Asymmetric Ciphers

CLASSICAL ENCRYPTION TECHNIQUES

Asymmetric Encryption

Asymmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the different keys—one a public key and one a private key. It is also known as public-key encryption

Asymmetric encryption transforms plaintext into ciphertext using a one of two keys and an encryption algorithm. Using the paired key and a decryption algorithm, the plaintext is recovered from the ciphertext

Asymmetric encryption can be used for confidentiality, authentication or both

The most widely used public-key cryptosystem is RSA. The difficulty of attacking RSA is based on the difficulty of finding the prime factors of a composite numbercan be used for confidentiality, authentication or both

Asymmetric Encryption

The security of any encryption scheme depends on the length of the key and the computational work involved in breaking a cipher

- Not dependent whether it is symmetric or asymmetric

Public-key encryption will not make symmetric encryption obsolete.

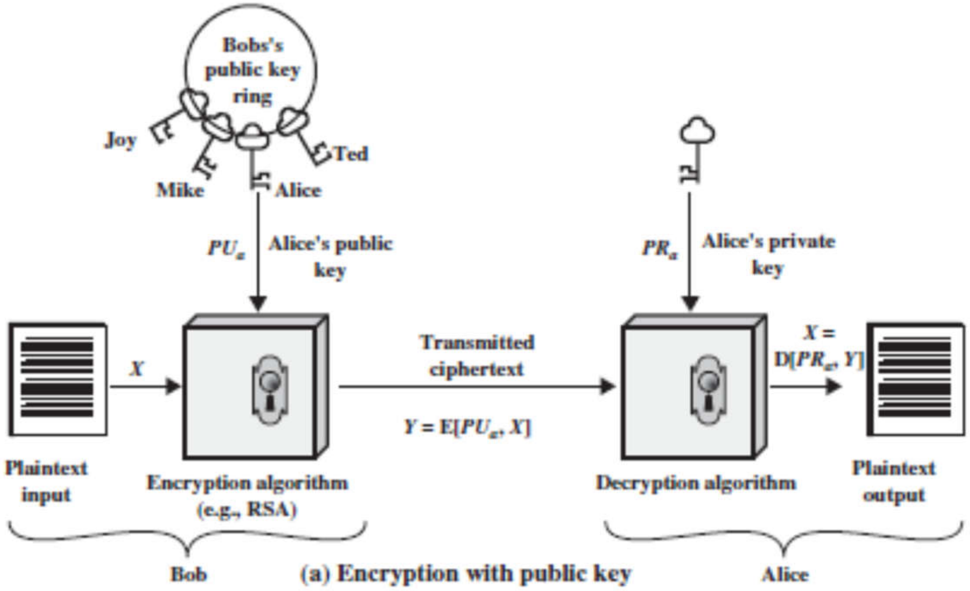
The procedures involved in distributing keys for asymmetric encryption are not simpler nor any more efficient than those required for symmetric encryption

Public-key Cryptosystem

It is computationally infeasible to determine the decryption key given only knowledge of the cryptographic algorithm and the encryption key

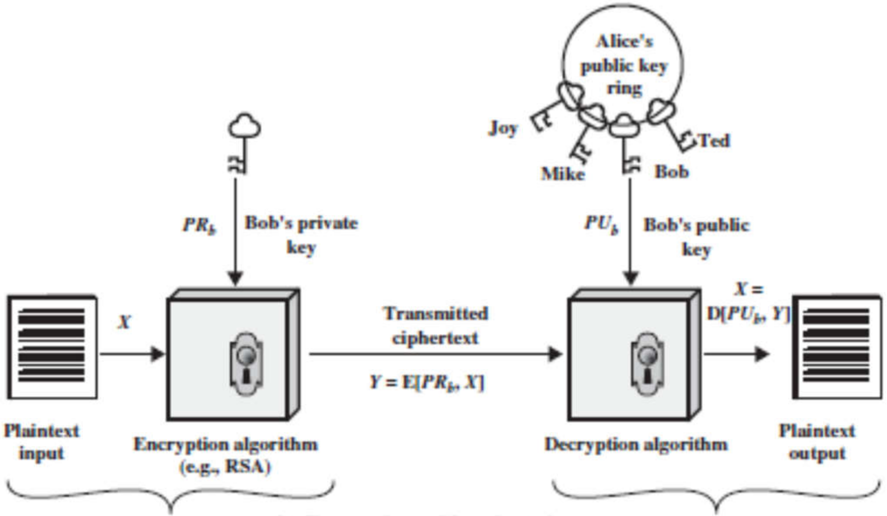
Either of the two related keys can be used for encryption, with the other used for decryption (True for some algorithm like RSA)

