Unconditional (Information-theoretical)	*Conditional (Computational)*

... security

Unconditional (Information-theoretical)

Provides security against an adversary with ***no restrictions***

(e.g., unlimited computing power, time, memory)

- (+) Stands against brute force
- (−) Good in theory, poor in practice

For all m possible plaintext (i.e., in $\mathcal{M}$) and any c ciphertext (i.e., in $\mathcal{C}$) such that $Pr[C=c]>0$, it holds:

$$Pr[M=m|C=c] = Pr[M=m]$$

Perfect secrecy (Shannon 1949)

For all m_0, m_1 plaintexts of the same length (i.e., $|m_0| = |m_1|$) and for all c ciphertext, it holds:

$$Pr[Enc(k,m_0) =c] = Pr[Enc(k,m_1)=c]$$

where the key k is randomly chosen in the key space $\mathcal{K}$

Theorem (limitation):

Let (Enc, Dec) be a perfectly-secret encryption scheme over a plaintext space $\mathcal{M}$ and a key space $\mathcal{K}$. Then it holds that $|\mathcal{K}| \geqslant |\mathcal{M}|$ (i.e., the length of the key is larger or equal to the length of the message).

Conditional (Computational)

Provides security against an adversary with ***computational restrictions***

(e.g., limited computing power, time, memory)

- (+) Suitable for practice
- (−) Weaker than unconditional security

A scheme is **secure** if any adversary $\mathcal{A}$ that runs the attack in a time t succeeds the attack with probability at most ε.

Time t, probability ε can be:

- *Fixed*
- *Functions of a security parameter: n*

PPT(Probabilistic Polynomial in Time) Adversary:

- $t(n)$ is **polynomial** in n
- $\varepsilon(n)$ is **negligible** in n:

$$\forall p(n),\ \exists\, n_d \text{ such that } \forall n \geqslant n_d \text{ it holds } \varepsilon(n) < 1/p(n)$$

$$p(n) = n^d \text{ and } d \text{ constant}$$