 0$.

We only need to consider $\Pr[M = m] > 0$ (otherwise the thesis is trivially true)

We have shown that: $\Pr[C = c] = \Pr[C = c \mid M = m]$

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

Proof of equivalence

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}\text{:}$$

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

$$\Downarrow$$

$\forall$ *probability distribution over* $\mathcal{M}$, $\forall m \in \mathcal{M}, c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$*:*

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

Consider an *arbitrary* distribution over $\mathcal{M}$, any $m \in \mathcal{M}$, and any c s.t. $\Pr[C = c] \neq 0$.

We only need to consider $\Pr[M = m] > 0$ (otherwise the thesis is trivially true)

We have shown that: $\Pr[C = c] = \Pr[C = c \mid M = m]$

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

Proof of equivalence

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}\textit{:}$$
$$\Pr[\textit{Enc}_K(m) = c] = \Pr[\textit{Enc}_K(m') = c]$$

$$\Downarrow$$

$\forall$ *probability distribution over* $\mathcal{M}$*,* $\forall m \in \mathcal{M}, c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$*:*
$$\Pr[M = m \mid C = c] = \Pr[M = m]$$

Consider an *arbitrary* distribution over $\mathcal{M}$, any $m \in \mathcal{M}$, and any c s.t. $\Pr[C = c] \neq 0$.

We only need to consider $\Pr[M = m] > 0$ (otherwise the thesis is trivially true)

We have shown that: $\Pr[C = c] = \Pr[C = c \mid M = m]$

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

Proof of equivalence

$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}$:

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

$$\Downarrow$$

$\forall$ *probability distribution over* $\mathcal{M}$, $\forall m \in \mathcal{M}, c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$:

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

Consider an *arbitrary* distribution over $\mathcal{M}$, any $m \in \mathcal{M}$, and any c s.t. $\Pr[C = c] \neq 0$.

We only need to consider $\Pr[M = m] > 0$ (otherwise the thesis is trivially true)

We have shown that: $\Pr[C = c] = \Pr[C = c \mid M = m]$

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

$\square$

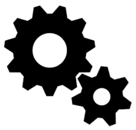
Perfect indistinguishability

Adversary $\mathcal{A}$ (deterministic, computationally unbounded algorithm)

Verifier

Perfect indistinguishability

Adversary $\mathcal{A}$ (deterministic, computationally unbounded algorithm)



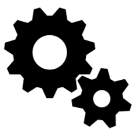
$m_0, m_1 \in \mathcal{M}$

Verifier

Perfect indistinguishability

Adversary $\mathcal{A}$ (deterministic, computationally unbounded algorithm)

Verifier



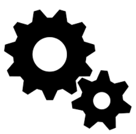
$m_0, m_1 \in \mathcal{M}$

$k \leftarrow$ Gen $\leftarrow$

Perfect indistinguishability

Adversary $\mathcal{A}$ (deterministic, computationally unbounded algorithm)

Verifier



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

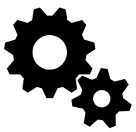
$k \leftarrow \boxed{\text{Gen}} \leftarrow$

$b \leftarrow \{0,1\}$

Perfect indistinguishability

Adversary $\mathcal{A}$ (deterministic, computationally unbounded algorithm)

