Hash Functions

One major drawback of plain RSA is that the document itself is the signature. How can we separate the signature from the document? For this purpose, **hash functions** are introduced.

Characteristics of Hash Functions (requirements)

- **Fixed-length output**: These are special functions that, given a variable-length input, produce a fixed-length output.

- **Pre-image resistance**: It is difficult to find an input x that matches a given hash output y, where $y = H(x)$.

- **Collision resistance**: It is hard to find two different inputs x and x' such that $H(x) = H(x')$ (i.e., both inputs produce the same hash code).

- **Efficiency**: Despite the complexity, $H(x)$ should be easy to compute.

- **Avalanche effect**: Even a small change in the input (such as flipping just one bit) should result in a significant and unpredictable change in the output, ideally altering about half of the output bits.

Well-known Hash Functions

- **SHA-1**

- **MD2**

- **MD5** (Message Digest 5)

Hash functions play a crucial role in cryptography by allowing us to generate a fixed-size “fingerprint” or “digest” of a document. This makes it possible to sign the hash of the document instead of the entire document itself, making digital signatures more efficient.