Chapter 2: Perfectly-Secret Encryption
2.1 Definitions and Basic Properties

We refer to probability distributions over $\mathcal{K}$, $\mathcal{M}$, and $\mathcal{C}$.

The distribution over $\mathcal{K}$ is simply the one that is defined by running $\text{Gen}$.

We let $\Pr[K = k]$ denote the probability that the key output by $\text{Gen}$ is equal to $k$. ($K$ is a random variable.)

We let $\Pr[M = m]$ denote the probability that the message is equal to $m$. 
Definitions and Basic Properties

As an example, the adversary may know that the encrypted message is either

"attack tomorrow" or "don’t attack".

The adversary may even know (by other means) that with probability 0.7 the message will be a command to attack and with probability 0.3 the opposite. In this case, we have

\[
\Pr[M = \text{"attack tomorrow"}] = 0.7 \quad \text{and} \quad \Pr[M = \text{"don’t attack"}] = 0.3.
\]
Definitions and Basic Properties

The distributions over $K$ and $M$ are independent.

This is the case because the key is chosen and fixed (i.e., shared by the communicating parties) before the message (and its distribution) is known.

The distribution over $K$ is fixed by the encryption scheme itself (since it is defined by $Gen$)
Definitions and Basic Properties

The distribution over $M$ may vary depending on the parties who are using the cipher.

For $c \in C$, we write $\Pr[C = c]$ to denote the probability that the ciphertext $C$ be $c$.

Given the encryption algorithm $Enc$, the distribution over $C$ is fully determined by the distributions over $K$ and $M$ (and the randomness of the encryption algorithm in case it is a probabilistic algorithm).
The Definition

Intuitively, we imagine an adversary who knows the probability distribution over $M$; that is, the adversary knows the likelihood that different messages will be sent (as in the example given above).

The adversary then observes some ciphertext being sent by one party to the other.
The Definition

Ideally, observing this ciphertext should have no effect on the knowledge of the adversary.

In other words, the a posteriori likelihood that some message \( m \) was sent (even given the ciphertext that was seen) should be no different from the a priori probability that \( m \) would be sent.

This should hold for any \( m \in M \).
The Definition
Insecure
The Definition

Insecure
The Definition

Secure
The Definition

Secure
Perfect Secrecy

**DEFINITION 2.3** An encryption scheme \((\text{Gen}, \text{Enc}, \text{Dec})\) over a message space \(M\) is perfectly secret if for every probability distribution over \(M\), every message \(m \in M\), and every ciphertext \(c \in C\) for which \(\Pr[C = c] > 0\):

\[
\Pr[M = m \mid C = c] = \Pr[M = m].
\]
Another way of interpreting Definition 2.3 is that a scheme is perfectly secret if the distributions over plaintexts and ciphertexts are independent.
Perfect indistinguishability

**LEMMA 2.4** An encryption scheme \((\text{Gen}, \text{Enc}, \text{Dec})\) over a message space \(M\) is perfectly secret if and only if for every probability distribution over \(M\), for every \(m, m' \in M\), and every \(c \in C\),

\[
\Pr[\text{Enc}_K(m) = c] = \Pr[\text{Enc}_K(m') = c].
\]
Perfect indistinguishability

PROOF
We show that if the stated condition holds, then the scheme is perfectly secret; the converse is left to Exercise 2.4.

Fix a distribution over $\mathcal{M}$, a message $m$, and a ciphertext $c$ for which $\Pr[C = c] > 0$. If $\Pr[M = m] = 0$ then we trivially have

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

So, assume $\Pr[M = m] > 0$. 
Perfect indistinguishability

PROOF
Notice first that

\[ \Pr[C = c | M = m] = \Pr[\text{Enc}_K(M) = c | M = m] = \Pr[\text{Enc}_K(m) = c], \]
where the first equality is by definition of the random variable \( C \), and the second is because we condition on the event that \( M \) is equal to \( m \).

