

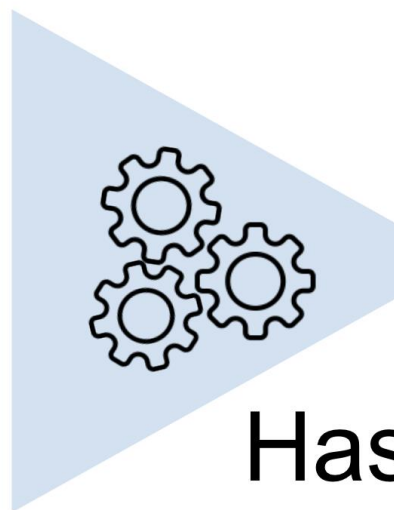
Bahan kuliah IF4020 Kriptografi

Fungsi Hash



Oleh: Rinaldi M

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
2026



dfd879...f8d2f4

Hash

Fungsi Hash

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

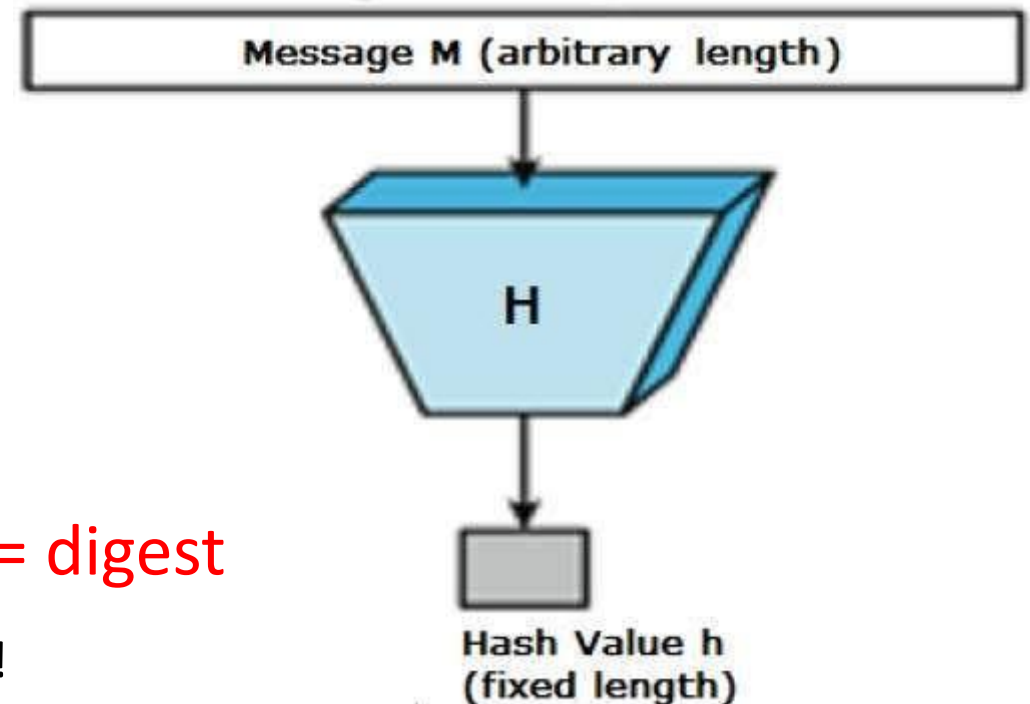
Fungsi Hash:

$$h = H(M)$$

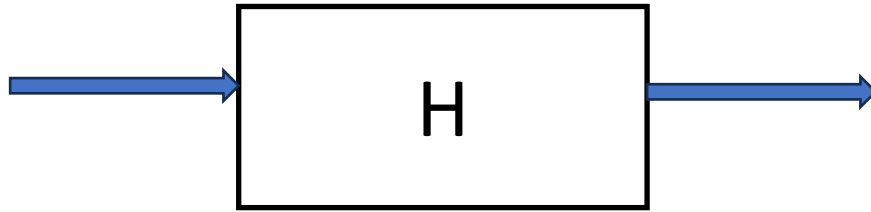
$\text{Length}(h) \lll \text{length}(M)$