Verifier



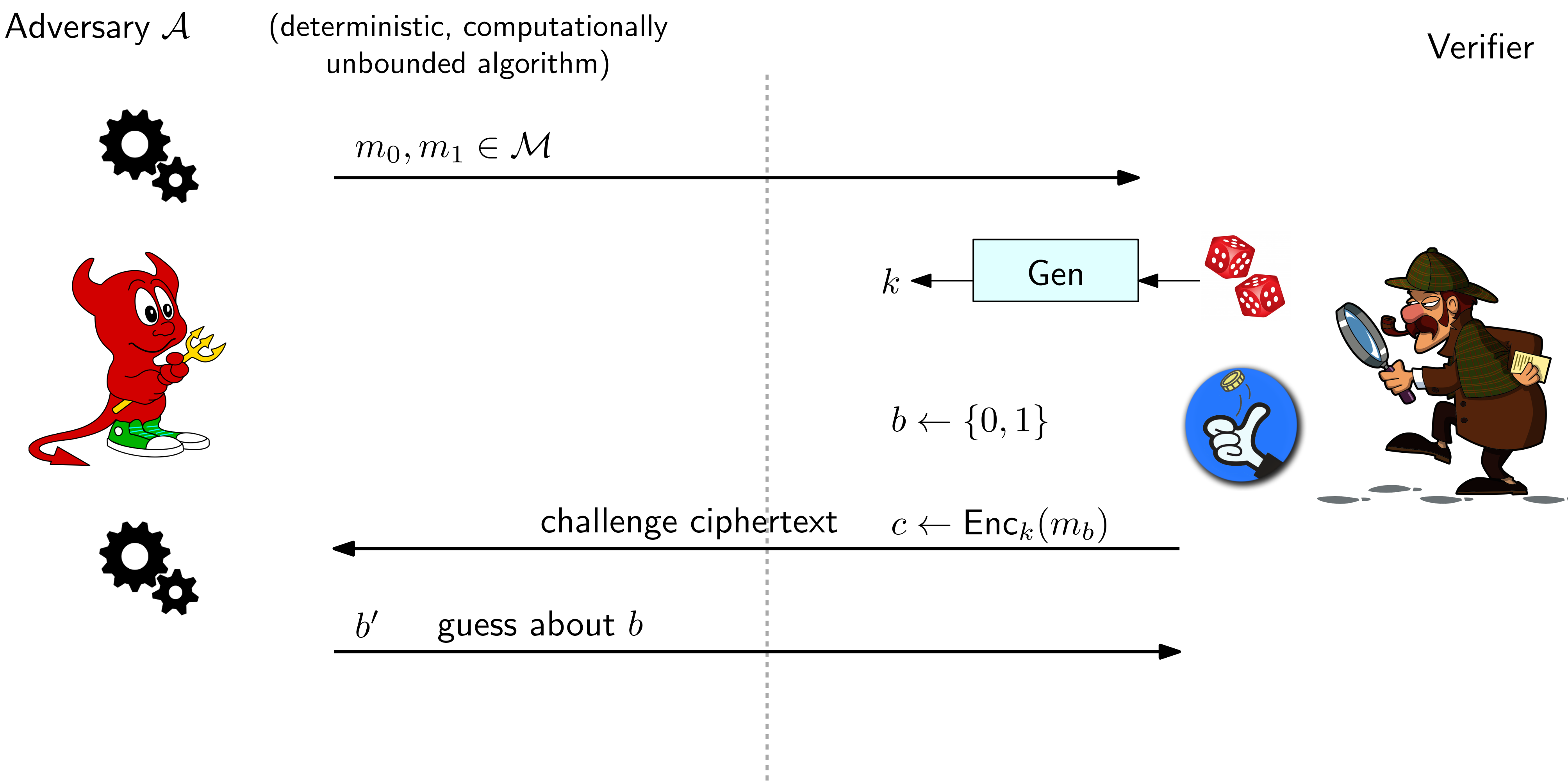
$m_0, m_1 \in \mathcal{M}$

$k \leftarrow$ Gen $\leftarrow$

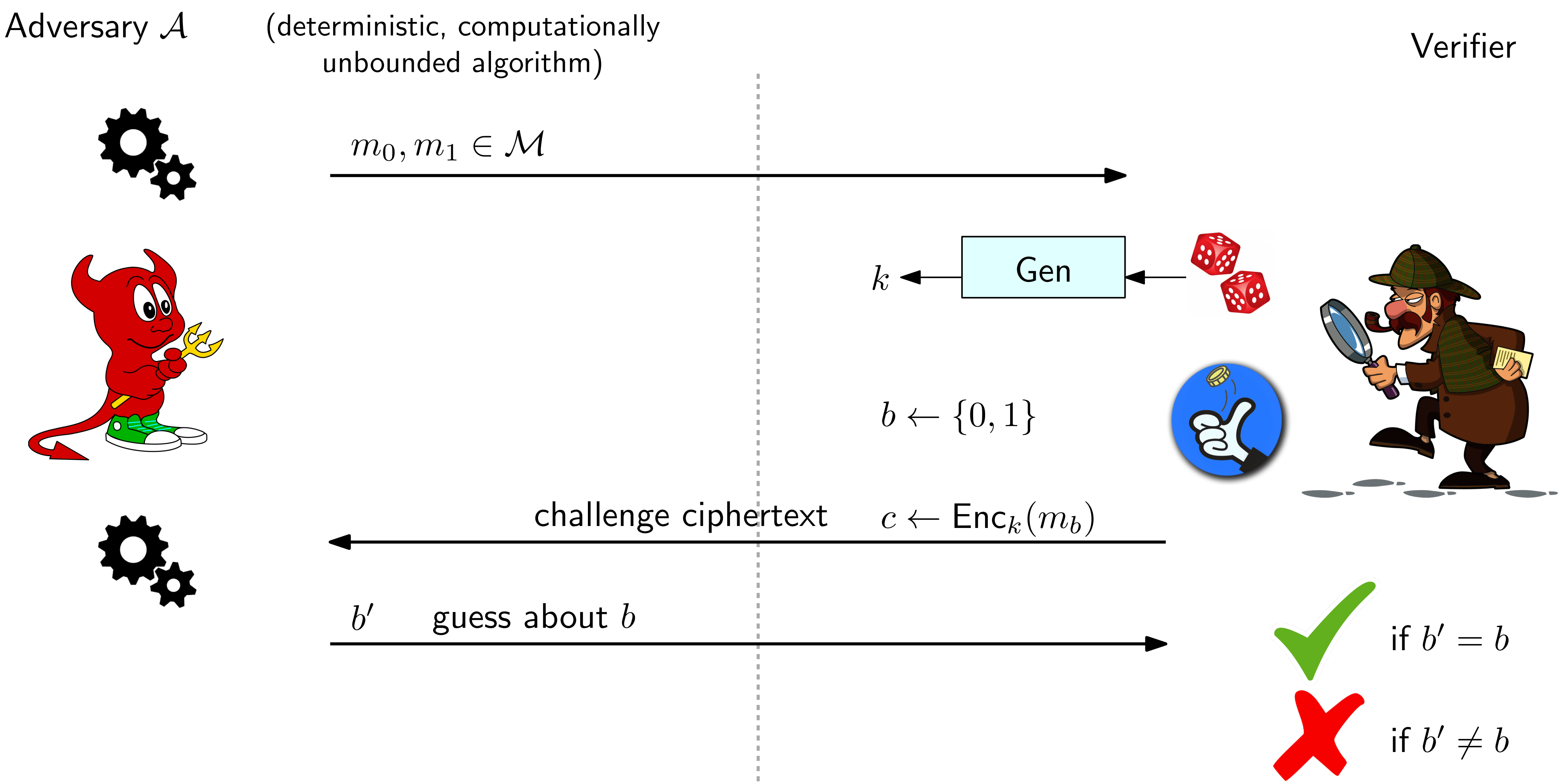
$b \leftarrow \{0,1\}$

challenge ciphertext $c \leftarrow \mathsf{Enc}_k(m_b)$

Perfect indistinguishability



Perfect indistinguishability



Perfect indistinguishability

Formally, if $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a private key encryption scheme with message space $\mathcal{M}$, we denote the previous experiment by $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$

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

Perfect indistinguishability

Formally, if $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a private key encryption scheme with message space $\mathcal{M}$, we denote the previous experiment by $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$

We are dealing with **priv**ate-**k**ey encryption schemes

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

Perfect indistinguishability

Formally, if $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a private key encryption scheme with message space $\mathcal{M}$, we denote the previous experiment by $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$

We are dealing with **priv**ate-**k**ey encryption schemes

We are considering ciphertext-only attacks, i.e., security against **eav**esdroppers

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

Perfect indistinguishability

Formally, if $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a private key encryption scheme with message space $\mathcal{M}$, we denote the previous experiment by $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$

We are dealing with **priv**ate-**k**ey encryption schemes

We are considering ciphertext-only attacks, i.e., security against **eav**esdroppers

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

The algorithm $\mathcal{A}$ used by the adversary

Perfect indistinguishability

Formally, if $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a private key encryption scheme with message space $\mathcal{M}$, we denote the previous experiment by $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$

We are dealing with **priv**ate-**k**ey encryption schemes

We are considering ciphertext-only attacks, i.e., security against **eav**esdroppers

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

The algorithm $\mathcal{A}$ used by the adversary

The considered encryption scheme

Perfect indistinguishability

Formally, if $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a private key encryption scheme with message space $\mathcal{M}$, we denote the previous experiment by $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$

- $\mathcal{A}$ chooses two messages $m_0, m_1 \in \mathcal{M}$
- A random key k is generated (by running Gen)
- A uniform random bit $b \in \{0, 1\}$ is generated
- The *challenge ciphertext* c is computed by running $\mathsf{Enc}_k(m_b)$, and it is given to $\mathcal{A}$
- $\mathcal{A}$ outputs a guess $b' \in \{0, 1\}$ about b

Perfect indistinguishability

Formally, if $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a private key encryption scheme with message space $\mathcal{M}$, we denote the previous experiment by $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$

- $\mathcal{A}$ chooses two messages $m_0, m_1 \in \mathcal{M}$
- A random key k is generated (by running Gen)
- A uniform random bit $b \in \{0, 1\}$ is generated
- The *challenge ciphertext* c is computed by running $\mathsf{Enc}_k(m_b)$, and it is given to $\mathcal{A}$
- $\mathcal{A}$ outputs a guess $b' \in \{0, 1\}$ about b

$\mathcal{A}$ knows neither k nor b!

