

Bahan kuliah IF4020 Kriptografi

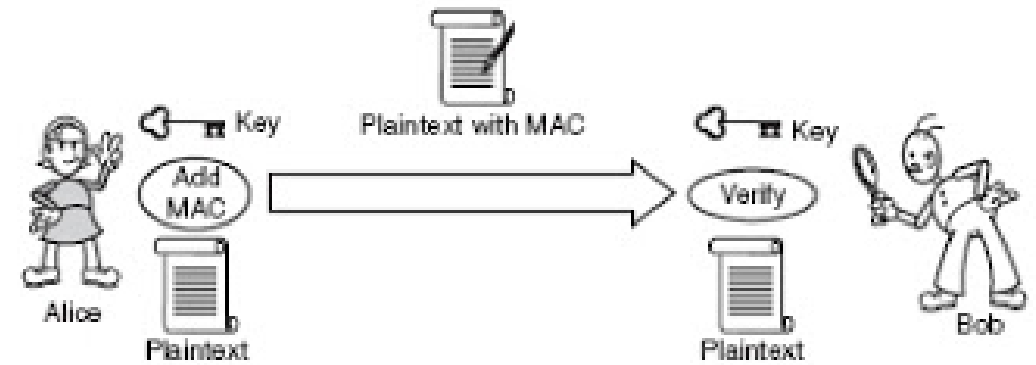


Figure 9.3 Message Authentication Code (MAC)

MAC

(Message Authentication Code)

Oleh: Rinaldi Munir

Program Studi Informatika
Sekolah Teknik Elektro dan Informatika
ITB – 2023

Definisi

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

$$MAC = C_K(M)$$

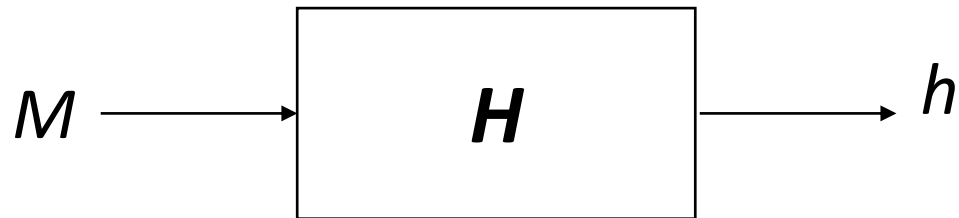
$MAC = \text{nilai hash}$

$C = \text{fungsi hash (atau algoritma MAC)}$

$K = \text{kunci rahasia}$

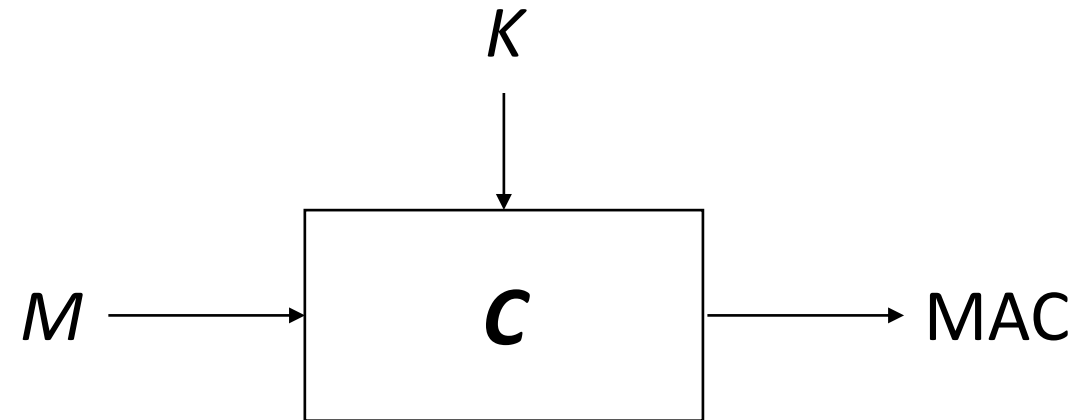
- Bandingkan dengan fungsi *hash* biasa seperti *MD5* atau *SHA* yang tidak memerlukan kunci dalam menghasilkan nilai *hash*.

