CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Introduction to Cryptography Tools

Hash Functions – Part 1

Video Summary

- What is Hashing?
- Message Authentication Code (MAC)
- Hash Functions
- Hash Algorithms
- Applications of Hashing
- Hash Implementation using OpenSSL

Hashing Algorithms

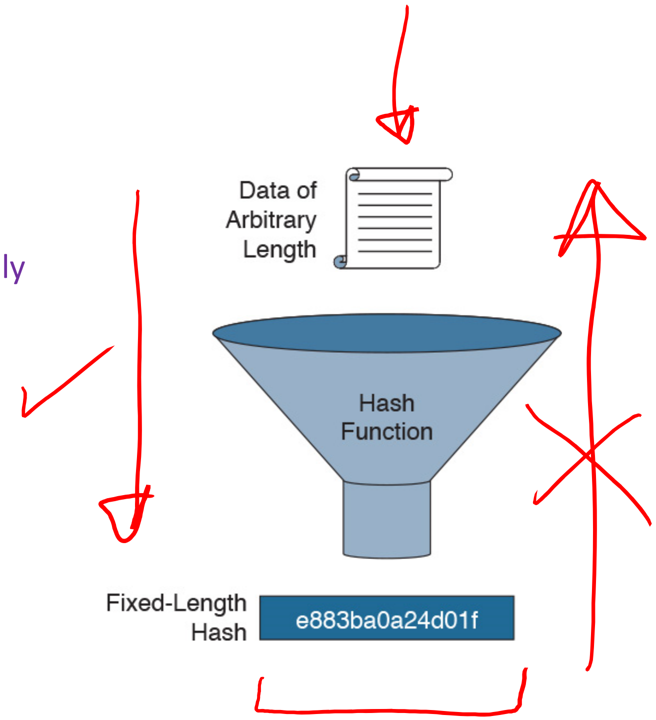
meat

ground
Beef

Hand meat grinder

Hashing Algorithms

- Hashing is a mechanism that is used for data integrity assurance
- Hashing is based on a one-way mathematical function that is relatively easy to compute but significantly difficult to reverse
- The result of hashing is having a fixed length hash which is known as the “digest” or “fingerprint”.



Integrity

Message Authentication Code (MAC)

- An authentication technique involves the use of a secret key to generate a small block of data
- The MAC is appended to the original message
- MAC assumes that user A and B are sharing a common secret key K_{AB}