Set \( \delta_c = \text{def} \Pr[\text{Enc}_K(m) = c] = \Pr[C = c | M = m] \). If the condition of the lemma holds, then for every \( m' \in M \) we have \( \Pr[\text{Enc}_K(m') = c] = \Pr[C = c | M = m'] = \delta_c. \)
Perfect indistinguishability

Using Bayes’ Theorem, we thus have

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

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

\[ = \frac{\delta_c \cdot \Pr[M = m]}{\sum_{m' \in M} \delta_c \cdot \Pr[M = m']} \]

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

where the summation is over \( m' \in M \) with \( \Pr[M = m'] > 0 \).
Perfect indistinguishability

**PROOF**
We conclude that for every \( m \in M \) and \( c \in C \) for which
\[
\Pr[C = c] > 0,
\]
it holds that
\[
\Pr[M = m \mid C = c] = \Pr[M = m],
\]
and so the scheme is perfectly secret.
Adversarial indistinguishability.

This other definition is based on an experiment involving an adversary $A$, and formalizes $A$’s inability to distinguish the encryption of one plaintext from the encryption of another; we thus call it adversarial indistinguishability.

This definition will serve as our starting point when we introduce the notion of computational security in the next chapter.
Adversarial indistinguishability.

The experiment is defined for any encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ over message space $M$ and for any adversary $A$.

We let $\text{PrivK}_{A,\Pi}^{\text{adv}}$ denote an execution of the experiment for a given $\Pi$ and $A$. The experiment is defined as follows:
\textbf{PrivK}_{A, \Pi}^{\text{eav}}

\begin{align*}
    k & \leftarrow \text{Gen} \\
    b & \leftarrow \{0, 1\} \\
    c & \leftarrow \text{Enc}_k(m_b)
\end{align*}

\begin{align*}
    m_0, m_1 & \in M \\
    \text{c} & \\
    b = b' \ ?
\end{align*}
Adversarial indistinguishability.

$\text{PrivK}_{A, \Pi}^{eav}$:

1. Adversary $A$ outputs a pair of messages $m_0, m_1 \in M$.

2. A random key $k$ is generated by running $\text{Gen}$, and a random bit $b \leftarrow \{0, 1\}$ is chosen (by some imaginary entity that is running the experiment with $A$.) A ciphertext $c \leftarrow \text{Enc}_k(m_b)$ is computed and given to $A$.

3. $A$ outputs a bit $b'$.

4. The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise.
Adversarial indistinguishability.

We write $\text{PrivK}^\text{eav}_{A,n} = 1$ if the output is 1 and in this case we say that $A$ succeeded.

One should think of $A$ as trying to guess the value of $b$ that is chosen in the experiment, and $A$ succeeds when its guess $b'$ is correct.

The alternate definition we now give states that an encryption scheme is perfectly secret if no adversary $A$ can succeed with probability any better than $1/2$. 
PrivK_{A, Π}^{eav}

\[ k \leftarrow \text{Gen} \]
\[ b \leftarrow \{0, 1\} \]
\[ c \leftarrow \text{Enc}_k(m_b) \]

perfection\text{ly secret}

\[ \Pr[b = b'] = \frac{1}{2} \]
DEFINITION 2.5 An encryption scheme $\Pi = (\text{Gen, Enc, Dec})$ over a message space $\mathcal{M}$ is perfectly secret if for every adversary $A$ it holds that

$$\Pr[\text{PrivK}_{A,\Pi} = 1] = \frac{1}{2}.$$
Adversarial indistinguishability.

PROPOSITION 2.6 Let \((\text{Gen}, \text{Enc}, \text{Dec})\) be an encryption scheme over a message space \(M\). Then \((\text{Gen}, \text{Enc}, \text{Dec})\) is perfectly secret with respect to Definition 2.3 if and only if it is perfectly secret with respect to Definition 2.5.
3 Equivalent Formulations

**DEFINITION 2.3** An encryption scheme \((\text{Gen}, \text{Enc}, \text{Dec})\) over a message space \(M\) is perfectly secret if for every probability distribution over \(M\), every message \(m \in M\), and every ciphertext \(c \in C\) for which \(\Pr[C = c] > 0\):

\[
\Pr[M = m | C = c] = \Pr[M = m].
\]

