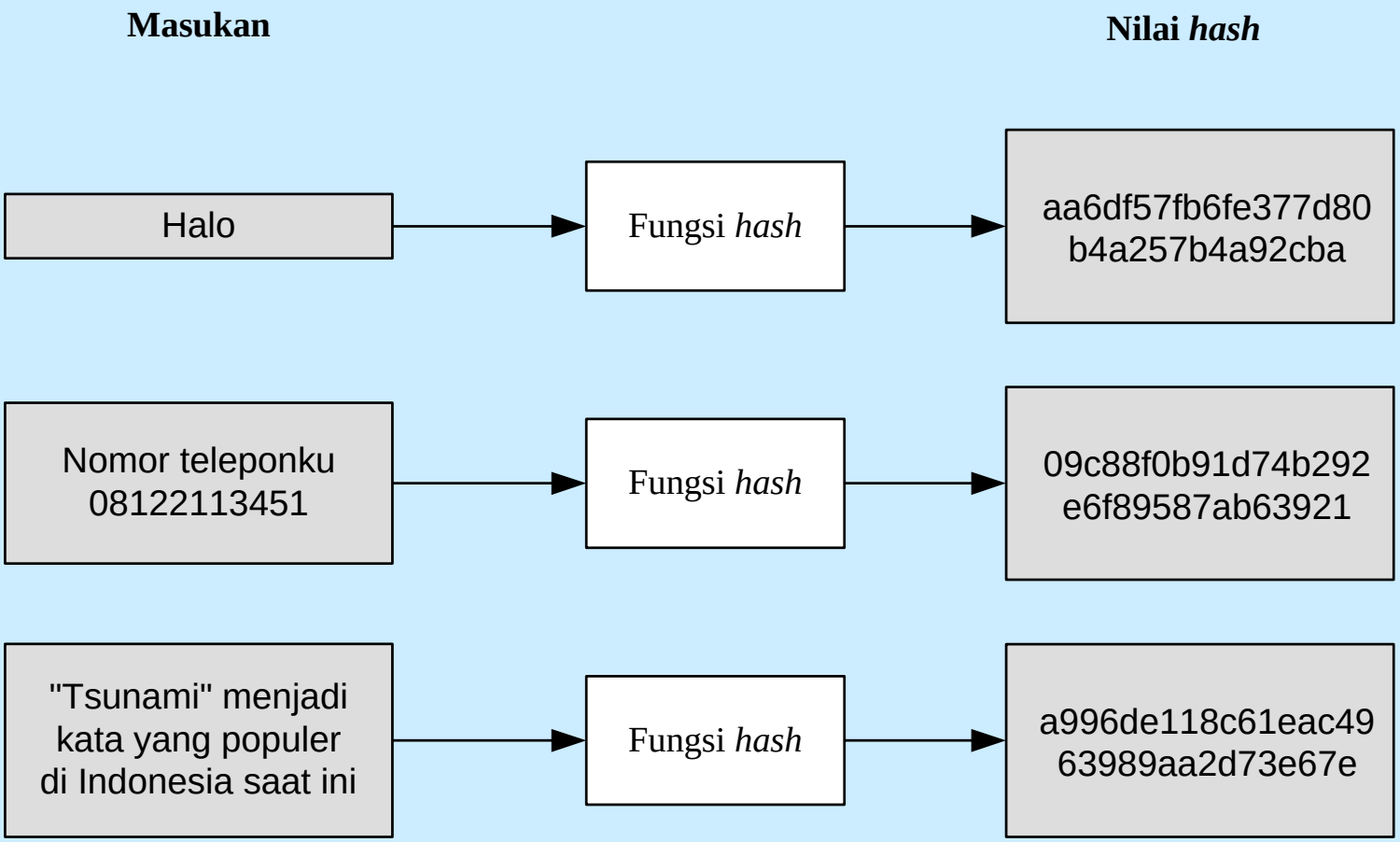
Fungsi *Hash*

Bahan Kuliah IF4020 Kriptografi

Pendahuluan

- Fungsi *hash* adalah fungsi yang
  - menerima masukan *string* yang panjangnya sembarang,
  - lalu mentransformasikannya menjadi *string* keluaran yang panjangnya tetap (*fixed*) (umumnya berukuran jauh lebih kecil daripada ukuran *string* semula).


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

- Persamaan fungsi *hash*:

  $h = H(M)$

  M = pesan kuran sembarang

  h = nilai *hash* atau pesan-ringkas (*message-digest*)

  h <<<< M

- Contoh: *size*(M) = 1 MB → *size*(h) = 128 bit !!!!
- Nama lain fungsi *hash* adalah:
  - *fungsi kompresi (compression function)*
  - *cetak-jari (fingerprint)*
  - *cryptographic checksum*
  - *message integrity check (MIC)*
  - *manipulation detection code (MDC)*

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*).