Perbedaan Algoritma MAC dengan Fungsi Hash biasa



$$h = H(M)$$

Message digest dengan fungsi hash



$$\text{MAC} = C_K(M)$$

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.

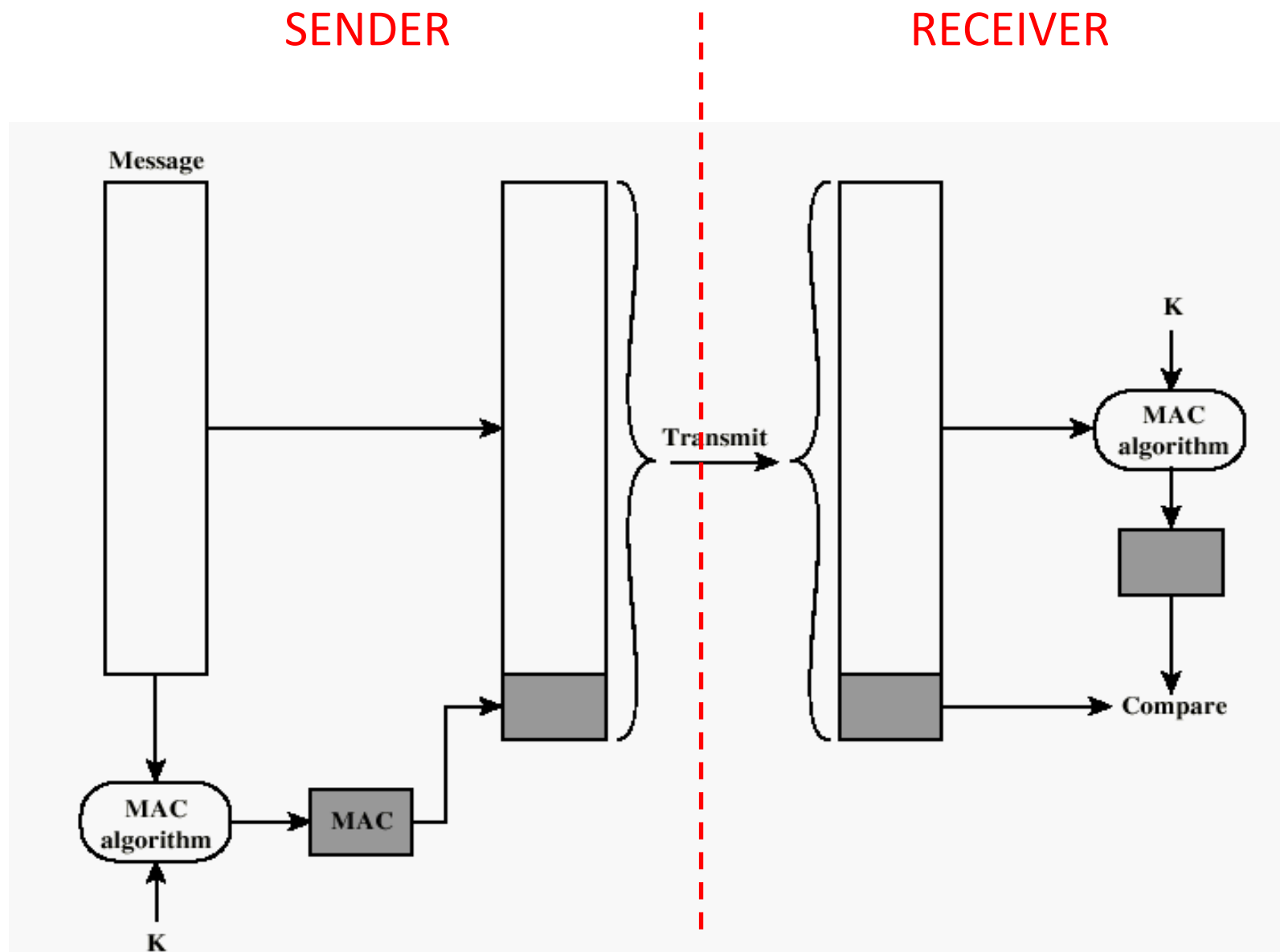
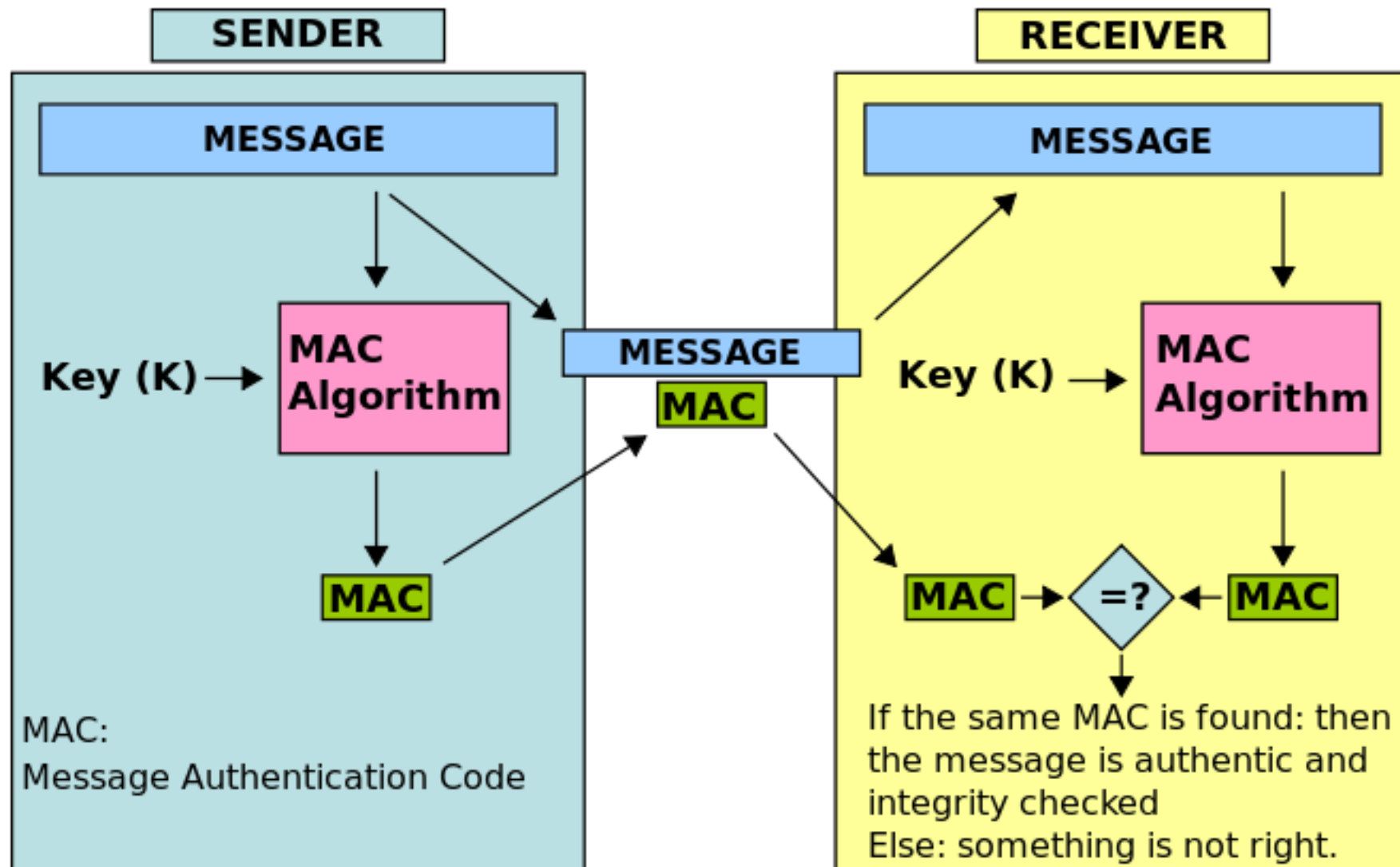


Figure 3.1 Message Authentication Using a Message Authentication Code (MAC)



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*.



e.g. Spyware Removal

Windows ▾

Go

Choose Download Location

Norton AntiVirus 2010

You have chosen to download **Norton AntiVirus 2010**. Check the file details to make sure this is the correct program and version, and that your operating system is supported.