Perfect indistinguishability

Formally, if $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a private key encryption scheme with message space $\mathcal{M}$, we denote the previous experiment by $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$

- $\mathcal{A}$ chooses two messages $m_0, m_1 \in \mathcal{M}$
- A random key k is generated (by running Gen)
- A uniform random bit $b \in \{0,1\}$ is generated

$\mathcal{A}$ knows neither k nor b!

- The *challenge ciphertext* c is computed by running $\mathsf{Enc}_k(m_b)$, and it is given to $\mathcal{A}$
- $\mathcal{A}$ outputs a guess $b' \in \{0,1\}$ about b
- The *output of the experiment* is defined to be 1 if $b' = b$, and 0 otherwise

We write $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1$ (resp. $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 0$) to denote that the output of the experiment is 1 (resp. 0)

Perfect indistinguishability

Definition: *A private key encryption scheme* $\Pi = (\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ *with message space* $\mathcal{M}$ *is* **perfectly indistinguishable** *if for every* $\mathcal{A}$ *it holds:*

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

Perfect indistinguishability

Definition: *A private key encryption scheme* $\Pi = (\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ *with message space* $\mathcal{M}$ *is* **perfectly indistinguishable** *if for every* $\mathcal{A}$ *it holds:*

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

Informally, any adversary $\mathcal{A}$ that tries to correctly guess which of two plaintexts corresponds to a given ciphertext cannot perform better than randomly guessing.

(even if the two candidate plaintexts are chosen by the adversary)

Perfect indistinguishability

Definition: *A private key encryption scheme* $\Pi = (\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ *with message space* $\mathcal{M}$ *is* **perfectly indistinguishable** *if for every* $\mathcal{A}$ *it holds:*

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

Informally, any adversary $\mathcal{A}$ that tries to correctly guess which of two plaintexts corresponds to a given ciphertext cannot perform better than randomly guessing.

(even if the two candidate plaintexts are chosen by the adversary)

If $\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \frac{1}{2} + \varepsilon$ for some $\varepsilon > 0$, the scheme is not perfectly indistinguishable

Perfect indistinguishability

Definition: *A private key encryption scheme* $\Pi = (\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ *with message space* $\mathcal{M}$ *is* **perfectly indistinguishable** *if for every* $\mathcal{A}$ *it holds:*

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

Informally, any adversary $\mathcal{A}$ that tries to correctly guess which of two plaintexts corresponds to a given ciphertext cannot perform better than randomly guessing.

(even if the two candidate plaintexts are chosen by the adversary)

If $\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \frac{1}{2} + \boxed{\varepsilon}$ for some $\varepsilon > 0$, the scheme is not perfectly indistinguishable

Advantage of $\mathcal{A}$

Perfect indistinguishability: Example

Consider the Vigenère cipher Π with:

$\mathcal{M} = \{a, b, \ldots, z\}^2$ $\quad$ $\mathcal{K} = \{A, \ldots, Z\} \cup \{A, \ldots, Z\}^2$ $\quad$ $\mathcal{C} = \{A, B, \ldots, Z\}^2$

Where the key is selected as follows:

- Pick a key length ℓ uniformly at random in $\{1, 2\}$
- Pick a key k uniformly at random in $\{A, \ldots, Z\}^\ell$

Perfect indistinguishability: Example

Consider the Vigenère cipher Π with:

$\mathcal{M} = \{a, b, \ldots, z\}^2$ $\mathcal{K} = \{A, \ldots, Z\} \cup \{A, \ldots, Z\}^2$ $\mathcal{C} = \{A, B, \ldots, Z\}^2$

Where the key is selected as follows:

- Pick a key length ℓ uniformly at random in $\{1, 2\}$
- Pick a key k uniformly at random in $\{A, \ldots, Z\}^\ell$

Is Π perfectly indistinguishable?

Perfect indistinguishability: Example

Consider the Vigenère cipher Π with:

$\mathcal{M} = \{a, b, \ldots, z\}^2$ $\mathcal{K} = \{A, \ldots, Z\} \cup \{A, \ldots, Z\}^2$ $\mathcal{C} = \{A, B, \ldots, Z\}^2$

Where the key is selected as follows:

- Pick a key length ℓ uniformly at random in $\{1, 2\}$
- Pick a key k uniformly at random in $\{A, \ldots, Z\}^\ell$

Is Π perfectly indistinguishable?

We need to devise a "distinguisher", i.e., an algorithm $\mathcal{A}$ that wins the $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$ experiment with probability greater than $\frac{1}{2}$

Perfect indistinguishability: Example

Algorithm $\mathcal{A}$:

- Output $m_0 = \texttt{aa}$, $m_1 = \texttt{ab}$
- Upon receiving the challenge ciphertext $c = c^{(1)}c^{(2)}$:
  - If $c^{(1)} = c^{(2)}$ output $b' = 0$
  - Otherwise (i..e, $c^{(1)} \neq c^{(2)}$) output $b' = 1$

Perfect indistinguishability: Example

Algorithm $\mathcal{A}$:

- Output $m_0 = \texttt{aa}$, $m_1 = \texttt{ab}$
- Upon receiving the challenge ciphertext $c = c^{(1)}c^{(2)}$:
  - If $c^{(1)} = c^{(2)}$ output $b' = 0$
  - Otherwise (i..e, $c^{(1)} \neq c^{(2)}$) output $b' = 1$

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

Perfect indistinguishability: Example

Algorithm $\mathcal{A}$:

- Output $m_0 = \mathtt{aa}$, $m_1 = \mathtt{ab}$
- Upon receiving the challenge ciphertext $c = c^{(1)}c^{(2)}$:
  - If $c^{(1)} = c^{(2)}$ output $b' = 0$
  - Otherwise (i..e, $c^{(1)} \neq c^{(2)}$) output $b' = 1$

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] \; = \tfrac{1}{2}\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \mid b = 0] + \tfrac{1}{2}\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \mid b = 1]$$

Perfect indistinguishability: Example

Algorithm $\mathcal{A}$:

- Output $m_0 = \texttt{aa}$, $m_1 = \texttt{ab}$
- Upon receiving the challenge ciphertext $c = c^{(1)}c^{(2)}$:
  - If $c^{(1)} = c^{(2)}$ output $b' = 0$
  - Otherwise (i..e, $c^{(1)} \neq c^{(2)}$) output $b' = 1$

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] \; = \tfrac{1}{2}\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \mid b = 0] + \tfrac{1}{2}\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \mid b = 1]$$

- When $b = 0$, $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \iff \ell = 1$ or $\ell = 2$ and the two characters of the key are equal

Perfect indistinguishability: Example

Algorithm $\mathcal{A}$:

- Output $m_0 = \texttt{aa}$, $m_1 = \texttt{ab}$
- Upon receiving the challenge ciphertext $c = c^{(1)}c^{(2)}$:
  - If $c^{(1)} = c^{(2)}$ output $b' = 0$
  - Otherwise (i..e, $c^{(1)} \neq c^{(2)}$) output $b' = 1$

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] \; = \tfrac{1}{2}\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \mid b = 0] + \tfrac{1}{2}\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \mid b = 1]$$

