#25

MATAKULIAH

KEAMANAN PERANGKAT LUNAK

Fungsi HASH Kriptografi & MAC

Syahrul Imardi, MT

STMIK Amik Riau

P25

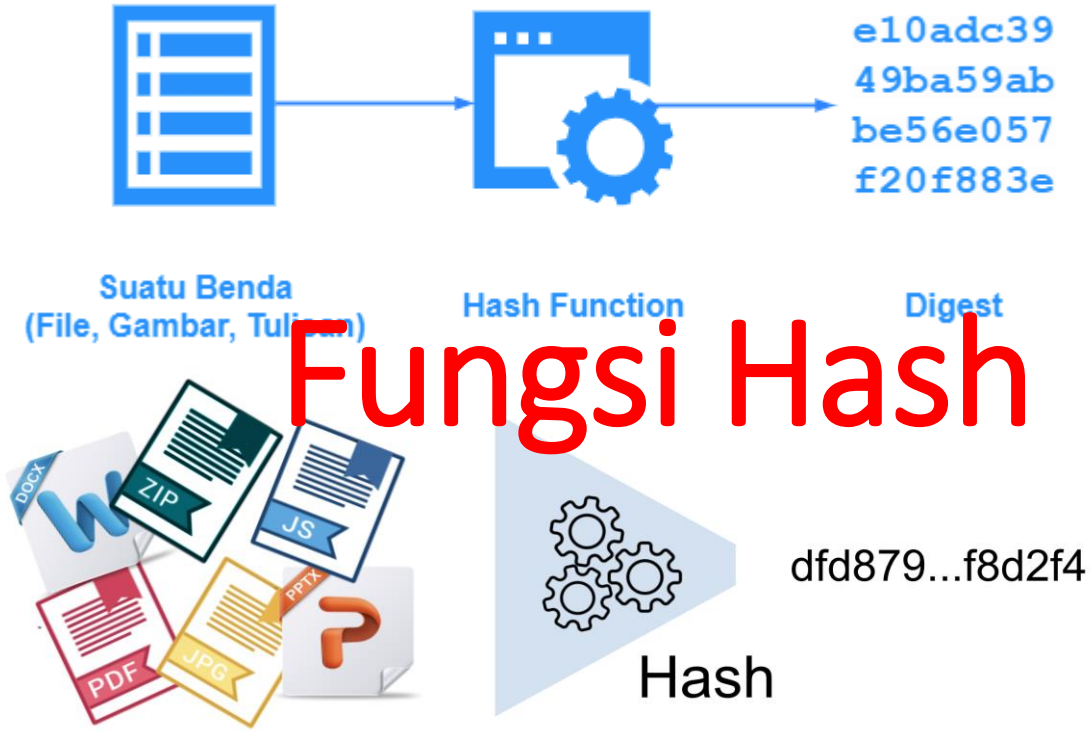
STMIK Amik Riau

HASH

MATAKULIAH
KEAMANAN PERANGKAT LUNAK

Syahrul Imardi, MT

P25: **Fungsi HASH Kriptografi dan MAC**


e10adc39
49ba59ab
be56e057
f20f883e
Suatu Benda
(File, Gambar, Tulisan)
Hash Function
Digest
Fungsi Hash
DOCX
ZIP
JS
PPTX
PDF
JPG
dfd879...f8d2f4
Hash

Fungsi Hash

- Fungsi yang mengkompresi pesan (M) berukuran sembarang menjadi *string* (*h*) yang berukuran *fixed*.
- Luaran (*output*) fungsi *hash* tersebut dinamakan pesan ringkas (*message-digest)* atau nilai hash (*hash value*)
- *Irreversible* (tidak bisa dikembalikan menjadi pesan semula)

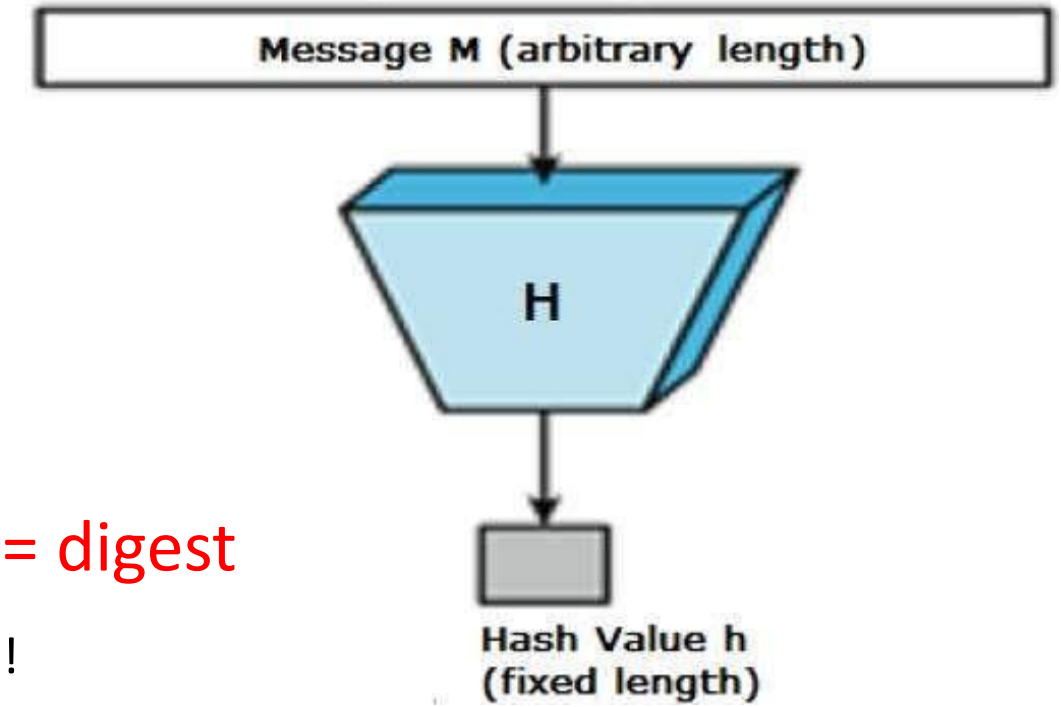
Fungsi Hash:

$$h = H(M)$$

h<<<<M

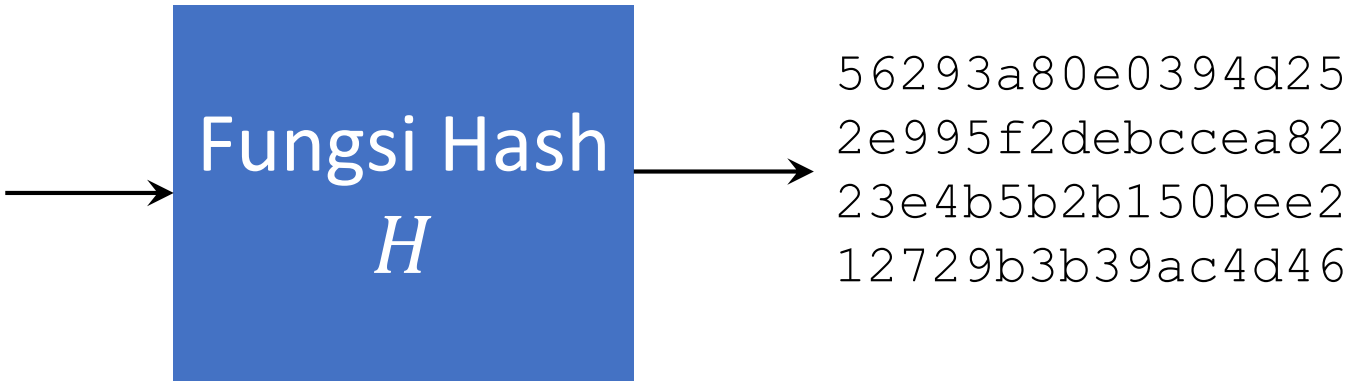
h = Hash value = message digest = digest

Contoh: *size*(*M*) = 1 MB → *size*(*h*) = 256 bit !!!!