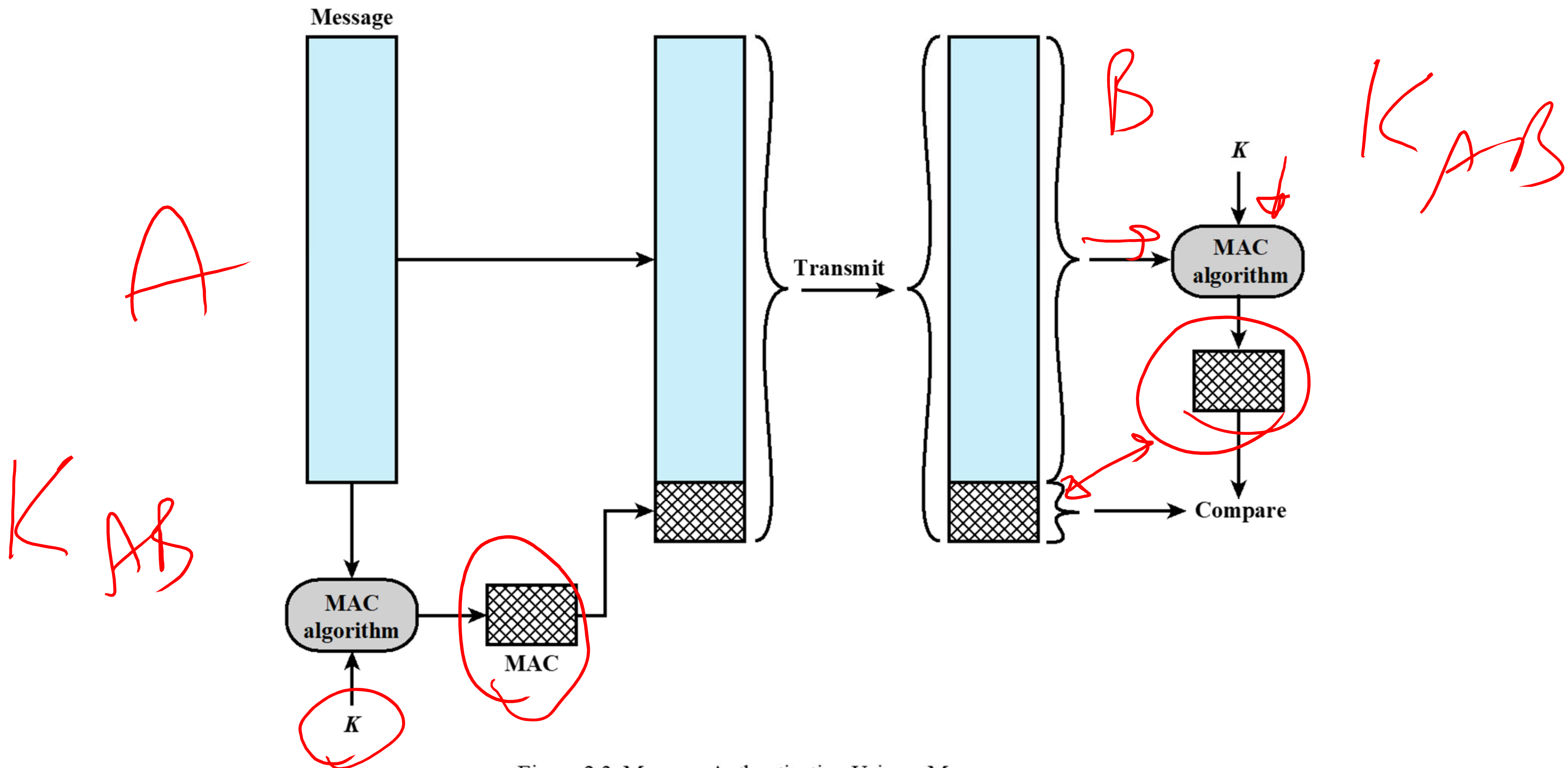


Figure 2.3 Message Authentication Using a Message Authentication Code (MAC).

Message Authentication Code (MAC)

- Append small, fixed-size block of data to message: cryptographic checksum or MAC

$$\mathrm{MAC} = \mathrm{F}(K, M)$$

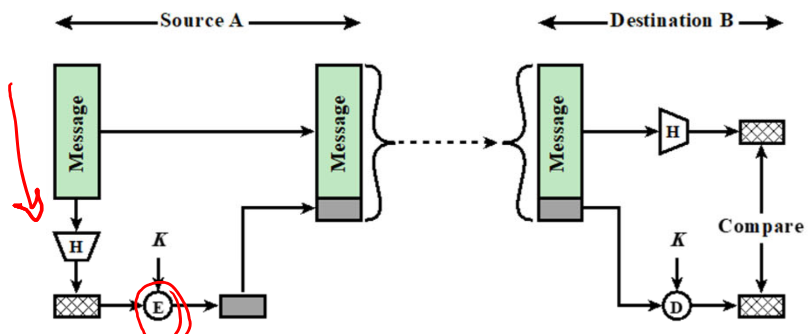
K_{AB}

M = input message
F = MAC function
K = shared secret key of k bits
MAC = message authentication code (or tag) of n bits

- MAC function also called *keyed hash function*
- MAC function similar to encryption, but does not need to be reversible
  - Easier to design stronger MAC functions than encryption functions

MAC Algorithms

- Data Authentication Algorithm (DAA): based on DES; considered insecure
- Cipher-Based Message Authentication Code (CMAC): mode of operation used with Triple-DES and AES
- OMAC, PMAC, UMAC, VMAC, . . .
- HMAC: MAC function derived from cryptographic hash functions



(a) Using symmetric encryption

Figure 2.5 Message Authentication Using a One-Way Hash Function.