h = Hash value = message digest = digest

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



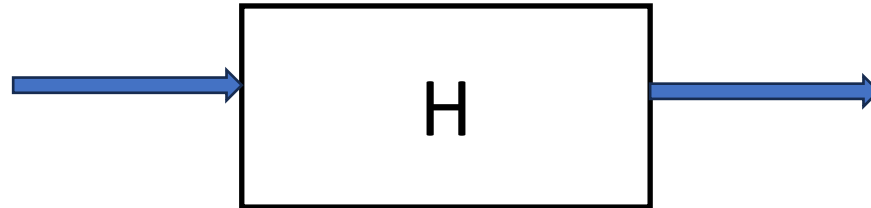
MyPassword



dc1e7c03e162397b355b6f
1c895dfdf3790d98c10b92
0c55e91272b8eecada2a

(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.

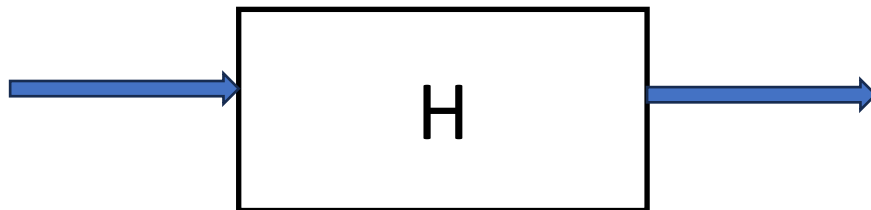


1a060afab8dbfde1cf0aff0
8ef3abfb5ec6eb1170ea9a
d15e8c9f830b24a994d

(256 bit)



Pepers512.bmp



28589a7700758ce63393f8
7d96f83d78206a6b8d375f
ca97d4ef78f9c0d7b307

(256 bit)



Hash Generator

Generate MD5, SHA-1, SHA-256, SHA-384, and SHA-512 hashes instantly.

By **Nethanel Bar**, Co-founder & CEO

Last updated April 25, 2026

☐ Uppercase hex

INPUT 26 bytes

INPUT	HASHES	
Runs in your browser	Click any value to copy	
Banyak musibah di negeriku	MD5 128-bit	f986cf199cb00ae8b1a5dbe4def368e4
	SHA-1 160-bit	3f7d679ffac3676c4291677bdf18322b704623fa
	SHA-256 256-bit	5c6a9f64f9f0bf3f6ec7577a48e712272e9c345b939040beccedc05b0d60545
	SHA-384 384-bit	49453970dd36f8a87b0e9819b4a9c4273f42cce1829f67b15e6c519a97ece532b48d0165d3a61f4fb3fa36185e55e61
	SHA-512 512-bit	e5903a70ae0b0e8a8af1cde3c7eeefa64600003820932a8df1f985e2a4926f52414b840761e27185abdb7dcdcde22a27985bb3f8b5a6ad88e1b31edd4396bf6c

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 dapat disebut sebagai fungsi enkripsi, meskipun nilai *hash* tidak memiliki makna,
- sebab, nilai *hash* tidak dapat ditransformasi balik menjadi pesan semula.
- Alasan lainnya, proses *hashing* tidak memerlukan 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>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

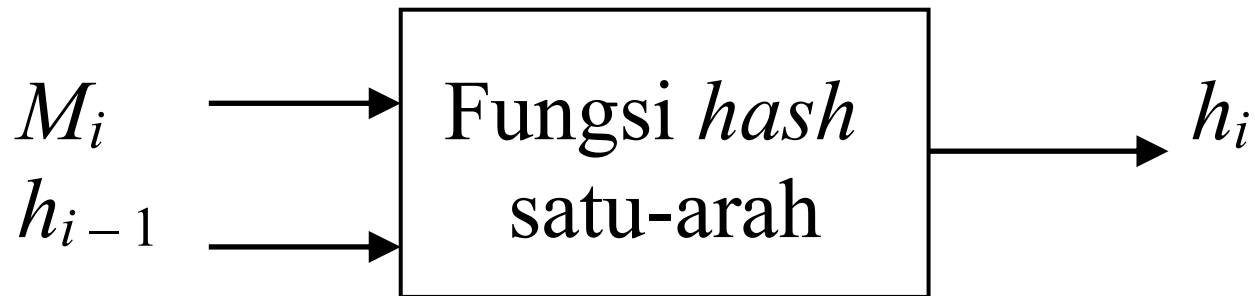
1. Menjaga integritas pesan

- 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

Hal ini karena masukan fungsi *hash* adalah blok pesan (M) dan luaran dari *hashing* blok pesan sebelumnya,