- When $b = 0$, $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \iff \ell = 1$ or $\ell = 2$ and the two characters of the key are equal

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \mid b = 0] = \tfrac{1}{2} + \tfrac{1}{2} \cdot \tfrac{1}{26}$$

Perfect indistinguishability: Example

Algorithm $\mathcal{A}$:

- Output $m_0 = \texttt{aa}$, $m_1 = \texttt{ab}$
- Upon receiving the challenge ciphertext $c = c^{(1)}c^{(2)}$:
  - If $c^{(1)} = c^{(2)}$ output $b' = 0$
  - Otherwise (i..e, $c^{(1)} \neq c^{(2)}$) output $b' = 1$

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] \;=\tfrac{1}{2}\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \mid b = 0] + \tfrac{1}{2}\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \mid b = 1]$$

- When $b = 0$, $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \iff \ell = 1$ or $\ell = 2$ and the two characters of the key are equal

  $$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \mid b = 0] = \tfrac{1}{2} + \tfrac{1}{2}\cdot\tfrac{1}{26}$$

- When $b = 1$, $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \iff$

Perfect indistinguishability: Example

Algorithm $\mathcal{A}$:

- Output $m_0 = \texttt{aa}$, $m_1 = \texttt{ab}$
- Upon receiving the challenge ciphertext $c = c^{(1)}c^{(2)}$:
  - If $c^{(1)} = c^{(2)}$ output $b' = 0$
  - Otherwise (i..e, $c^{(1)} \neq c^{(2)}$) output $b' = 1$

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] \;= \tfrac{1}{2}\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \mid b = 0] + \tfrac{1}{2}\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \mid b = 1]$$

- When $b = 0$, $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \iff \ell = 1$ or $\ell = 2$ and the two characters of the key are equal

  $$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \mid b = 0] = \tfrac{1}{2} + \tfrac{1}{2} \cdot \tfrac{1}{26}$$

- When $b = 1$, $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \iff \ell = 1$ or $\ell = 2$ and the key $k = k_1k_2$ satisfies $k_1 \neq k_2 + 1 \pmod{26}$

Perfect indistinguishability: Example

Algorithm $\mathcal{A}$:

- Output $m_0 = \texttt{aa}$, $m_1 = \texttt{ab}$
- Upon receiving the challenge ciphertext $c = c^{(1)}c^{(2)}$:
  - If $c^{(1)} = c^{(2)}$ output $b' = 0$
  - Otherwise (i..e, $c^{(1)} \neq c^{(2)}$) output $b' = 1$

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] \;= \tfrac{1}{2}\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \mid b = 0] + \tfrac{1}{2}\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \mid b = 1]$$

- When $b = 0$, $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \iff \ell = 1$ or $\ell = 2$ and the two characters of the key are equal

  $$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \mid b = 0] = \tfrac{1}{2} + \tfrac{1}{2} \cdot \tfrac{1}{26}$$

- When $b = 1$, $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \iff \ell = 1$ or $\ell = 2$ and the key $k = k_1k_2$ satisfies $k_1 \neq k_2 + 1 \pmod{26}$

  $$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \mid b = 1] = \tfrac{1}{2} + \tfrac{1}{2} \cdot \tfrac{25}{26}$$

Perfect indistinguishability: Example

Algorithm $\mathcal{A}$:

- Output $m_0 = \texttt{aa}$, $m_1 = \texttt{ab}$
- Upon receiving the challenge ciphertext $c = c^{(1)}c^{(2)}$:
  - If $c^{(1)} = c^{(2)}$ output $b' = 0$
  - Otherwise (i..e, $c^{(1)} \neq c^{(2)}$) output $b' = 1$

$$\begin{aligned}\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] &= \tfrac{1}{2}\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \mid b = 0] + \tfrac{1}{2}\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \mid b = 1] \\ &= \tfrac{1}{2}\cdot(\tfrac{1}{2} + \tfrac{1}{2}\cdot\tfrac{1}{26}) + \tfrac{1}{2}\cdot(\tfrac{1}{2} + \tfrac{1}{2}\cdot\tfrac{25}{26})\end{aligned}$$

Perfect indistinguishability: Example

Algorithm $\mathcal{A}$:

- Output $m_0 = \texttt{aa}$, $m_1 = \texttt{ab}$
- Upon receiving the challenge ciphertext $c = c^{(1)}c^{(2)}$:
  - If $c^{(1)} = c^{(2)}$ output $b' = 0$
  - Otherwise (i..e, $c^{(1)} \neq c^{(2)}$) output $b' = 1$

$$\begin{aligned}
\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] &= \tfrac{1}{2}\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \mid b = 0] + \tfrac{1}{2}\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \mid b = 1] \\
&= \tfrac{1}{2}\cdot(\tfrac{1}{2} + \tfrac{1}{2}\cdot\tfrac{1}{26}) + \tfrac{1}{2}\cdot(\tfrac{1}{2} + \tfrac{1}{2}\cdot\tfrac{25}{26}) \quad = \tfrac{3}{4} = \tfrac{1}{2} + \tfrac{1}{4} > \tfrac{1}{2}
\end{aligned}$$

Perfect indistinguishability: Example

Algorithm $\mathcal{A}$:

- Output $m_0 = \texttt{aa}$, $m_1 = \texttt{ab}$
- Upon receiving the challenge ciphertext $c = c^{(1)}c^{(2)}$:
  - If $c^{(1)} = c^{(2)}$ output $b' = 0$
  - Otherwise (i..e, $c^{(1)} \neq c^{(2)}$) output $b' = 1$

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \frac{1}{2} \Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \mid b = 0] + \frac{1}{2} \Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1 \mid b = 1]$$

$$= \frac{1}{2} \cdot \left(\frac{1}{2} + \frac{1}{2} \cdot \frac{1}{26}\right) + \frac{1}{2} \cdot \left(\frac{1}{2} + \frac{1}{2} \cdot \frac{25}{26}\right) = \frac{3}{4} = \frac{1}{2} + \frac{1}{4} > \frac{1}{2}$$

Advantage of $\mathcal{A}$

Perfect secrecy & perfect indistinguishability

A private key encryption scheme is **perfectly secret** if and only if it is **perfectly indistinguishable**.