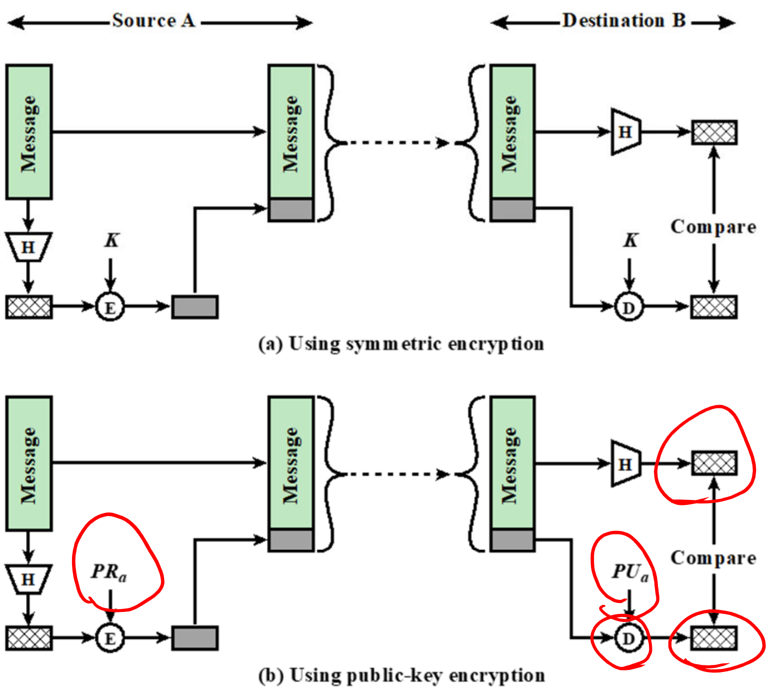


Figure 2.5 Message Authentication Using a One-Way Hash Function.

