Cryptography 101: The Shannon's Theorem

ComCom X • 9 Feb 2026

Let $\mathcal{M}, \mathcal{K}$ and $\mathcal{C}$ be the spaces of messages, keys, and ciphertexts, respectively.

Definition 1 (Encryption scheme)**.** *An encryption scheme is a triple* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *where*

- $\mathsf{KeyGen}()$ *outputs a key* $k \in \mathcal{K}$
- $\mathsf{Enc}(k, m)$ *outputs a ciphertext* $c \in \mathcal{C}$ *given a key* $k \in \mathcal{K}$ *and a message* $m \in \mathcal{M}$
- $\mathsf{Dec}(k, c)$ *outputs a message* $\hat{m} \in \mathcal{M}$ *given a key* $k \in \mathcal{K}$ *and a ciphertext* $c \in \mathcal{C}$*.*

Definition 2 (Correctness)**.** *An encryption scheme is said to be correct if for any* $m \in \mathcal{M}$*,*

$$\Pr_{k \leftarrow \mathsf{KeyGen}()}[\mathsf{Dec}(k, \mathsf{Enc}(k, m)) = m] = 1.$$

Definition 3 (Perfect indistinguishability)**.** *Let* $C(m)$ *be a random variable over* $\mathcal{C}$ *corresponding to* Enc*. An encryption scheme is said to be perfect indistinguishable if for any* $m_0, m_1 \in \mathcal{M}$ *and* $c \in \mathcal{C}$*, we have*

$$\Pr[C(m_0) = c] = \Pr[C(m_1) = c].$$

Definition 4 (One-time pad encryption scheme)**.** *Let* $\mathcal{M}, \mathcal{K}$ *and* $\mathcal{C}$ *all be* $\{0,1\}^n$ *for some* $n \in \mathbb{N}$*. The one-time pad encryption scheme is defined as:*

- $\mathsf{KeyGen}()$*: sample* k *uniformly from* $\{0,1\}^n$
- $\mathsf{Enc}(k, m)$*: output* $k \oplus m$
- $\mathsf{Dec}(k, c)$*: output* $k \oplus c$*.*

Theorem 5 (One-time pad)**.** *The one-time pad encryption scheme satisfies both correctness and perfect indistinguishability.*

Proof. Correctness: for any $k \in \mathcal{K}$, we have

$$\mathsf{Dec}(k, \mathsf{Enc}(k, m)) = \mathsf{Dec}(k, k \oplus m) = k \oplus m \oplus k = m.$$

Perfect indistinguishability: for any k, m and c, we have

$$\begin{aligned} \Pr[\mathsf{Enc}(k, m) = c] &= \Pr[k \oplus m = c] \\ &= \Pr[k \oplus m \oplus m = c \oplus m] \\ &= \Pr[k = c \oplus m] \\ &= \frac{1}{2^n}. \end{aligned}$$

□

Theorem 6 (Shannon's theorem, 1949)**.** *In any encryption scheme that satisfies both correctness and perfect indistinguishability, it is necessarily that* $|\mathcal{K}| \geq \mathcal{M}$*.*

Proof. Assume for contradiction that there exists an encryption scheme that satisfies both correctness and perfect indistinguishability with $|\mathcal{K}| < |\mathcal{M}|$. Consider a message $m_0 \in \mathcal{M}$, a key $k_0 \in \mathcal{K}$, and $c = \mathsf{Enc}(k_0, m_0)$. Due to the correctness, there is exactly one message in $\mathcal{M}$ that is mapped to c by the key k_0. Therefore, there are at most $|\mathcal{K}|$ messages that can be mapped to c by any key $k \in \mathcal{K}$. This means that there exists a message $m_1 \in \mathcal{M}$ that is not mapped to c by any key $k \in \mathcal{K}$, i.e., $\Pr_{k \leftarrow \mathsf{GenKey}()}[\mathsf{Enc}(k, m_1) = c] = 0$. Since we know that $c = \mathsf{Enc}(k_0, m_0)$, we have $\Pr_{k \leftarrow \mathsf{GenKey}()}[\mathsf{Enc}(k, m_0) = c] > 0$, which contradicts the perfect indistinguishability. □