

Penggunaan Kripto Kunci Publik



- Secure Socket Layer (SSL)
 - HTTPS
 - SSH
 - STUNNEL
- Pretty Good Privacy (PGP) dan GNU Privacy Guard (GPG)

MARET 2006

PENGANTAR KRIPTOGRAFI - INDOCISC

28

Bank Mandiri - Internet Banking - Microsoft Internet Explorer

Address: https://it.bankmandiri.co.id/retail/Login.do?action=form&lang=in_ID

BANK MANDIRI HOME | SITE MAP | CONTACT US

internet banking MANDIRI

LOGIN HELP

Masukkan USER ID Anda :

Masukkan PIN Internet Banking :

BATAL **KIRIM**

Caution

1. Isilah kolom 'Masukkan USER ID Anda' dengan USER ID yang telah Anda buat (merupakan kombinasi huruf dan angka sebanyak 6-10 karakter).
2. Isilah kolom 'Masukkan PIN INTERNET BANKING Anda' dengan nomor sandi rahasia yang telah Anda buat (hanya berupa angka, sebanyak 6 karakter).
3. Tekan tombol "KIRIM" untuk melanjutkan atau tombol "BATAL" untuk melakukan pembatalan.

Caution

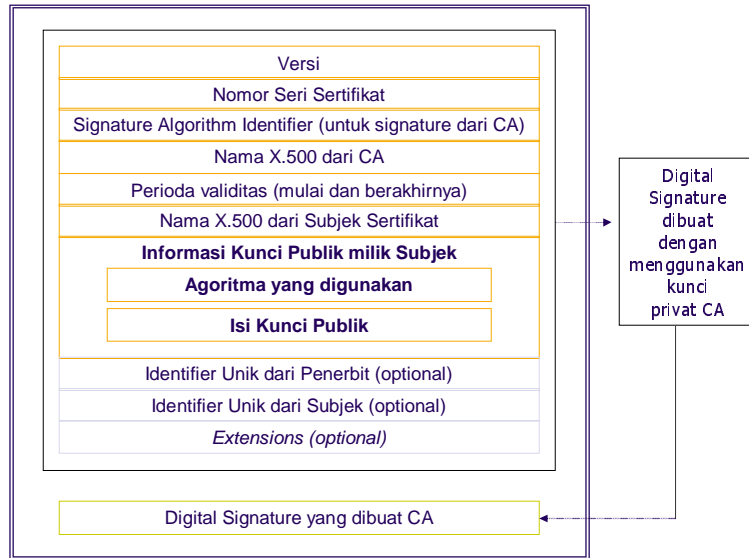
1. Untuk LOGIN kedalam layanan INTERNET BANKING MANDIRI Anda akan selalu diminta untuk memasukkan USER ID dan PIN INTERNET BANKING sebagai proses verifikasi.
2. USER ID dan PIN INTERNET BANKING merupakan sandi rahasia yang diberikan kepada Nasabah sebagai kewenangan penggunaan INTERNET BANKING MANDIRI.
3. Jagalah selalu USER ID dan PIN INTERNET BANKING untuk menghindari penyalahgunaan oleh orang lain yang tidak berhak.
4. Apabila Anda mendapatkan masalah dengan INTERNET BANKING MANDIRI Anda, silahkan hubungi CallMandiri di (021) 5299-7777.