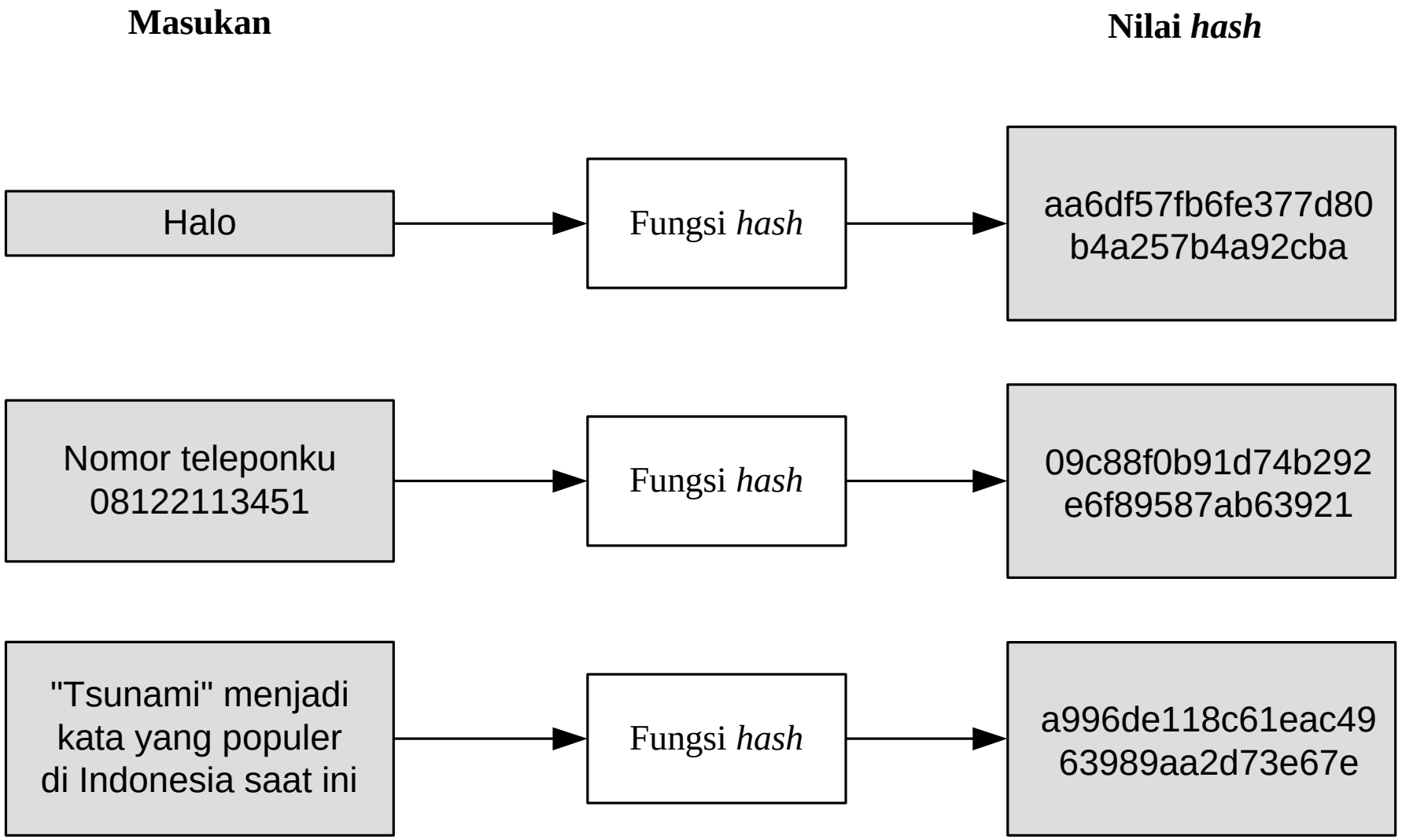


Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Pesan input



Nilai hash
(256 bit)


Masukan
Nilai *hash*
Halo
Fungsi *hash*
aa6df57fb6fe377d80
b4a257b4a92cba
Nomor teleponku
08122113451
Fungsi *hash*
09c88f0b91d74b292
e6f89587ab63921
"Tsunami" menjadi
kata yang populer
di Indonesia saat ini
Fungsi *hash*
a996de118c61eac49
63989aa2d73e67e

Fungsi *Hash* Satu-Arah

- Fungsi *hash* satu-arah (*one-way function*):
  - fungsi *hash* yang bekerja dalam satu arah.
  - satu arah: pesan yang sudah diubah menjadi *message digest* tidak dapat dikembalikan lagi menjadi pesan semula (*irreversible*).

Sifat-sifat fungsi *hash H*:

a) collision resistance : sangat sukar menemukan dua input a dan b sedemikian sehingga $H(a) = H(b)$

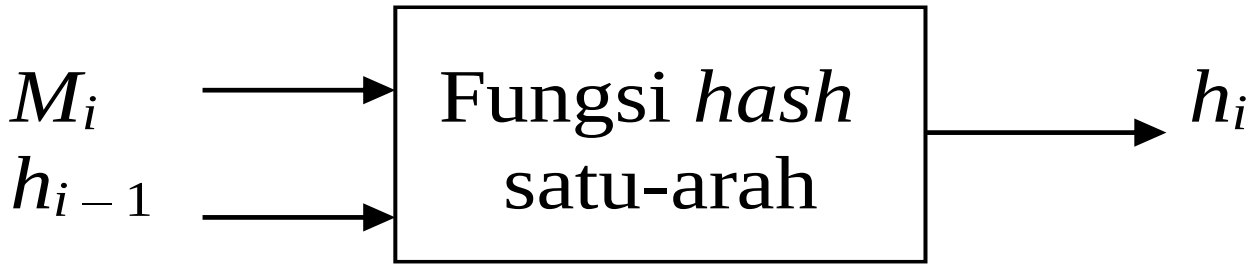
b) preimage resistance: untuk sembarang output y, sukar menemukan input a sedemikian sehingga $H(a) = y$

c) second preimage resistance – untuk input a dan output $y = H(a)$, sukar menemukan input kedua b sedemikian sehingga $H(b) = y$

Masukan fungsi *hash* adalah blok pesan (M) dan keluaran dari *hashing* blok pesan sebelumnya,

$$h_i = H(M_i, h_{i-1})$$

Skema fungsi *hash* ditunjukkan pada Gambar di bawah:



Gambar Fungsi *hash* satu-arah

- Fungsi *hash* satu arah tidak tepat disebut sebagai sebuah proses enkripsi, meskipun nilai hash tidak memiliki makna,

- sebab, nilai *hash* tidak dapat ditransformasi balik menjadi pesan semula.