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

Skema fungsi *hash* ditunjukkan pada Gambar di bawah:



Jika satu bit M_i berubah, maka h_i juga berubah, dan ini mempengaruhi luaran blok-blok berikutnya (merambat)

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 hash: **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 hash: **2D1436293FAEAF405C27A151C0491267**

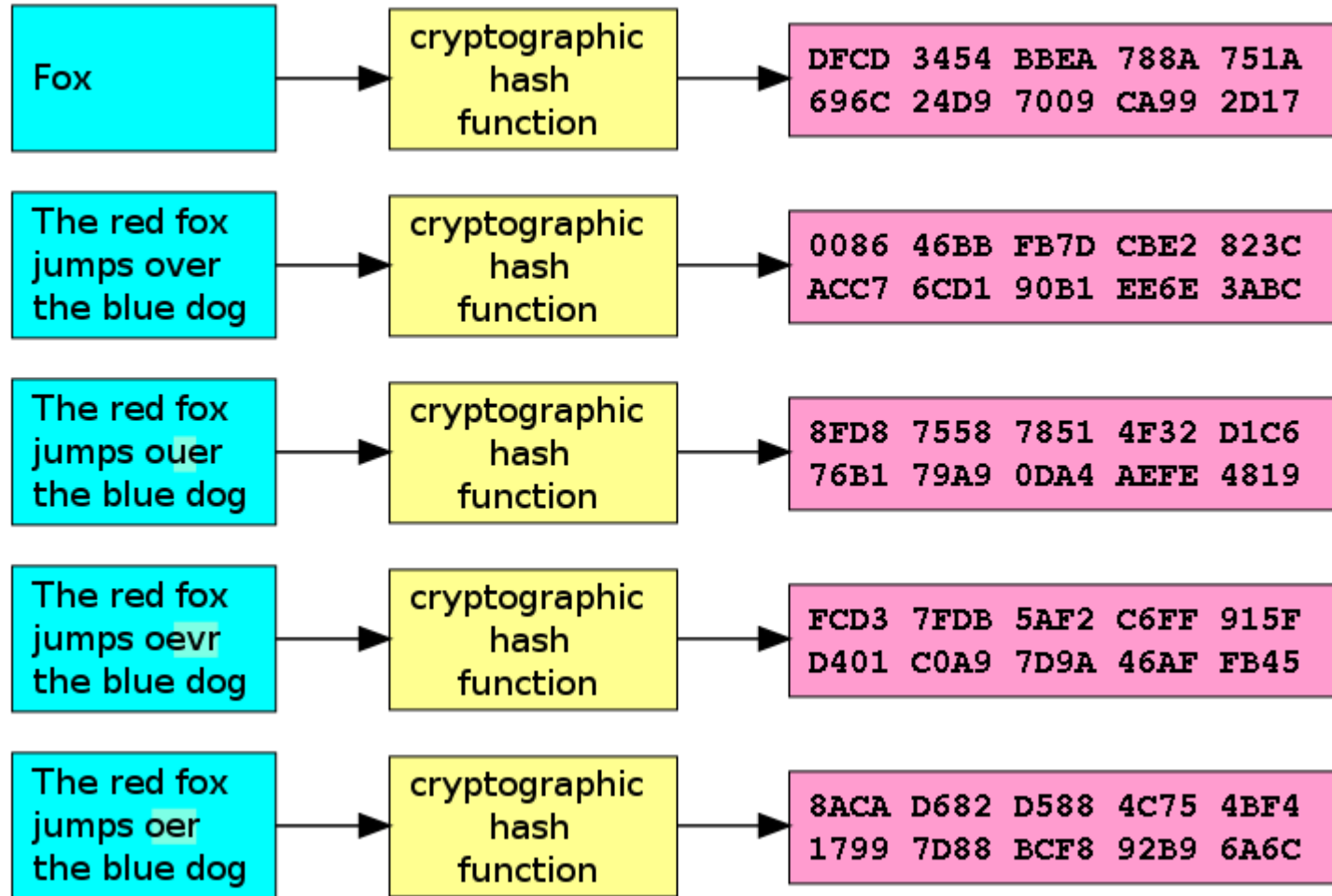
Sebelum diubah : Nilai hash (lama) = **2F82D0C845121B953D57E4C3C5E91E63**

