

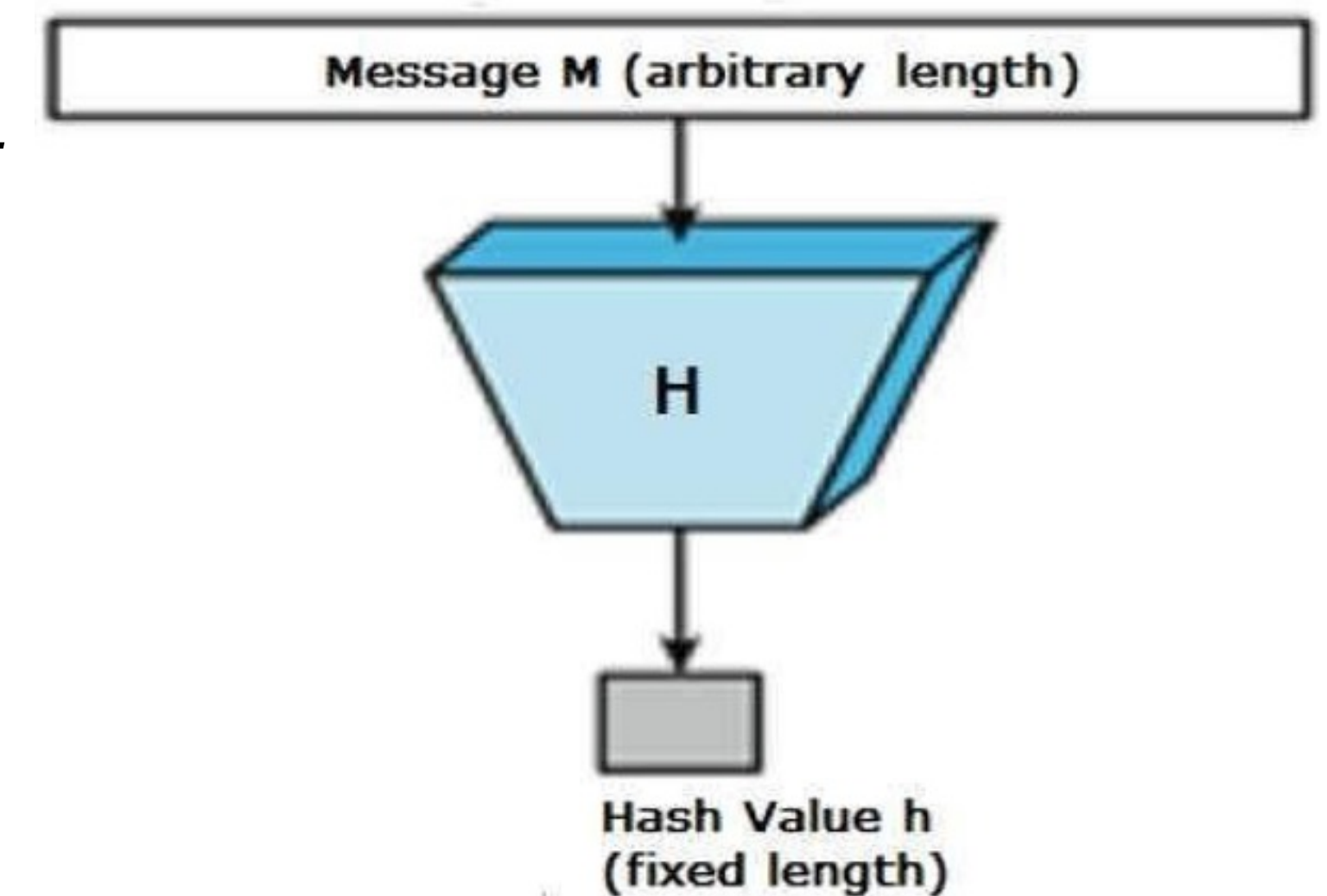
# Fungsi Hash

## Bahan Kuliah Keamanan Data

Sevi Nurafni

**Fakultas Sains dan Teknologi**  
**Universitas Koperasi Indonesia 2025**

- 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:

