Chapter 2

Perfectly-Secret Encryption

In the previous chapter, we presented historical encryption schemes (ciphers) and showed how they can be completely broken with very little computational effort. In this chapter, we look at the other extreme and study encryption schemes that are *provably secure* even against an adversary who has unbounded computational power. Such schemes are called *perfectly secret.* We will see under what conditions perfect secrecy can and cannot be achieved, and why this is the case.

The material in this chapter belongs, in some sense, more to the world of "classical cryptography" than to the world of "modern cryptography". Besides the fact that all the material introduced here was developed before the revolution in cryptography that took place in the mid-'70s and early-'80s, the constructions we study in this chapter rely only on the first and third principles outlined in Section 1.4. That is, precise mathematical definitions will be given and rigorous proofs will be shown, but it will not be necessary to rely on any unproven assumptions. This is clearly advantageous. We will see, however, that such an approach has inherent limitations. Thus, in addition to serving as a good basis for understanding the principles underlying modern cryptography, the results of this chapter also justify our later adoption of all three of the aforementioned principles.

In this chapter, we assume a familiarity with basic probability. The relevant notions are reviewed in Section A.3 of Appendix A.

2.1 Definitions and Basic Properties

We begin by briefly recalling some of the syntax that was introduced in the previous chapter. An encryption scheme is defined by three algorithms Gen, Enc, and Dec, as well as a specification of a message space $\mathcal{M}$ with $|\mathcal{M}| > 1$.[1] The key-generation algorithm Gen is a probabilistic algorithm that outputs a key k chosen according to some distribution. We denote by $\mathcal{K}$ the

[1] If $|\mathcal{M}| = 1$ there is only one message and there is no point in communicating, let alone encrypting.

key space, i.e., the set of all possible keys that can be output by Gen, and require $\mathcal{K}$ to be finite. The encryption algorithm Enc takes as input a key $k \in \mathcal{K}$ and a message $m \in \mathcal{M}$, and outputs a ciphertext c; we denote this by $\mathsf{Enc}_k(m)$. The encryption algorithm may be probabilistic, so that $\mathsf{Enc}_k(m)$ might output a different ciphertext when run multiple times. To emphasize this, we write $c \leftarrow \mathsf{Enc}_k(m)$ to denote the (possibly probabilistic) process by which message m is encrypted using key k to give ciphertext c. (In case Enc is deterministic, we may emphasize this by writing $c := \mathsf{Enc}_k(m)$.) We let $\mathcal{C}$ denote the set of all possible ciphertexts that can be output by $\mathsf{Enc}_k(m)$, for all possible choices of $k \in \mathcal{K}$ and $m \in \mathcal{M}$ (and for all random choices of Enc in case it is randomized). The decryption algorithm Dec takes as input a key $k \in \mathcal{K}$ and a ciphertext $c \in \mathcal{C}$ and outputs a message $m \in \mathcal{M}$. Throughout the book, we assume encryption schemes are *perfectly correct*; that is, that for all $k \in \mathcal{K}$, $m \in \mathcal{M}$, and any ciphertext c output by $\mathsf{Enc}_k(m)$, it holds that $\mathsf{Dec}_k(c) = m$ with probability 1. This implies that we may assume Dec is deterministic without loss of generality (since $\mathsf{Dec}_k(c)$ must give the same output every time it is run). We will thus write $m := \mathsf{Dec}_k(c)$ to denote the process of decrypting ciphertext c using key k.

In the definitions and theorems below, 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 Gen and taking the output. For $k \in \mathcal{K}$, we let $\Pr[K = k]$ denote the probability that the key output by Gen is equal to k. (Formally, K is a random variable denoting the value of the key.) Similarly, for $m \in \mathcal{M}$ we let $\Pr[M = m]$ denote the probability that the message that is sent is equal to m. That the message is being chosen according to some distribution (rather than being fixed) is meant to model the fact that, at least from the point of view of the adversary, different messages may have different probabilities of being sent. (If the adversary knows what message is being sent, then it doesn't need to decrypt anything and there is no need for the parties to use encryption!) As an example, the adversary may know that the encrypted message is either `attack tomorrow` or `don't attack`. Furthermore, 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 message will be a command not to attack. In this case, we have $\Pr[M = \texttt{attack tomorrow}] = 0.7$ and $\Pr[M = \texttt{don't attack}] = 0.3$.

We assume that the distributions over $\mathcal{K}$ and $\mathcal{M}$ are independent, i.e., that the key and message are chosen independently. This is required because the key is chosen and fixed (i.e., shared by the communicating parties) before the message is known. Actually, recall that the distribution over $\mathcal{K}$ is fixed by the encryption scheme itself (since it is defined by Gen) while the distribution over $\mathcal{M}$ may vary depending on the parties who are using the encryption scheme.