Done Internet

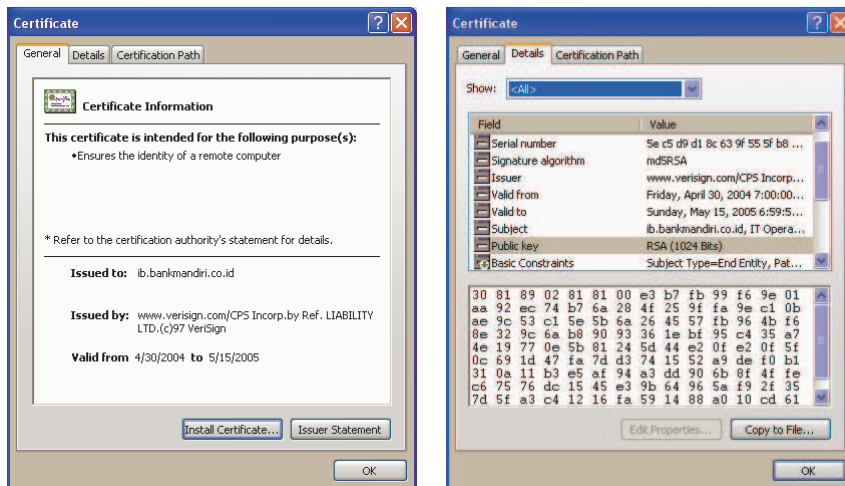


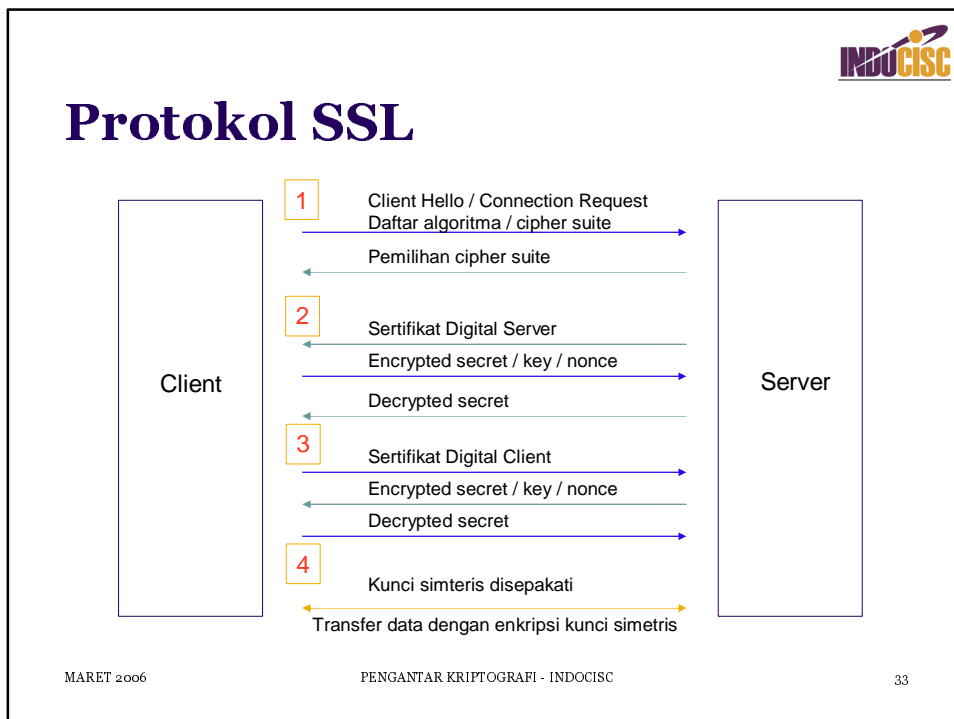
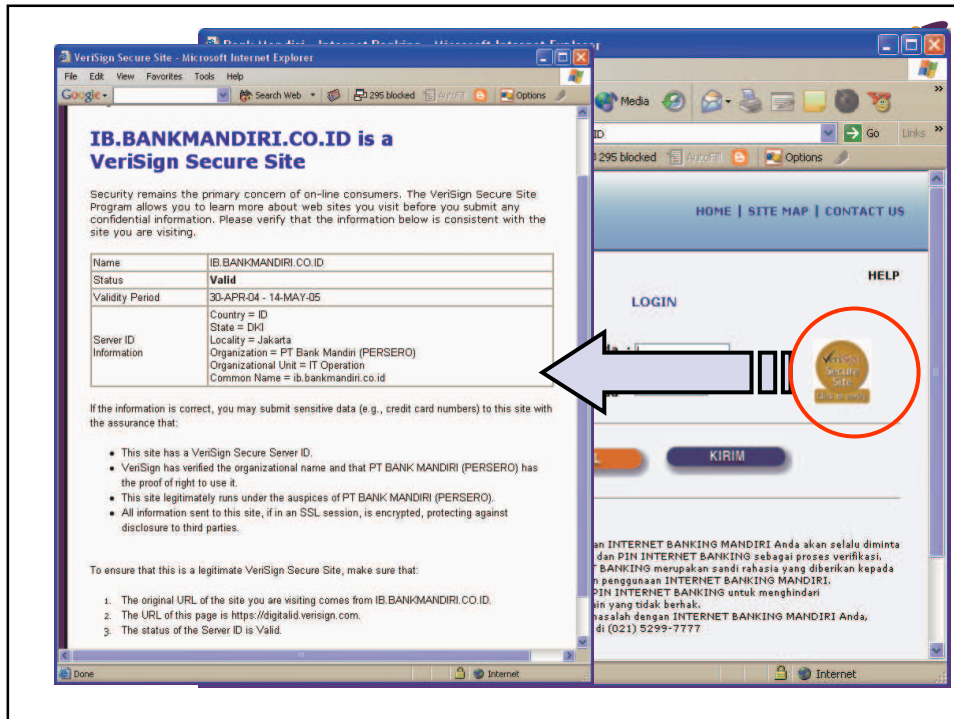
29