$$h = H(M)$$

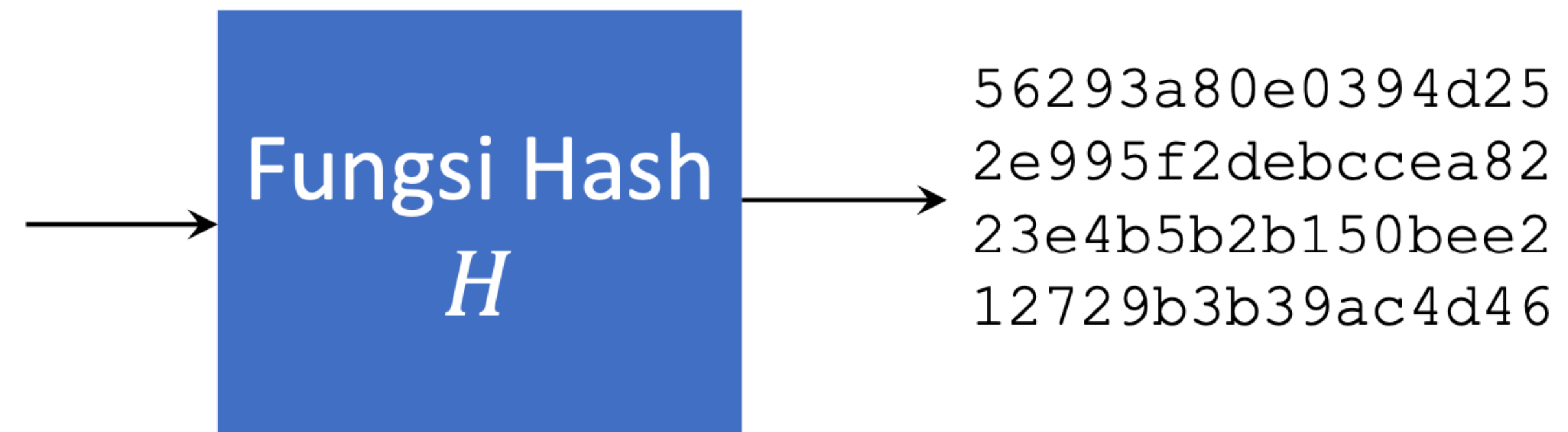
$$h \lll M$$

$h$  = Hash value = message digest = digest

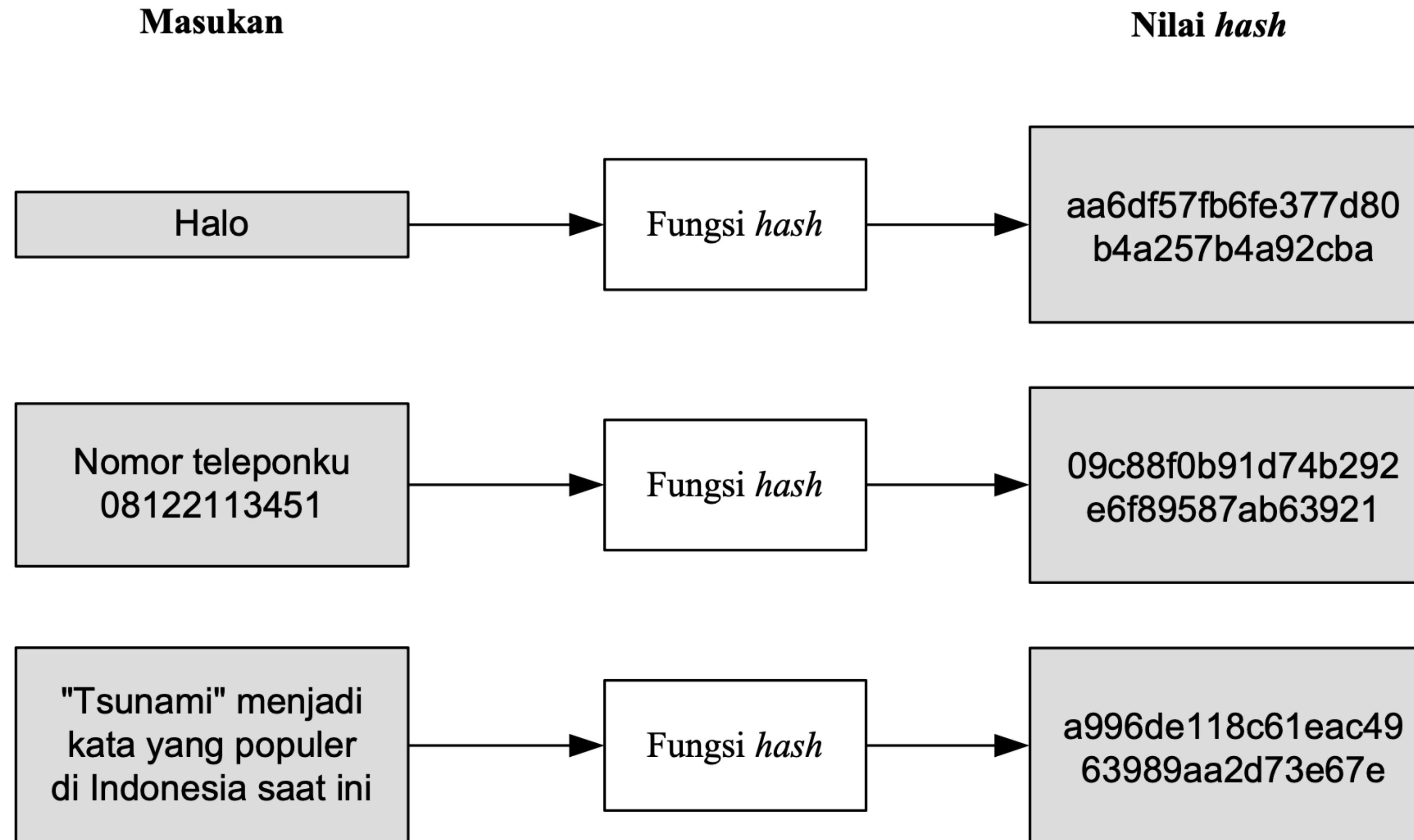
Contoh:  $size(M) = 1 \text{ MB} \rightarrow size(h) = 256 \text{ bit}$

