Message Authentication Code (MAC)

Bahan Kuliah Keamanan Data

Sevi **Nurafni**

Fakultas Sains dan Teknologi
Universitas Koperasi Indonesia 2025

Definisi

- MAC (message authentication code): kode yang dihasilkan oleh fungsi hash satu-arah namun menggunakan kunci rahasia (secret key) dalam pembangkitan nilai hash.

$$MAC = C_K(M)$$

MAC = nilai hash

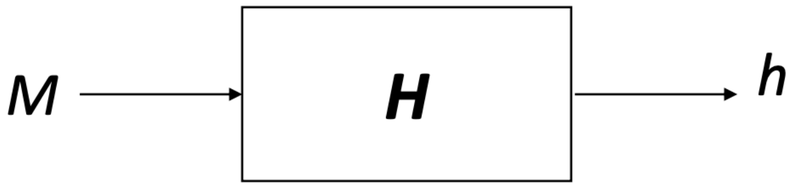
C = fungsi hash (atau algoritma MAC)

K = kunci rahasia

- Bandingkan dengan fungsi hash biasa seperti MD5 atau SHA yang tidak memerlukan kunci dalam menghasilkan nilai hash.

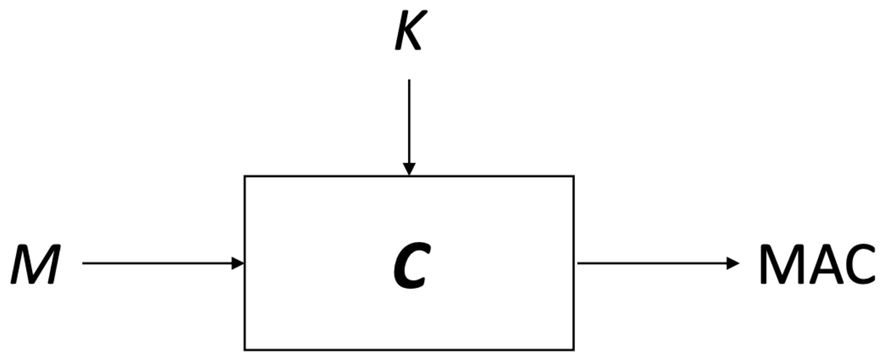
Algoritma MAC vs Fungsi Hash

Perbedaan Algoritma MAC dengan Fungsi Hash biasa



$h = H(M)$

Message digest dengan fungsi *hash*



$MAC = C_K(M)$

MAC dengan fungsi *hash*

- *MAC* dilekatkan (*embed*) pada pesan.
- *MAC* digunakan untuk memeriksa integritas (keaslian) pesan.
- Jika MAC yang dikirim sama dengan MAC yang dihitung oleh penerima, maka pesan masih asli.