- Alasan lainnya, proses *hashing* tidak menggunakan kunci.

- Ada beberapa fungsi *hash* satu-arah yang terdapat di dalam kriptografi:

Algoritma	Ukuran *message digest* (bit)
MD2/MD4/MD5	128
RIPEMD	128
RIPEMD-128/256	128/256
RIPEMD-160/320	160/320
SHA-1	160
SHA-256/SHA-224	256/224
SHA-512/SHA-384	512/384
SHA-3 (Keccak)	sembarang
WHIRLPOOL	512
Snefru	128 atau 256
BLAKE 256/512	156/512
Grøstl	max 512

SHA-2

Aplikasi Fungsi *Hash* Satu-Arah

1. Menjaga integritas pesan

   - Fungsi *hash* sangat peka terhadap perubahan 1 bit pada pesan

   - Pesan berubah 1 bit, nilai *hash* berubah sangat signifikan.

   - Bandingkan nilai *hash* baru dengan nilai *hash* lama. Jika sama, pesan masih asli. Jika tidak sama, pesan sudah dimodifikasi

Contoh:

(i) Pesan (berupa *file*) asli

```
Pada bulan Oktober 2004 ini, suhu udara kota Bandung terasa
lebih panas dari hari-hari biasanya. Menurut laporan Dinas
Meteorologi Kota Bandung, suhu tertinggi kota Bandung
adalah 33 derajat Celcius pada Hari Rabu, 17 Oktober yang
lalu. Suhu terseut sudah menyamai suhu kota Jakarta pada
hari-hari biasa. Menurut Kepala Dinas Meteorologi,
peningkatan suhu tersebut terjadi karena posisi bumi
sekarang ini lebih dekat ke matahari daripada hari-hari
biasa.

Sebutan Bandung sebagai kota sejuk dan dingin mungkin tidak
lama lagi akan tinggal kenangan. Disamping karena faktor
alam, jumlah penduduk yang padat, polusi dari pabrik di
sekita Bandung, asap knalpot kendaraan, ikut menambah
kenaikan suhu udara kota.
```

Nilai MD5: **2F82D0C845121B953D57E4C3C5E91E63**

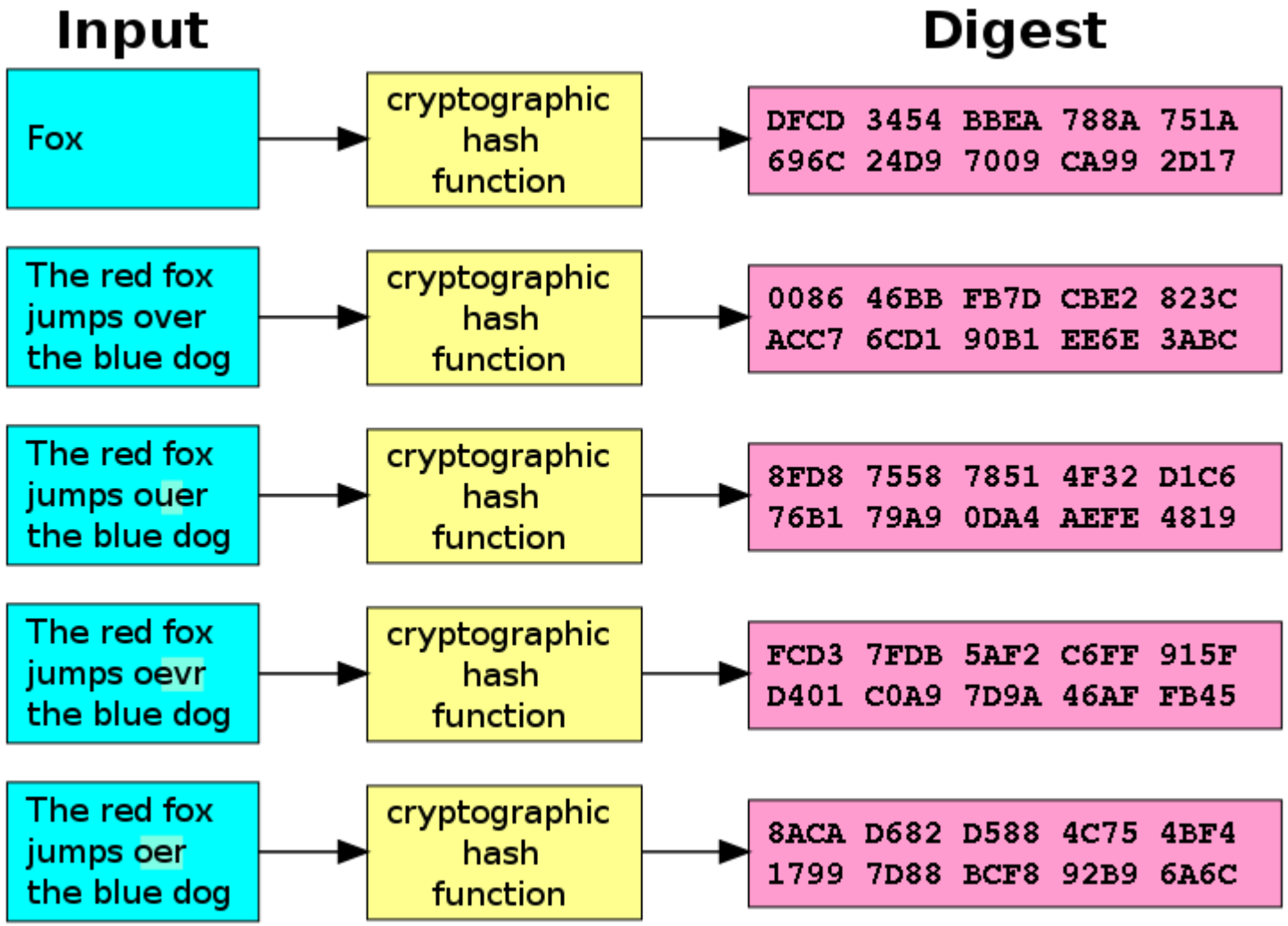
(ii) Misal 33 diubah menjadi 32

Pada bulan Oktober 2004 ini, suhu udara kota Bandung terasa lebih panas dari hari-hari biasanya. Menurut laporan Dinas Meteorologi Kota Bandung, suhu tertinggi kota Bandung adalah 32 derajat Celcius pada Hari Rabu, 17 Oktober yang lalu. Suhu terseut sudah menyamai suhu kota Jakarta pada hari-hari biasa. Menurut Kepala Dinas Meteorologi, peningkatan suhu tersebut terjadi karena posisi bumi sekarang ini lebih dekat ke matahari daripada hari-hari biasa.