For $c \in \mathcal{C}$, we write $\Pr[C = c]$ to denote the probability that the ciphertext is c. Note that, given Enc, the distribution over $\mathcal{C}$ is fixed by the distributions over $\mathcal{K}$ and $\mathcal{M}$.

The actual definition. We are now ready to define the notion of perfect secrecy. Intuitively, we imagine an adversary who knows the probability distribution over $\mathcal{M}$; that is, the adversary knows the likelihood that different messages will be sent (as in the example given above). Then the adversary observes some ciphertext being sent by one party to the other. 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 $m \in \mathcal{M}$. Furthermore, this should hold even if the adversary has unbounded computational power. This means that a ciphertext reveals nothing about the underlying plaintext, and thus an adversary who intercepts a ciphertext learns absolutely nothing about the plaintext that was encrypted.

Formally:

DEFINITION 2.1 *An encryption scheme* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *over a message space* $\mathcal{M}$ *is* perfectly secret *if for every probability distribution over* $\mathcal{M}$*, every message* $m \in \mathcal{M}$*, and every ciphertext* $c \in \mathcal{C}$ *for which* $\Pr[C = c] > 0$*:*

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

(The requirement that $\Pr[C = c] > 0$ is a technical one needed to prevent conditioning on a zero-probability event.) Another way of interpreting Definition 2.1 is that a scheme is perfectly secret if the distributions over messages and ciphertexts are *independent*.

A simplifying convention. In this chapter, we are going to consider only probability distributions over $\mathcal{M}$ and $\mathcal{C}$ that assign non-zero probabilities to all $m \in \mathcal{M}$ and $c \in \mathcal{C}$.[2] This significantly simplifies the presentation because we often need to divide by $\Pr[M = m]$ or $\Pr[C = c]$, which is a problem if they may equal zero. Likewise, as in Definition 2.1 we sometimes need to condition on the event $C = c$ or $M = m$. This too is problematic if those events have zero probability.

We stress that this convention is only meant to simplify the exposition and is not a fundamental limitation. In particular all the theorems we prove can be appropriately adapted to the case of arbitrary distributions over $\mathcal{M}$ and $\mathcal{C}$ (that may assign some messages or ciphertexts probability 0). See also Exercise 2.6.

An equivalent formulation. The following lemma gives an equivalent formulation of Definition 2.1.

[2] We remark that this holds always for $k \in \mathcal{K}$ because the distribution is defined by Gen and so only keys that can be output by Gen are included in the set $\mathcal{K}$ to start with.

LEMMA 2.2 *An encryption scheme* (Gen, Enc, Dec) *over a message space* $\mathcal{M}$ *is perfectly secret if and only if for every probability distribution over* $\mathcal{M}$*, every message* $m \in \mathcal{M}$*, and every ciphertext* $c \in \mathcal{C}$*:*

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

PROOF Fix a distribution over $\mathcal{M}$ and arbitrary $m \in \mathcal{M}$ and $c \in \mathcal{C}$. Say

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

Multiplying both sides of the equation by $\Pr[M = m]/\Pr[C = c]$ gives

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

Using Bayes' theorem (see Theorem A.8), the left-hand-side is exactly equal to $\Pr[M = m \mid C = c]$. Thus, $\Pr[M = m \mid C = c] = \Pr[M = m]$ and the scheme is perfectly secret.

The other direction of the proof is left as an exercise. ■

We emphasize that in the above proof, we used the fact that both $m \in \mathcal{M}$ and $c \in \mathcal{C}$ are assigned non-zero probabilities (and thus $\Pr[M = m] > 0$ and $\Pr[C = c] > 0$, enabling us to divide by $\Pr[C = c]$ and condition on the event $M = m$). This explains our convention stated earlier, by which $\mathcal{M}$ and $\mathcal{C}$ only contain messages/ciphertexts that occur with non-zero probability.

Perfect indistinguishability. We now use Lemma 2.2 to obtain another equivalent and useful formulation of perfect secrecy. This formulation states that the probability distribution over $\mathcal{C}$ is independent of the plaintext. That is, let $\mathcal{C}(m)$ denote the distribution over the ciphertext when the message being encrypted is $m \in \mathcal{M}$ (this distribution depends on the choice of key, as well as the randomness of the encryption algorithm in case it is probabilistic). Then the claim is that for every $m_0, m_1 \in \mathcal{M}$, the distributions $\mathcal{C}(m_0)$ and $\mathcal{C}(m_1)$ are identical. This is just another way of saying that the ciphertext contains no information about the plaintext. We refer to this formulation as *perfect indistinguishability* because it implies that it is impossible to distinguish an encryption of m_0 from an encryption of m_1 (due to the fact that the distribution over the ciphertext is the same in each case).