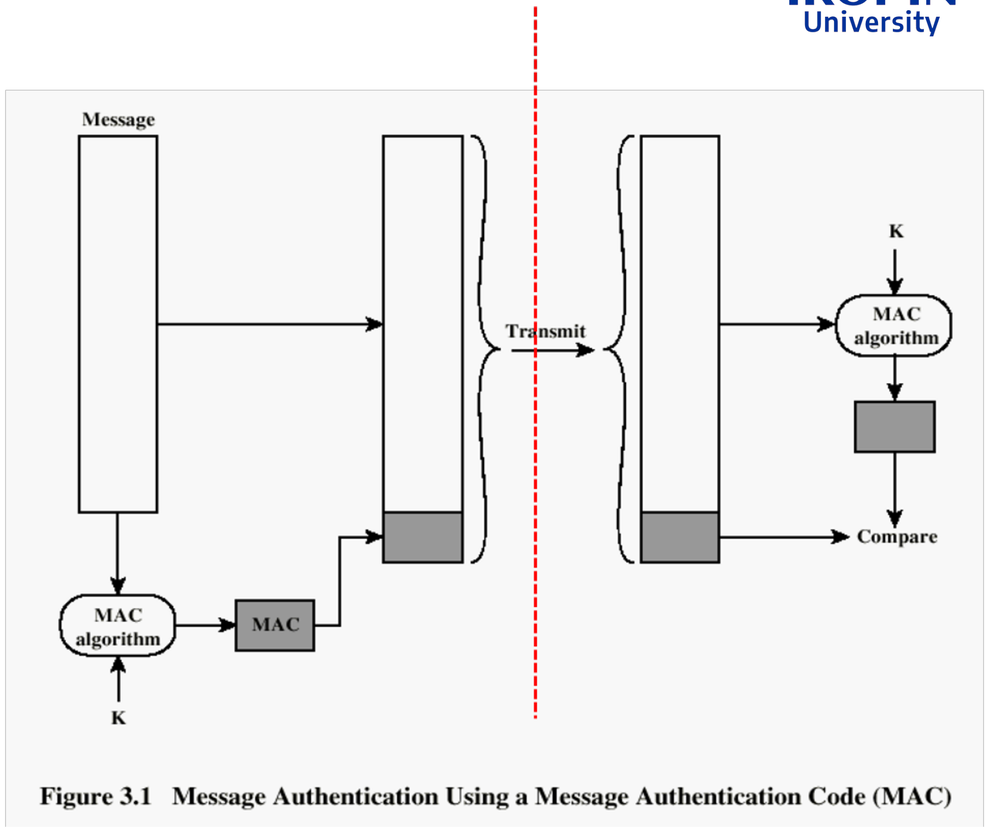
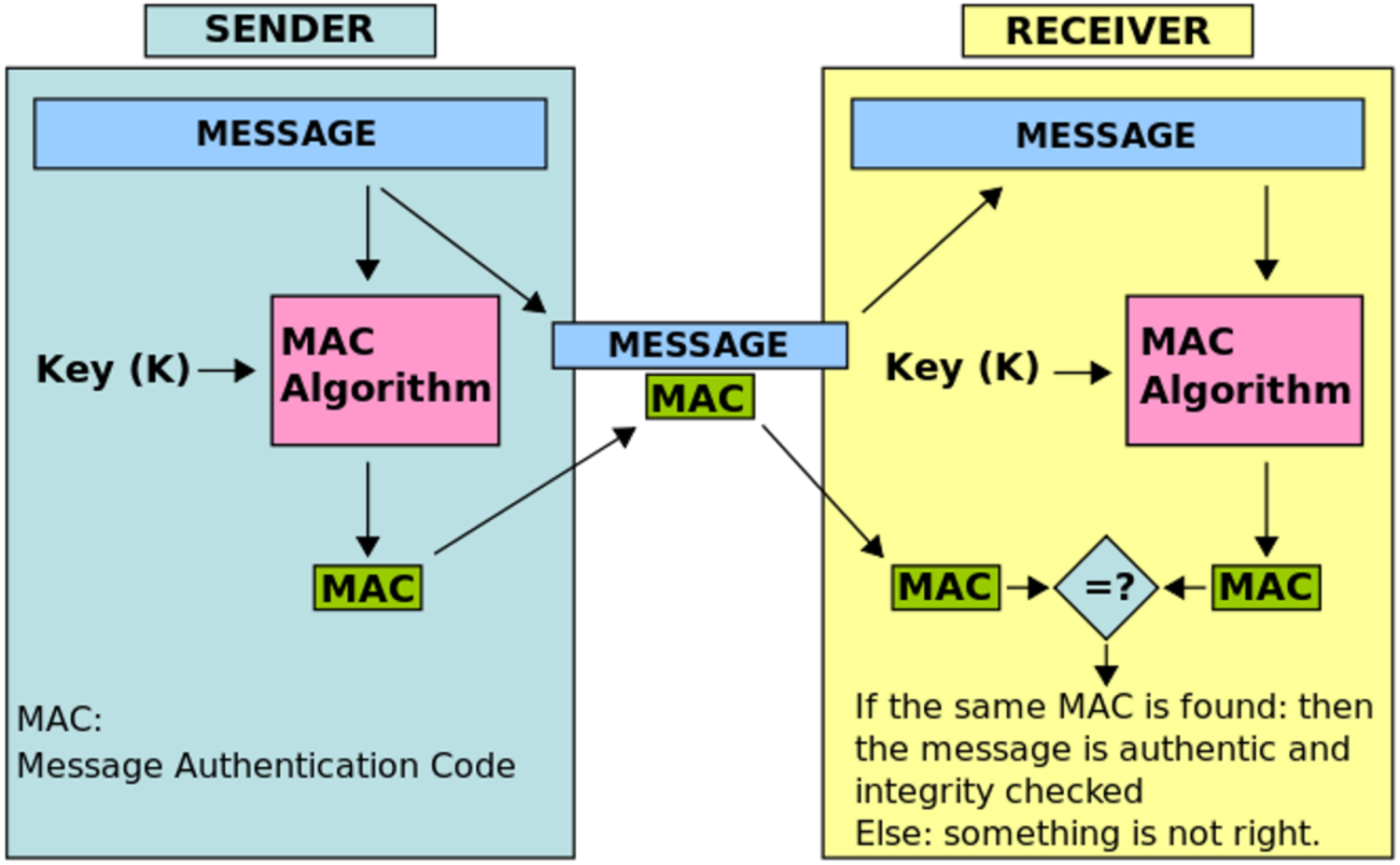