Sesudah diubah : Nilai hash (baru) = **2D1436293FAEAF405C27A151C0491267**

Verifikasi: Nilai hash (lama) $\neq$ (Nilai hash baru) $\rightarrow$ Kesimpulan: pesan sudah diubah)

Input

Digest



- 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 memastikan 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

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

Google Search ABC 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.

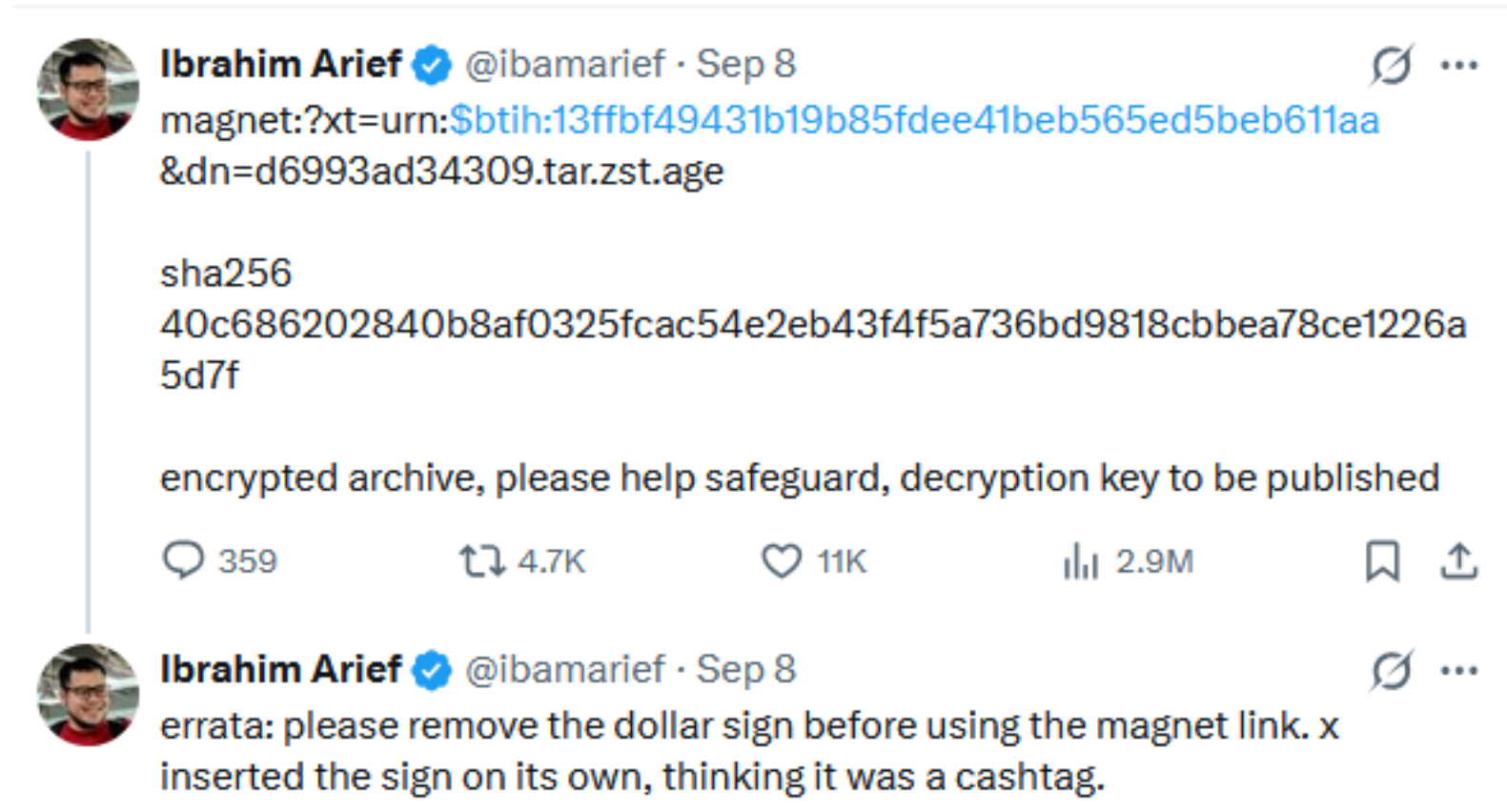
Filename	Creation Date	Release Date	File Size
20051026-007-i32.exe	October 26, 2005	October 26, 2005	9.01 MB
MD5: 869D3E6E2557D2683A435288427AD03B all MD5 hashes			