Download Details

OPERATING SYSTEMS 7 / XP / VISTA

FILE NAME NAV60TMD.exe

MD5 HASH CE0F5F1BF0F165465BE97BAEB4BD940C

FILE SIZE 85.03 MB

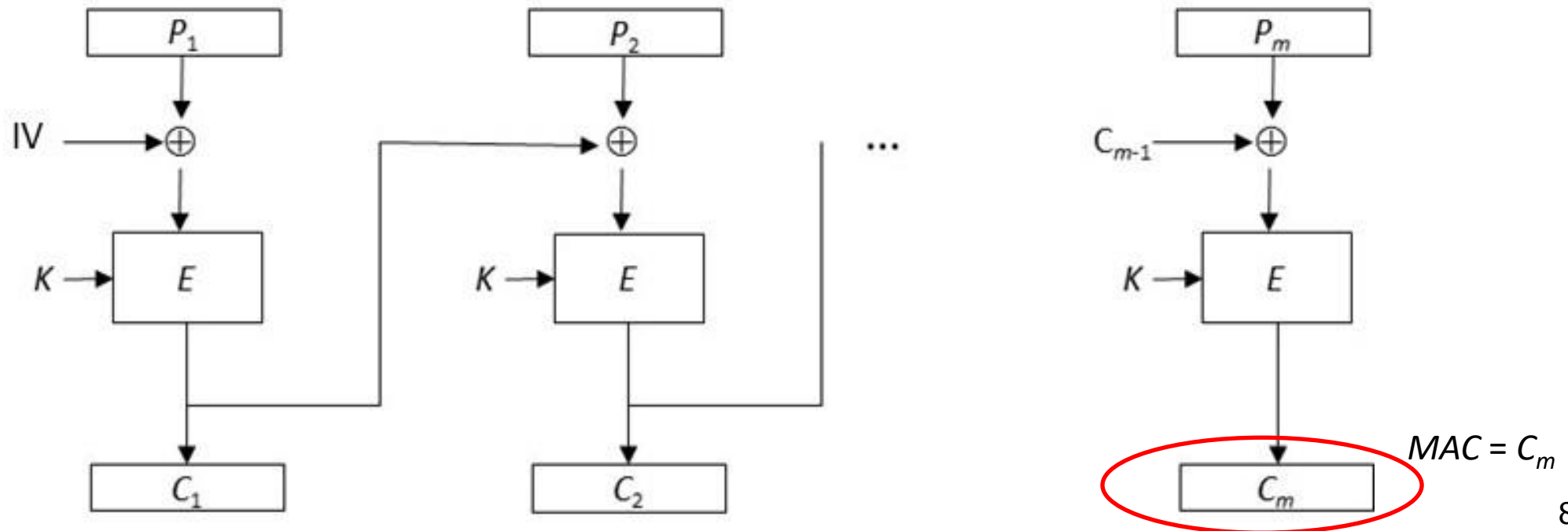
In order to make the download process as fast for you as possible, this file exists on several Tucows Downloads servers around the world. Please choose the location closest to you from which to download the file.