Public-key Cryptosystem



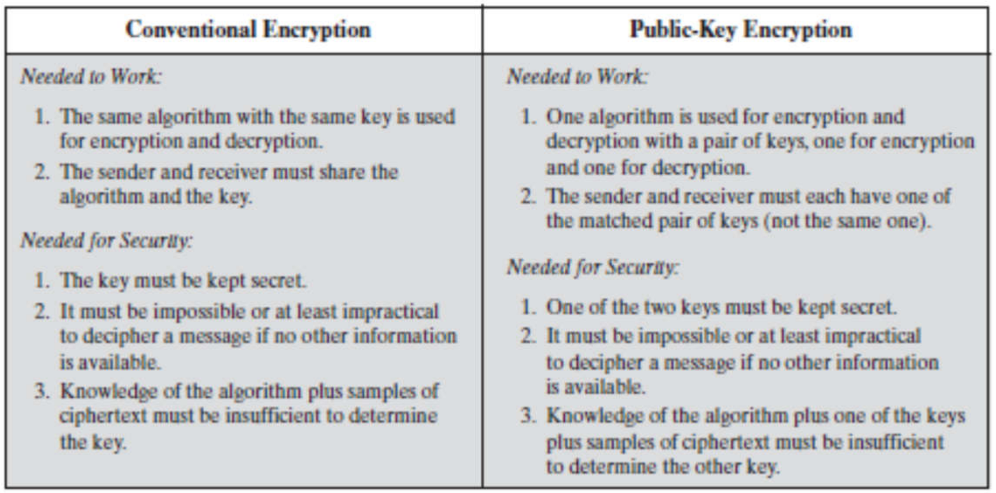
(a) Encryption with public key

Public-key Cryptosystem



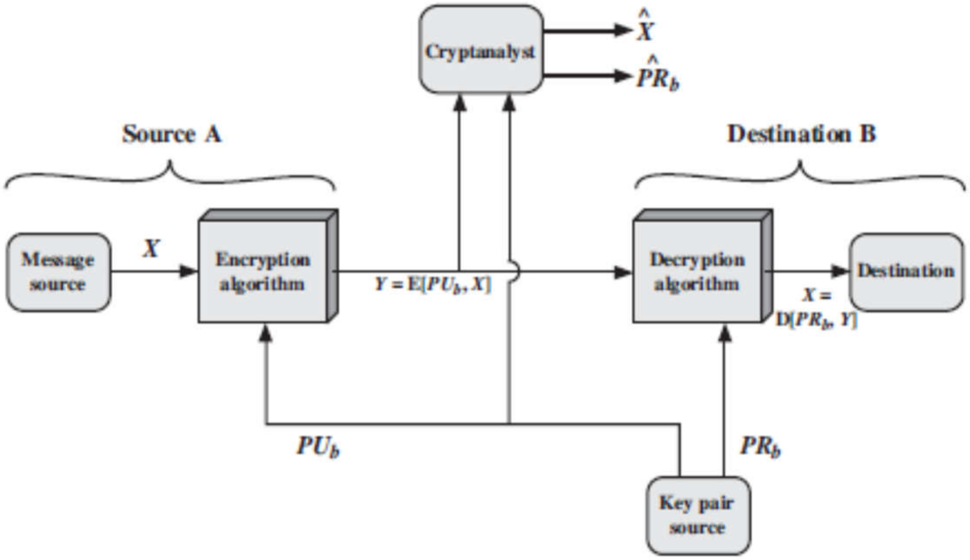
(b) Encryption with private key

Conventional and Public-key Encryption

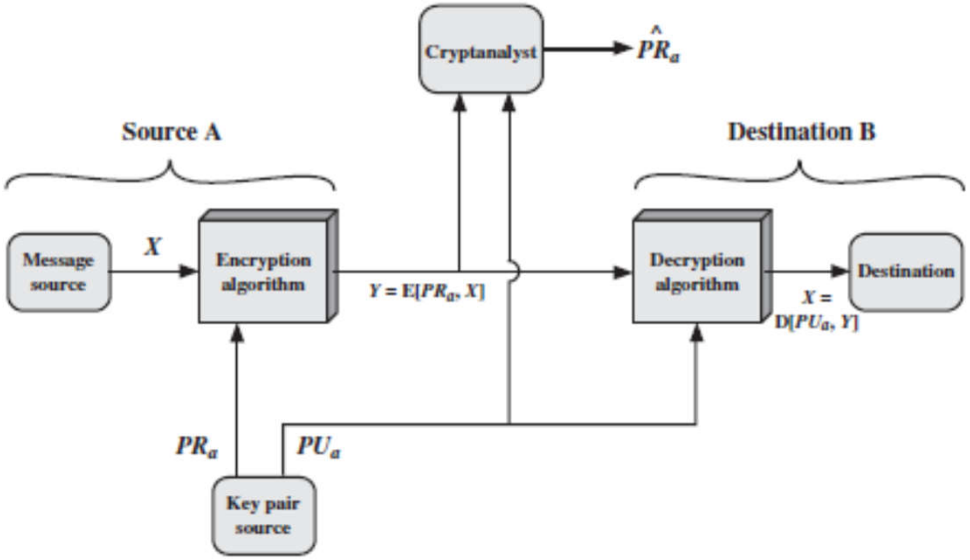


Conventional Encryption	**Public-Key Encryption**
Needed to Work: 1. The same algorithm with the same key is used for encryption and decryption. 2. The sender and receiver must share the algorithm and the key.	*Needed to Work:* 1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption. 2. The sender and receiver must each have one of the matched pair of keys (not the same one).
Needed for Security: 1. The key must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.	*Needed for Security:* 1. One of the two keys must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