Sertifikat Digital X.509 versi 3



Contoh Sertifikat





Algoritma Kunci Privat

- Beberapa contoh algoritma
 - XOR: mudah dipecahkan
 - DES: sudah dianggap tidak bagus lagi
 - 3DES: menggunakan DES 3 kali
 - AES: pengganti DES

Substitusi: XOR data

- Data tersimpan dalam bentuk bilangan biner
- Data di-XOR dengan sebuah kunci
- Tugas
 - Membuat program yang melakukan proses XOR data dengan kunci

Message Digest

- Menghasilkan summary (*digest*) dari sebuah pesan (file, stream data)
- Menggunakan *hash function* untuk menghasilkan digest tersebut

Fungsi Hash (Hash Function)

- Merupakan fungsi satu arah (*one way function*) yang dapat menghasilkan ciri (*signature*) dari data (berkas, stream)
- Perubahan satu bit saja akan mengubah keluaran hash secara drastis
- Digunakan untuk menjamin integritas dan digital signature

Contoh Hash Function

- Contoh: MD4, MD5, SHA-1

```
unix$ md5sum /bin/login
af005c0810eeca2d50f2904d87d9ba1c /bin/login
```

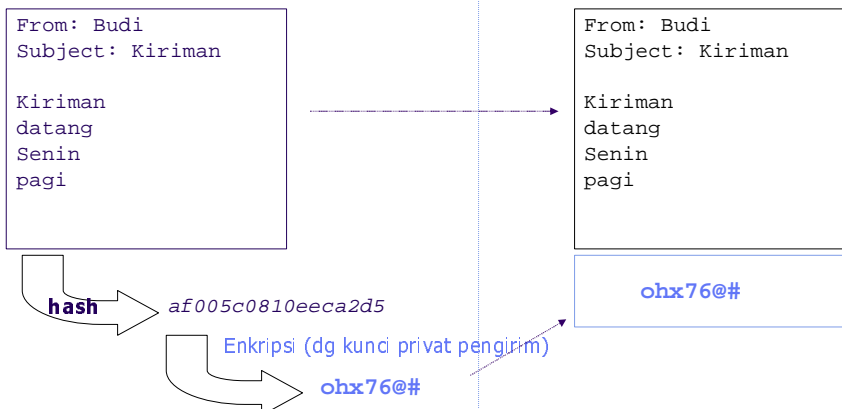
- Program md5sum untuk windows merupakan bagian dari *Cygwin distribution* yang dapat diperoleh dari