LEMMA 2.3 *An encryption scheme* (Gen, Enc, Dec) *over a message space* $\mathcal{M}$ *is perfectly secret if and only if for every probability distribution over* $\mathcal{M}$*, every* $m_0, m_1 \in \mathcal{M}$*, and every* $c \in \mathcal{C}$*:*

$$\Pr[C = c \mid M = m_0] = \Pr[C = c \mid M = m_1].$$

PROOF Assume that the encryption scheme is perfectly secret and fix $m_0, m_1 \in \mathcal{M}$ and $c \in \mathcal{C}$. By Lemma 2.2 we have that $\Pr[C = c \mid M = m_0] = \Pr[C = c]$ and $\Pr[C = c \mid M = m_1] = \Pr[C = c]$. Thus,

$$\Pr[C = c \mid M = m_0] = \Pr[C = c] = \Pr[C = c \mid M = m_1],$$

completing the proof of the first direction.

Assume next that for every distribution over $\mathcal{M}$, every $m_0, m_1 \in \mathcal{M}$, and every $c \in \mathcal{C}$ it holds that $\Pr[C = c \mid M = m_0] = \Pr[C = c \mid M = m_1]$. Fix some distribution over $\mathcal{M}$, and arbitrary $m_0 \in \mathcal{M}$ and $c \in \mathcal{C}$. Define $\gamma \stackrel{\text{def}}{=} \Pr[C = c \mid M = m_0]$. Since $\Pr[C = c \mid M = m] = \Pr[C = c \mid M = m_0] = \gamma$ for all m, we have

$$\begin{aligned}
\Pr[C = c] &= \sum_{m \in \mathcal{M}} \Pr[C = c \mid M = m] \cdot \Pr[M = m] \\
&= \sum_{m \in \mathcal{M}} \gamma \cdot \Pr[M = m] \\
&= \gamma \cdot \sum_{m \in \mathcal{M}} \Pr[M = m] \\
&= \gamma \\
&= \Pr[C = c \mid M = m],
\end{aligned}$$

where the final equality holds for all $m \in \mathcal{M}$. So we have shown that $\Pr[C = c] = \Pr[C = c \mid M = m]$ for all $c \in \mathcal{C}$ and $m \in \mathcal{M}$. Applying Lemma 2.2, we conclude that the encryption scheme is perfectly secret. ■

Adversarial indistinguishability. We conclude this section by presenting an additional equivalent definition of perfect secrecy. This definition is based on an *experiment* involving an adversary $\mathcal{A}$ and its inability to distinguish the encryption of one plaintext from the encryption of another, and 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.

We define an experiment that we call $\mathsf{PrivK}^{\mathsf{eav}}$ since it considers the setting of private-key encryption and an eavesdropping adversary (the adversary is eavesdropping because it only receives a ciphertext c and then tries to determine something about the plaintext). The experiment is defined for any encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ over message space $\mathcal{M}$ and for any adversary $\mathcal{A}$. We let $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$ denote an execution of the experiment for a given Π and $\mathcal{A}$. The experiment is defined as follows:

The adversarial indistinguishability experiment $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$:

1. *The adversary $\mathcal{A}$ outputs a pair of messages $m_0, m_1 \in \mathcal{M}$.*

2. *A random key k is generated by running* Gen*, and a random bit $b \leftarrow \{0,1\}$ is chosen.* (*These are chosen by some imaginary entity that is running the experiment with $\mathcal{A}$.*) *Then, the ciphertext $c \leftarrow \mathsf{Enc}_k(m_b)$ is computed and given to $\mathcal{A}$.*
3. *$\mathcal{A}$ outputs a bit b'.*
4. *The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise. We write $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1$ if the output is 1 and in this case we say that $\mathcal{A}$* succeeded*.*

One should think of $\mathcal{A}$ as trying to guess the value of b that is chosen in the experiment, and $\mathcal{A}$ succeeds when its guess b' is correct. Observe that it is always possible for $\mathcal{A}$ to succeed in the experiment with probability one half by just guessing b' randomly. The question is whether it is possible for $\mathcal{A}$ to do any better than this. The alternate definition we now give states that an encryption scheme is perfectly secret if *no* adversary $\mathcal{A}$ can succeed with probability any better than one half. We stress that, as is the case throughout this chapter, there is no limitation whatsoever on the computational power of $\mathcal{A}$.

