

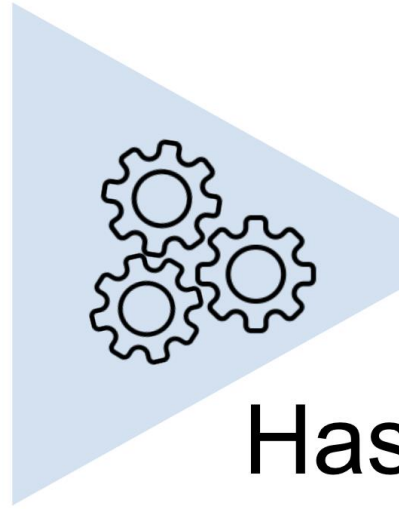
Bahan kuliah IF4020 Kriptografi

Fungsi Hash



Oleh: Rinaldi Munir

Program Studi Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
2024



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)

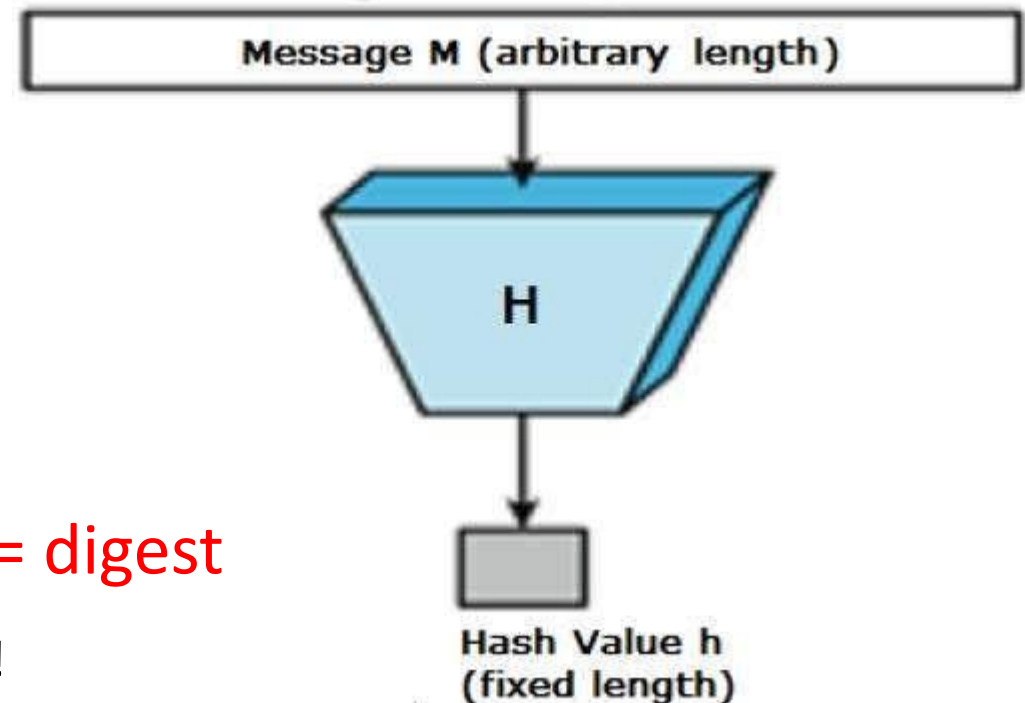
Fungsi Hash:

$$h = H(M)$$

$$h \lll M$$

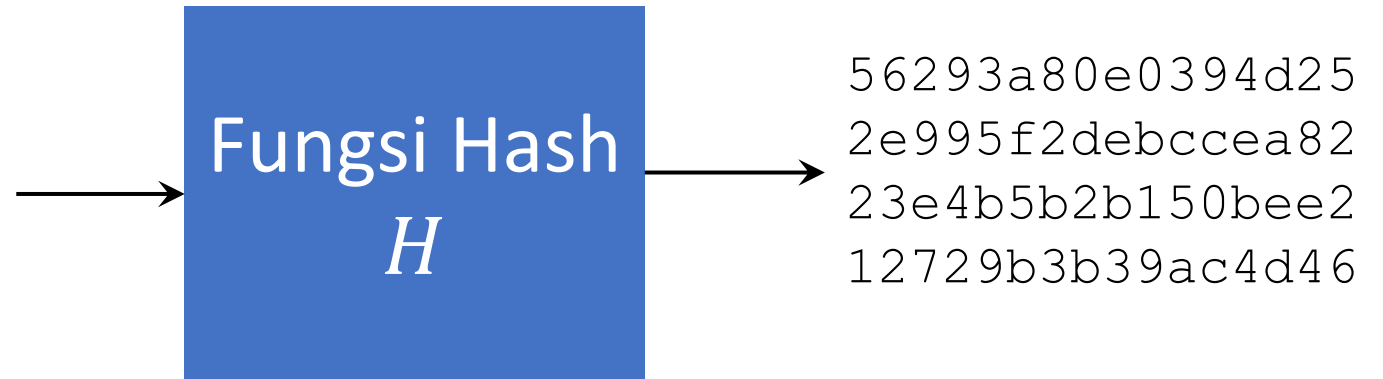
$h = \text{Hash value} = \text{message digest} = \text{digest}$