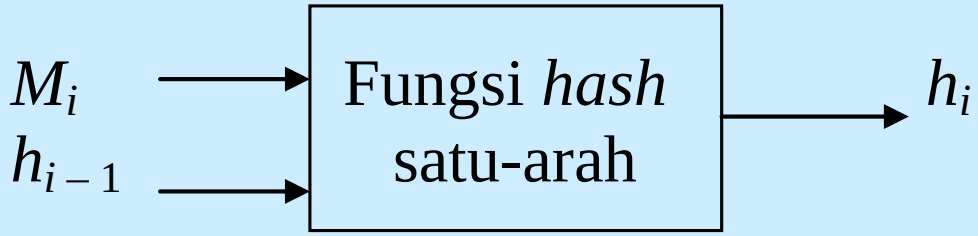
Sifat-sifat fungsi *hash* satu-arah adalah sebagai berikut:

1. Fungsi H dapat diterapkan pada blok data berukuran berapa saja.
2. H menghasilkan nilai (h) dengan panjang tetap (*fixed-length output*).
3. $H(x)$ mudah dihitung untuk setiap nilai x yang diberikan.
4. Untuk setiap h yang dihasilkan, tidak mungkin dikembalikan nilai x sedemikian sehingga $H(x) = h$. Itulah sebabnya fungsi H dikatakan fungsi *hash* satu-arah (*one-way hash function*).
5. Untuk setiap x yang diberikan, tidak mungkin mencari $y \neq x$ sedemikian sehingga $H(y) = H(x)$.
6. Tidak mungkin mencari pasangan x dan y sedemikian sehingga $H(x) = H(y)$.

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:

  - *MD2*, *MD4*, *MD5*,
  - *Secure Hash Function* (*SHA*),
  - *Snefru*,
  - *N-hash*,
  - *RIPE-MD*, dan lain-lain

- (Catatan: *MD* adalah singkatan dari *Message Digest*).