Figure 3.1 Message Authentication Using a Message Authentication Code (MAC)


SENDER
MESSAGE
Key (K)
MAC Algorithm
MAC
MESSAGE
MAC
MAC:
Message Authentication Code
RECEIVER
MESSAGE
Key (K)
MAC Algorithm
MAC
=?
MAC
If the same MAC is found: then the message is authentic and integrity checked
Else: something is not right.

Kegunaan MAC

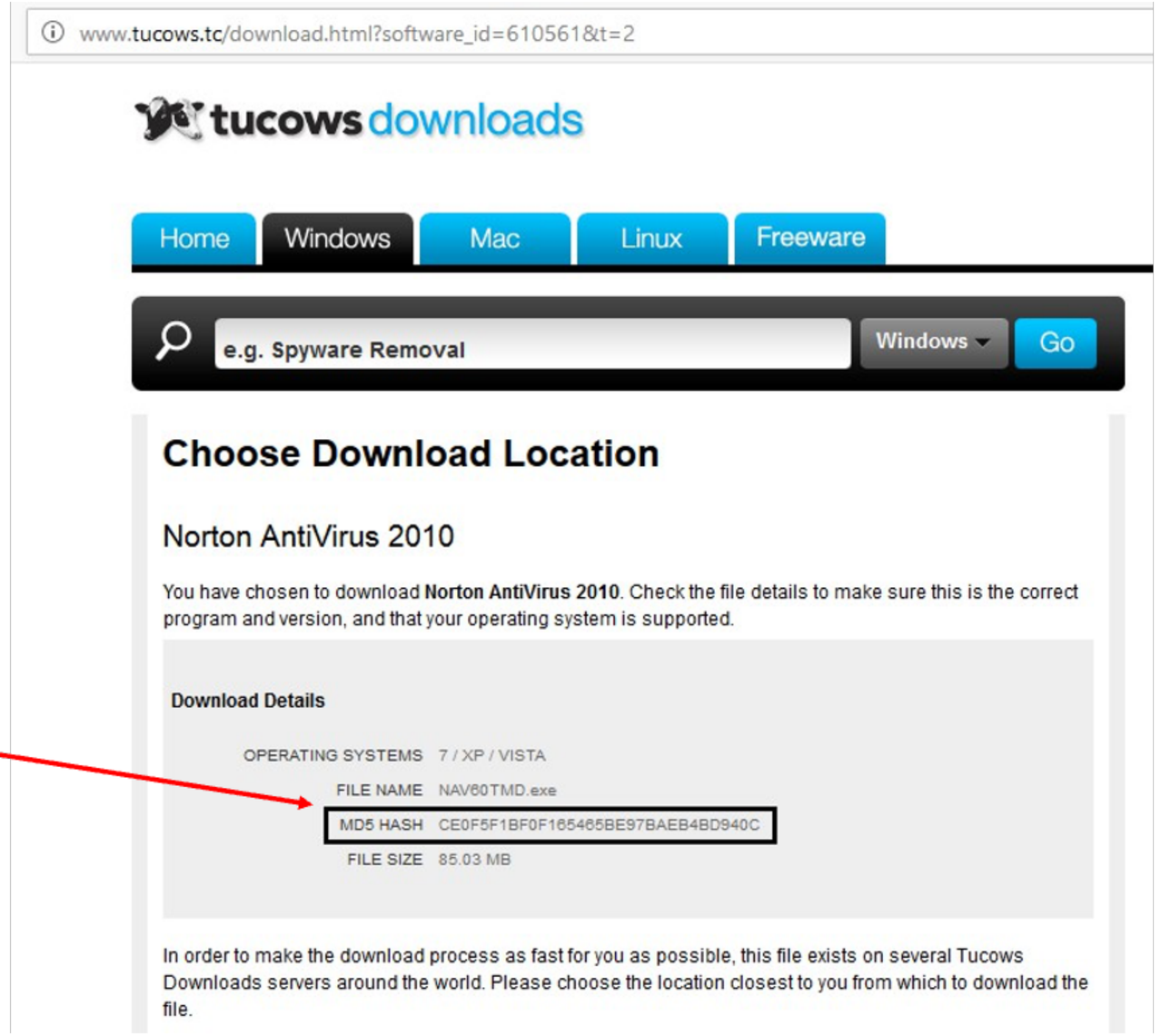
- Kegunaan: otentikasi dokumen (file)