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

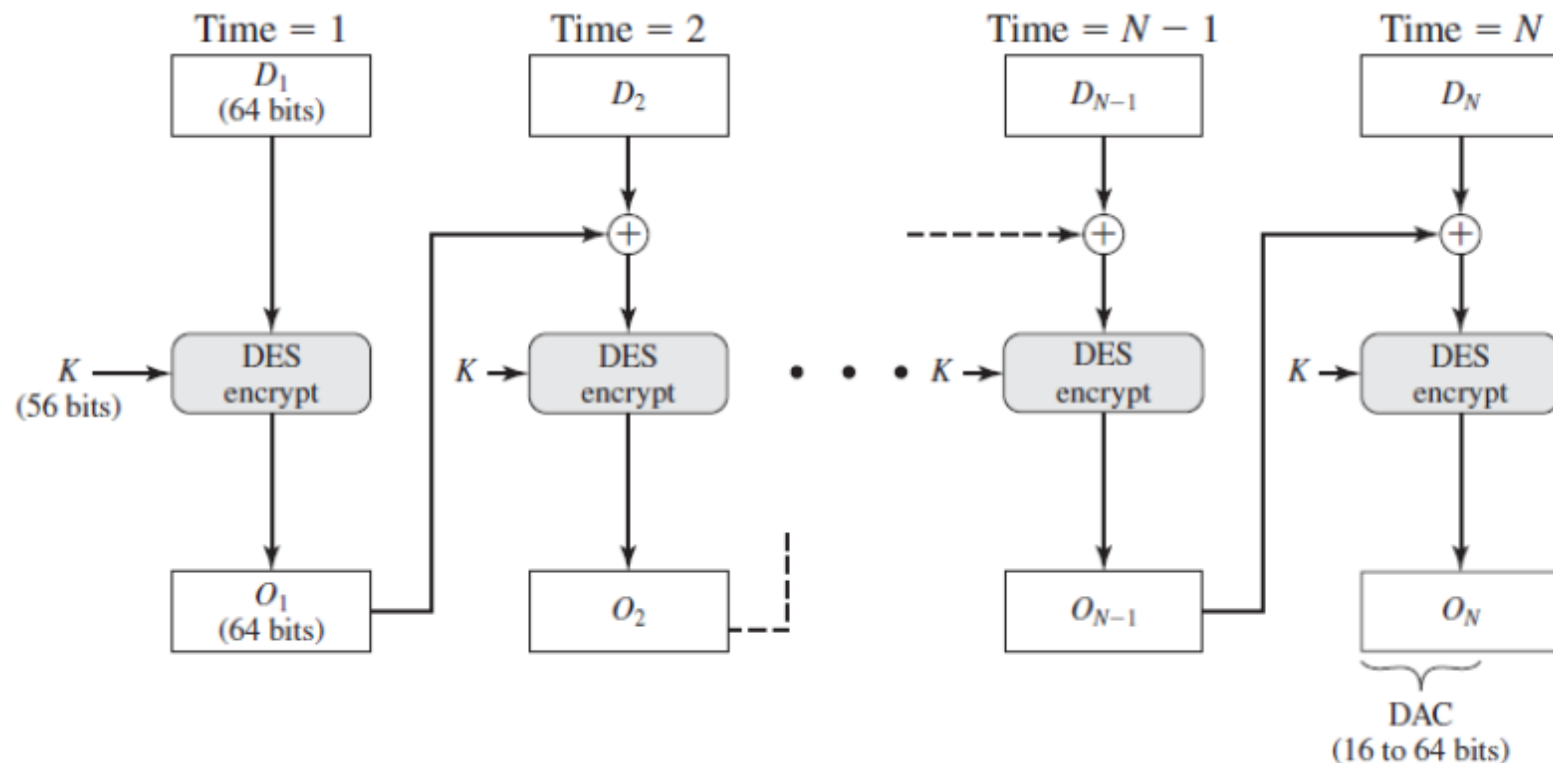
Algoritma MAC

(a) Algoritma MAC berbasis *block cipher*

- *MAC* dibangkitkan dari *block cipher* dengan mode *CBC* atau *CFB*.
- Nilai *hash*-nya (yang menjadi *MAC*) adalah hasil enkripsi blok terakhir.