Supports the following versions of Symantec antivirus software:

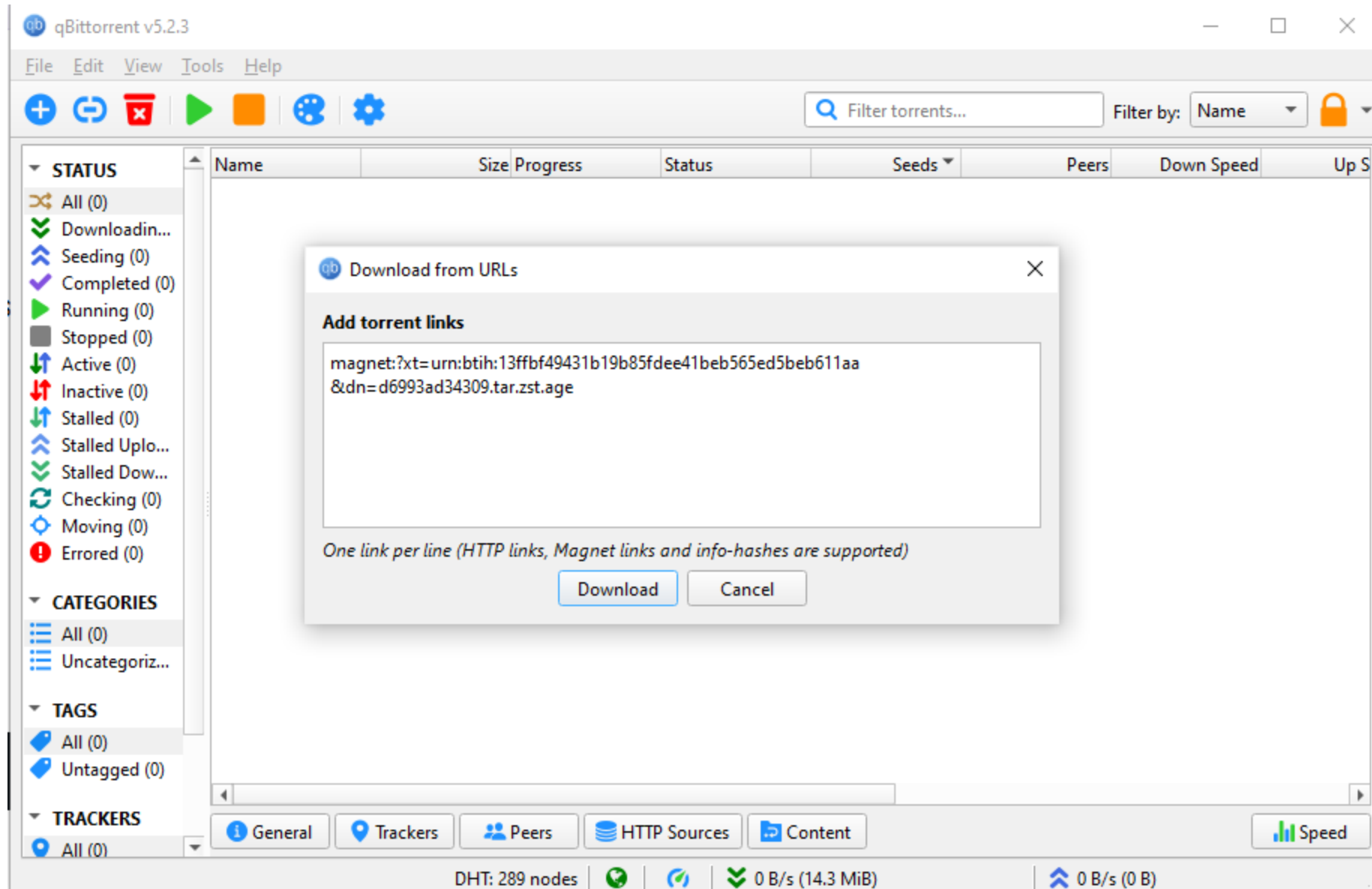
Norton AntiVirus 2002 Professional Edition
Norton AntiVirus 2002 for Windows 98/Me/NT/2000/XP Home/XP Pro