DEFINITION 2.4 (perfect secrecy — alternative definition): *An encryption scheme* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *over a message space $\mathcal{M}$ is* perfectly secret *if for every adversary $\mathcal{A}$ it holds that*

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

The following proposition states that Definition 2.4 is equivalent to Definition 2.1. We leave the proof of the proposition as an exercise.

PROPOSITION 2.5 *Let* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *be an encryption scheme over a message space $\mathcal{M}$. Then,* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is perfectly secret with respect to Definition 2.1 if and only if it is perfectly secret with respect to Definition 2.4.*

2.2 The One-Time Pad (Vernam's Cipher)

In 1917, Vernam patented a cipher that obtains perfect secrecy. There was no proof of this fact at the time (in fact, there was not yet a notion of what perfect secrecy was). Rather, approximately 25 years later, Shannon introduced the notion of perfect secrecy and demonstrated that the one-time pad (sometimes known as Vernam's cipher) achieves this level of security.

Let $a \oplus b$ denote the *bitwise exclusive-or* (XOR) of two binary strings a and b (i.e., if $a = a_1, \ldots, a_\ell$ and $b = b_1, \ldots, b_\ell$, then $a \oplus b = a_1 \oplus b_1, \ldots, a_\ell \oplus b_\ell$). The one-time pad encryption scheme is defined as follows:

1. Fix an integer $\ell > 0$. Then the message space $\mathcal{M}$, key space $\mathcal{K}$, and ciphertext space $\mathcal{C}$ are all equal to $\{0,1\}^\ell$ (i.e., the set of all binary strings of length ℓ).

2. The key-generation algorithm Gen works by choosing a string from $\mathcal{K} = \{0,1\}^\ell$ according to the uniform distribution (i.e., each of the 2^ℓ strings in the space is chosen as the key with probability exactly $2^{-\ell}$).

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

4. Decryption Dec works as follows: given a key $k \in \{0,1\}^\ell$ and a ciphertext $c \in \{0,1\}^\ell$, output $m := k \oplus c$.

Before discussing the security of the one-time pad, we note that for every k and every m it holds that $\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = k \oplus k \oplus m = m$ and so the one-time pad constitutes a legal encryption scheme.

Intuitively, the one-time pad is perfectly secret because given a ciphertext c, there is no way an adversary can know which plaintext m it originated from. In order to see why this is true, notice that for every possible m there exists a key k such that $c = \mathsf{Enc}_k(m)$; namely, take $k = m \oplus c$. Furthermore, each key is chosen with uniform probability and so no key is more likely than any other. Combining the above, we obtain that c reveals nothing whatsoever about which plaintext m was encrypted, because every plaintext is equally likely to have been encrypted (of course, this is true as long as k is completely hidden from the adversary). We now prove this intuition formally:

THEOREM 2.6 *The one-time pad is a perfectly-secret encryption scheme.*

PROOF We work directly with the original definition of perfect secrecy (Definition 2.1), though with our convention that all messages occur with non-zero probability. (For the one-time pad, this implies that all ciphertexts occur with non-zero probability.) Fix some distribution over $\mathcal{M}$ and arbitrary $m_0 \in \mathcal{M}$ and $c \in \mathcal{C}$. The key observation is that, for every $m \in \mathcal{M}$,

$$\begin{aligned}\Pr[C = c \mid M = m] &= \Pr[M \oplus K = c \mid M = m] \\ &= \Pr[m \oplus K = c] = \Pr[K = m \oplus c] = 2^{-\ell}.\end{aligned}$$

A simple calculation (using Bayes' theorem for the first equality) then gives

$$\begin{aligned}
\Pr[M = m_0 \mid C = c] &= \frac{\Pr[M = m_0 \wedge C = c]}{\Pr[C = c]} \\
&= \frac{\Pr[C = c \mid M = m_0] \cdot \Pr[M = m_0]}{\sum_{m \in \mathcal{M}} \Pr[C = c \mid M = m] \cdot \Pr[M = m]} \\
&= \frac{2^{-\ell} \cdot \Pr[M = m_0]}{\sum_{m \in \mathcal{M}} 2^{-\ell} \cdot \Pr[M = m]} \\
&= \frac{\Pr[M = m_0]}{\sum_{m \in \mathcal{M}} \Pr[M = m]} \;=\; \Pr[M = m_0]\,,
\end{aligned}$$