$\forall$ *probability distribution over* $\mathcal{M}$, $\forall m \in \mathcal{M}, c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$*:*

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

$$\Updownarrow$$

$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}$*:*

$$\Pr[Enc_K(m) = c] = \Pr[Enc_K(m') = c]$$

$$\Updownarrow$$

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

Proof of equivalence

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}\text{:}$$

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

$$\Downarrow$$

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

Proof of equivalence

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}\text{:}$$
$$\Pr[\mathit{Enc}_K(m) = c] = \Pr[\mathit{Enc}_K(m') = c]$$

$$\Downarrow$$

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

Fix any algorithm $\mathcal{A}$, and let m_0, m_1 be the messages output by $\mathcal{A}$

Partition $\mathcal{C}$ into $\mathcal{C}_0, \mathcal{C}_1$, where C_i is the set of ciphertexts for which $\mathcal{A}$ guesses $b' = i$

Proof of equivalence

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}\text{:}$$
$$\Pr[\mathit{Enc}_K(m) = c] = \Pr[\mathit{Enc}_K(m') = c]$$

$$\Downarrow$$

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

Fix any algorithm $\mathcal{A}$, and let m_0, m_1 be the messages output by $\mathcal{A}$

Partition $\mathcal{C}$ into $\mathcal{C}_0, \mathcal{C}_1$, where C_i is the set of ciphertexts for which $\mathcal{A}$ guesses $b' = i$

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

Proof of equivalence

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}\text{:}$$
$$\Pr[\mathit{Enc}_K(m) = c] = \Pr[\mathit{Enc}_K(m') = c]$$

$$\Downarrow$$

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

Fix any algorithm $\mathcal{A}$, and let m_0, m_1 be the messages output by $\mathcal{A}$

Partition $\mathcal{C}$ into $\mathcal{C}_0, \mathcal{C}_1$, where C_i is the set of ciphertexts for which $\mathcal{A}$ guesses $b' = i$

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] \ = \tfrac{1}{2} \cdot \Pr[b' = 0 \mid b = 0] + \tfrac{1}{2} \cdot \Pr[b' = 1 \mid b = 1]$$

Proof of equivalence

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}\text{:}$$

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

$$\Downarrow$$

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

Fix any algorithm $\mathcal{A}$, and let m_0, m_1 be the messages output by $\mathcal{A}$

Partition $\mathcal{C}$ into $\mathcal{C}_0, \mathcal{C}_1$, where C_i is the set of ciphertexts for which $\mathcal{A}$ guesses $b' = i$

$$\begin{aligned} \Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] &= \tfrac{1}{2} \cdot \Pr[b' = 0 \mid b = 0] + \tfrac{1}{2} \cdot \Pr[b' = 1 \mid b = 1] \\ &= \tfrac{1}{2} \cdot \Pr[\mathsf{Enc}_K(m_0) \in \mathcal{C}_0] + \tfrac{1}{2} \cdot \Pr[\mathsf{Enc}_K(m_1) \in \mathcal{C}_1] \end{aligned}$$

Proof of equivalence

$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}$:

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

$$\Downarrow$$

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

Fix any algorithm $\mathcal{A}$, and let m_0, m_1 be the messages output by $\mathcal{A}$

Partition $\mathcal{C}$ into $\mathcal{C}_0, \mathcal{C}_1$, where C_i is the set of ciphertexts for which $\mathcal{A}$ guesses $b' = i$

$$\begin{aligned}
\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] &= \tfrac{1}{2} \cdot \Pr[b' = 0 \mid b = 0] + \tfrac{1}{2} \cdot \Pr[b' = 1 \mid b = 1] \\
&= \tfrac{1}{2} \cdot \Pr[\mathsf{Enc}_K(m_0) \in \mathcal{C}_0] + \tfrac{1}{2} \cdot \Pr[\mathsf{Enc}_K(m_1) \in \mathcal{C}_1] \\
&= \tfrac{1}{2} \cdot \textstyle\sum_{c \in \mathcal{C}_0} \Pr[\mathsf{Enc}_K(m_0) = c] + \tfrac{1}{2} \cdot \textstyle\sum_{c \in \mathcal{C}_1} \Pr[\mathsf{Enc}_K(m_1) = c]
\end{aligned}$$

Proof of equivalence

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}:$$
$$\Pr[\mathit{Enc}_K(m) = c] = \Pr[\mathit{Enc}_K(m') = c]$$

$$\Downarrow$$

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

Fix any algorithm $\mathcal{A}$, and let m_0, m_1 be the messages output by $\mathcal{A}$

Partition $\mathcal{C}$ into $\mathcal{C}_0, \mathcal{C}_1$, where C_i is the set of ciphertexts for which $\mathcal{A}$ guesses $b' = i$

$$\begin{aligned}
\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] &= \tfrac{1}{2} \cdot \Pr[b' = 0 \mid b = 0] + \tfrac{1}{2} \cdot \Pr[b' = 1 \mid b = 1] \\
&= \tfrac{1}{2} \cdot \Pr[\mathsf{Enc}_K(m_0) \in \mathcal{C}_0] + \tfrac{1}{2} \cdot \Pr[\mathsf{Enc}_K(m_1) \in \mathcal{C}_1] \\
&= \tfrac{1}{2} \cdot \textstyle\sum_{c \in \mathcal{C}_0} \Pr[\mathsf{Enc}_K(m_0) = c] + \tfrac{1}{2} \cdot \sum_{c \in \mathcal{C}_1} \Pr[\mathsf{Enc}_K(\color{red}{m_0}) = c]
\end{aligned}$$

Proof of equivalence

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}\text{:}$$
$$\Pr[\mathit{Enc}_K(m) = c] = \Pr[\mathit{Enc}_K(m') = c]$$

$$\Downarrow$$

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

Fix any algorithm $\mathcal{A}$, and let m_0, m_1 be the messages output by $\mathcal{A}$

Partition $\mathcal{C}$ into $\mathcal{C}_0, \mathcal{C}_1$, where C_i is the set of ciphertexts for which $\mathcal{A}$ guesses $b' = i$

$$\begin{aligned}
\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] &= \tfrac{1}{2} \cdot \Pr[b' = 0 \mid b = 0] + \tfrac{1}{2} \cdot \Pr[b' = 1 \mid b = 1] \\
&= \tfrac{1}{2} \cdot \Pr[\mathsf{Enc}_K(m_0) \in \mathcal{C}_0] + \tfrac{1}{2} \cdot \Pr[\mathsf{Enc}_K(m_1) \in \mathcal{C}_1] \\
&= \tfrac{1}{2} \cdot \textstyle\sum_{c \in \mathcal{C}_0} \Pr[\mathsf{Enc}_K(m_0) = c] + \tfrac{1}{2} \cdot \textstyle\sum_{c \in \mathcal{C}_1} \Pr[\mathsf{Enc}_K(\color{red}{m_0}) = c] \\
&= \tfrac{1}{2} \cdot \textstyle\sum_{c \in \mathcal{C}} \Pr[\mathsf{Enc}_K(m_0) = c]
\end{aligned}$$

Proof of equivalence

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}:$$
$$\Pr[\mathit{Enc}_K(m) = c] = \Pr[\mathit{Enc}_K(m') = c]$$

$$\Downarrow$$

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

Fix any algorithm $\mathcal{A}$, and let m_0, m_1 be the messages output by $\mathcal{A}$