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)



https://codebeautify.org/md5-hash-generator

 **Code Beautify**

JSON FormatterXML FormatterCalculatorsJSON BeautifierRecent LinksSitemapFavs 

Login

MD2 Hash Generator

MD4 Hash Generator

**MD5 Hash Generator**

NTLM Hash Generator

SHA1 Hash Generator

SHA2 Hash Generator

SHA224 Hash Generator

SHA256 Hash Generator

SHA384 Hash Generator

SHA512 Hash Generator

SHA512/224 Hash Generator

SHA512/256 Hash Generator

SHA3-224 Hash Generator

SHA3-256 Hash Generator

SHA3-384 Hash Generator

SHA3-512 Hash Generator

# MD5 Hash Generator

 Add to Fav

New

Save & Share

Enter the plain or Cipher Text:

Sample

sebentar lagi UAS, semangat!



Size : **28** B, 28 Characters

☒ Auto

Generate

 File..

 Load URL

Result of MD5 Generated Hash:

Upper CaseLower Case

181a65782d59bd5bc6a51ec408874d03

Size : **32** B, 32 Characters

# 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 $H$ :

1. *Collision resistance* : sangat sukar menemukan dua input  $a$  dan  $b$  sedemikian sehingga  $H(a) = H(b)$
2. *Preimage resistance* : untuk sembarang output  $y$ , sukar menemukan input  $a$  sedemikian sehingga  $H(a) = y$
3. *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:





- Ingat: Fungsi hash satu arah tidak tepat disebut sebagai sebuah fungsi 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 <i>message digest</i> (bit)
<i>MD2/MD4/MD5</i>	128
<i>RIPEMD</i>	128
<i>RIPEMD-128/256</i>	128/256
<i>RIPEMD-160/320</i>	160/320
<i>SHA-1</i>	160
<i>SHA-256/SHA-224</i>	256/224
<i>SHA-512/SHA-384</i>	512/384
<i>SHA-3 (Keccak)</i>	sembarang
<i>WHIRLPOOL</i>	512
<i>Snefru</i>	128 atau 256
<i>BLAKE 256/512</i>	156/512
<i>Grøstl</i>	max 512

# 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



## a. 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**



# Contoh



## b. Misal 33 diubah menjadi 32

Sebelum diubah :

$MD5_1 = 2F82D0C845121B953D57E4C3C5E91E63$

Sesudah diubah :

