Bahan kuliah IF4031 Kriptografi dan Koding

Fungsi Hash

Oleh: Rinaldi Munir

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

Otentikasi Pesan dan Pengirim

- Masalah otentikasi (*authentication*) berhubungan dengan keaslian pesan dan keaslian pengirim pesan

- Otentikasi pesan: memastikan bahwa pesan masih asli, utuh, tidak mengalami perubahan selama ditransmisikan ke penerima pesan.

- Otentikasi pengirim: memastikan bahwa pesan berasal dari pengirim yang asli atau pengirim yang sesungguhnya, bukan dari pihak lain

Ingat Kembali empat layanan kriptografi

1. Kerahasiaan pesan (*Confidentiality/privacy/secrecy*)

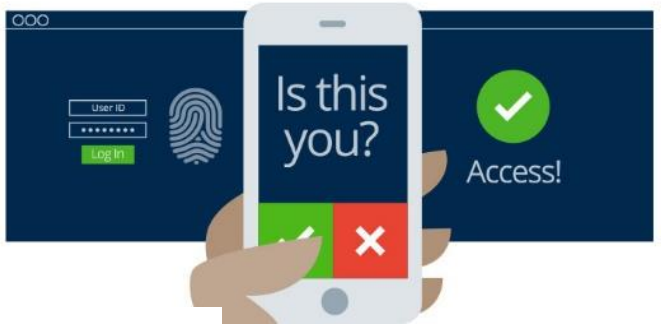
   → dengan mengenkripsi pesan

2. Keaslian pesan (*Data integrity*)

   → menggunakan fungsi hash atau MAC

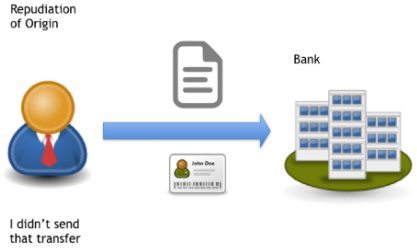
3. Keaslian pengirim dan penerima pesan (*Authentication*)

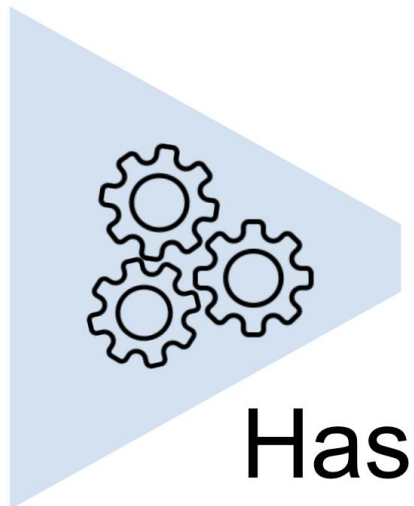
   → menggunakan MAC atau digital signature



4. Anti penyangkalan (*Non-repudiation*)

   → mengguanakan digital signature





Hash

dfd879...f8d2f4

Fungsi Hash

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

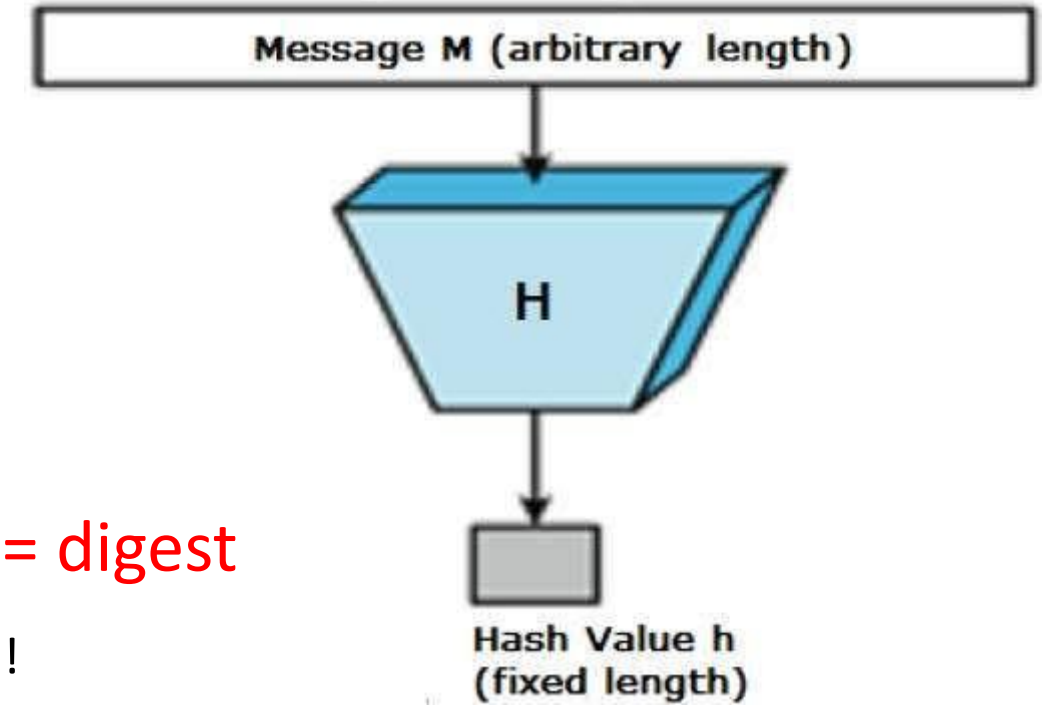
Fungsi Hash:

$$h = H(M)$$

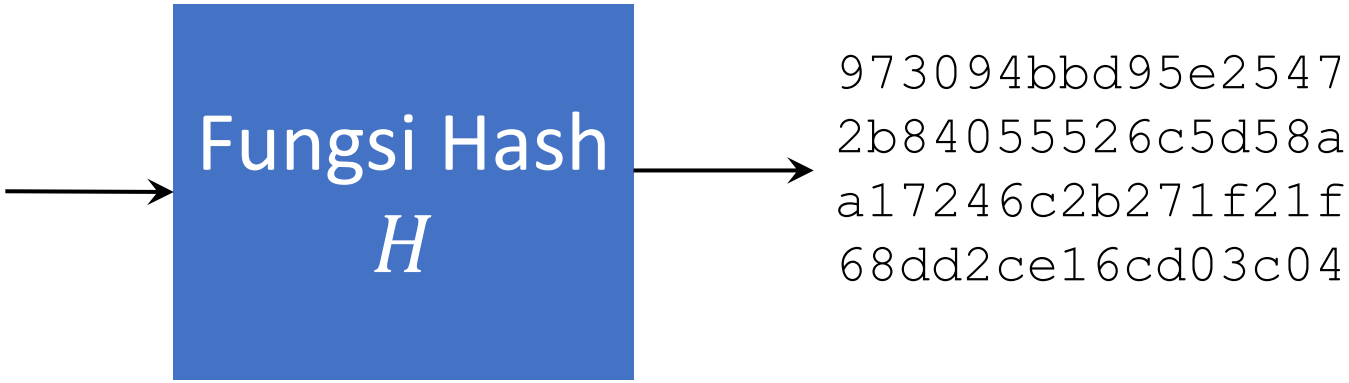
$|h| <<<< |M|$

h = Hash value = message digest = digest

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

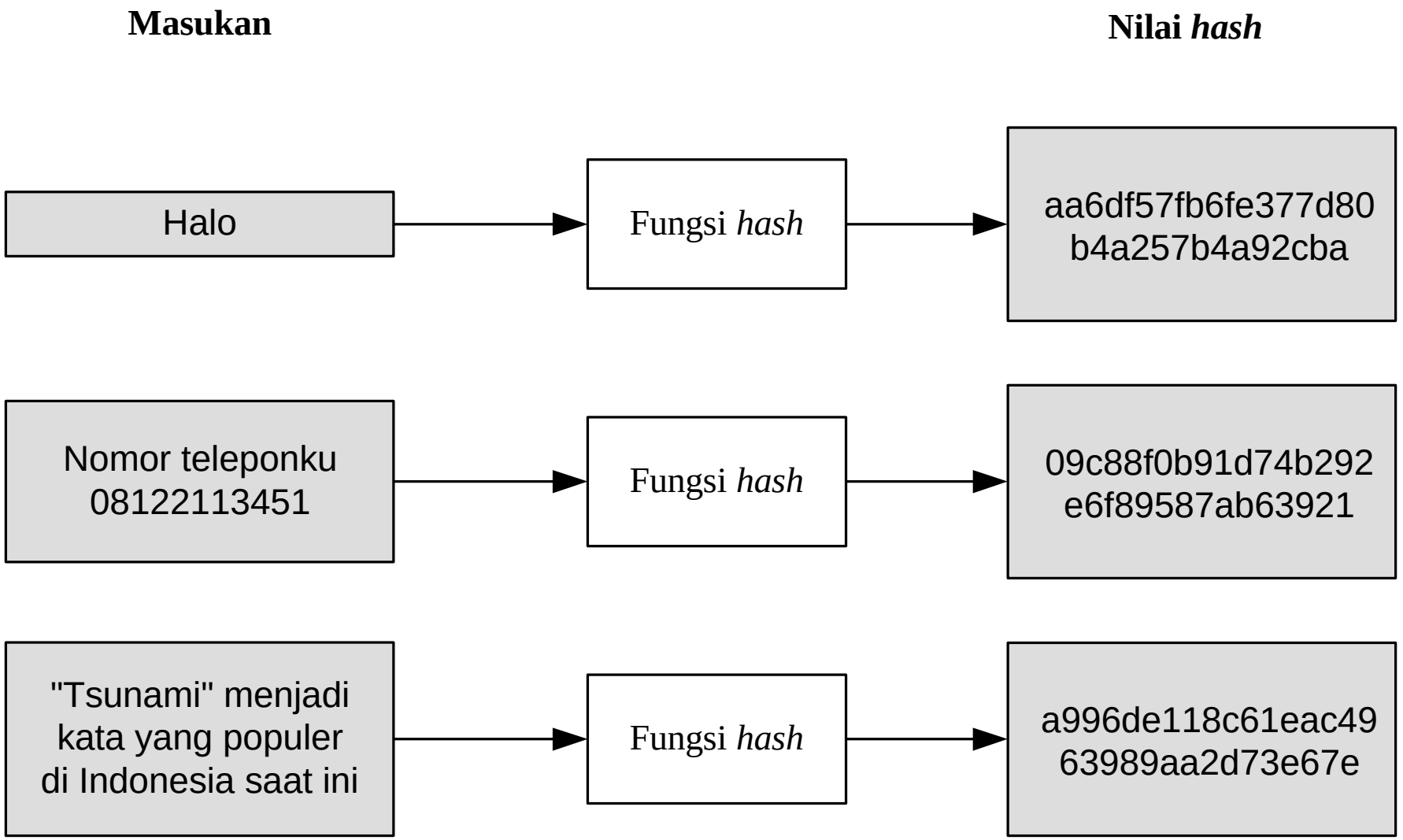


Tolong kirimkan kapal ke pulau Atol. Ada gunung berapi meletus, penduduk pulau harus diungsikan. Kalau perlu dua kapal dikirim berikut makanan buat pengungsi. Nanti malam saya kontak lagi