Partition $\mathcal{C}$ into $\mathcal{C}_0, \mathcal{C}_1$, where C_i is the set of ciphertexts for which $\mathcal{A}$ guesses $b' = i$

$$\begin{aligned}
\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] &= \tfrac{1}{2} \cdot \Pr[b' = 0 \mid b = 0] + \tfrac{1}{2} \cdot \Pr[b' = 1 \mid b = 1] \\
&= \tfrac{1}{2} \cdot \Pr[\mathsf{Enc}_K(m_0) \in \mathcal{C}_0] + \tfrac{1}{2} \cdot \Pr[\mathsf{Enc}_K(m_1) \in \mathcal{C}_1] \\
&= \tfrac{1}{2} \cdot \textstyle\sum_{c \in \mathcal{C}_0} \Pr[\mathsf{Enc}_K(m_0) = c] + \tfrac{1}{2} \cdot \textstyle\sum_{c \in \mathcal{C}_1} \Pr[\mathsf{Enc}_K({\color{red}m_0}) = c] \\
&= \tfrac{1}{2} \cdot \textstyle\sum_{c \in \mathcal{C}} \Pr[\mathsf{Enc}_K(m_0) = c] \quad = \tfrac{1}{2}
\end{aligned}$$

Proof of equivalence

NOT

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}:$$
$$\Pr[\mathit{Enc}_K(m) = c] = \Pr[\mathit{Enc}_K(m') = c]$$

$$\Downarrow$$

NOT

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

Proof of equivalence

NOT

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}\text{:}$$
$$\Pr[\mathit{Enc}_K(m) = c] = \Pr[\mathit{Enc}_K(m') = c]$$

$$\Downarrow$$

NOT

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

Pick $m_0, m_1 \in \mathcal{M}, c^* \in \mathcal{C}$ s.t. $\Pr[\mathsf{Enc}_K(m_0) = c^*] \neq \Pr[\mathsf{Enc}_K(m_1) = c^*]$

Proof of equivalence

NOT

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}\text{:}$$
$$\Pr[\mathit{Enc}_K(m) = c] = \Pr[\mathit{Enc}_K(m') = c]$$

$$\Downarrow$$

NOT

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

Pick $m_0, m_1 \in \mathcal{M}, c^* \in \mathcal{C}$ s.t. $\Pr[\mathsf{Enc}_K(m_0) = c^*] \neq \Pr[\mathsf{Enc}_K(m_1) = c^*]$

Algorithm $\mathcal{A}$:

- Output m_0, m_1
- Upon receiving the challenge ciphertext c
  - If $c = c^*$ output $b' = 0$
  - Otherwise output a b' chosen u.a.r. in $\{0, 1\}$

Proof of equivalence

NOT

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}\text{:}$$
$$\Pr[\mathit{Enc}_K(m) = c] = \Pr[\mathit{Enc}_K(m') = c]$$

$$\Downarrow$$

NOT

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

Pick $m_0, m_1 \in \mathcal{M}, c^* \in \mathcal{C}$ s.t. $\Pr[\mathsf{Enc}_K(m_0) = c^*] \neq \Pr[\mathsf{Enc}_K(m_1) = c^*]$

$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \frac{1}{2} \cdot \Pr[b' = 0 \mid b = 0] + \frac{1}{2} \cdot \Pr[b' = 1 \mid b = 1]$

Proof of equivalence

NOT

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}\text{:}$$
$$\Pr[\mathit{Enc}_K(m) = c] = \Pr[\mathit{Enc}_K(m') = c]$$

$$\Downarrow$$

NOT

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

Pick $m_0, m_1 \in \mathcal{M}, c^* \in \mathcal{C}$ s.t. $\Pr[\mathsf{Enc}_K(m_0) = c^*] \neq \Pr[\mathsf{Enc}_K(m_1) = c^*]$

$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \frac{1}{2} \cdot \Pr[b' = 0 \mid b = 0] + \frac{1}{2} \cdot \Pr[b' = 1 \mid b = 1]$

$\Pr[b' = 0 \mid b = 0] = \Pr[b' = 0 \wedge \mathsf{Enc}_K(m_0) = c^*] + \Pr[b' = 0 \wedge \mathsf{Enc}_K(m_0) \neq c^*]$

Proof of equivalence

NOT

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}:$$
$$\Pr[\mathit{Enc}_K(m) = c] = \Pr[\mathit{Enc}_K(m') = c]$$

$$\Downarrow$$

NOT

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

Pick $m_0, m_1 \in \mathcal{M}, c^* \in \mathcal{C}$ s.t. $\Pr[\mathsf{Enc}_K(m_0) = c^*] \neq \Pr[\mathsf{Enc}_K(m_1) = c^*]$

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \tfrac{1}{2} \cdot \Pr[b' = 0 \mid b = 0] + \tfrac{1}{2} \cdot \Pr[b' = 1 \mid b = 1]$$

$$\begin{aligned}\Pr[b' = 0 \mid b = 0] &= \Pr[b' = 0 \wedge \mathsf{Enc}_K(m_0) = c^*] + \Pr[b' = 0 \wedge \mathsf{Enc}_K(m_0) \neq c^*] \\ &= \Pr[\mathsf{Enc}_K(m_0) = c^*] + \Pr[b' = 0 \mid \mathsf{Enc}_K(m_0) \neq c^*] \cdot \Pr[\mathsf{Enc}_K(m_0) \neq c^*]\end{aligned}$$

Proof of equivalence

NOT

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}\text{:}$$

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

$$\Downarrow$$

NOT

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

Pick $m_0, m_1 \in \mathcal{M}, c^* \in \mathcal{C}$ s.t. $\Pr[\mathsf{Enc}_K(m_0) = c^*] \neq \Pr[\mathsf{Enc}_K(m_1) = c^*]$

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \tfrac{1}{2} \cdot \Pr[b' = 0 \mid b = 0] + \tfrac{1}{2} \cdot \Pr[b' = 1 \mid b = 1]$$

$$\begin{aligned}
\Pr[b' = 0 \mid b = 0] &= \Pr[b' = 0 \wedge \mathsf{Enc}_K(m_0) = c^*] + \Pr[b' = 0 \wedge \mathsf{Enc}_K(m_0) \neq c^*] \\
&= \Pr[\mathsf{Enc}_K(m_0) = c^*] + \Pr[b' = 0 \mid \mathsf{Enc}_K(m_0) \neq c^*] \cdot \Pr[\mathsf{Enc}_K(m_0) \neq c^*] \\
&= \Pr[\mathsf{Enc}_K(m_0) = c^*] + \tfrac{1}{2} \cdot \Pr[\mathsf{Enc}_K(m_0) \neq c^*]
\end{aligned}$$

Proof of equivalence

NOT

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}\text{:}$$
$$\Pr[\mathit{Enc}_K(m) = c] = \Pr[\mathit{Enc}_K(m') = c]$$

$$\Downarrow$$

NOT

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

Pick $m_0, m_1 \in \mathcal{M}, c^* \in \mathcal{C}$ s.t. $\Pr[\mathsf{Enc}_K(m_0) = c^*] \neq \Pr[\mathsf{Enc}_K(m_1) = c^*]$