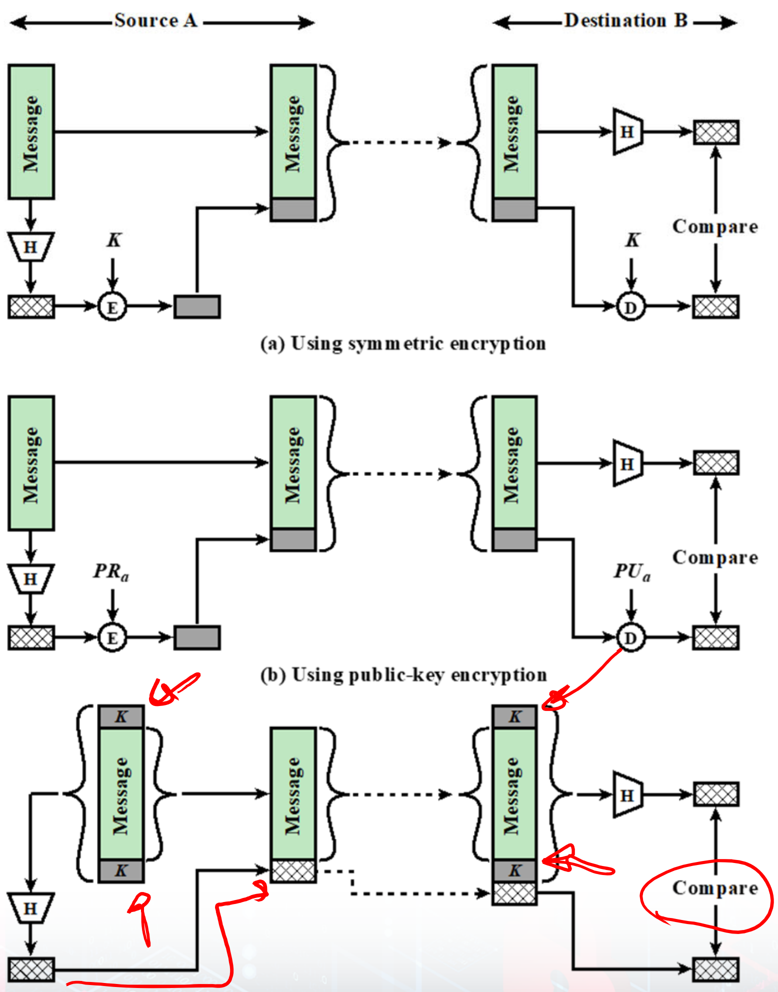


Figure 2.5 Message Authentication Using a One-Way Hash Function.

A

B

KAB

MAC vs. HASH

- The main difference between MAC and Hash is that the MAC is always taking a key as an input to its algorithm which is used to encrypt the data while digesting the message