  → Menjaga integritas (keaslian) isi arsip terhadap perubahan oleh pihak lawan, misalnya akibat serangan *hacker*, virus, dsb.

- Jika pengguna menggunakan fungsi hash satu-arah biasa (seperti MD5), maka pihak lawan dapat menghitung message digest yang baru dari dokumen yang sudah diubah, lalu menggantinya.

  Tetapi, jika digunakan *MAC*, pihak lawan tidak dapat melakukan hal ini karena ia tidak mengetahui kunci yang asli untuk menghitung MAC.

Hacker bisa mengganti file dengan file lain, mengganti nilai MD5 semula dengan nilai MD5 yang baru. Pengunduh file tidak dapat menyadarinya.

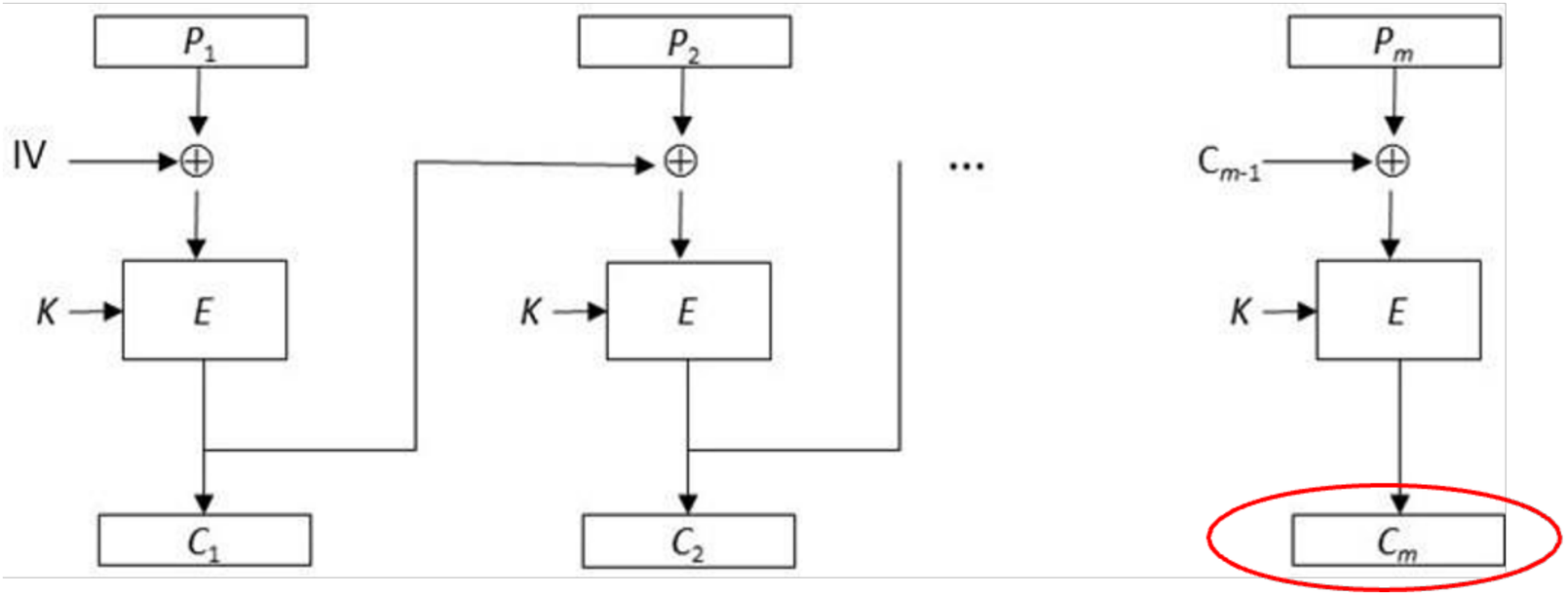


Agoritma MAC

1. Berbasis Block Cipher

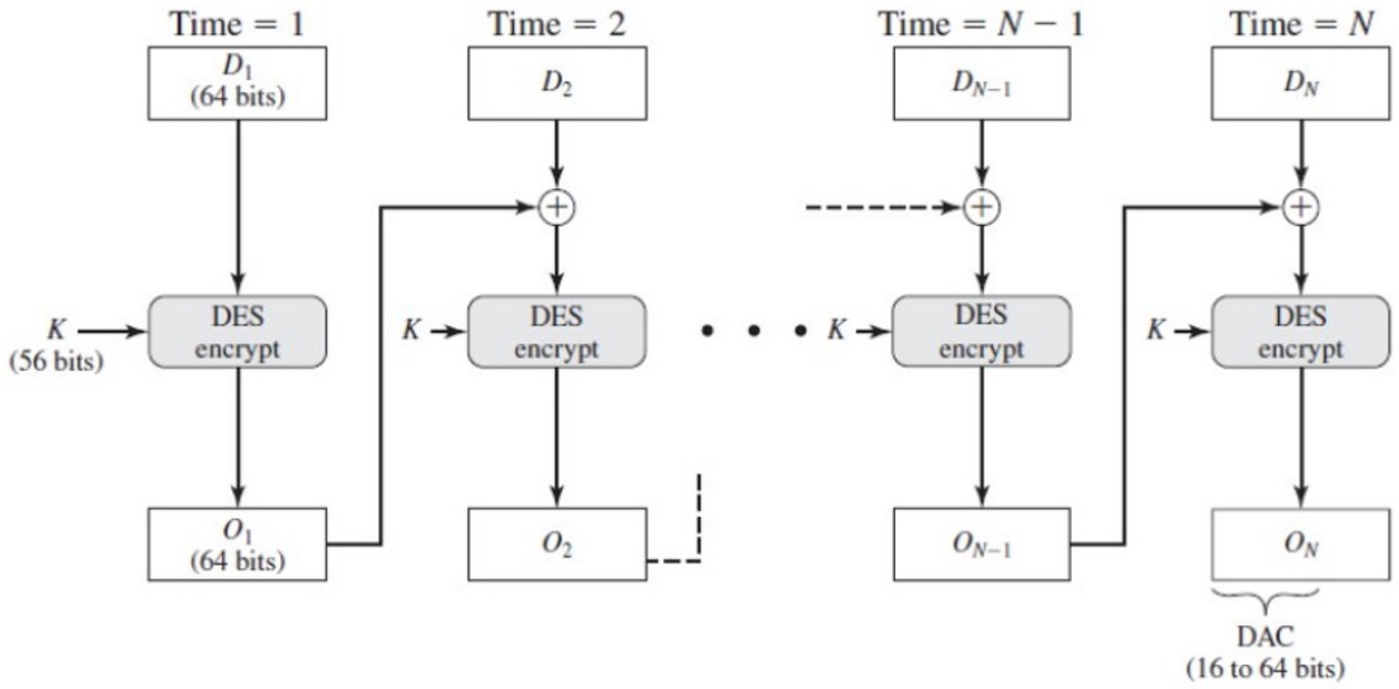
MAC dibangkitkan dari *block cipher* dengan mode *CBC* atau *CFB*.