Sebutan Bandung sebagai kota sejuk dan dingin mungkin tidak lama lagi akan tinggal kenangan. Disamping karena faktor alam, jumlah penduduk yang padat, polusi dari pabrik di sekita Bandung, asap knalpot kendaraan, ikut menambah kenaikan suhu udara kota.

Nilai MD5: **2D1436293FAEAF405C27A151C0491267**

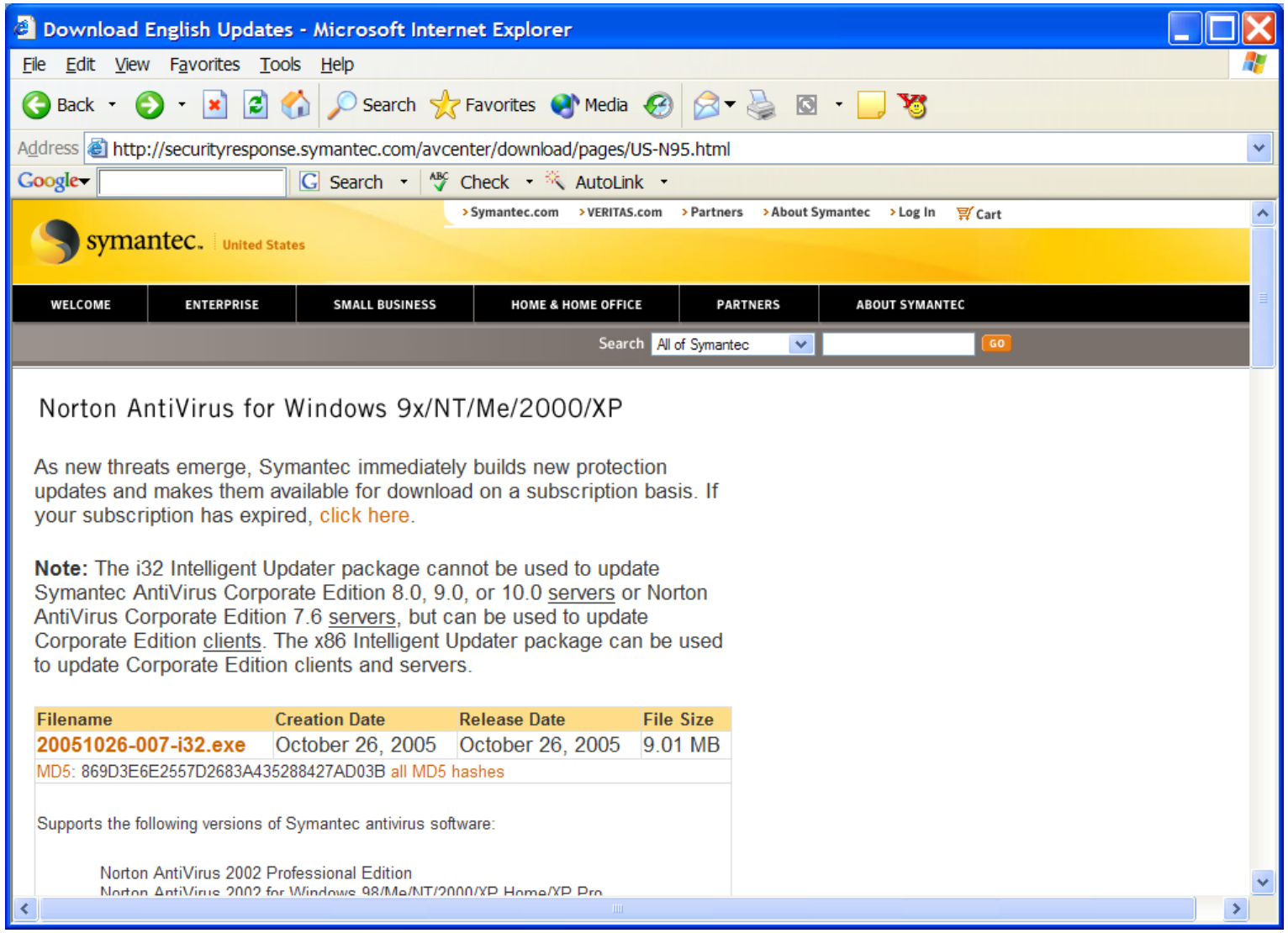
Sebelum diubah : $MD5_1$ = **2F82D0C845121B953D57E4C3C5E91E63**
Sesudah diubah : $MD5_2$ = **2D1436293FAEAF405C27A151C0491267**
Verifikasi: $MD5_1 \neq MD5_2$ (arsip sudah diubah)


Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

- Karena kegunaan untuk mendeteksi perubahan pesan, maka fungsi hash dinamakan juga:

  - *cryptographic checksum*
  - *message integrity check (MIC)*
  - *manipulation detection code (MDC)*

- Program yang di-*downlaod* dari internet sering dilengkapi dengan nilai *hash* untuk menjamin integritas *file*.



2. Menghemat waktu pengiriman.

- Misal untuk memverifikasi sebuah salinan arsip dengan arsip asli.
- Salinan dokumen berada di tempat yang jauh dari basisdata arsip asli
- Ketimbang mengirim salinan arsip tersebut secara keseluruhan ke komputer pusat (yang membutuhkan waktu transmisi lama), lebih mangkus mengirimkan *message digest*-nya.
- Jika *message digest* salinan arsip sama dengan *message digest* arsip asli, berarti salinan arsip tersebut sama dengan arsip master.

3. Menormalkan panjang data yang beraneka ragam.

- Misalkan *password* panjangnya bebas (minimal 8 karakter)
- *Password* disimpan di komputer *host* (*server*) untuk keperluan otentikasi pemakai komputer.
- *Password* disimpan di dalam basisdata.
- Untuk menyeragamkan panjang *field password* di dalam basisdata, *password* disimpan dalam bentuk nilai *hash* (panjang nilai *hash* tetap).

Kolisi

- Kolisi (*collision*) adalah kondisi dua *string* sembarang memiliki nilai *hash* yang sama.