$MD5_2 = 2D1436293FAEAF405C27A151C0491267$

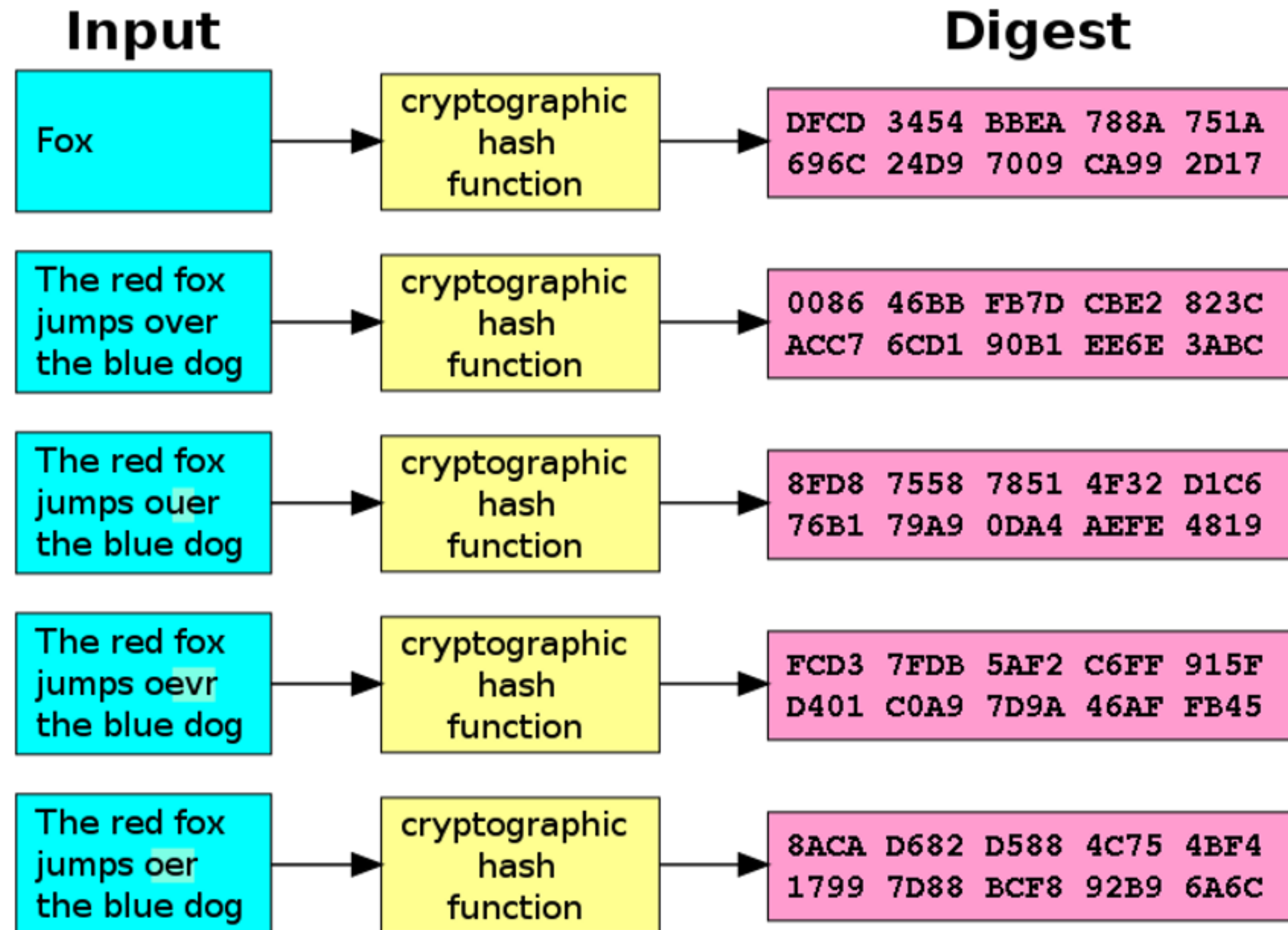
Verifikasi:  $MD5_1 \neq MD5_2$  (arsip sudah diubah)

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 tersebut 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**