**Lemma 2.4** An encryption scheme \((\text{Gen}, \text{Enc}, \text{Dec})\) over a message space \(M\) is perfectly secret if and only if for every probability distribution over \(M\), for every \(m, m' \in M\), and every \(c \in C\):

\[
\Pr[\text{Enc}_K(m) = c] = \Pr[\text{Enc}_K(m') = c].
\]

**Definition 2.5** An encryption scheme \(\Pi = (\text{Gen}, \text{Enc}, \text{Dec})\) over a message space \(M\) is perfectly secret if for every adversary \(A\) it holds that

\[
\Pr[\text{Priv}_{A\Pi}^\text{Sam} = 1] = \frac{1}{2}.
\]
Chapter 2: Perfectly-Secret Encryption
2.2 The One-Time Pad
(Vernam’s Cipher)

In 1917, Vernam patented a cipher now called the one-time pad. There was no proof of perfect secrecy at the time.

Rather, approximately 25 years later, Shannon introduced the notion of perfect secrecy and demonstrated that the one-time pad achieves this level of security.

The invention of the one-time pad is generally credited to Gilbert S. Vernam and Joseph O. Mauborgne. It was indeed invented 35 years earlier by a Sacramento banker named Frank Miller.
The One-Time Pad

One-time pad encryption is defined as follows:

1. Fix an integer $\ell > 0$. Then the message space $M$, key space $K$, and ciphertext space $C$ are all $\{0, 1\}^\ell$.

2. The key-generation algorithm $\text{Gen}$ works by uniformly choosing a string from $K = \{0, 1\}^\ell$. 
The One-Time Pad

Let $a \oplus b$ denote the bitwise exclusive-or (XOR) of binary strings $a$ and $b$.

1. Encryption $\text{Enc}$ : given a key $k \in \{0, 1\}^\ell$ and a message $m \in \{0, 1\}^\ell$, output $c := k \oplus m$.

2. Decryption $\text{Dec}$ : given a key $k \in \{0, 1\}^\ell$ and a ciphertext $c \in \{0, 1\}^\ell$, output $m := k \oplus c$. 
The One-Time Pad

Before discussing the security of the one-time pad, we note that $\text{Dec}_k(\text{Enc}_k(m)) = k \oplus k \oplus m = m$ (a correct encryption scheme).

Intuitively, the one-time pad is perfectly secret because given a ciphertext $c$, there is no way to know which plaintext $m$ it comes from.
The One-Time Pad

In order to see why this is true, notice that for every possible \( m \) there exists a key \( k \) such that \( c = \text{Enc}_k(m) \); namely, take \( k = m \oplus c \).

Each key is chosen with uniform probability (and hidden from the adversary) and so no key is more likely than any other.
The One-Time Pad

THEOREM 2.9 The one-time pad encryption scheme is perfectly-secret.

PROOF Fix some distribution over $M$ and fix arbitrary $m \in M$ and $c \in C$. The key observation is that for the one-time pad,

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

$$= \Pr[m \oplus K = c]$$

$$= \Pr[K = m \oplus c]$$

$$= \frac{1}{2^\ell}.$$
The One-Time Pad

Now fix any probability distribution over \( M \). For any \( c \in C \), we have

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

\[
= \sum_{m \in M} \Pr[M = m] / 2^\ell
\]

\[
= 1/2^\ell
\]

where the summation is over \( m \in M \) with \( \Pr[M=m] > 0 \).
Using Bayes’ Theorem, we thus have

\[
\Pr[M = m \mid C = c] = \frac{\Pr[C = c \mid M = m] \cdot \Pr[M = m]}{\Pr[C = c]} \cdot \frac{1}{2^\ell} \cdot \Pr[M = m] = \Pr[M = m]
\]

We conclude that the one-time pad is perfectly secret.
The One-Time Pad

Unfortunately, the one-time pad encryption scheme has a number of drawbacks.

the key is required to be as long as the message.

a long key must be securely stored,

limits applicability of the scheme if we send very long messages

As the name indicates — One-time pad is only “secure” if keys are used once.
The One-Time Pad

- In particular, say two messages $m, m'$ are encrypted using the same key $k$.