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



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

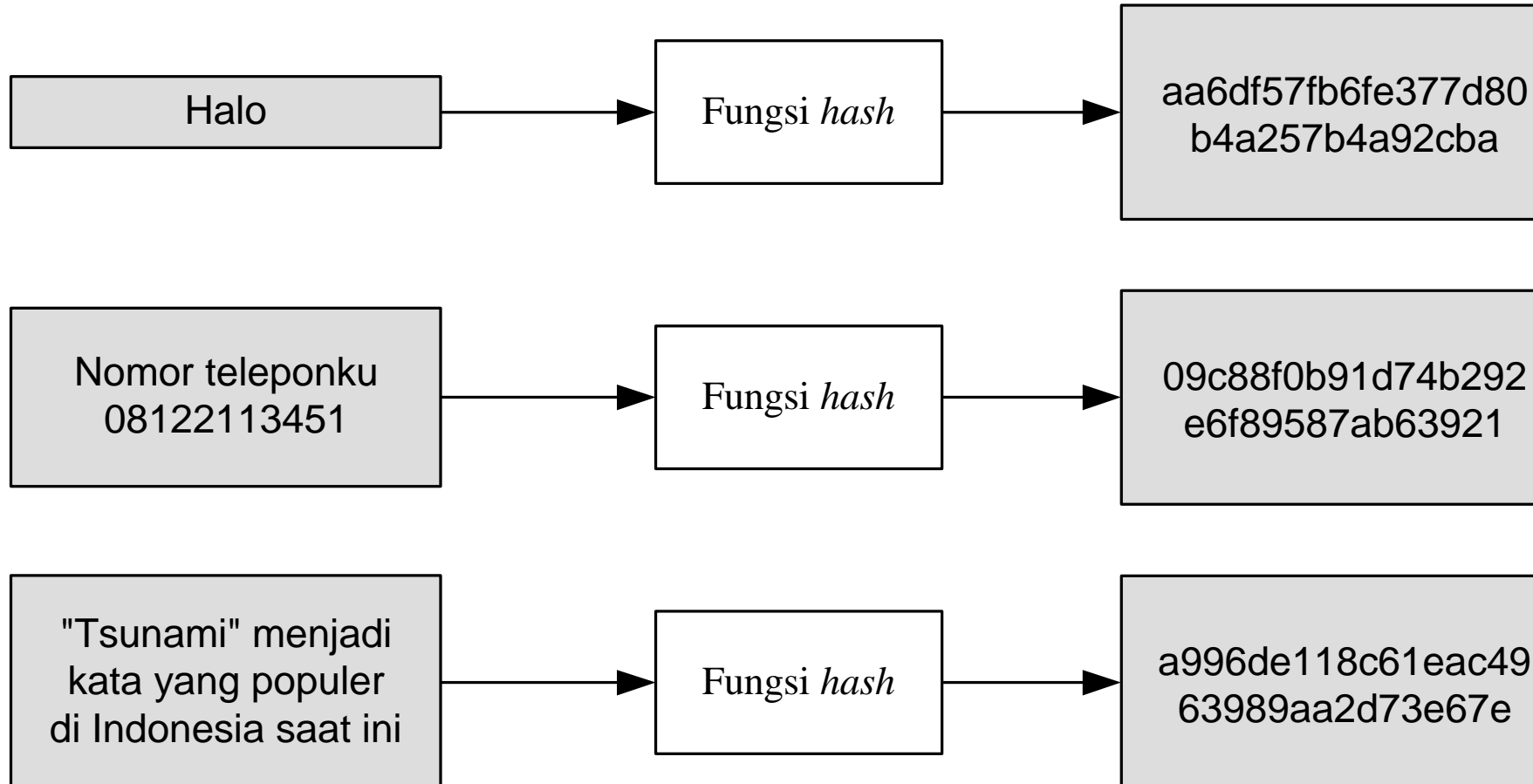


56293a80e0394d25
2e995f2debccea82
23e4b5b2b150bee2
12729b3b39ac4d46

**Nilai hash
(256 bit)**

Masukan

Nilai *hash*



The screenshot shows a web browser at the URL <https://codebeautify.org/md5-hash-generator>. On the left is a sidebar menu with various hash generators, with "MD5 Hash Generator" selected. The main content area features the title "MD5 Hash Generator" and a "Save & Share" button. Below the title is a text input field containing the sample text "Halo gaes, tetap semangat belajar meski berpuasa" with a red wavy underline. To the right of the input field are icons for refresh, folder, save, trash, and copy, along with the word "Sample". Below the input field, it displays "Size : 48 B, 48 Characters". There are four buttons: "Auto" (checked), "Generate" (with a gear icon), "File.." (with an upload icon), and "Load URL" (with a link icon). Below these buttons is the label "Result of MD5 Generated Hash:" followed by "Upper Case" and "Lower Case" options, and a copy icon. The output field contains the MD5 hash "e0cde99e50c6aa443357885af1395be9".

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

- 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:

SHA-2 {

Algoritma	Ukuran <i>message digest</i> (bit)
<i>MD2/MD4/MD5</i>	128
<i>RIPEND</i>	128
<i>RIPEND-128/256</i>	128/256
<i>RIPEND-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:

(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 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**

(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 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.