Nilai *hash*-nya (yang menjadi *MAC*) adalah hasil enkripsi blok terakhir.



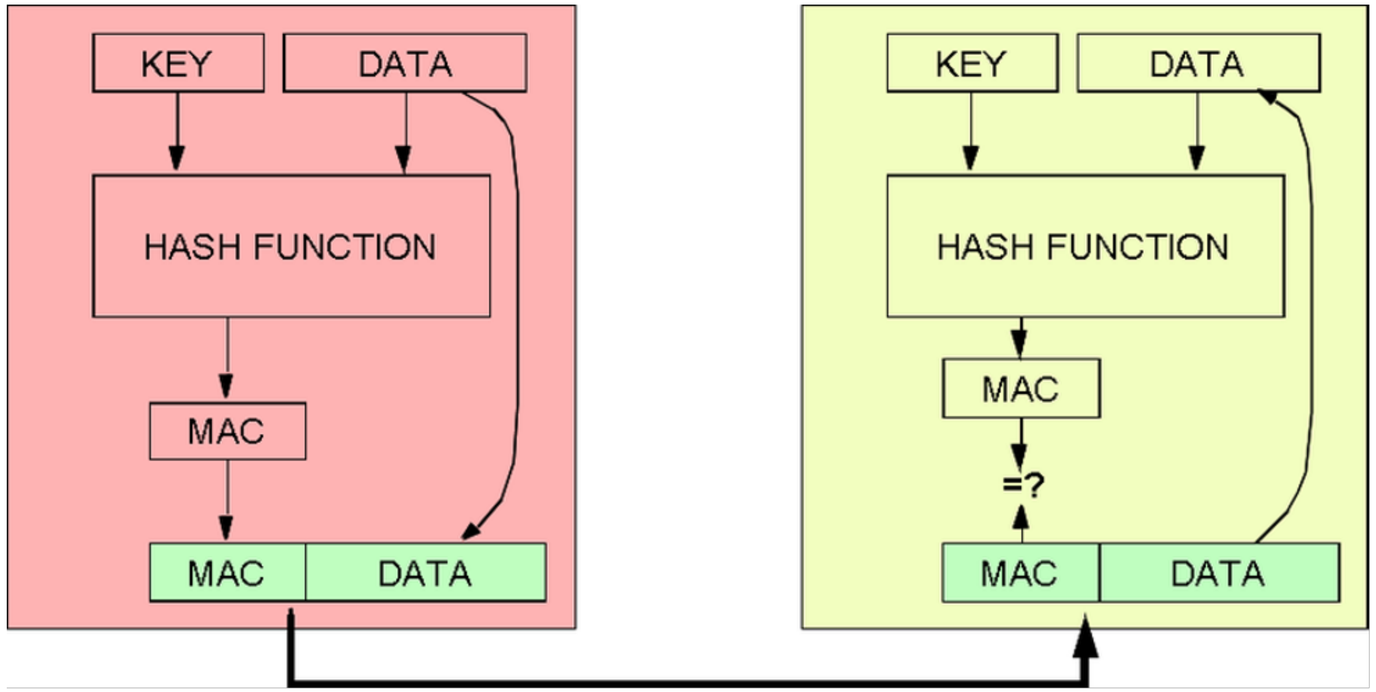
- Misalkan *DES* digunakan sebagai *cipher* blok, maka MAC = ukuran blok = 64 bit, dan kunci rahasia *MAC* adalah kunci DES yang panjangnya 56 bit.

- Data Authentication Algorithm (DAA) adalah algoritma MAC berbasis DES-CBC yang digunakan secara luas:



2. Berbasis Fungsi Hash satu-arah (HMAC)

- Fungsi *hash* seperti *MD5* dan SHA dapat digunakan sebagai *MAC*
- Misalkan Alice dan Bob akan saling bertukar DATA. Alice dan Bob telah berbagi sebuah kunci rahasia *KEY*.



Contoh

M = Halo, Bob!

K = 12345678

Fungsi Hash: SHA-1

MAC = 6f8605c7c3a649a40abfb87b44aa21f356e931a0

SELAMAT BELAJAR