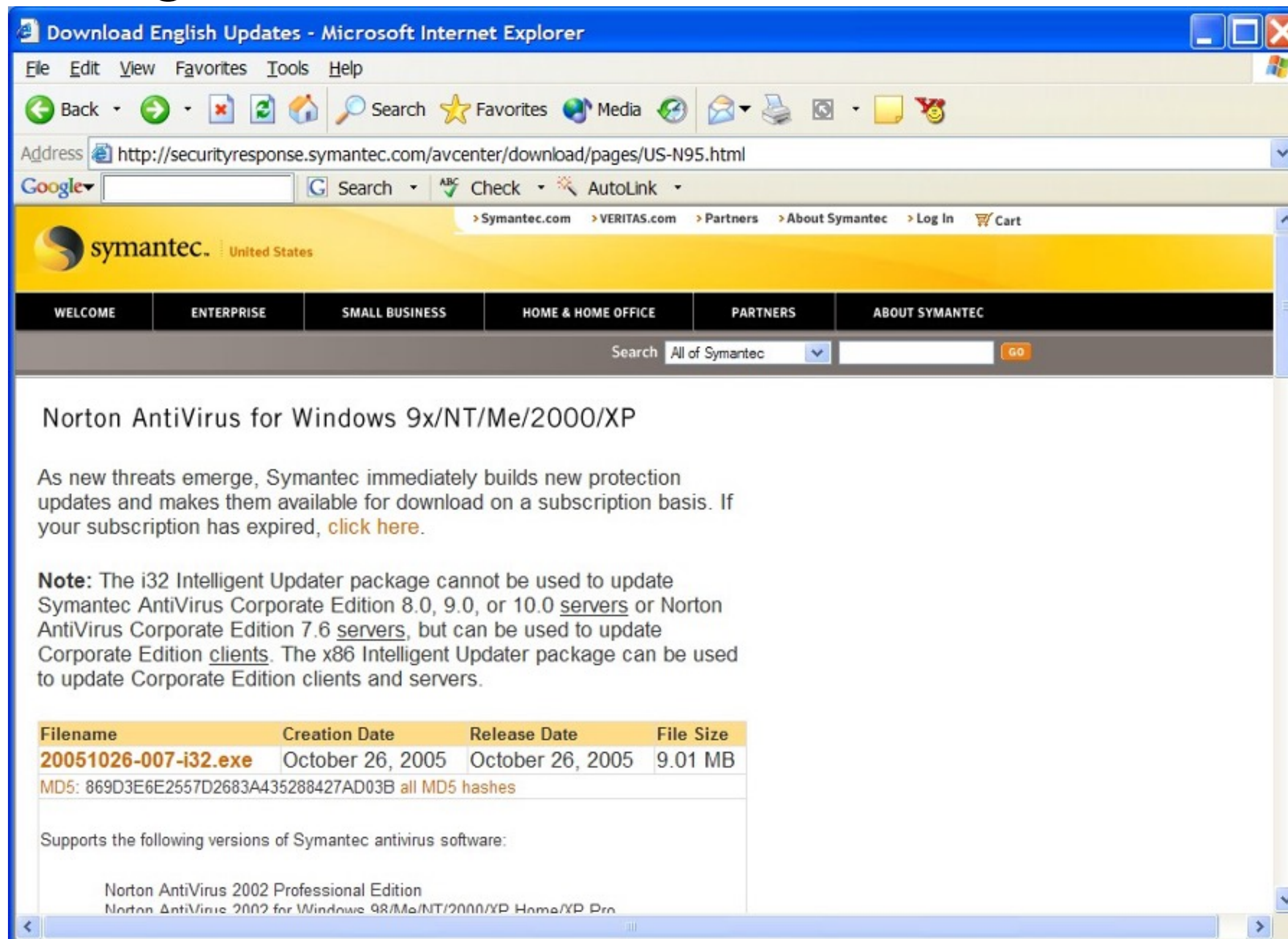


- Karena kegunaan untuk mendeteksi perubahan pesan, maka fungsi hash dinamakan juga:
  - *cryptographic checksum*
  - *message integrity check (MIC)*
  - *manipulation detection code (MDC)*





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



Download English Updates - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print Mail News RSS Feeds

Address <http://securityresponse.symantec.com/avcenter/download/pages/US-N95.html>

Google Search Check AutoLink

Symantec.com VERITAS.com Partners About Symantec Log In Cart

symantec. United States

WELCOME ENTERPRISE SMALL BUSINESS HOME & HOME OFFICE PARTNERS ABOUT SYMANTEC

Search All of Symantec GO

### Norton AntiVirus for Windows 9x/NT/Me/2000/XP

As new threats emerge, Symantec immediately builds new protection updates and makes them available for download on a subscription basis. If your subscription has expired, [click here](#).

**Note:** The i32 Intelligent Updater package cannot be used to update Symantec AntiVirus Corporate Edition 8.0, 9.0, or 10.0 servers or Norton AntiVirus Corporate Edition 7.6 servers, but can be used to update Corporate Edition clients. The x86 Intelligent Updater package can be used to update Corporate Edition clients and servers.

Filename	Creation Date	Release Date	File Size
<b>20051026-007-i32.exe</b>	October 26, 2005	October 26, 2005	9.01 MB

MD5: 869D3E6E2557D2683A435288427AD03B [all MD5 hashes](#)

Supports the following versions of Symantec antivirus software:

- Norton AntiVirus 2002 Professional Edition
- Norton AntiVirus 2002 for Windows 98/Me/NT/2000/XP Home/XP Pro

## 2. Menghemat Waktu Pengiriman

- Misal untuk memverifikasi sebuah salinan arsip dengan arsip asli.
- Salinan dokumen berada di tempat yang jauh dari basis data arsip asli.
- Ketimbang mengirim salinan arsip tersebut secara keseluruhan ke komputer pusat (yang membutuhkan waktu transmisi lama), lebih efisien 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 basis data.
- 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



## 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

**SELAMAT  
BELAJAR**