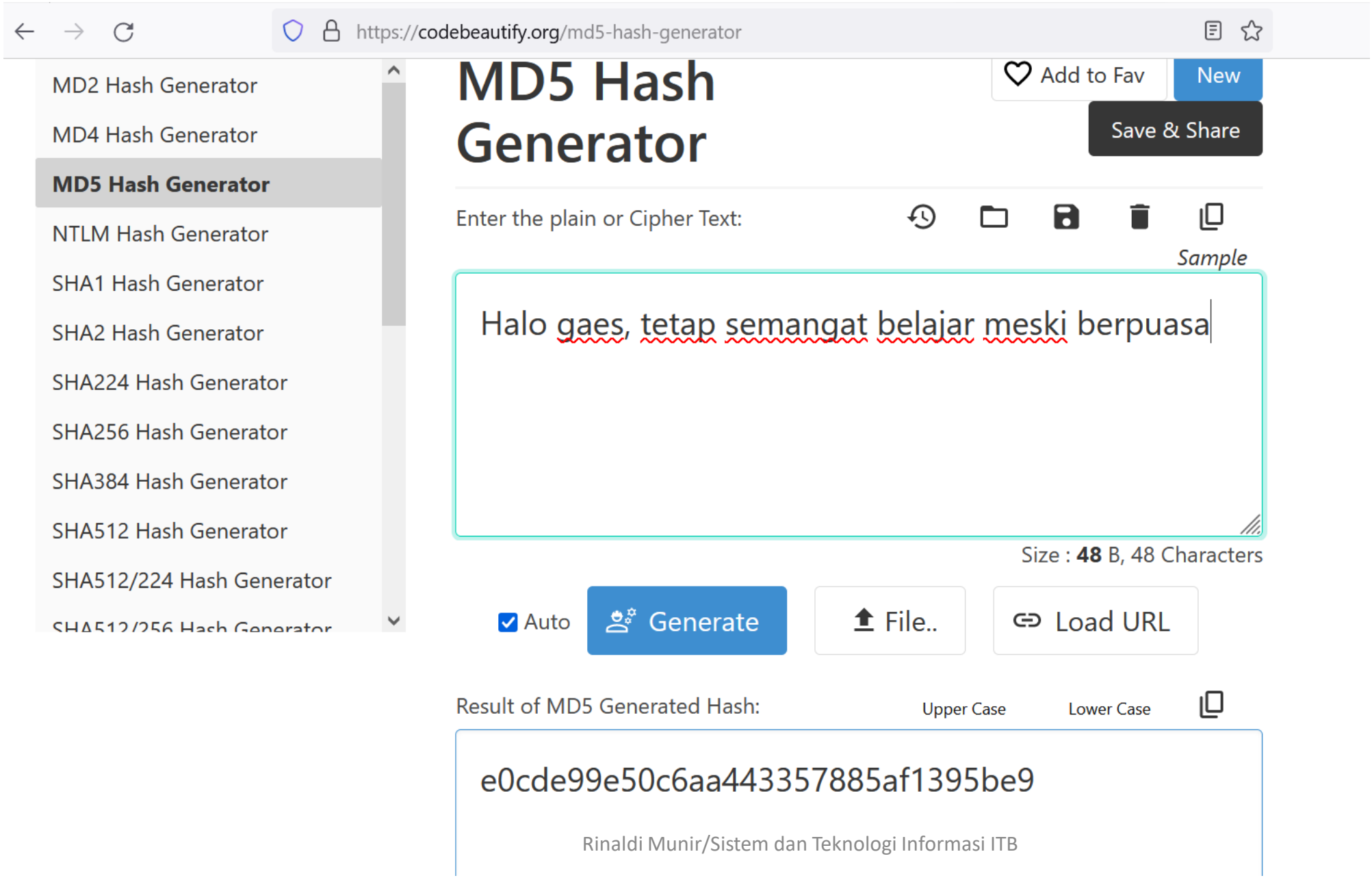


Pesan input

Nilai hash
(256 bit = 64 karakter hexadecimal)


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

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



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 $H(b) = y$

- 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.

- Cukup banyak fungsi *hash* yang terdapat di dalam kriptografi:

Name	Length
BLAKE-256	256 bits
BLAKE-512	512 bits
BLAKE2s	up to 256 bits
BLAKE2b	up to 512 bits
BLAKE2X	arbitrary
BLAKE3	arbitrary
ECOH	224 to 512 bits
FSB	160 to 512 bits
GOST	256 bits
Grøstl	up to 512 bits
HAS-160	160 bits
HAVAL	128 to 256 bits
JH	224 to 512 bits
LSH[19]	256 to 512 bits
MD2	128 bits
MD4	128 bits
MD5	128 bits
MD6	up to 512 bits
RadioGatún	arbitrary
RIPEMD	128 bits
RIPEMD-128	128 bits
RIPEMD-160	160 bits
RIPEMD-256	256 bits
RIPEMD-320	320 bits
SHA-1	160 bits
SHA-224	224 bits
SHA-256	256 bits
SHA-384	384 bits
SHA-512	512 bits
SHA-3 (subset of Keccak)	arbitrary
Skein	arbitrary
Snefru	128 or 256 bits
Spectral Hash	512 bits
Streebog	256 or 512 bits
SWIFFT	512 bits
Tiger	192 bits
Whirlpool	512 bits