- Adanya kolisi menunjukkan fungsi *hash* tidak aman secara kriptografis

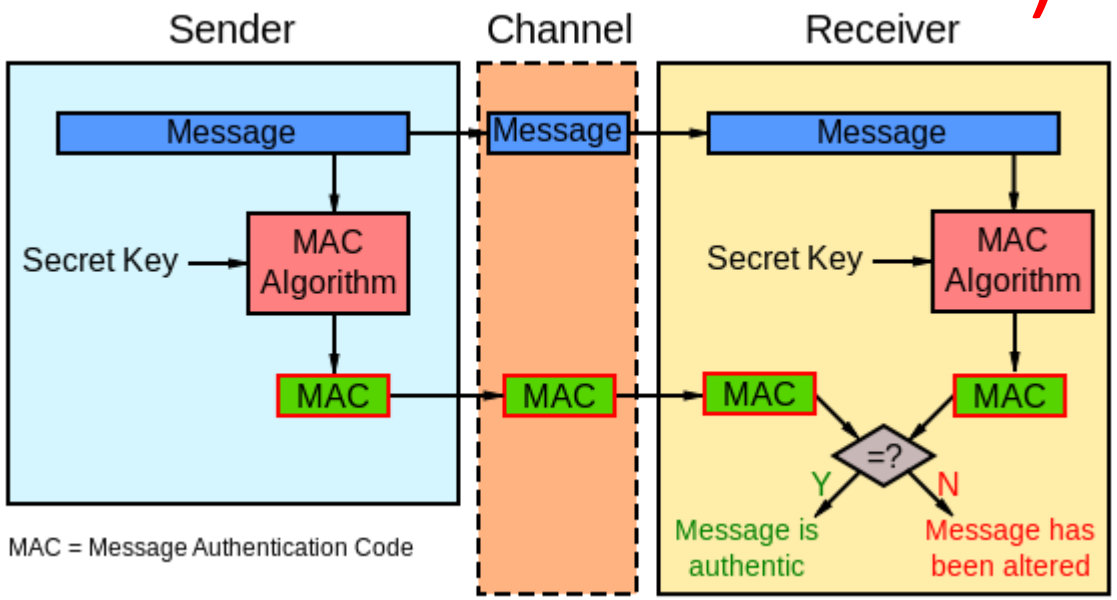
Tabel 12.1 Beberapa fungsi *hash*

Algoritma	Ukuran *message digest* (bit)	Ukuran blok pesan	Kolisi
MD2	128	128	Ya
MD4	128	512	Hampir
MD5	128	512	Ya
RIPEMD	128	512	Ya
RIPEMD-128/256	128/256	512	Tidak
RIPEMD-160/320	160/320	512	Tidak
SHA-0	160	512	Ya
SHA-1	160	512	Ada cacat
SHA-256/224	256/224	512	Tidak
SHA-512/384	512/384	1024	Tidak
WHIRLPOOL	512	512	Tidak

Figure 9.3 Message Authentication Code (MAC)

MAC

(*Message Authentication Code*)



Definisi

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

  MAC = $C_K(M)$

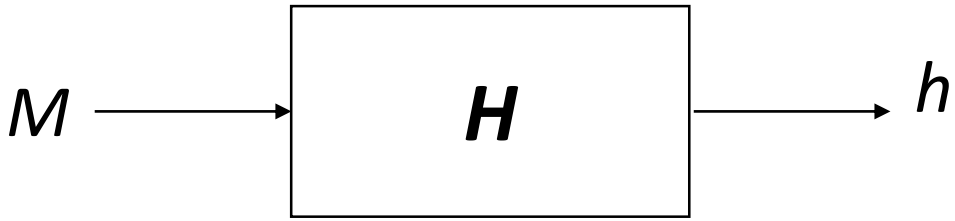
  MAC = nilai hash

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

  K = kunci rahasia

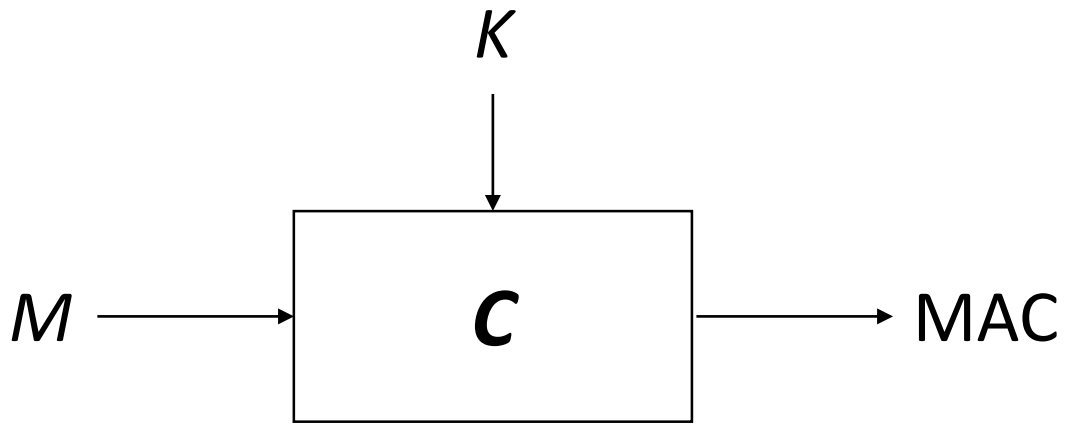
- Bandingkan dengan fungsi *hash* biasa seperti *MD5* atau *SHA* yang tidak memerlukan kunci dalam menghasilkan nilai *hash*.

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.

