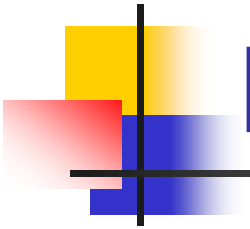
MAC
(*Message Authentication Code*)

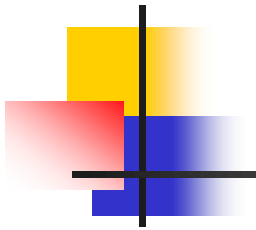
Bahan Kuliah

IF4020 Kriptografi



Definisi

- MAC: fungsi satu-arah yang menggunakan kunci rahasia (*secret key*) dalam pembangkitan nilai *hash*
- Bandingkan dengan *MD5* atau *SHA* yang tidak memerlukan kunci untuk menghasilkan nilai *hash*.
- Nilai hash yang dihasilkan selalu berukuran tetap (fixed) untuk ukuran pesan berapa saja
- *MAC* dilekatkan (*embed*) pada pesan. Selanjutnya, *MAC* digunakan untuk otentikasi tanpa perlu merahasiakan pesan.
- MAC bukanlah tanda-tangan digital. MAC hanya menyediakan otentikasi pengirim dan integritas pesan saja.



- MAC secara matematis:

$$MAC = C_K(M)$$

MAC = nilai *hash*

C = fungsi *hash* (atau algoritma *MAC*)

K = kunci rahasia

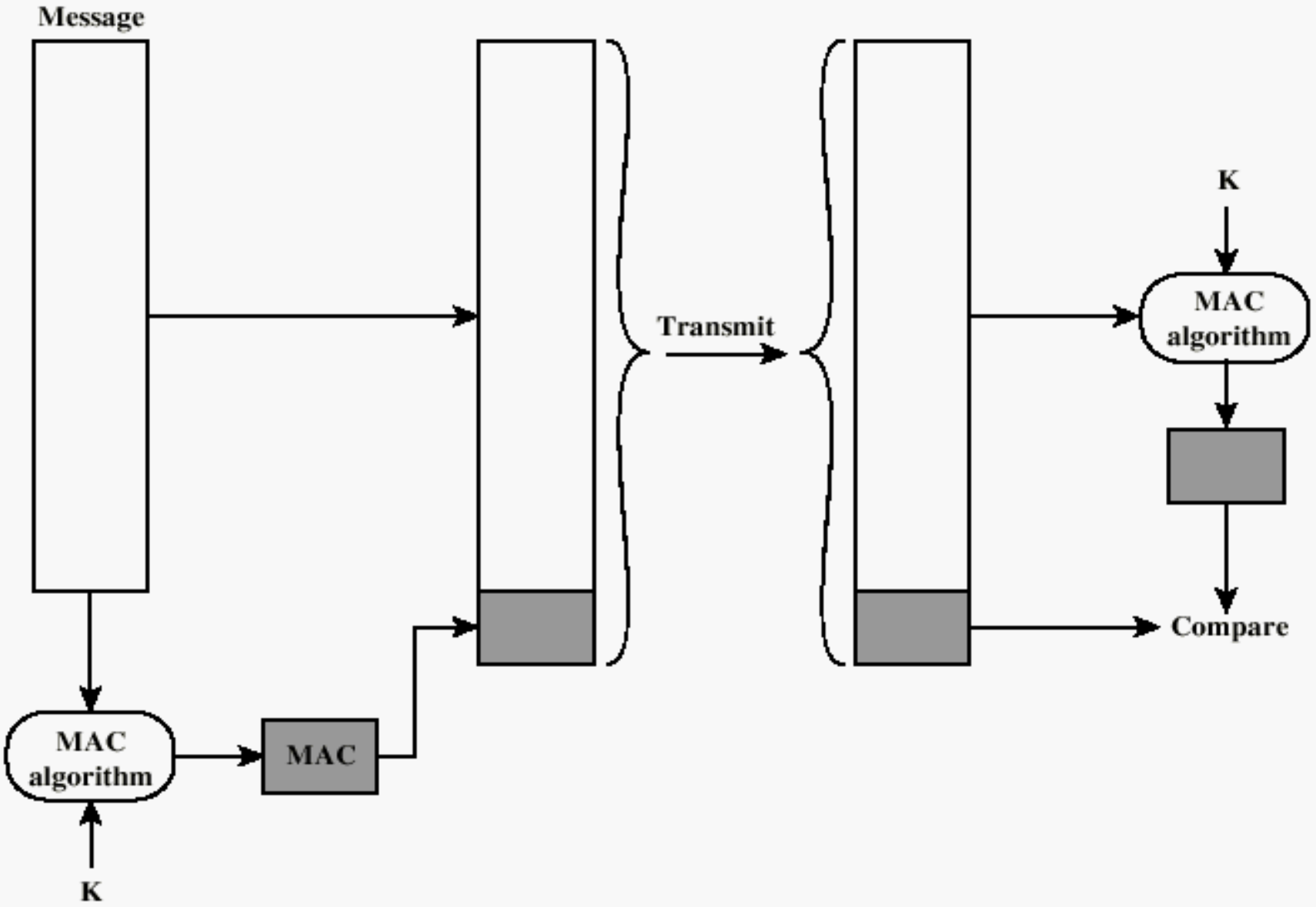


Figure 3.1 Message Authentication Using a Message Authentication Code (MAC)

Aplikasi MAC

- Otentikasi arsip yang digunakan oleh dua atau lebih pengguna
- Menjaga integritas (keaslian) isi arsip terhadap perubahan, misalnya karena serangan virus.

  Caranya sbb: hitung *MAC* dari arsip, simpan *MAC* di dalam sebuah tabel.

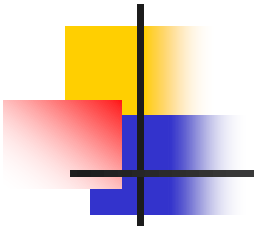
  Jika pengguna menggunakan fungsi *hash* satu-arah biasa (seperti *MD5*), maka virus dapat menghitung nilai *hash* yang baru dari arsip yang sudah diubah, lalu mengganti nilai *hash* yang lama di dalam tabel.

  Tetapi, jika digunakan *MAC*, virus tidak dapat melakukan hal ini karena ia tidak mengetahui kunci.

Algoritma MAC

(a) Algoritma MAC berbasis cipher blok

- *MAC* dibangkitkan dengan menggunakan algoritma *cipher* blok dengan mode *CBC* atau *CFB*.
- Nilai *hash*-nya (yang menjadi *MAC*) adalah hasil enkripsi blok terakhir.
- Misalkan *DES* digunakan sebagai *cipher* blok, maka ukuran blok adalah 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

- Fungsi *hash* seperti *MD5* dapat digunakan sebagai *MAC*.
- Caranya:

  - Misalkan *A* dan *B* akan bertukar pesan. *A* dan *B* berbagi sebuah kunci rahasia *K*.
  - *A* menyambung (*concate*) pesan *M* dengan *K*, lalu menghitung nilai *hash* dari hasil penyambungan itu: $H(M, K)$
  - Nilai *hash* ini adalah *MAC* dari pesan tersebut. *A* lalu mengirim *M* dan *MAC* kepada *B*.
  - *B* dapat melakukan otentikasi terhadap pesan karena ia mengetahui kunci *K*.