Public-key Cryptosystem - Secrecy



Public-key Cryptosystem - Authentication



Public-key Crypt.

The entire message is encrypted

- validates both author and contents
- requires a great deal of storage

Each document must be kept in plaintext to be used for practical purposes

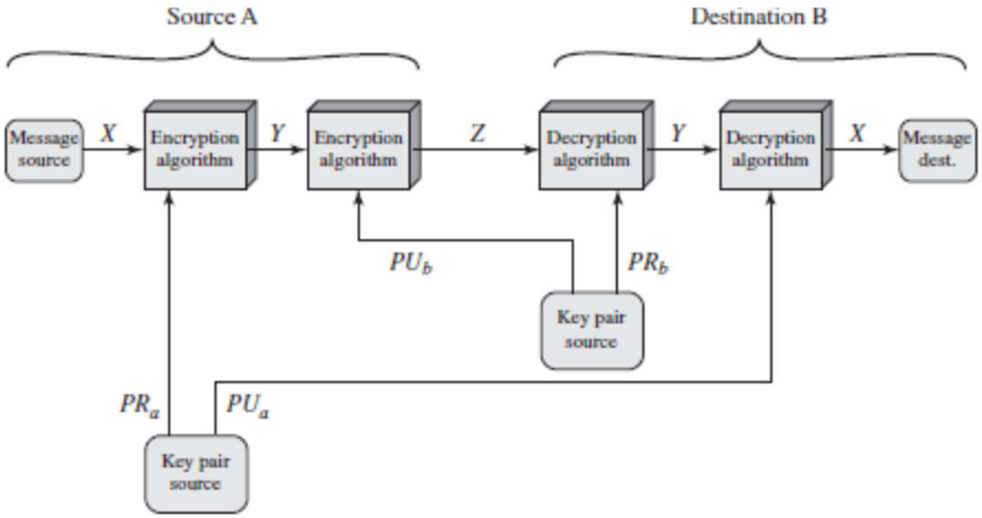
A copy also must be stored in ciphertext so that the origin and contents can be verified in case of a dispute

Alternate option: Authenticator

- To encrypt a small block of bits that is a function of the document
- It is infeasible to change the document without changing the authenticator.

Public-key Crypt. – Secrecy and Auth.

$$Z = \mathrm{E}(PU_b, \mathrm{E}(PR_a, X))$$
$$X = \mathrm{D}(PU_a, \mathrm{D}(PR_b, Z))$$



Use of Public-key Cryptosystem

Encryption /decryption

Digital signature

Key exchange

Requirements for Public-key Crypt.