Aplikasi Fungsi *Hash* Satu-Arah

1. Menjaga integritas data
   - 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

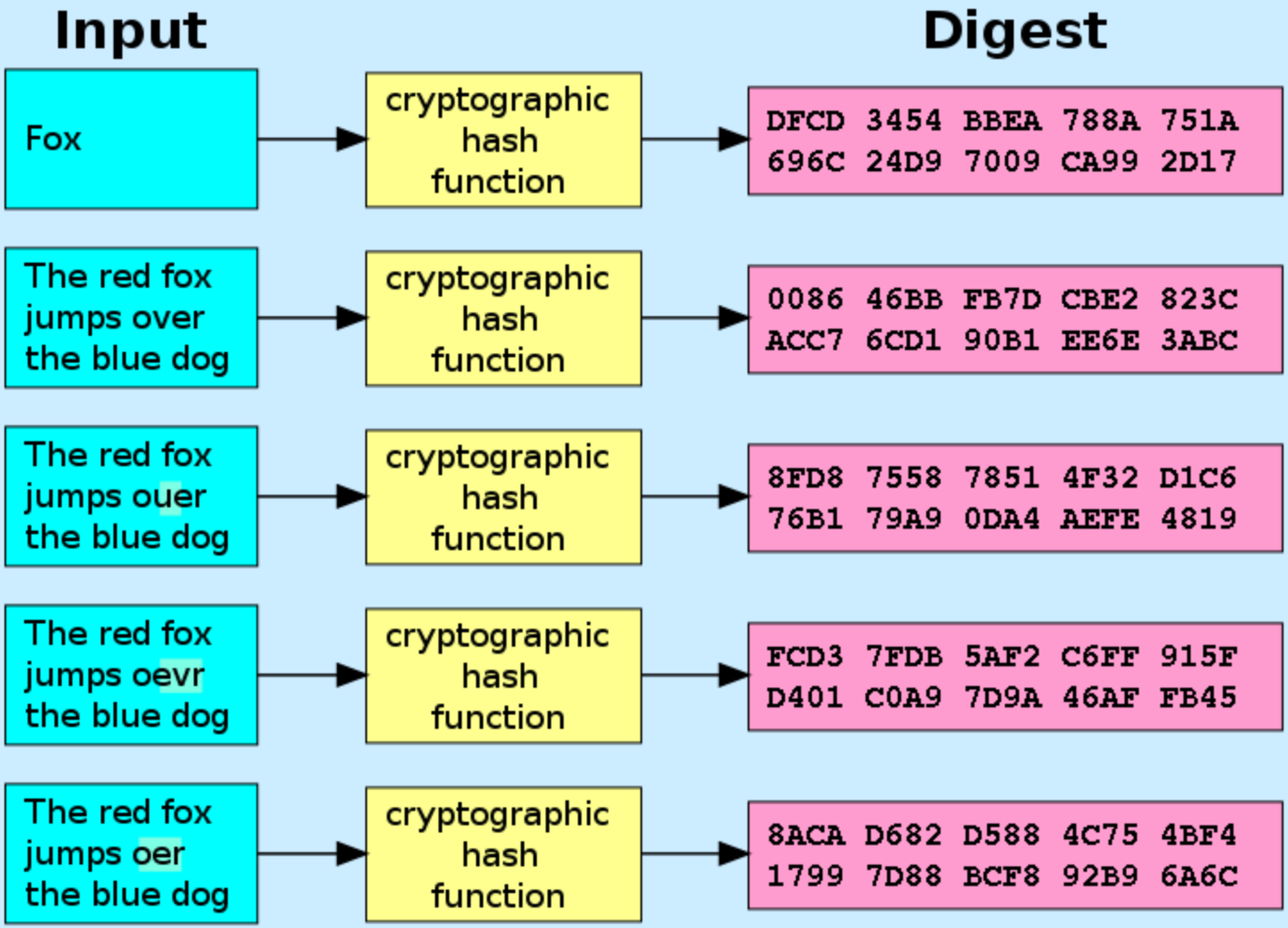
```
Pada bulan Oktober 2004 ini, suhu udara kota Bandung terasa
lebih panas dari hari-hari biasanya. Menurut laporan Dinas
Meteorologi Kota Bandung, suhu tertinggi kota Bandung
adalah 32 derajat Celcius pada Hari Rabu, 17 Oktober yang
lalu. Suhu terseut sudah menyamai suhu kota Jakarta pada
hari-hari 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**

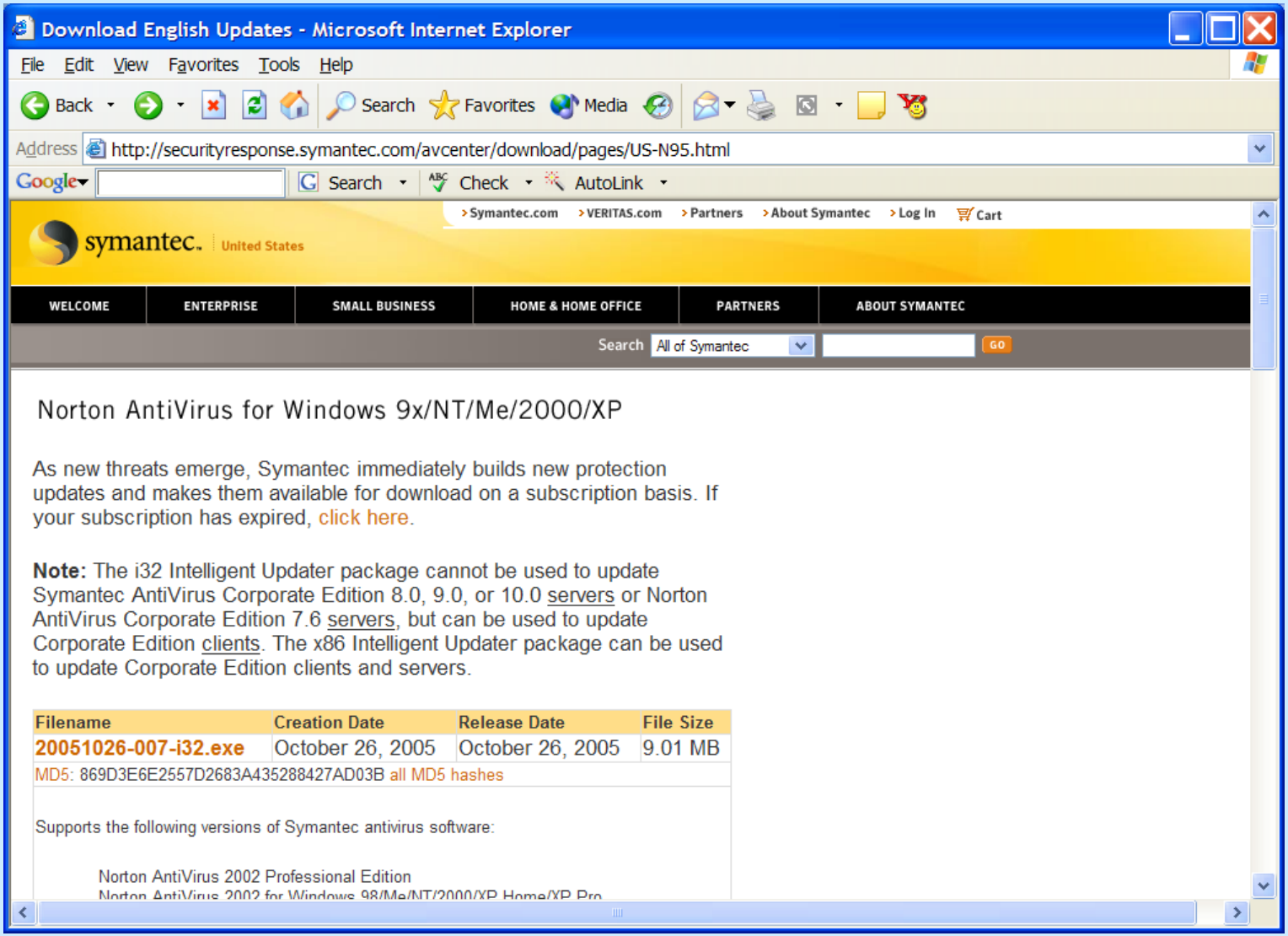
Sesudah diubah : $MD5_2$ = **2D1436293FAEAF405C27A151C0491267**

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



Sumber gambar: Wikipedia

- 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