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \tfrac{1}{2} \cdot \Pr[b' = 0 \mid b = 0] + \tfrac{1}{2} \cdot \Pr[b' = 1 \mid b = 1]$$

$$\begin{aligned}\Pr[b' = 0 \mid b = 0] &= \Pr[b' = 0 \wedge \mathsf{Enc}_K(m_0) = c^*] + \Pr[b' = 0 \wedge \mathsf{Enc}_K(m_0) \neq c^*] \\ &= \Pr[\mathsf{Enc}_K(m_0) = c^*] + \Pr[b' = 0 \mid \mathsf{Enc}_K(m_0) \neq c^*] \cdot \Pr[\mathsf{Enc}_K(m_0) \neq c^*] \\ &= \Pr[\mathsf{Enc}_K(m_0) = c^*] + \tfrac{1}{2} \cdot (1 - \Pr[\mathsf{Enc}_K(m_0) = c^*])\end{aligned}$$

Proof of equivalence

NOT

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}\text{:}$$
$$\Pr[\mathit{Enc}_K(m) = c] = \Pr[\mathit{Enc}_K(m') = c]$$

$$\Downarrow$$

NOT

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

Pick $m_0, m_1 \in \mathcal{M}, c^* \in \mathcal{C}$ s.t. $\Pr[\mathsf{Enc}_K(m_0) = c^*] \neq \Pr[\mathsf{Enc}_K(m_1) = c^*]$

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \tfrac{1}{2} \cdot \Pr[b' = 0 \mid b = 0] + \tfrac{1}{2} \cdot \Pr[b' = 1 \mid b = 1]$$

$$\begin{aligned}
\Pr[b' = 0 \mid b = 0] &= \Pr[b' = 0 \wedge \mathsf{Enc}_K(m_0) = c^*] + \Pr[b' = 0 \wedge \mathsf{Enc}_K(m_0) \neq c^*] \\
&= \Pr[\mathsf{Enc}_K(m_0) = c^*] + \Pr[b' = 0 \mid \mathsf{Enc}_K(m_0) \neq c^*] \cdot \Pr[\mathsf{Enc}_K(m_0) \neq c^*] \\
&= \Pr[\mathsf{Enc}_K(m_0) = c^*] + \tfrac{1}{2} \cdot (1 - \Pr[\mathsf{Enc}_K(m_0) = c^*]) \\
&= \tfrac{1}{2} + \tfrac{1}{2} \Pr[\mathsf{Enc}_K(m_0) = c^*]
\end{aligned}$$

Proof of equivalence

NOT

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}\text{:}$$
$$\Pr[\mathit{Enc}_K(m) = c] = \Pr[\mathit{Enc}_K(m') = c]$$

$$\Downarrow$$

NOT

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

Pick $m_0, m_1 \in \mathcal{M}, c^* \in \mathcal{C}$ s.t. $\Pr[\mathsf{Enc}_K(m_0) = c^*] \neq \Pr[\mathsf{Enc}_K(m_1) = c^*]$

$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \frac{1}{2} \cdot \Pr[b' = 0 \mid b = 0] + \frac{1}{2} \cdot \Pr[b' = 1 \mid b = 1]$

$\Pr[b' = 0 \mid b = 0] = \frac{1}{2} + \frac{1}{2} \cdot \Pr[\mathsf{Enc}_K(m_0) = c^*]$

Proof of equivalence

NOT

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}\text{:}$$
$$\Pr[\mathit{Enc}_K(m) = c] = \Pr[\mathit{Enc}_K(m') = c]$$

$$\Downarrow$$

NOT

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

Pick $m_0, m_1 \in \mathcal{M}, c^* \in \mathcal{C}$ s.t. $\Pr[\mathsf{Enc}_K(m_0) = c^*] \neq \Pr[\mathsf{Enc}_K(m_1) = c^*]$

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \tfrac{1}{2} \cdot \Pr[b' = 0 \mid b = 0] + \tfrac{1}{2} \cdot \Pr[b' = 1 \mid b = 1]$$

$$\Pr[b' = 0 \mid b = 0] = \tfrac{1}{2} + \tfrac{1}{2} \cdot \Pr[\mathsf{Enc}_K(m_0) = c^*]$$

$$\Pr[b' = 1 \mid b = 1] = \Pr[b' = 1 \land \mathsf{Enc}_K(m_1) = c^*] + \Pr[b' = 1 \land \mathsf{Enc}_K(m_1) \neq c^*]$$

Proof of equivalence

NOT

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}\text{:}$$

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

$$\Downarrow$$

NOT

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

Pick $m_0, m_1 \in \mathcal{M}, c^* \in \mathcal{C}$ s.t. $\Pr[\mathsf{Enc}_K(m_0) = c^*] \neq \Pr[\mathsf{Enc}_K(m_1) = c^*]$

$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \frac{1}{2} \cdot \Pr[b' = 0 \mid b = 0] + \frac{1}{2} \cdot \Pr[b' = 1 \mid b = 1]$

$\Pr[b' = 0 \mid b = 0] = \frac{1}{2} + \frac{1}{2} \cdot \Pr[\mathsf{Enc}_K(m_0) = c^*]$

$\Pr[b' = 1 \mid b = 1] = \cancel{\Pr[b' = 1 \wedge \mathsf{Enc}_K(m_1) = c^*]} + \Pr[b' = 1 \wedge \mathsf{Enc}_K(m_1) \neq c^*]$

Proof of equivalence

NOT

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}:$$

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

$$\Downarrow$$

NOT

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

Pick $m_0, m_1 \in \mathcal{M}, c^* \in \mathcal{C}$ s.t. $\Pr[\mathsf{Enc}_K(m_0) = c^*] \neq \Pr[\mathsf{Enc}_K(m_1) = c^*]$

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \tfrac{1}{2} \cdot \Pr[b' = 0 \mid b = 0] + \tfrac{1}{2} \cdot \Pr[b' = 1 \mid b = 1]$$

$$\Pr[b' = 0 \mid b = 0] = \tfrac{1}{2} + \tfrac{1}{2} \cdot \Pr[\mathsf{Enc}_K(m_0) = c^*]$$

$$\Pr[b' = 1 \mid b = 1] = \cancel{\Pr[b' = 1 \wedge \mathsf{Enc}_K(m_1) = c^*]} + \Pr[b' = 1 \wedge \mathsf{Enc}_K(m_1) \neq c^*]$$

$$= \Pr[b' = 1 \mid \mathsf{Enc}_K(m_1) \neq c^*] \cdot \Pr[\mathsf{Enc}_K(m_1) \neq c^*]$$

Proof of equivalence

NOT

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}\text{:}$$

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

$$\Downarrow$$

NOT

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

Pick $m_0, m_1 \in \mathcal{M}, c^* \in \mathcal{C}$ s.t. $\Pr[\mathsf{Enc}_K(m_0) = c^*] \neq \Pr[\mathsf{Enc}_K(m_1) = c^*]$