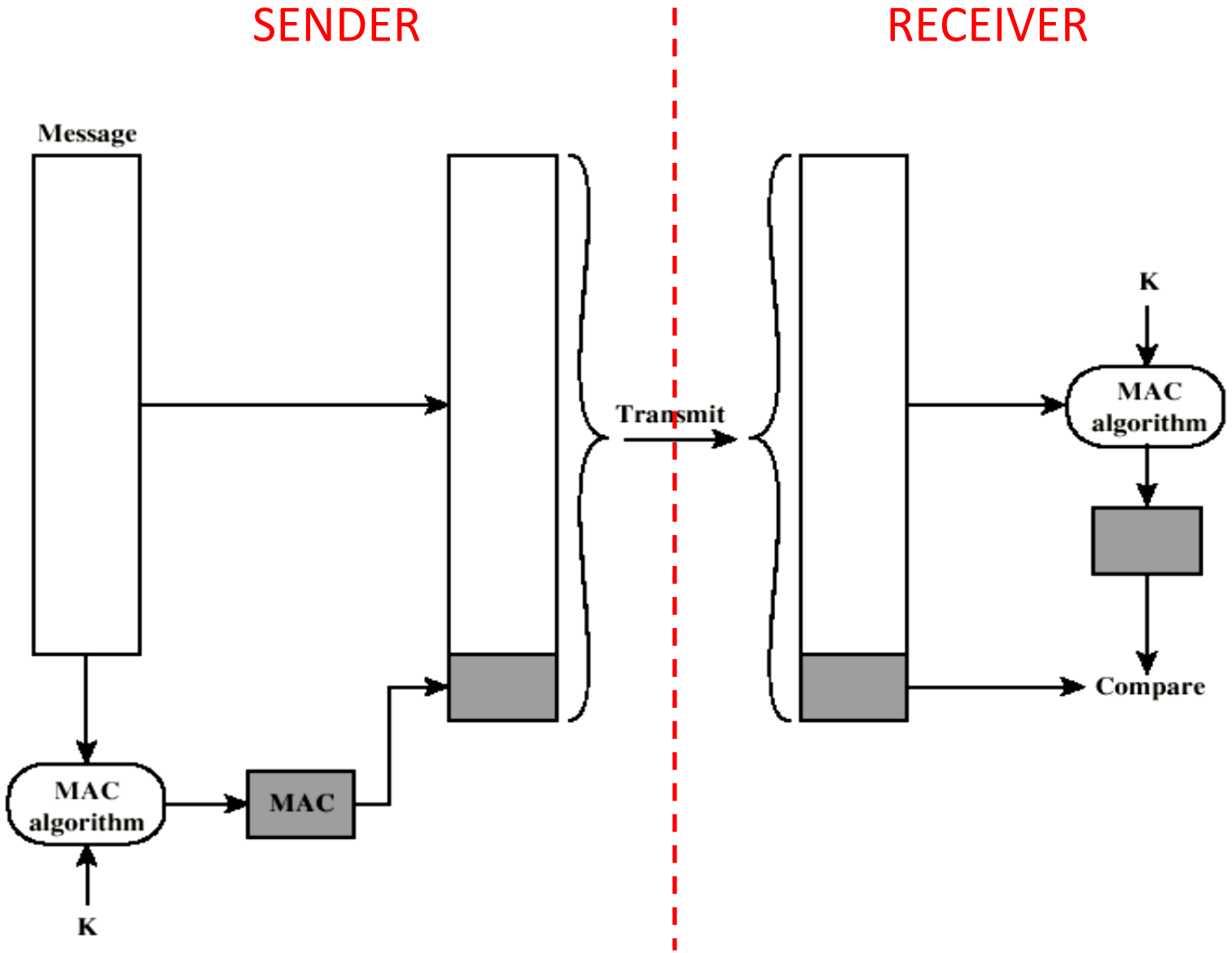
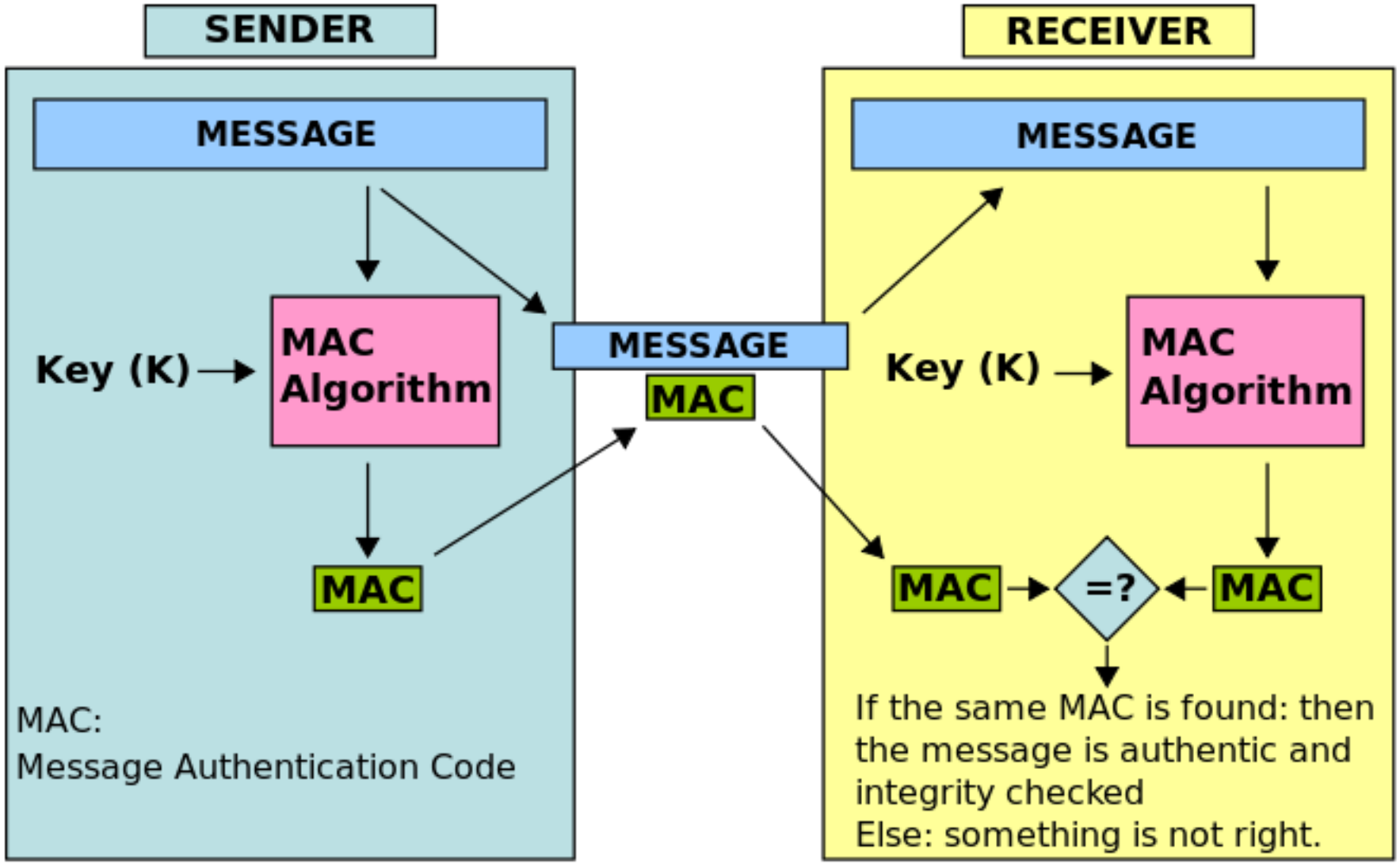


Figure 3.1 Message Authentication Using a Message Authentication Code (MAC)