Studi kasus: File yang dirilis oleh Ibam memiliki nilai hash (SHA256):

40c686202840b8af0325fcac54e2eb43f4f5a736bd9818cbbea78ce1226a5d7f

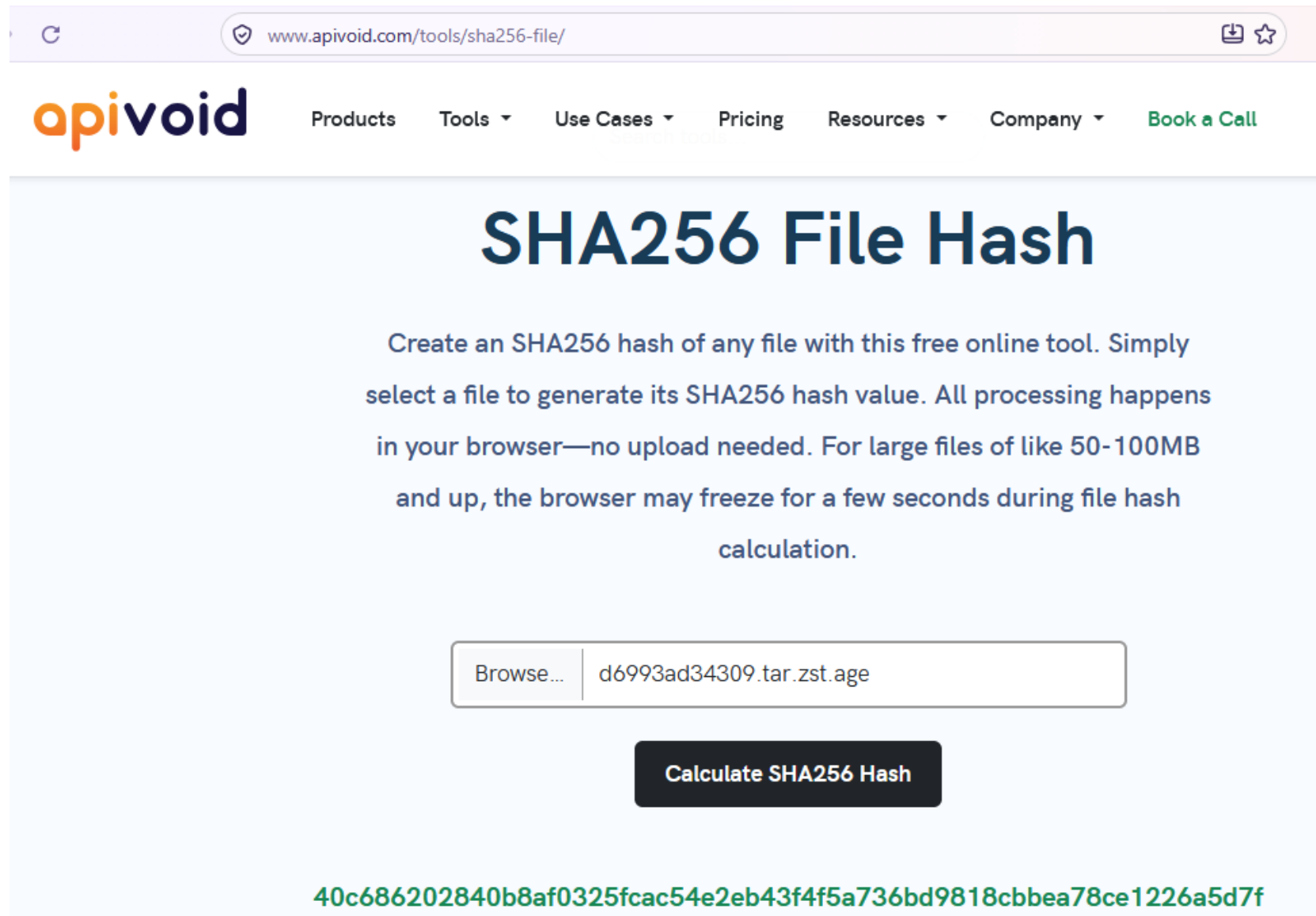


Unduh file Ibam melalui aplikasi bittorrent



Hitung nilai hash file lbam: d6993ad34309.tar.zst

<https://www.apivoid.com/tools/sha256-file/>



The screenshot shows the 'SHA256 File Hash' tool interface. At the top, the 'apivoid' logo is on the left, and navigation links for 'Products', 'Tools', 'Use Cases', 'Pricing', 'Resources', 'Company', and 'Book a Call' are on the right. The main heading is 'SHA256 File Hash'. Below it, a paragraph explains the tool's functionality: 'Create an SHA256 hash of any file with this free online tool. Simply select a file to generate its SHA256 hash value. All processing happens in your browser—no upload needed. For large files of like 50-100MB and up, the browser may freeze for a few seconds during file hash calculation.' A file input field contains the text 'Browse...' and 'd6993ad34309.tar.zst.age'. Below the input field is a dark button labeled 'Calculate SHA256 Hash'. At the bottom, the resulting hash is displayed in green text: '40c686202840b8af0325fcac54e2eb43f4f5a736bd9818cbbea78ce1226a5d7f'.

apivoid

Products Tools Use Cases Pricing Resources Company Book a Call

SHA256 File Hash

Create an SHA256 hash of any file with this free online tool. Simply select a file to generate its SHA256 hash value. All processing happens in your browser—no upload needed. For large files of like 50-100MB and up, the browser may freeze for a few seconds during file hash calculation.

