Information Security Definitions

Cryptography

Perfect Secrecy Encryption scheme is perfectly secret if either:

1. For random M, C and every $m \in M$, $c \in C$ it holds that $P(M = m) = P(M = m\bar{C} = c)$.
2. For M, C, we have that M and C are independent.
3. For every m_0, m_1, we have that $Enc(K, m_0)$ and $Enc(K, m_1)$ have the same distribution.

(Shannon's Theorem) In every perfectly secret encryption scheme, $|K| \geq |M|$.

Semantically Secure / CPA-Secure / IND-CPA In a learning phase, an adversary chooses $m'_0, \cdots, m'_t$ and receives $c'_0, \cdots, c'_t$ from the oracle.

In a challenge phase, the adversary chooses m_0, m_1 and the oracle returns $c = Enc(k, m_b)$.

The encryption is CPA-secure if every randomized poly-time adversary guesses b correctly with probability at most $0.5 + \epsilon(n)$, where ϵ is negligible.

(Observation) Every CPA-secure encryption has to be randomized or have a state.

Security Properties

Confidentiality No improper disclosure of information.

Integrity No improper modification of information.

Availability No improper impairment of functionality/service.

Authenticity Message originated from correct actor.

Non-Repudiation / Accountability Responsibility for actions can be established.

Hash Functions

Collision Resistant

Preimage Resistant Given y, it is infeasible to find x such that $H(x) = y$.

Second Preimage Resistant Given x, it is infeasible to find $x \neq x'$ such that $H(x) = H(x')$.

Commitments

Perfectly Hiding

Perfectly Binding

Authentication

Weak Agreement

- b has been running the protocol believing to be communication with a.

Non-Injective Agreement

- Weak agreement is satisfied.
- a and b agree on the contents of all the messages exchanged.

Injective Agreement

- Non-injective agreement is satisfied.
- Each run of A corresponds to a unique run of B.