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

Fungsi MAC

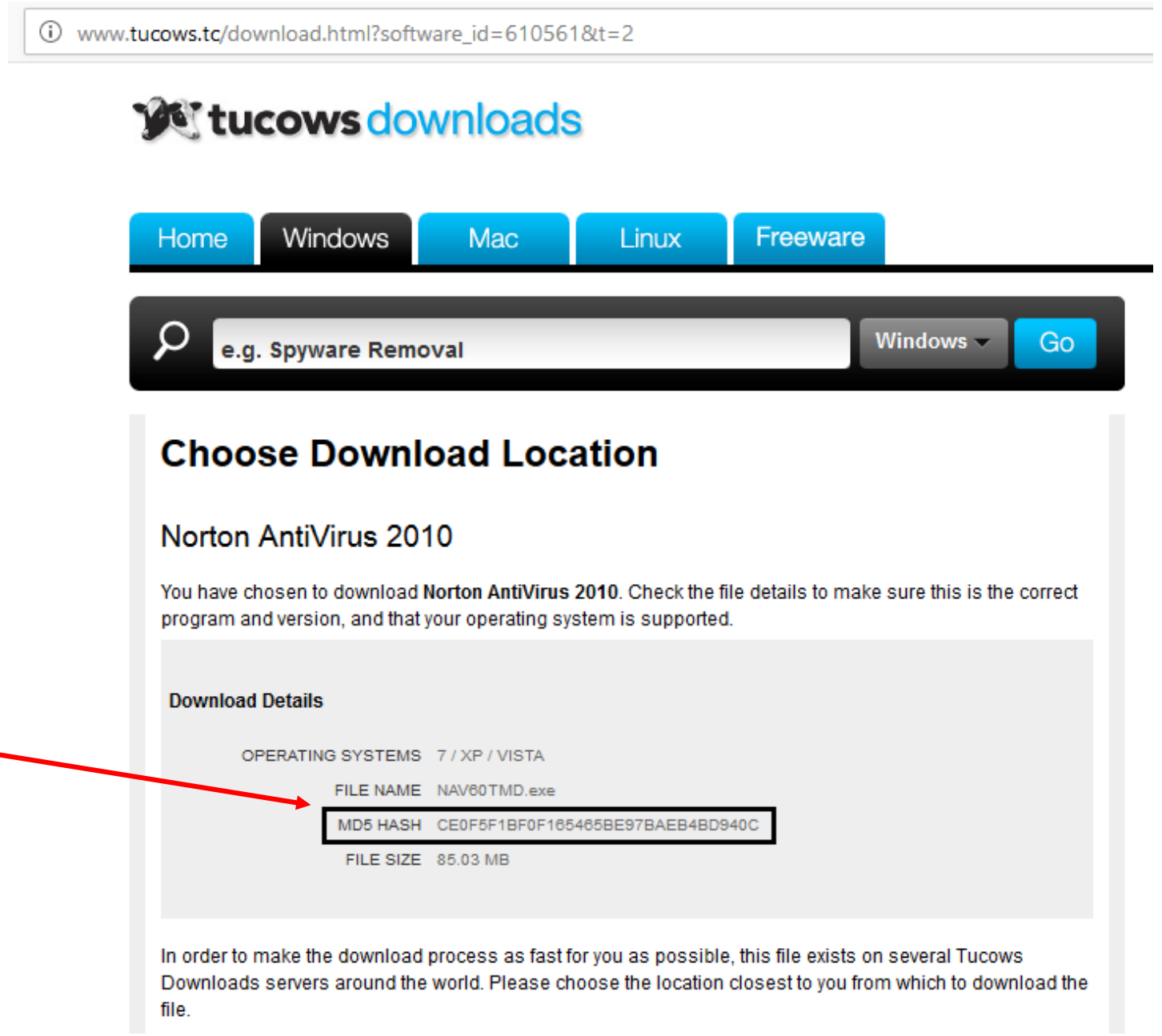
- Kegunaan: otentikasi dokumen (file)

  → 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.

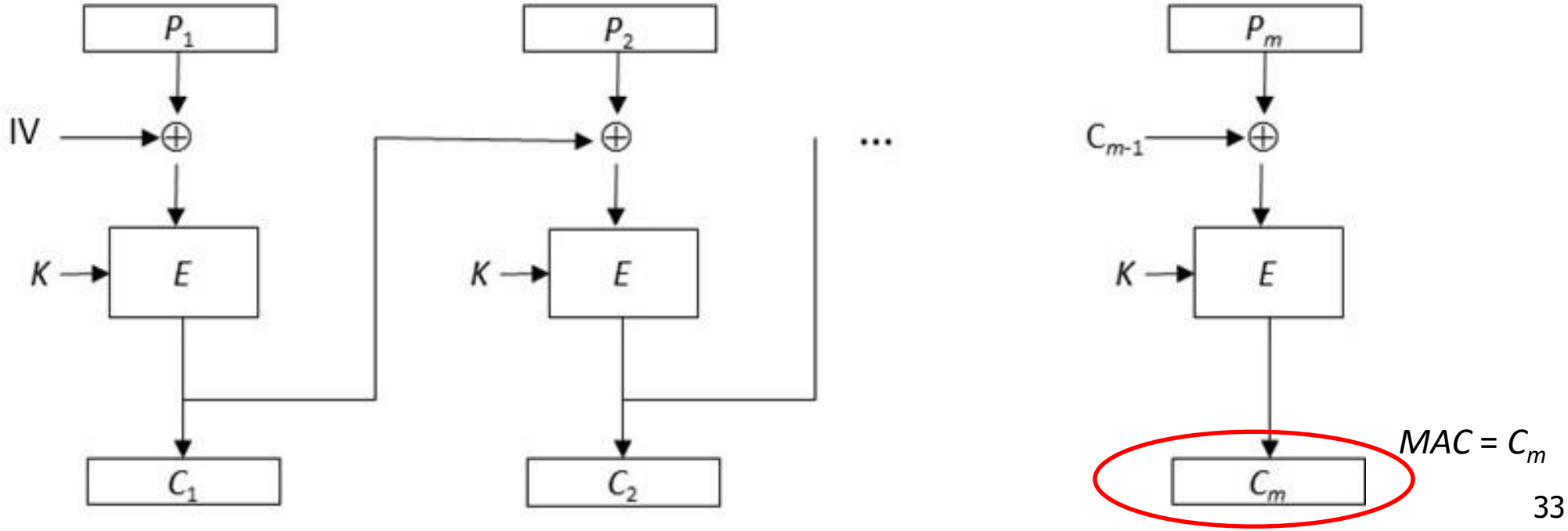
Hacker bisa mengganti file dengan file lain, mengganti nilai MD5 semula dengan nilai MD5 yang baru. Pengunduh file tidak dapat menyadarinya.