It is computationally easy for a party B to generate a pair (public key *PUb*, private key *PRb*)

It is computationally easy for a sender A, knowing the public key and the message to be encrypted,*M*, to generate the corresponding ciphertext

It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message

It is computationally infeasible for an adversary, knowing the public key, *PUb*, to determine the private key,*PRb*

It is computationally infeasible for an adversary, knowing the public key, *PUb*, and a ciphertext, *C*, to recover the original message,*M*

Public-key Cryptanalysis

A public-key encryption scheme is vulnerable to a brute-force attack

- Use large key

Public-key systems depend on the use of some sort of invertible mathematical function

- The complexity increases rapidly with key size not linearly

Tradeoff of key size

Probable attacke: Compute the private key given the public key

Exception: 56-bit DES key

- Checking each possible key and match with encrypted data

Cryptographic Hash Functions

A hash function maps a variable-length message into a fixed-length hash value, or message digest

Virtually all cryptographic hash functions involve the iterative use of a compression function

The compression function used in secure hash algorithms falls into one of two categories

- A function specifically designed for the hash function (SHA)
- An algorithm based on a symmetric block cipher (Whirlpool)

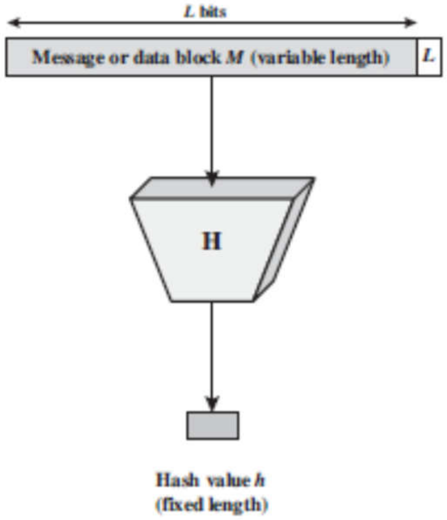
In Cryptographic Hash Algorithm it is computationally infeasible to find

- A data object that maps to a pre-specified hash result (the one-way property)
- Two data objects that map to the same hash result (the collision-free property)

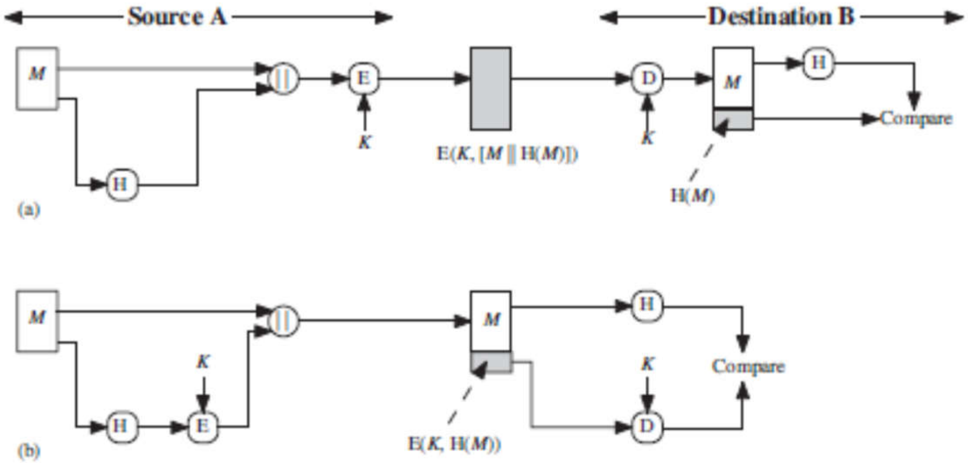
Cryptographic hash Functions

The input is padded out to an integer multiple of some fixed length (e.g., 1024bits)