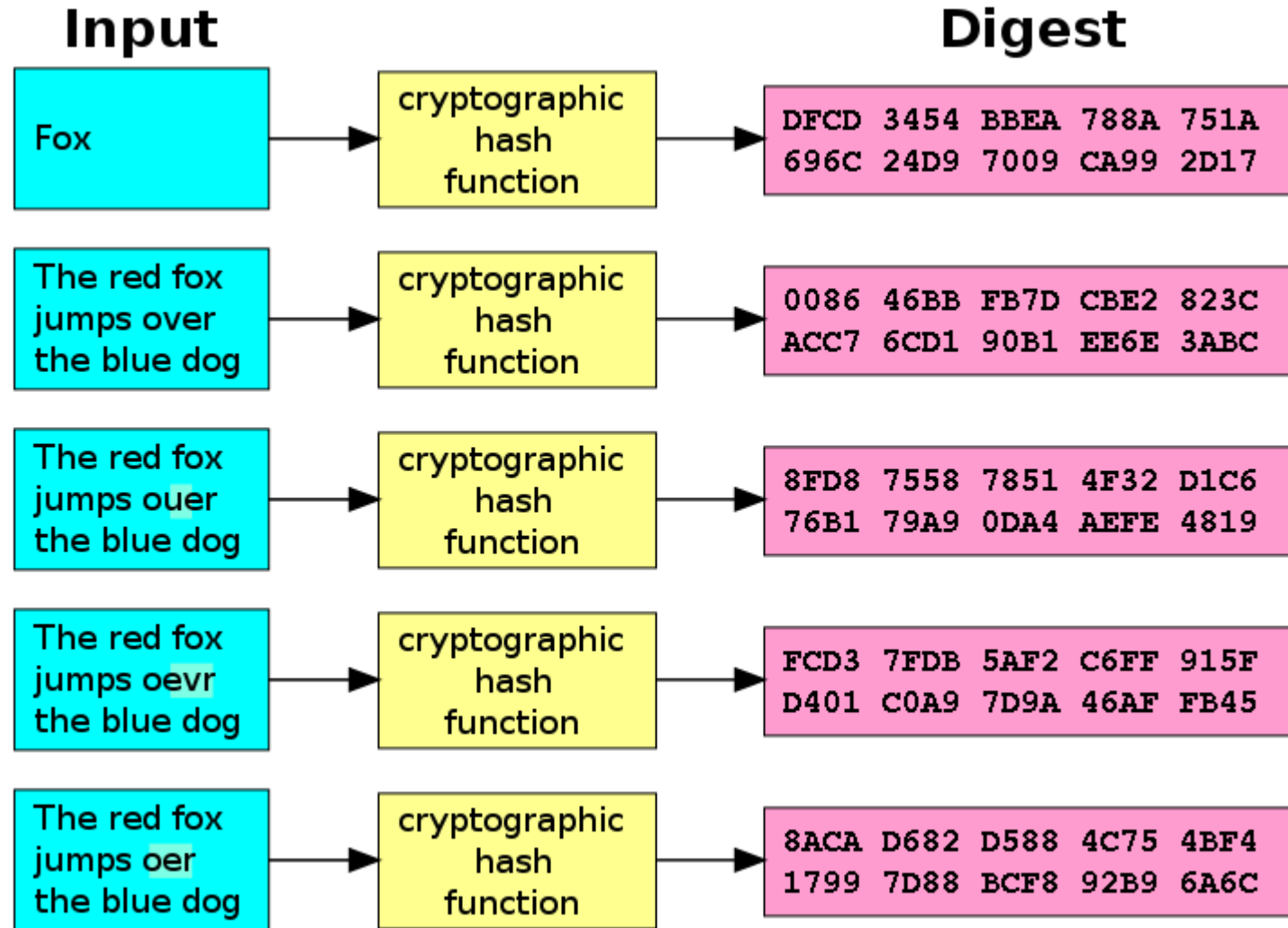
Sebutan Bandung sebagai kota sejuk dan dingin mungkin tidak lama lagi akan tinggal kenangan. Disamping karena faktor alam, jumlah penduduk yang padat, polusi dari pabrik di sekita Bandung, asap knalpot kendaraan, ikut menambah kenaikan suhu udara kota.