as required by Definition 2.1. ■

We conclude that perfect secrecy is attainable. Unfortunately, the one-time pad encryption scheme has a number of drawbacks. Most prominent is that *the key is required to be as long as the message*. This limits applicability of the scheme if we want to send very long messages (as it may be difficult to securely store a very long key) or if we don't know in advance an upper bound on how long the message will be (since we can't share a key of unbounded length). Moreover, the one-time pad scheme — as the name indicates — *is only "secure" if used once (with the same key)*. Although we did not yet define a notion of security when multiple messages are encrypted, it is easy to see informally that encrypting more than one message leaks a lot of information. 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

$$c \oplus c' = m \oplus m'$$

and thus learn something about the exclusive-or of the two messages. While this may not seem very significant, it is enough to rule out any claims of perfect secrecy when encrypting two messages. Furthermore, if the messages correspond to English-language text, then given the exclusive-or of sufficiently-many message pairs it is possible to perform frequency analysis (as in the previous chapter, though more complex) and recover the messages themselves.

Finally, the one-time pad encryption scheme is *only secure against a ciphertext-only attack*. Although we have again not yet defined security against stronger attacks, it is easy to see that the one-time pad scheme is insecure against, e.g., a known-message attack. An adversary who obtains the encryption c of a known message m can compute the key $k = c \oplus m$ and then decrypt any subsequent ciphertexts computed using this same key.

2.3 Limitations of Perfect Secrecy

In this section, we show that one of the aforementioned limitations of the one-time pad encryption scheme is *inherent*. Specifically, 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. Thus, the problem of a large key length is not specific to the one-time pad, but is inherent to any scheme achieving perfect secrecy. (The other limitations mentioned above are also inherent in the context of perfect secrecy; see, e.g., Exercise 2.9.)

THEOREM 2.7 *Let* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *be a perfectly-secret encryption scheme over a message space* $\mathcal{M}$*, and let* $\mathcal{K}$ *be the key space as determined by* Gen*. Then* $|\mathcal{K}| \geq |\mathcal{M}|$*.*

PROOF We show that if $|\mathcal{K}| < |\mathcal{M}|$ then the scheme is not perfectly secret. Assume $|\mathcal{K}| < |\mathcal{M}|$. Take the uniform distribution over $\mathcal{M}$ and let $m \in \mathcal{M}$ be arbitrary. Let c be a ciphertext that corresponds to a possible encryption of m; i.e., there exists a $k \in \mathcal{K}$ such that $\mathsf{Enc}_k(m) = c$. (If Enc is randomized, this means there is some non-zero probability that $\mathsf{Enc}_k(m)$ outputs c.) By correctness, we know that $\mathsf{Dec}_k(c) = m$.

Consider the set $\mathcal{M}(c)$ of all possible messages that correspond to c; that is

$$\mathcal{M}(c) \overset{\text{def}}{=} \{\hat{m} \mid \hat{m} = \mathsf{Dec}_{\hat{k}}(c) \text{ for some } \hat{k} \in \mathcal{K}\}.$$

We know that $m \in \mathcal{M}(c)$. Furthermore, $|\mathcal{M}(c)| \leq |\mathcal{K}|$ since for each message $\hat{m} \in \mathcal{M}(c)$ we can identify at least one key $\hat{k} \in \mathcal{K}$ for which $\hat{m} = \mathsf{Dec}_{\hat{k}}(c)$. (Recall that we assume Dec is deterministic.) This means there is some $m' \in \mathcal{M}$ with $m' \neq m$ 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 above 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

In his breakthrough work on perfect secrecy, Shannon also provided a characterization of perfectly-secret encryption schemes. As we shall see below, this characterization says that, assuming $|\mathcal{K}| = |\mathcal{M}| = |\mathcal{C}|$, the key-generation algorithm Gen must choose a secret key *uniformly* from the set of all possible keys (as in the one-time pad), and that for every plaintext message and ciphertext there exists a *single* key mapping the plaintext to the ciphertext (again, as in the one-time pad). Beyond being interesting in its own right, this theorem is a powerful tool for proving (or contradicting) the perfect secrecy of suggested schemes. We discuss this further below after the proof.

As before, we assume that the probability distributions over $\mathcal{M}$ and $\mathcal{C}$ are such that all $m \in \mathcal{M}$ and $c \in \mathcal{C}$ are assigned non-zero probabilities. The theorem here considers the special case when $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$, meaning that the sets of plaintexts, keys, and ciphertexts are all of the same size. We have already seen that $|\mathcal{K}| \geq |\mathcal{M}|$. It is easy to see that $|\mathcal{C}|$ must also be at least the size of $|\mathcal{M}|$ (because otherwise for every key, there must be two plaintexts that are mapped to a single ciphertext, making it impossible to unambiguously decrypt). Therefore, in some sense, the case of $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$ is the "most efficient". We are now ready to state the theorem:

THEOREM 2.8 (Shannon's theorem) *Let* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *be an encryption scheme over a message space* $\mathcal{M}$ *for which* $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$*. This scheme is perfectly secret if and only if:*

1. *Every key* $k \in \mathcal{K}$ *is chosen with equal probability* $1/|\mathcal{K}|$ *by algorithm* Gen.
2. *For every* $m \in \mathcal{M}$ *and every* $c \in \mathcal{C}$*, there exists a single key* $k \in \mathcal{K}$ *such that* $\mathsf{Enc}_k(m)$ *outputs* c.