<http://sunsite.bilkent.edu.tr/pub/cygwin/cygwin-b20/full.exe>

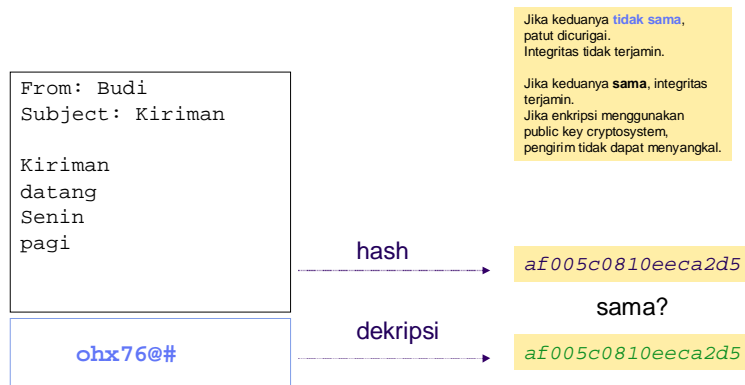
Penggunaan Hash: Pengirim

Isi email tidak dirahasiakan.
Diinginkan terjaganya integritas dan non-repudiation

Keduanya disatukan dan dikirimkan



Pada Penerima



Contoh Penggunaan Hash

- Hasil hash dienkripsi untuk menjamin keamanannya (integritas)
- Ukuran hasil hash yang lebih kecil dibandingkan ukuran pesan asalnya membutuhkan waktu enkripsi yang lebih singkat (dibandingkan jika mengenkripsi seluruh pesan)
- Digital Signature
- Pesan juga dapat dienkripsi jika diinginkan kerahasiaan
- Contoh aplikasi lain: hash encrypted password

Permasalahan Hash

- Karena range (space) dari hasil hash lebih kecil (dalam jumlah bit) dari sumber informasinya, maka dimungkinkan adanya “collision” – yaitu dua data dipetakan ke hash yang sama
- Ini sudah dibuktikan dengan pecahnya MD5 dan SHA-1
 - http://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html
 - MD5 (1992) merupakan penyempurnaan dari MD4 (1990)
 - SHA merupakan buatan NSA (1993) yang mirip dengan MD5
- Meskipun dua data yang dipetakan itu tidak mudah dibuat dan kadang-kadang *completely useless*

Tugas

- Efek perubahan pada image
 - Buat sebuah image (BMP, GIF, JPG)
 - Ubah sedikit (1 pixel, beberapa pixels, rotate, crop, dll.)
 - Lihat efeknya pada hash function
- Lakukan hal yang sama dengan berkas yang lain; MP3, AVI

Masalah Seputar Kripto

- Memastikan keamanan algoritma enkripsi
 - Algoritma harus dievaluasi oleh pakar
 - Algoritma yang tertutup (tidak dibuka kepada publik) dianggap tidak aman
 - Membuat algoritma yang aman tidak mudah
 - *Code maker vs code breakers* akan terus berlangsung



Bahan Bacaan

- Simon Singh, "*Code Book: the secret history of codes & code-breaking*," Fourth Estate, 1999.
- Bruce Schneier, "*Applied Cryptography: protocols, algorithms, and source code in C*," 2nd edition, John Wiley & Sons, Inc., 1996.
- Steven Levy, "*crypto: how the code rebels beat the government - saving privacy in the digital age*," penguin books, 2001
- Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, "*Handbook of Applied Cryptography*"
<http://www.cacr.math.uwaterloo.ca/hac/>
- Cryptography Research Crypto FAQ:
<http://www.cryptography.com/faq/index.html>
- Basic Cryptanalysis
<http://www.umich.edu/~umich/fm-34-40-2/>