- An adversary who obtains $c = m \oplus k$ and $c' = m' \oplus k$ can compute $c \oplus c' = (m \oplus k) \oplus (m' \oplus k) = m \oplus m'$ and thus learn something about the exclusive-or of the two messages.

- If the messages correspond to English-language text, then given the exclusive-or of two sufficiently-long messages, it has been shown to be possible to perform frequency analysis and recover the messages.
2.3 Limitations of Perfect Secrecy

We prove that any perfectly-secret encryption scheme must have a key space that is at least as large as the message space.

If the key space consists of fixed-length keys, and the message space consists of all messages of some fixed length, this implies that the key must be at least as long as the message.

The other limitation regarding the fact that the key can only be used once is also inherent.
THEOREM 2.10 Let $(\text{Gen}, \text{Enc}, \text{Dec})$ be a perfectly-secret encryption scheme over a message space $M$, and let $\mathcal{K}$ be the key space as determined by $\text{Gen}$. Then $|\mathcal{K}| \geq |M|$. 
Limitations of Perfect Secrecy

PROOF

We show that if $|\mathcal{K}| < |\mathcal{M}|$ then the scheme is not perfectly secret. Assume $|\mathcal{K}| < |\mathcal{M}|$. Consider the uniform distribution over $\mathcal{M}$ and let $c \in \mathcal{C}$ be a ciphertext that occurs with non-zero probability.

Let $\mathcal{M}(c)$ be the set of all possible messages which are possible decryptions of $c$; that is

$$\mathcal{M}(c) \stackrel{\text{def}}{=} \{ m \mid m = \text{Dec}_k(c) \text{ for some } k \in \mathcal{K} \}.$$
Limitations of Perfect Secrecy

Clearly $|\mathcal{M}(c)| \leq |\mathcal{K}|$ since for each message $m \in \mathcal{M}(c)$ we can identify at least one key $k \in \mathcal{K}$ for which $m = \text{Dec}_k(c)$.

(Recall that we assume $\text{Dec}$ is deterministic.)

Under the assumption that $|\mathcal{K}| < |\mathcal{M}|$, this means that there is some $m' \in \mathcal{M}$ such that $m' \notin \mathcal{M}(c)$. But then

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

and so the scheme is not perfectly secret.
Perfect secrecy at a lower price?

The theorem shows an inherent limitation of schemes that achieve perfect secrecy.

Even so, it is often claimed by individuals and/or companies that they have developed a radically new encryption scheme that is unbreakable and achieves the security level of the one-time pad without using long keys. The above proof demonstrates that such claims cannot be true; the person claiming them either knows very little about cryptography or is blatantly lying.
2.4 Shannon’s Theorem
THEOREM 2.11 (Shannon’s theorem)
Let \((\text{Gen}, \text{Enc}, \text{Dec})\) be an encryption scheme over a message space \(M\) for which \(|M| = |\mathcal{K}| = |C|\).

The scheme is perfectly secret if and only if:

1. Every \(k \in \mathcal{K}\) is chosen with equal prob. \(= \frac{1}{|\mathcal{K}|}\) by \(\text{Gen}\).

2. For every \(m \in M\) and every \(c \in C\), there exists a unique key \(k \in \mathcal{K}\) such that \(\text{Enc}_k(m)\) outputs \(c\).
Uses of Shannon’s theorem.

Theorem 2.11 is of interest in its own right in that it essentially gives a complete characterization of perfectly-secret encryption schemes.

In addition, since items (1) and (2) have nothing to do with the probability distribution over the set of plaintexts \( M \), the theorem implies that if there exists an encryption scheme that provides perfect secrecy for a specific probability distribution over \( M \) then it actually provides perfect secrecy in general (i.e., for all probability distributions over \( M \)).
Uses of Shannon’s theorem.

Shannon’s theorem is extremely useful for proving whether a scheme is or is not perfectly secret.

Item (1) is easy to confirm and item (2) can be demonstrated (or contradicted) without analyzing any probabilities.

The perfect secrecy of the one-time pad is trivial to prove using Shannon’s theorem.

Theorem 2.11 only holds if $|M| = |K| = |C|$, and so one must be careful to apply it only in this case.
Chapter 2: Perfectly-Secret Encryption