Nilai MD5: **2D1436293FAEAF405C27A151C0491267**

Sebelum diubah : MD5₁ = **2F82D0C845121B953D57E4C3C5E91E63**

Sesudah diubah : MD5₂ = **2D1436293FAEAF405C27A151C0491267**

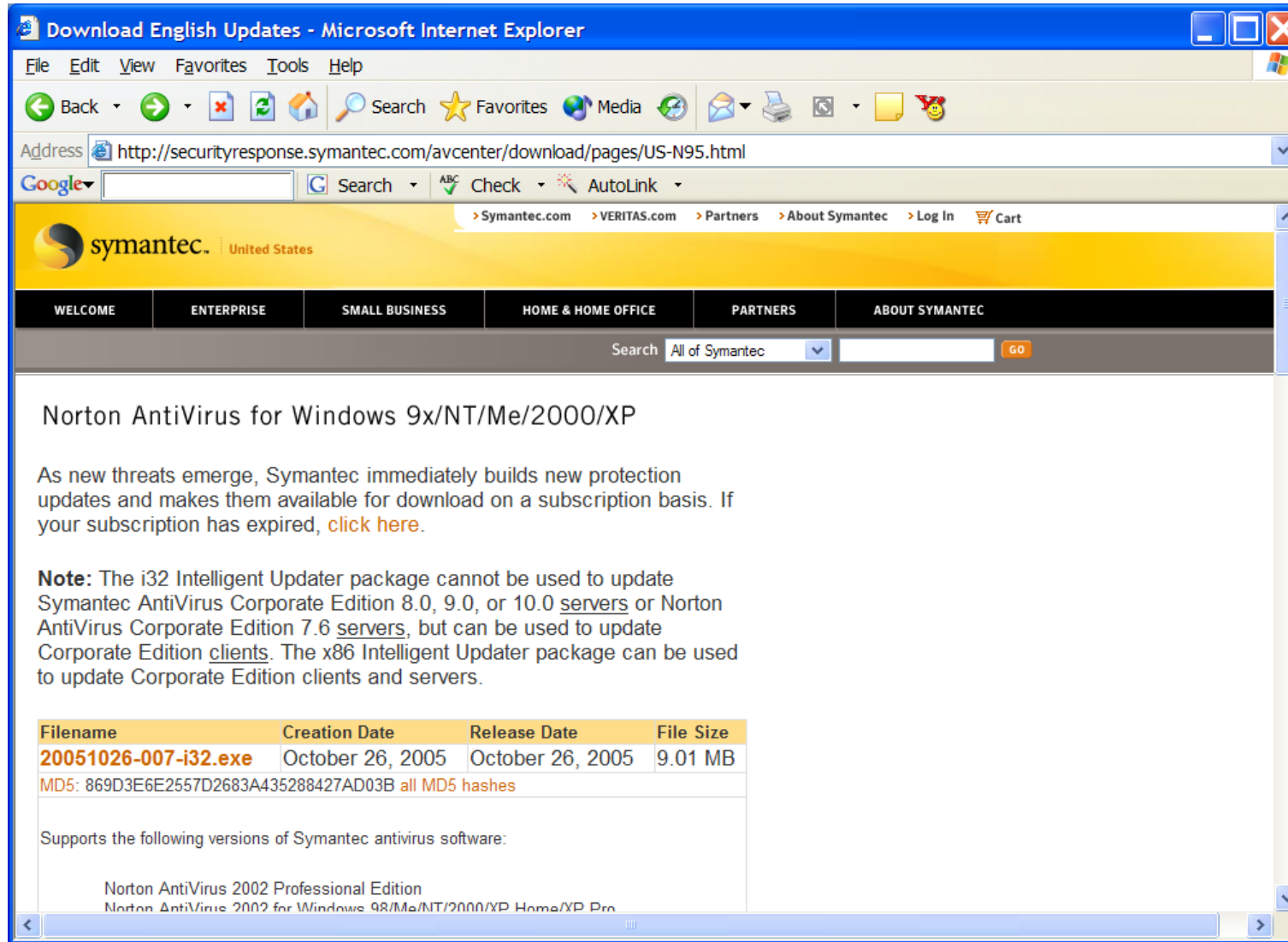
Verifikasi: MD5₁ ≠ MD5₂ (arsip sudah diubah)



- 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*.



Download English Updates - Microsoft Internet Explorer

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

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
20051026-007-i32.exe	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 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 <i>message digest</i> (bit)	Ukuran blok pesan	Kolisi
<i>MD2</i>	128	128	Ya
<i>MD4</i>	128	512	Hampir
<i>MD5</i>	128	512	Ya
<i>RIPEMD</i>	128	512	Ya
<i>RIPEMD-128/256</i>	128/256	512	Tidak
<i>RIPEMD-160/320</i>	160/320	512	Tidak
<i>SHA-0</i>	160	512	Ya
<i>SHA-1</i>	160	512	Ada cacat
<i>SHA-256/224</i>	256/224	512	Tidak
<i>SHA-512/384</i>	512/384	1024	Tidak
<i>WHIRLPOOL</i>	512	512	Tidak