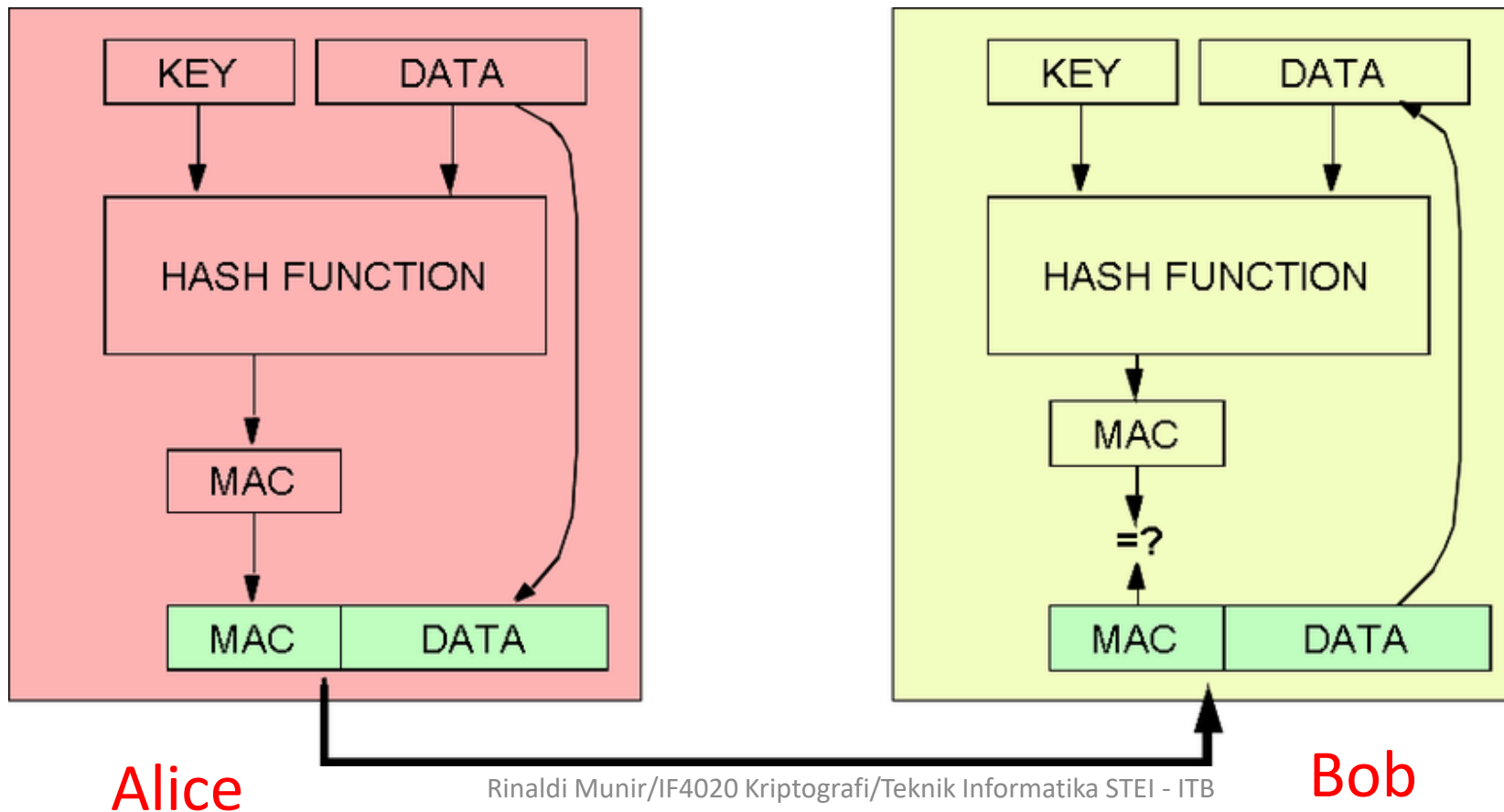


- Misalkan *DES* digunakan sebagai *cipher* blok, maka MAC = ukuran blok = 64 bit, dan kunci rahasia *MAC* adalah kunci DES yang panjangnya 56 bit.
- *Data Authentication Algorithm (DAA)* adalah algoritma *MAC* berbasis *DES-CBC* yang digunakan secara luas:



(b) Algoritma MAC 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:

$M = \textit{Halo, Bob!}$

$K = 12345678$

Fungsi Hash: SHA-1

$MAC = 6f8605c7c3a649a40abfb87b44aa21f356e931a0$

Sumber: MAC online <https://www.freeformatter.com/hmac-generator.html>

SELAMAT BELAJAR