PROOF The intuition behind the proof of this theorem is as follows. First, if a scheme fulfills item (2) then a given ciphertext c could be the result of encrypting any possible plaintext m (this holds because for every m there exists a key k mapping it to c). Combining this with the fact that exactly one key maps each m to c, and by item (1) each key is chosen with the same probability, perfect secrecy can be shown as in the case of the one-time pad. For the other direction, the intuition is that if $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$ then there must be exactly one key mapping each m to each c. (Otherwise, either some m is not mapped to a given c contradicting perfect secrecy, or some m is mapped by more than one key to c, resulting in another m' not being mapped to c again contradicting perfect secrecy.) Once this fact is given, it must hold that each key is chosen with equal probability or some plaintexts would be more likely than others, contradicting perfect secrecy. The formal proof follows.

Let $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme over $\mathcal{M}$ where $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$. For simplicity, we assume Enc is deterministic. We first prove that if $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is perfectly secret, then items (1) and (2) hold. As in the proof of Theorem 2.7, it is not hard to see that for every $m \in \mathcal{M}$ and $c \in \mathcal{C}$, there exists *at least one* key $k \in \mathcal{K}$ such that $\mathsf{Enc}_k(m) = c$. (Otherwise, $\Pr[M = m \mid C = c] = 0 \neq \Pr[M = m]$.) For a fixed m, consider now the set $\{\mathsf{Enc}_k(m)\}_{k \in \mathcal{K}}$. By the above, $|\{\mathsf{Enc}_k(m)\}_{k \in \mathcal{K}}| \geq |\mathcal{C}|$ (because for every $c \in \mathcal{C}$ there exists a $k \in \mathcal{K}$ such that $\mathsf{Enc}_k(m) = c$). In addition, since $\mathsf{Enc}_k(m) \in \mathcal{C}$ we trivially have $|\{\mathsf{Enc}_k(m)\}_{k \in \mathcal{K}}| \leq |\mathcal{C}|$. We conclude that

$$|\{\mathsf{Enc}_k(m)\}_{k \in \mathcal{K}}| = |\mathcal{C}|.$$

Since $|\mathcal{K}| = |\mathcal{C}|$, it follows that $|\{\mathsf{Enc}_k(m)\}_{k \in \mathcal{K}}| = |\mathcal{K}|$. This implies that for every m and c, there do not exist distinct keys $k_1, k_2 \in \mathcal{K}$ with $\mathsf{Enc}_{k_1}(m) = \mathsf{Enc}_{k_2}(m) = c$. That is, for every m and c, there exists *at most* one key $k \in \mathcal{K}$ such that $\mathsf{Enc}_k(m) = c$. Combining the above (i.e., the existence of at least one key and at most one key), we obtain item (2).

We proceed to show that for every $k \in \mathcal{K}$, $\Pr[\mathcal{K} = k] = 1/|\mathcal{K}|$. Let $n = |\mathcal{K}|$ and $\mathcal{M} = \{m_1, \ldots, m_n\}$ (recall, $|\mathcal{M}| = |\mathcal{K}| = n$), and *fix* a ciphertext c. Then, we can label the keys $k_1, \ldots, k_n$ such that for every i $(1 \leq i \leq n)$ it holds that $\mathsf{Enc}_{k_i}(m_i) = c$. This labeling can be carried out because (as just shown) for every c and m_i there exists a *unique* k such that $\mathsf{Enc}_k(m_i) = c$, and furthermore these keys are distinct for distinct m_i, m_j. By perfect secrecy we have that for every i:

$$\begin{aligned}\Pr[M = m_i] &= \Pr[M = m_i \mid C = c] \\ &= \frac{\Pr[C = c \mid M = m_i] \cdot \Pr[M = m_i]}{\Pr[C = c]} \\ &= \frac{\Pr[K = k_i] \cdot \Pr[M = m_i]}{\Pr[C = c]},\end{aligned}$$

where the second equality is by Bayes' theorem and the third equality holds by the labelling above (i.e., k_i is the unique key that maps m_i to c). From the above, it follows that for every i,

$$\Pr[K = k_i] = \Pr[C = c].$$

Therefore, for every i and j, $\Pr[K = k_i] = \Pr[C = c] = \Pr[K = k_j]$ and so all keys are chosen with the same probability. We conclude that keys are chosen according to the uniform distribution, and $\Pr[\mathcal{K} = k_i] = 1/|\mathcal{K}|$ as required.