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**

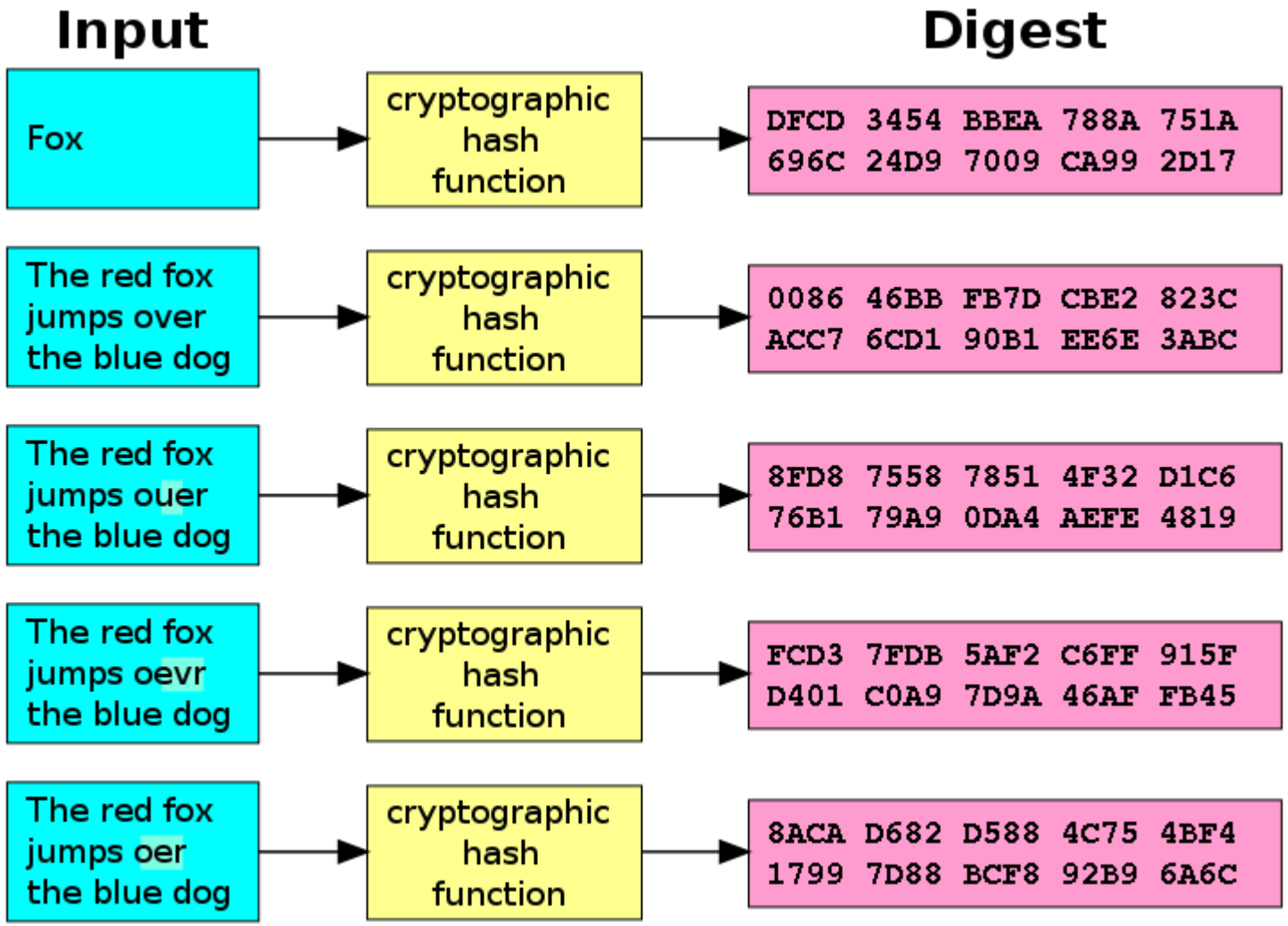
(ii) Misal 33 diubah menjadi 32

```
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**

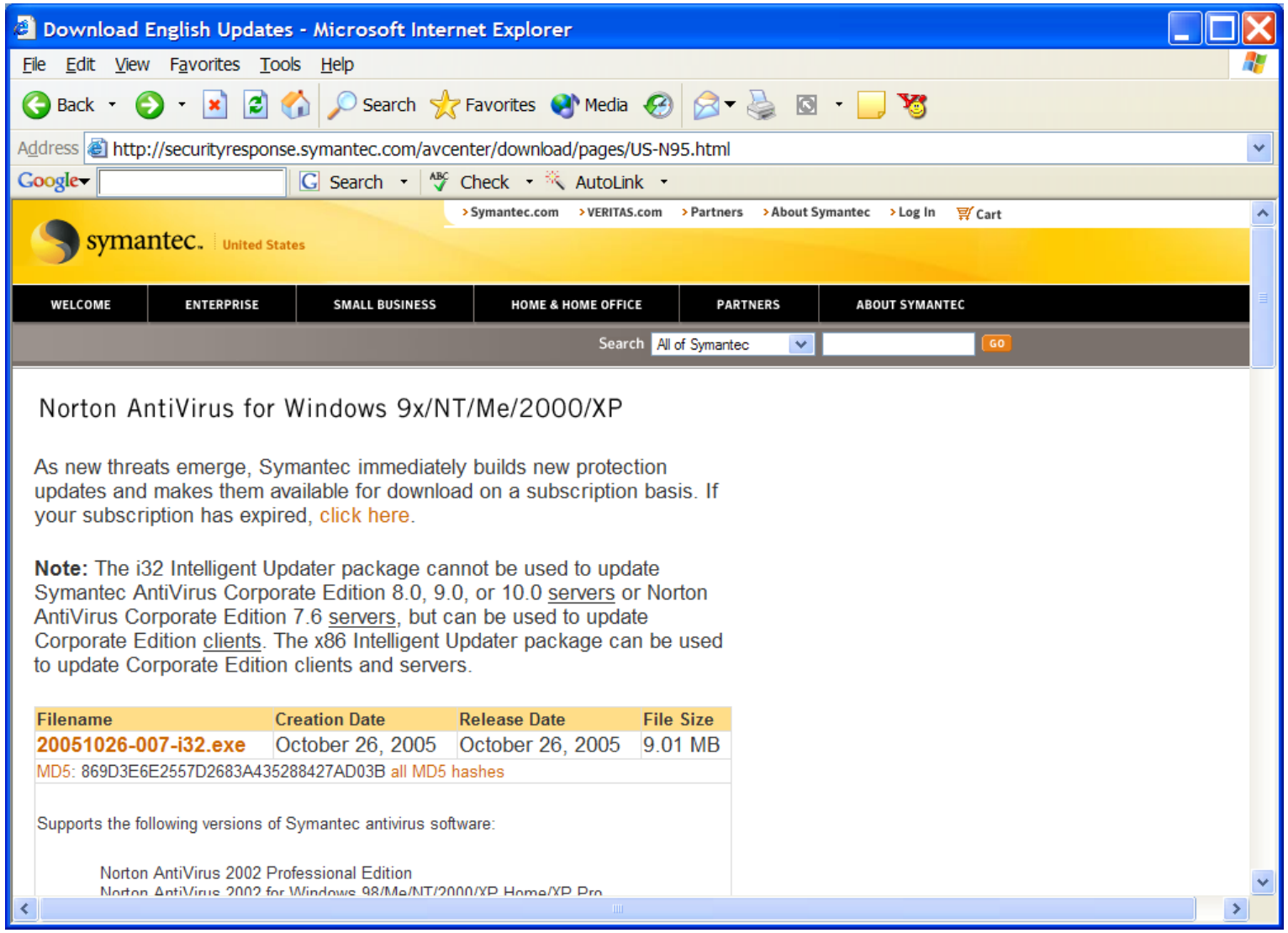
Sebelum diubah : $MD5_1$ = **2F82D0C845121B953D57E4C3C5E91E63**
Sesudah diubah : $MD5_2$ = **2D1436293FAEAF405C27A151C0491267**
Verifikasi: $MD5_1 \neq MD5_2$ (arsip sudah diubah)


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 dokumen dengan dokumen aslinya yang berukuran sangat besar (missal 3 MB).
- Salinan dokumen berada di tempat yang jauh dari dokumen asli
- Ketimbang mengirim salinan dokumen tersebut secara keseluruhan ke kantor pusat (yang membutuhkan waktu transmisi lama), lebih sangkil mengirimkan *message digest*-nya.
- Jika *message digest* salinan dokumen sama dengan *message digest* dokumen yang asli, berarti salinan dokumen tersebut sama dengan dokumen asli.

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