Algoritma MAC

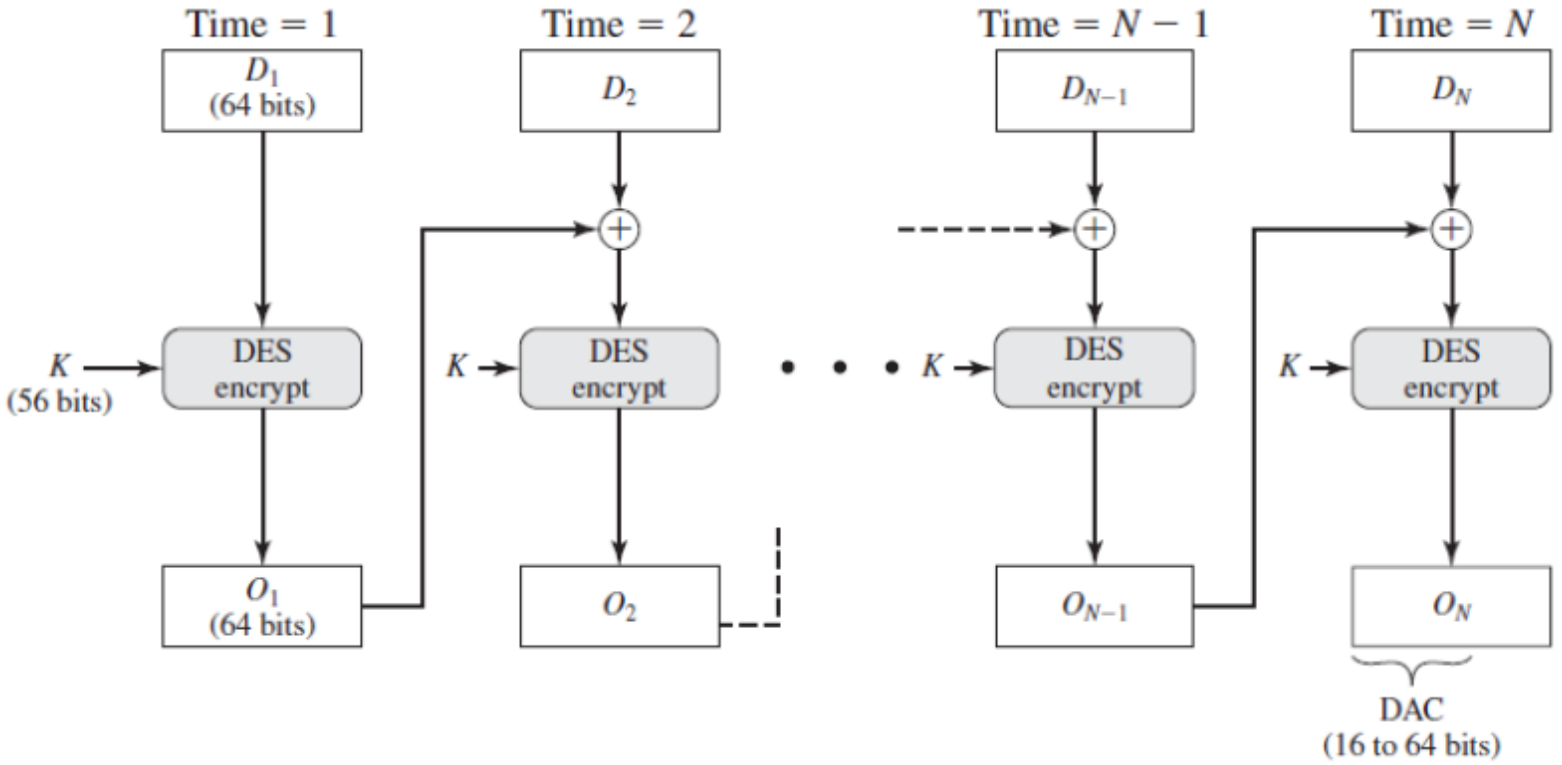
(a) Algoritma MAC berbasis *block cipher*

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



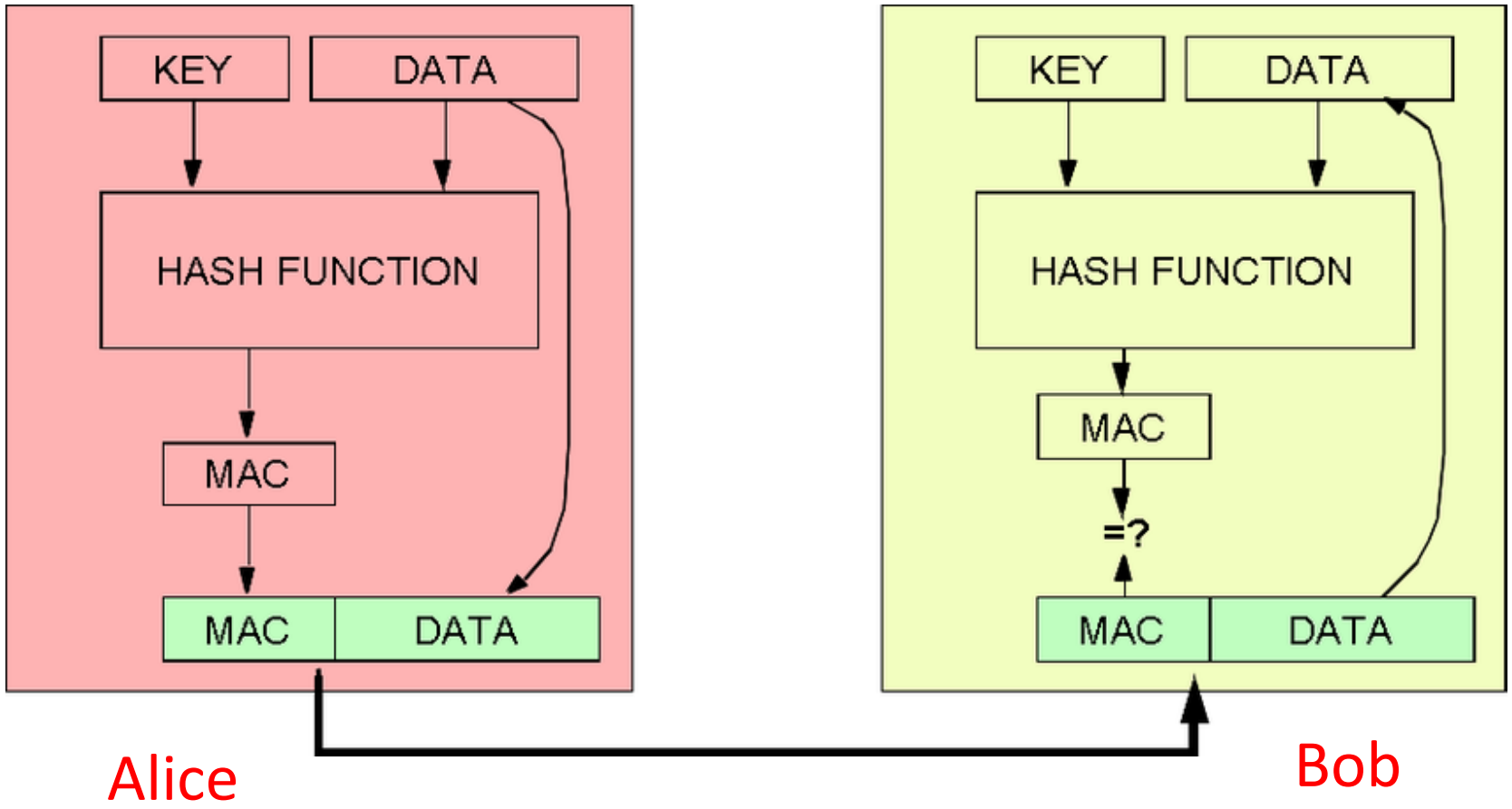
- Misalkan *DES* digunakan sebagai *cipher* blok, maka MAC = ukuran blok = 64 bit, dan kunci rahasia *MAC* adalah kunci DES yang panjangnya 56 bit.

- *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 = *Halo, Bob!*

K = 12345678

Fungsi Hash: SHA-1

MAC = 6f8605c7c3a649a40abfb87b44aa21f356e931a0

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

Referensi utama :

>> Michael Felderer , Riccardo Scandariato (editor) - Exploring Security in Software Architecture and Design, 2018.

>> Nancy R. Mead, Carol Woody - Cyber Security Engineering_ A Practical Approach for Systems and Software Assurance-Addison-Wesley Professional (2016)

>> James Helfrich - Security for Software Engineers-CRC Press (2019)

>> Pete Loshin - Simple Steps to Data Encryption_ A Practical Guide to Secure Computing-Syngress (2013)

>> Tevfik Bultan,Fang Yu,Muath Alkhalaf,Abdulbaki Aydin (auth.) - String Analysis for Software Verification and Security (2017


Ada pertanyaan?