We now prove the other direction of the theorem. Assume that every key is obtained with probability $1/|\mathcal{K}|$ and that for every $m \in \mathcal{M}$ and $c \in \mathcal{C}$ there exists a single key $k \in \mathcal{K}$ such that $\mathsf{Enc}_k(m) = c$. This immediately implies that for every m and c,

$$\Pr[C = c \mid M = m] = \frac{1}{|\mathcal{K}|}$$

irrespective of the probability distribution over $\mathcal{M}$. Thus, for every probability distribution over $\mathcal{M}$, every $m, m' \in \mathcal{M}$, and every $c \in \mathcal{C}$ we have

$$\Pr[\mathcal{C} = c \mid \mathcal{M} = m] = \frac{1}{|\mathcal{K}|} = \Pr[\mathcal{C} = c \mid \mathcal{M} = m']$$

and so by Lemma 2.3, the encryption scheme is perfectly secret. ■

Uses of Shannon's theorem. Theorem 2.8 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 $\mathcal{M}$, the theorem implies that if there exists an encryption scheme that provides perfect secrecy for a specific probability distribution over $\mathcal{M}$ then it actually provides perfect secrecy in general (i.e., for all probability distributions over $\mathcal{M}$). Finally, Shannon's theorem is extremely useful for proving whether a given 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 (in contrast to working with, say, Definition 2.1). For example, the perfect secrecy of the one-time pad (Theorem 2.6) is trivial to prove using Shannon's theorem. We warn, however, that Theorem 2.8 only holds if $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$, and so one must careful to apply it only in this case.

2.5 Summary

This completes our treatment of perfectly-secret encryption. The main lesson of this chapter is that *perfect secrecy is attainable*, meaning that there exist encryption schemes with the property that the ciphertext reveals absolutely nothing about the plaintext even to an adversary with unlimited computational power. However, all such schemes have the limitation that the key must be at least as long as the message. In practice, therefore perfectly-secret encryption is rarely used. We remark that it is rumored that the "red phone" linking the White House and the Kremlin during the Cold War was protected using one-time pad encryption. Of course, the governments of the US and USSR could exchange extremely long random keys without great difficulty, and therefore practically use the one-time pad. However, in most settings (especially commercial ones), the limitation regarding the key length makes the one-time pad or any other perfectly-secret scheme unusable.

References and Additional Reading

The notion of perfectly-secret encryption was introduced and studied in ground-breaking work by Shannon [113]. In addition to introducing the notion, he proved that the one-time pad (originally introduced by Vernam [126]) is perfectly secret, and also proved the theorems characterizing perfectly-secret schemes (and their implied limitations). Stinson [124] contains further discussion of perfect secrecy.

In this chapter we have briefly studied perfectly-secure *encryption.* There are other cryptographic problems that can also be solved with "perfect security". A notable example is the problem of message authentication where the aim is to prevent an adversary from modifying a message (in an undetectable manner) en route from one party to another; we study this problem in depth in Chapter 4. The reader interested in learning about perfectly-secure message authentication is referred to the paper by Stinson [122], the survey by Simmons [120], or the first edition of Stinson's textbook [123, Chapter 10] for further information.

Exercises

2.1 Prove the second direction of Lemma 2.2.

2.2 Prove or refute: For every encryption scheme that is perfectly secret it holds that for every distribution over the message space $\mathcal{M}$, every $m, m' \in \mathcal{M}$, and every $c \in \mathcal{C}$:

$$\Pr[\mathcal{M} = m \mid \mathcal{C} = c] = \Pr[\mathcal{M} = m' \mid \mathcal{C} = c].$$

2.3 When using the one-time pad (Vernam's cipher) with the key $k = 0^\ell$, it follows that $\mathsf{Enc}_k(m) = k \oplus m = m$ and the message is effectively sent in the clear! It has therefore been suggested to improve the one-time pad by only encrypting with a key $k \neq 0^\ell$ (i.e., to have Gen choose k uniformly at random from the set of *non-zero* keys of length ℓ). Is this an improvement? In particular, is it still perfectly secret? Prove your answer. If your answer is positive, explain why the one-time pad is not described in this way. If your answer is negative, reconcile this fact with the fact that encrypting with 0^ℓ doesn't change the plaintext.