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \tfrac{1}{2} \cdot \Pr[b' = 0 \mid b = 0] + \tfrac{1}{2} \cdot \Pr[b' = 1 \mid b = 1]$$

$$\Pr[b' = 0 \mid b = 0] = \tfrac{1}{2} + \tfrac{1}{2} \cdot \Pr[\mathsf{Enc}_K(m_0) = c^*]$$

$$\begin{aligned}\Pr[b' = 1 \mid b = 1] &= \cancel{\Pr[b' = 1 \wedge \mathsf{Enc}_K(m_1) = c^*]} + \Pr[b' = 1 \wedge \mathsf{Enc}_K(m_1) \neq c^*] \\ &= \Pr[b' = 1 \mid \mathsf{Enc}_K(m_1) \neq c^*] \cdot \Pr[\mathsf{Enc}_K(m_1) \neq c^*] \\ &= \tfrac{1}{2} \cdot \Pr[\mathsf{Enc}_K(m_1) \neq c^*]\end{aligned}$$

Proof of equivalence

NOT

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}:$$
$$\Pr[\mathit{Enc}_K(m) = c] = \Pr[\mathit{Enc}_K(m') = c]$$

$$\Downarrow$$

NOT

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

Pick $m_0, m_1 \in \mathcal{M}, c^* \in \mathcal{C}$ s.t. $\Pr[\mathsf{Enc}_K(m_0) = c^*] \neq \Pr[\mathsf{Enc}_K(m_1) = c^*]$

$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \frac{1}{2} \cdot \Pr[b' = 0 \mid b = 0] + \frac{1}{2} \cdot \Pr[b' = 1 \mid b = 1]$

$\Pr[b' = 0 \mid b = 0] = \frac{1}{2} + \frac{1}{2} \cdot \Pr[\mathsf{Enc}_K(m_0) = c^*]$

$\Pr[b' = 1 \mid b = 1] = \frac{1}{2} \cdot \Pr[\mathsf{Enc}_K(m_1) \neq c^*]$

Proof of equivalence

NOT

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}\text{:}$$
$$\Pr[\textit{Enc}_K(m) = c] = \Pr[\textit{Enc}_K(m') = c]$$

$$\Downarrow$$

NOT

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

Pick $m_0, m_1 \in \mathcal{M}, c^* \in \mathcal{C}$ s.t. $\Pr[\mathsf{Enc}_K(m_0) = c^*] \neq \Pr[\mathsf{Enc}_K(m_1) = c^*]$

$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \frac{1}{2} \cdot \Pr[b' = 0 \mid b = 0] + \frac{1}{2} \cdot \Pr[b' = 1 \mid b = 1]$

$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \frac{1}{4} + \frac{1}{4} \cdot \Pr[\mathsf{Enc}_K(m_0) = c^*] + \frac{1}{4} \cdot \Pr[\mathsf{Enc}_K(m_1) \neq c^*]$

Proof of equivalence

NOT

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}:$$
$$\Pr[\mathit{Enc}_K(m) = c] = \Pr[\mathit{Enc}_K(m') = c]$$

$$\Downarrow$$

NOT

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

Pick $m_0, m_1 \in \mathcal{M}, c^* \in \mathcal{C}$ s.t. $\Pr[\mathsf{Enc}_K(m_0) = c^*] \neq \Pr[\mathsf{Enc}_K(m_1) = c^*]$

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \tfrac{1}{2} \cdot \Pr[b' = 0 \mid b = 0] + \tfrac{1}{2} \cdot \Pr[b' = 1 \mid b = 1]$$

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \tfrac{1}{4} + \tfrac{1}{4} \cdot \Pr[\mathsf{Enc}_K(m_0) = c^*] + \tfrac{1}{4} \cdot \Pr[\mathsf{Enc}_K(m_1) \neq c^*]$$

$$\neq \tfrac{1}{4} + \tfrac{1}{4} \cdot \Pr[\mathsf{Enc}_K(m_1) = c^*] + \tfrac{1}{4} \cdot \Pr[\mathsf{Enc}_K(m_1) \neq c^*]$$

Proof of equivalence

NOT

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}\text{:}$$
$$\Pr[\mathit{Enc}_K(m) = c] = \Pr[\mathit{Enc}_K(m') = c]$$

$$\Downarrow$$

NOT

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

Pick $m_0, m_1 \in \mathcal{M}, c^* \in \mathcal{C}$ s.t. $\Pr[\mathsf{Enc}_K(m_0) = c^*] \neq \Pr[\mathsf{Enc}_K(m_1) = c^*]$

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \tfrac{1}{2} \cdot \Pr[b' = 0 \mid b = 0] + \tfrac{1}{2} \cdot \Pr[b' = 1 \mid b = 1]$$

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \tfrac{1}{4} + \tfrac{1}{4} \cdot \Pr[\mathsf{Enc}_K(m_0) = c^*] + \tfrac{1}{4} \cdot \Pr[\mathsf{Enc}_K(m_1) \neq c^*]$$

$$\neq \tfrac{1}{4} + \tfrac{1}{4} \cdot \Pr[\mathsf{Enc}_K(m_1) = c^*] + \tfrac{1}{4} \cdot \Pr[\mathsf{Enc}_K(m_1) \neq c^*]$$

Proof of equivalence

NOT

$$\forall m, m' \in \mathcal{M}, c \in \mathcal{C}\text{:}$$
$$\Pr[\mathit{Enc}_K(m) = c] = \Pr[\mathit{Enc}_K(m') = c]$$

$$\Downarrow$$

NOT

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

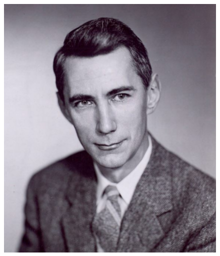
Pick $m_0, m_1 \in \mathcal{M}, c^* \in \mathcal{C}$ s.t. $\Pr[\mathsf{Enc}_K(m_0) = c^*] \neq \Pr[\mathsf{Enc}_K(m_1) = c^*]$

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \tfrac{1}{2} \cdot \Pr[b' = 0 \mid b = 0] + \tfrac{1}{2} \cdot \Pr[b' = 1 \mid b = 1]$$

$$\begin{aligned}\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] &= \tfrac{1}{4} + \tfrac{1}{4} \cdot \Pr[\mathsf{Enc}_K(m_0) = c^*] + \tfrac{1}{4} \cdot \Pr[\mathsf{Enc}_K(m_1) \neq c^*] \\ &\neq \tfrac{1}{4} + \tfrac{1}{4} \cdot \Pr[\mathsf{Enc}_K(m_1) = c^*] + \tfrac{1}{4} \cdot \Pr[\mathsf{Enc}_K(m_1) \neq c^*] \\ &= \tfrac{1}{4} + \tfrac{1}{4} = \tfrac{1}{2}\end{aligned}$$

$\square$

Recap: Equivalent definitions



Definition: *An encryption scheme* (Gen, Enc, Dec) *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** *probability distribution over* $\mathcal{M}$*,* **every** *message* $m \in \mathcal{M}$*, and* **every** *ciphertext* $c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$*:*

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

Definition: *An encryption scheme* (Gen, Enc, Dec) *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** $m, m' \in \mathcal{M}$*, and* **every** $c \in \mathcal{C}$*:*

$$\Pr[Enc_K(m) = c] = \Pr[Enc_K(m') = c]$$

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

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