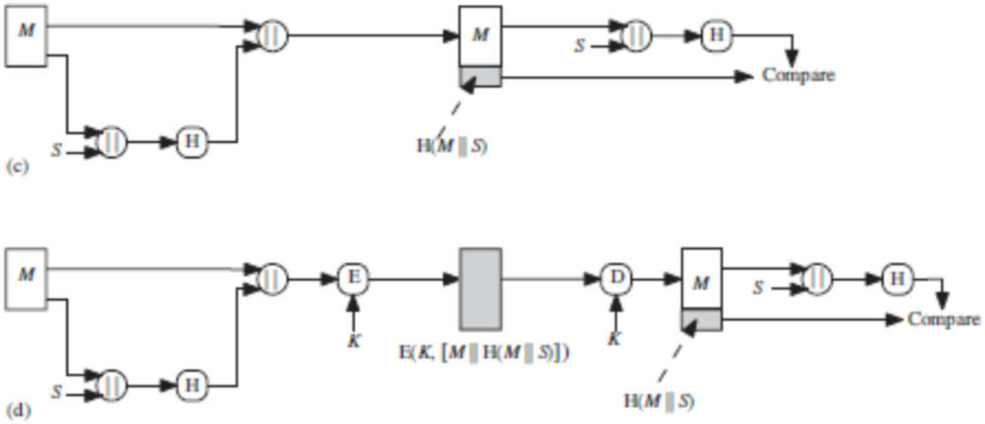
- Padding includes the data length
- Increases the difficulty for an attacker to produce alternate message with same hash value



Message Authentications



Message Authentications



Message Authentications

Encryption software is relatively slow. Even though the amount of data to be encrypted per message is small, there may be a steady stream of messages into and out of a system.

Encryption hardware costs are not negligible. Low-cost chip implementations of DES are available, but the cost adds up if all nodes in a network must have this capability.

Encryption hardware is optimized toward large data sizes. For small blocks of data, a high proportion of the time is spent in initialization/invocation overhead.

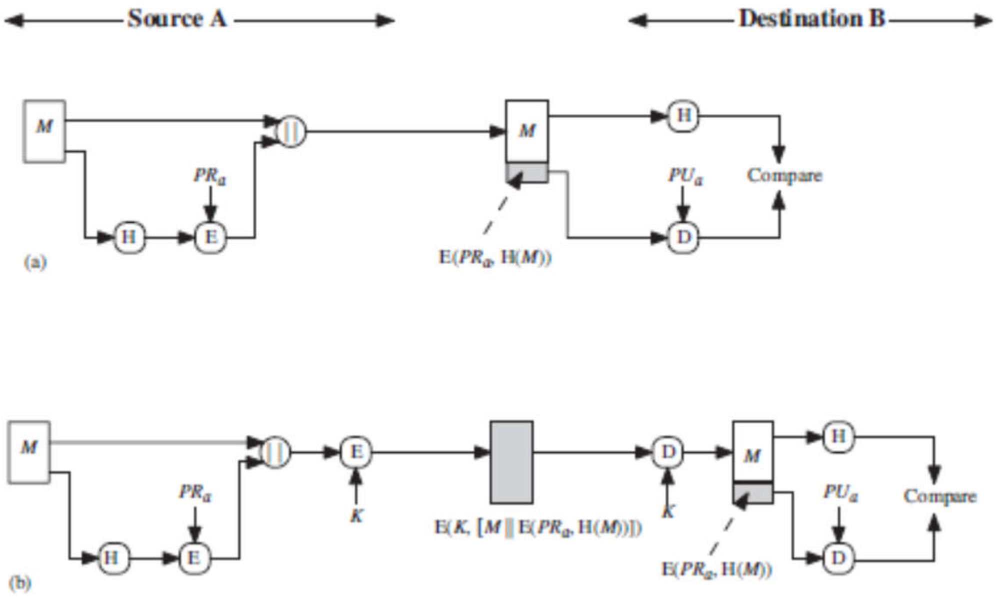
Encryption algorithms may be covered by patents, and there is a cost associated with licensing their use.

MAC- Message Authentication Code – Keyed Hash Function

Digital Signature

The hash value of a message is encrypted with a user's private key

Anyone who knows the user's public key can verify the integrity of the message that is associated with the digital signature