2.4 In this exercise, we study conditions under which the shift, mono-alphabetic substitution, and Vigenére ciphers are perfectly secret:

(a) Prove that if only a single character is encrypted, then the shift cipher is perfectly secret.

(b) Describe the largest plaintext space $\mathcal{M}$ for which the mono-alphabetic substitution cipher provides perfect secrecy. (Note: this space does not need to contain words that "make sense".)

(c) Show how to use the Vigenére cipher to encrypt any word of length n so that perfect secrecy is obtained (note: you can choose the length of the key). Prove your answer.

Reconcile the above with the attacks that were shown in the previous chapter.

2.5 Prove or refute: Every encryption scheme for which the size of the key space equals the size of the message space, and for which the key is chosen uniformly from the key space, is perfectly secret.

2.6 Prove that if an encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is perfectly secret for a message space $\mathcal{M}$ assuming all messages in $\mathcal{M}$ are assigned non-zero probability, then it is perfectly secret for any message space $\mathcal{M}' \subset \mathcal{M}$.

Hint: Use Shannon's theorem.

2.7 Prove the first direction of Proposition 2.5. That is, prove that Definition 2.1 implies Definition 2.4.

Hint: Use Exercise 2.6 to argue that perfect secrecy holds for the uniform distribution over any two plaintexts (and in particular, the two messages output by $\mathcal{A}$ in the experiment). Then apply Lemma 2.3.

2.8 Prove the second direction of Proposition 2.5. That is, prove that Definition 2.4 implies Definition 2.1.

Hint: If a scheme Π is not perfectly secret with respect to Definition 2.1, then Lemma 2.3 shows that there exist messages $m_0, m_1 \in \mathcal{M}$ and $c \in \mathcal{C}$ for which $\Pr[C = c \mid M = m_0] \neq \Pr[C = c \mid M = m_1]$. Use these m_0 and m_1 to construct an $\mathcal{A}$ for which $\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] > \frac{1}{2}$.

2.9 Consider the following definition of perfect secrecy for the encryption of *two* messages. An encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ over a message space $\mathcal{M}$ is *perfectly-secret for two messages* if for all distributions over $\mathcal{M}$, all $m, m' \in \mathcal{M}$, and all $c, c' \in \mathcal{C}$ with $\Pr[C = c \wedge C' = c] > 0$:

$$\Pr\left[M = m \wedge M' = m' \mid C = c \wedge C' = c'\right] = \Pr[M = m \wedge M' = m'],$$

where m and m' are sampled independently from the same distribution over $\mathcal{M}$. Prove that *no* encryption scheme satisfies this definition.

Hint: Take $m \neq m'$ but $c = c'$.

2.10 Consider the following definition of perfect secrecy for the encryption of two messages. Encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ over a message space $\mathcal{M}$ is *perfectly-secret for two messages* if for all distributions over $\mathcal{M}$, all $m, m' \in \mathcal{M}$ with $m \neq m'$, and all $c, c' \in \mathcal{C}$ with $c \neq c'$ and $\Pr[C = c \wedge C' = c] > 0$:

$$\begin{aligned}\Pr[M = m \wedge M' = m' \mid C = c \wedge C' = c'] \\ = \Pr[M = m \wedge M' = m' \mid M \neq M'],\end{aligned}$$

where m and m' are sampled independently from the same distribution over $\mathcal{M}$. Show an encryption scheme that provably satisfies this definition. How long are the keys compared to the length of a message?

2.11 Say we require only that an encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ over a message space $\mathcal{M}$ satisfy the following: for all $m \in \mathcal{M}$, the probability that $\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m$ is at least 2^{-t}. (This probability is taken over choice of k as well as any randomness that may be used during encryption or decryption.) Show that perfect secrecy (as in Definition 2.1) can be achieved with $|\mathcal{K}| < |\mathcal{M}|$.

2.12 Prove an analogue of Theorem 2.7 for the case of "almost perfect" secrecy. That is, let $\varepsilon < 1$ be a constant and say we only require that for any distribution over $\mathcal{M}$, any $m \in \mathcal{M}$, and any $c \in \mathcal{C}$;

$$|\Pr[M = m \mid C = c] - \Pr[M = m]| < \varepsilon.$$

Prove a lower bound on the size of the key space $\mathcal{K}$ relative to $\mathcal{M}$ for any encryption scheme that meets this definition.

Hint: Consider the uniform distribution over $\mathcal{M}$ and fix a ciphertext c. Then show that for a $(1-\varepsilon)$ fraction of the messages $m \in \mathcal{M}$, there must exist a key mapping m to c.