- The Hash function is not taking any key during the hashing process

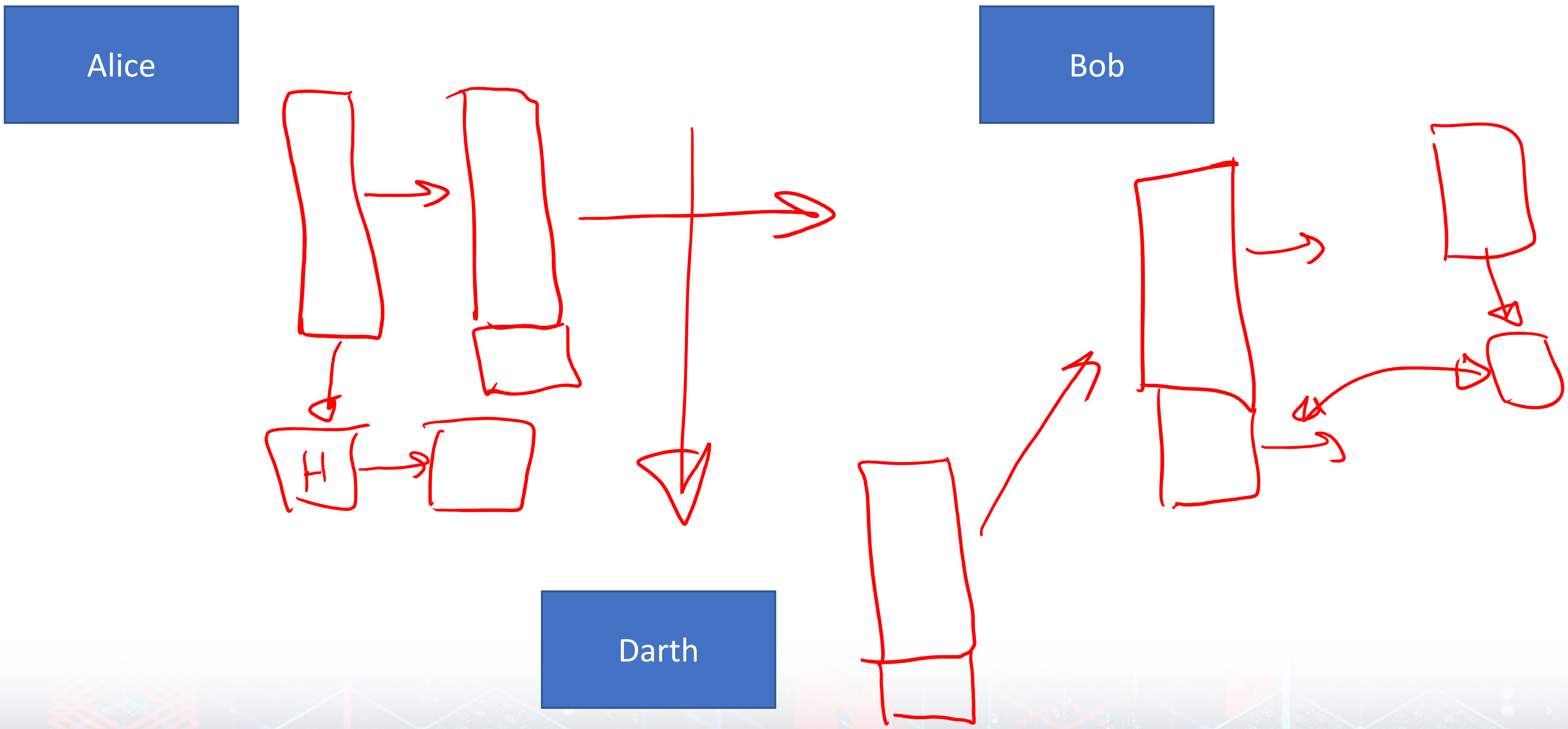
Authentication using Hash Functions

$h = H(M)$

fixed size hash

- Hash function H: variable-length block of data M input; fixed-size hash value $h = \mathrm{H}(M)$ output
- Applying H to large set of inputs should produce evenly distributed and random looking outputs
- Cryptographic hash function: computationally infeasible to find:
    1. M that maps to known h (one-way property)
    2. M_1 and M_2 that produce same h (collision-free property)
- Append hash value to message; receiver verifies if message changed

Authentication using Hash Functions



Hash Security Requirements and Attacks

Preimage resistant: For any given h, computationally infeasible to find y such that $\mathrm{H}(y) = h$ (*one-way property*)

Second preimage resistant: For any given x, computationally infeasible to find $y \neq x$ with $\mathrm{H}(y) = \mathrm{H}(x)$ (*weak collision resistant*)

Collision resistant: Computationally infeasible to find any pair (x, y) such that $\mathrm{H}(x) = \mathrm{H}(y)$ (*strong collision resistant*)

$y \neq x$

$H(y) = H(x)$

x

Brute Force Attacks

- Depend on hash value length of n bits
- Preimage and second preimage resistant: 2^n
- Collision resistant: $2^{n/2}$

Hashing Algorithms

Message Digest 5 (MD5): MD5 produces a 128-bit hash and is now considered a legacy algorithm that should be avoided

Secure Hash Algorithm 1 (SHA-1): SHA-1 takes a message of up to 2^64 bits in length and produces a 160-bit message digest. The algorithm is slightly slower than MD5, but the larger message digest makes it more secure against brute-force collision and inversion attacks.

Secure Hash Algorithm 2 (SHA-2): SHA-2 algorithms are the secure hash algorithms that the U.S. government requires by law for use in certain applications. The SHA-2 family includes 224-bit, 256-bit, 384-bit, and 512-bit functions. When choosing a hashing algorithm, use SHA-256 or higher, as they are currently the most secure

Secure Hash Algorithm 3 (SHA-3) is the latest member of the Secure Hash Algorithm family of standards, released by NIST on August 5, 2015. Although part of the same series of standards, SHA-3 is internally different from the MD5-like structure of SHA-1 and SHA-2.

Hashing Algorithms

	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
Message Digest Size	160	224	256	384	512
Message Size	$< 2^{64}$	$< 2^{64}$	$< 2^{64}$	$< 2^{128}$	$< 2^{128}$
Block Size	512	512	512	1024	1024
Word Size	32	32	32	64	64
Number of Steps	80	64	64	80	80

Video Summary

- What is Hashing?
- Message Authentication Code (MAC)
- Hash Functions
- Hash Algorithms
- Applications of Hashing
- Hash Implementation using OpenSSL