Other application

One-way password file

Intrusion detection and virus detection

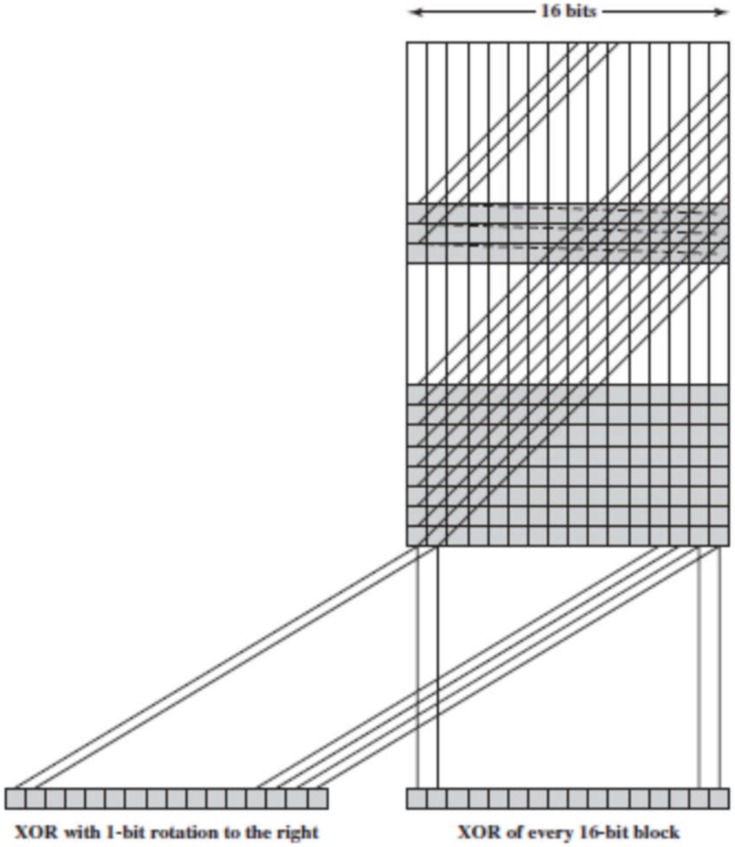
Pseudorandom Number Generation (PRNG)

Simple hash Function

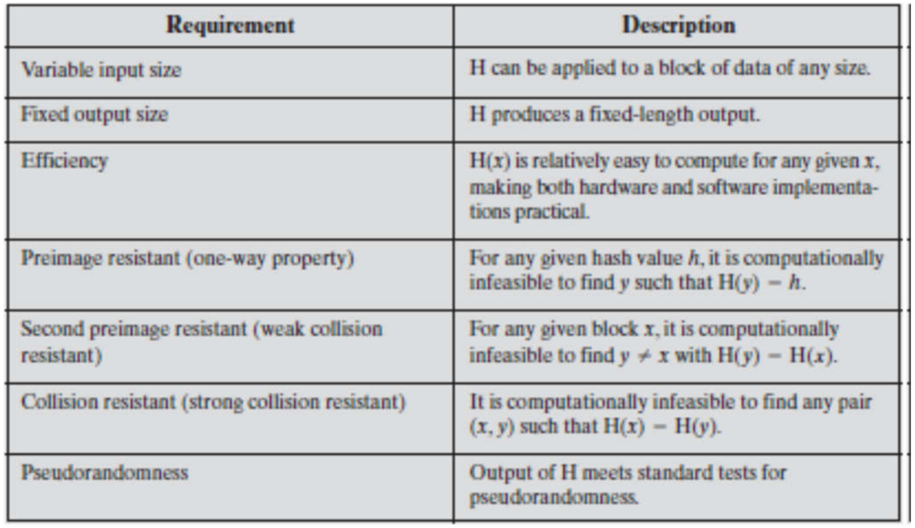
$$C_i = b_{i1} \oplus b_{i2} \oplus \dots \oplus b_{im}$$

where

- C_i = ith bit of the hash code, $1 \leq i \leq n$
- m = number of n-bit blocks in the input
- b_{ij} = ith bit in jth block
- $\oplus$ = XOR operation


16 bits
XOR with 1-bit rotation to the right
XOR of every 16-bit block

Requirement and Security



Requirement	Description
Variable input size	H can be applied to a block of data of any size.
Fixed output size	H produces a fixed-length output.
Efficiency	H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical.
Preimage resistant (one-way property)	For any given hash value h, it is computationally infeasible to find y such that H(y) = h.
Second preimage resistant (weak collision resistant)	For any given block x, it is computationally infeasible to find $y \neq x$ with H(y) = H(x).
Collision resistant (strong collision resistant)	It is computationally infeasible to find any pair (x, y) such that H(x) = H(y).
Pseudorandomness	Output of H meets standard tests for pseudorandomness.

Reference books

Cryptography and Network Security Principles and Practices

- William Stallings

Network Security PRIVATE Communication in a PUBLIC World

- Chalie Kaufman, Radia Perlman, Mike Speciner