Browse... d6993ad34309.tar.zst.age

Calculate SHA256 Hash

40c686202840b8af0325fcac54e2eb43f4f5a736bd9818cbbea78ce1226a5d7f

Bandingkan: 40c686202840b8af0325fcac54e2eb43f4f5a736bd9818cbbea78ce1226a5d7f

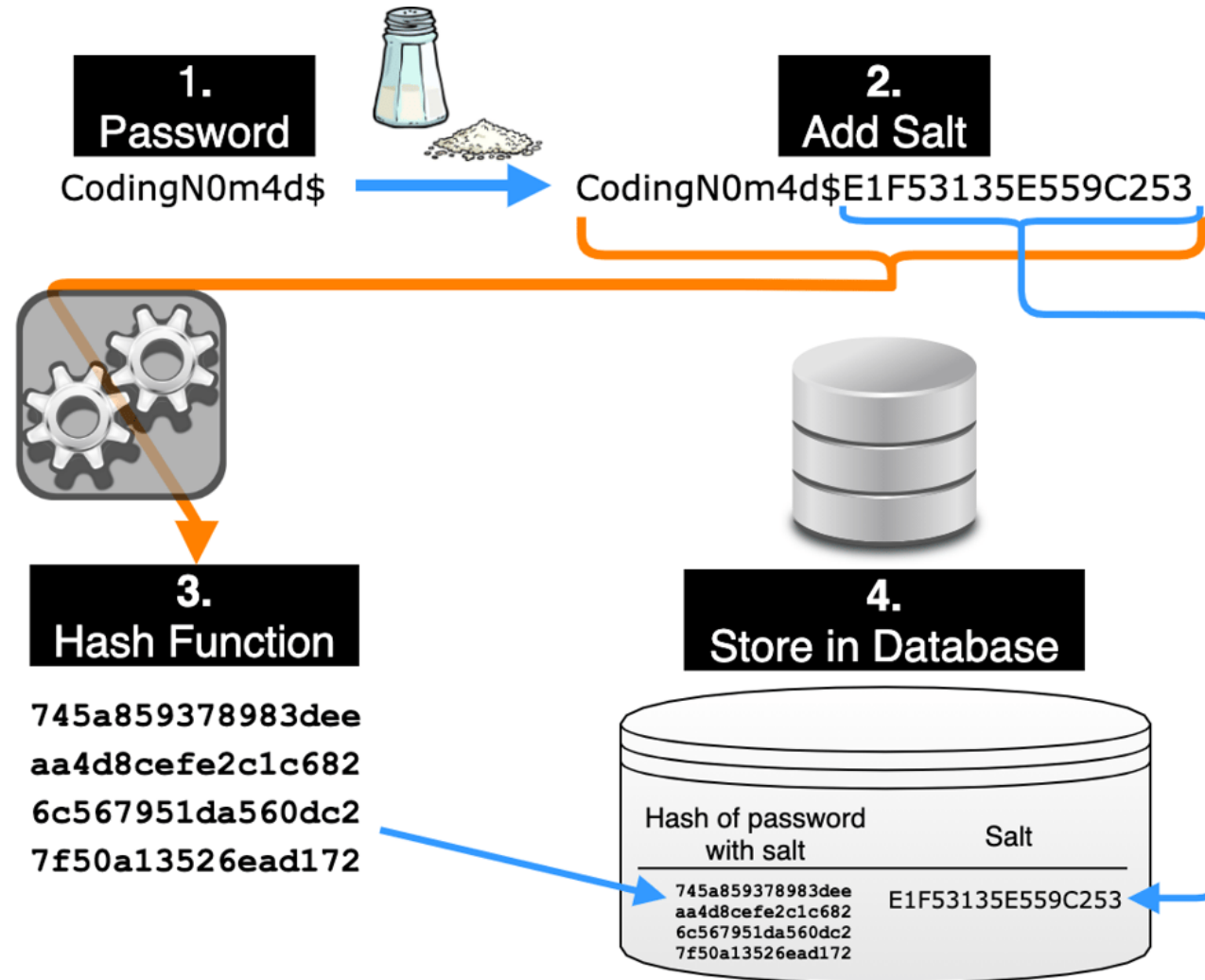
2. Menghemat waktu pengiriman.

- Misal untuk memverifikasi apakah salinan (copy) dokumen isinya tetap sama dengan dokumen asli.
- Salinan dokumen berada di tempat yang jauh dari dokumen asli
- Ketimbang mengirim salinan dokumen tersebut secara keseluruhan via email atau whatsapp ke tempat verifikasi (yang membutuhkan *bandwidth* besar), lebih sangkil mengirimkan *message digest*-nya saja.
- Jika *message digest* salinan dokumen sama dengan *message digest* dokumen asli, berarti salinan dokumen tersebut sama dengan dokumen asli

3. Menormalkan panjang data yang beraneka ragam.

- Misalkan *password* panjangnya bebas (minimal 8 karakter), tiap pengguna punya *password* dengan panjang berbeda-beda
- *Password* disimpan di dalam basisdata pada komputer *server* untuk keperluan otentikasi pengguna komputer.
- Karena panjang *password* tiap pengguna tidak sama, maka timbul kesulitan dalam menentukan lebar *field* password di dalam basisdata
- Untuk menyeragamkan panjang *field password* di dalam basisdata, maka *password* tidak disimpan dalam bentuk aktual, tetapi berupa nilai *hash* password saja (panjang nilai *hash* selalu tetap).

Biasanya sebelum *di-hash*, *password* ditambahkan garam (*salt*) sejumlah beberapa karakter



Kolisi

- Kolisi (*collision*) adalah kejadian dua *string* sembarang memiliki nilai *hash* yang sama.
- Adanya kolisi menunjukkan fungsi *hash* tidak aman secara kriptografis, karena dimungkinkan merekayasa dua pesan berbeda memiliki nilai hash yang sama.

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