Ir. Budi Rahardjo, M. Sc., Ph.D

Teknik Komputer – STEI ITB

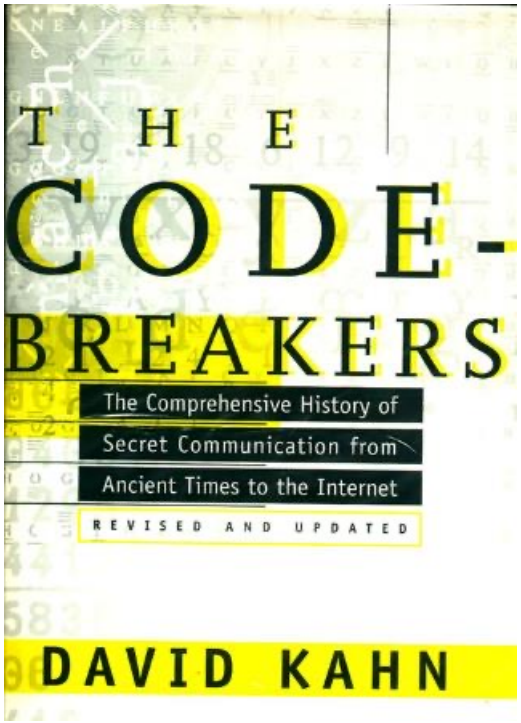
Keamanan Informasi

Pengantar Kriptografi

II3230 - Keamanan Informasi

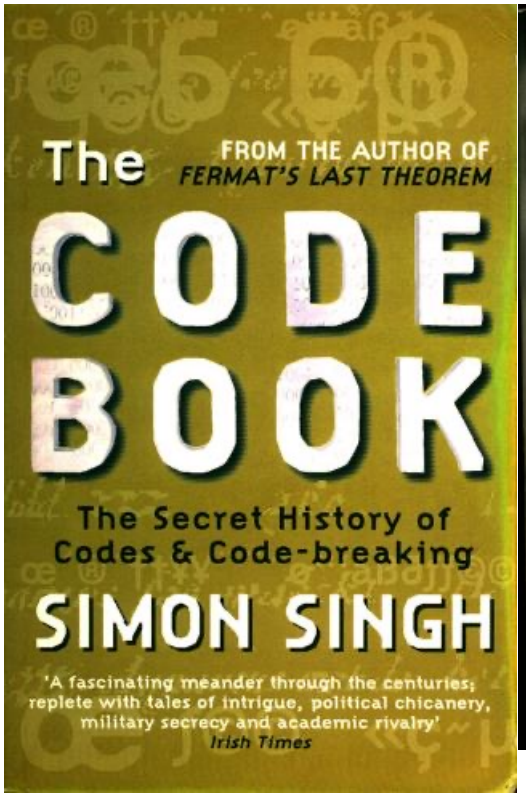
Dark Art!

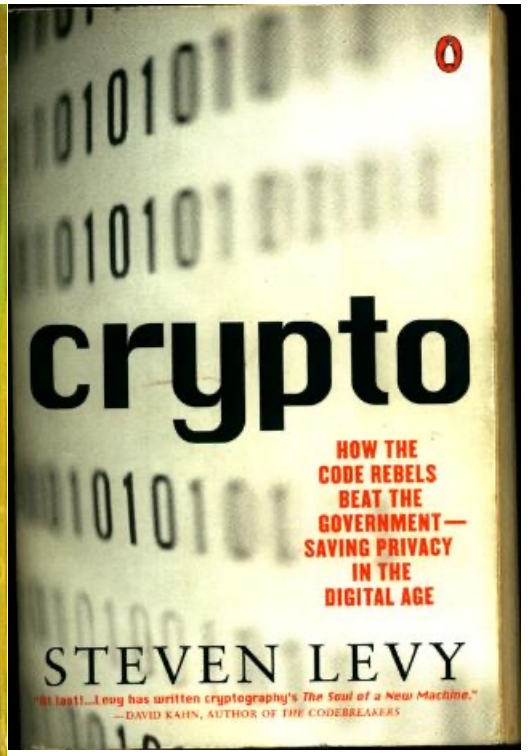
- Sebelum tahun 1970-an, **`kriptografi`** merupakan sebuah **dark art** – ilmu yang tidak diajarkan secara umum
- Sampai munculnya buku "*The Code Breakers*" dari David Kahn.



Buku Lainnya

- *Code Book*
  Simon Singh
- *Crypto*
  Steven Levy





Security & Intelligence

Pengamanan

- Signal Security
  - Steganography
  - Traffic security (call sign changes, dummy msg, radio silence)
  - Cryptography
- Electronic Security
  - Emission security (shifting radar freq.)
  - Counter -Countermeasures (looking through jammed radar)

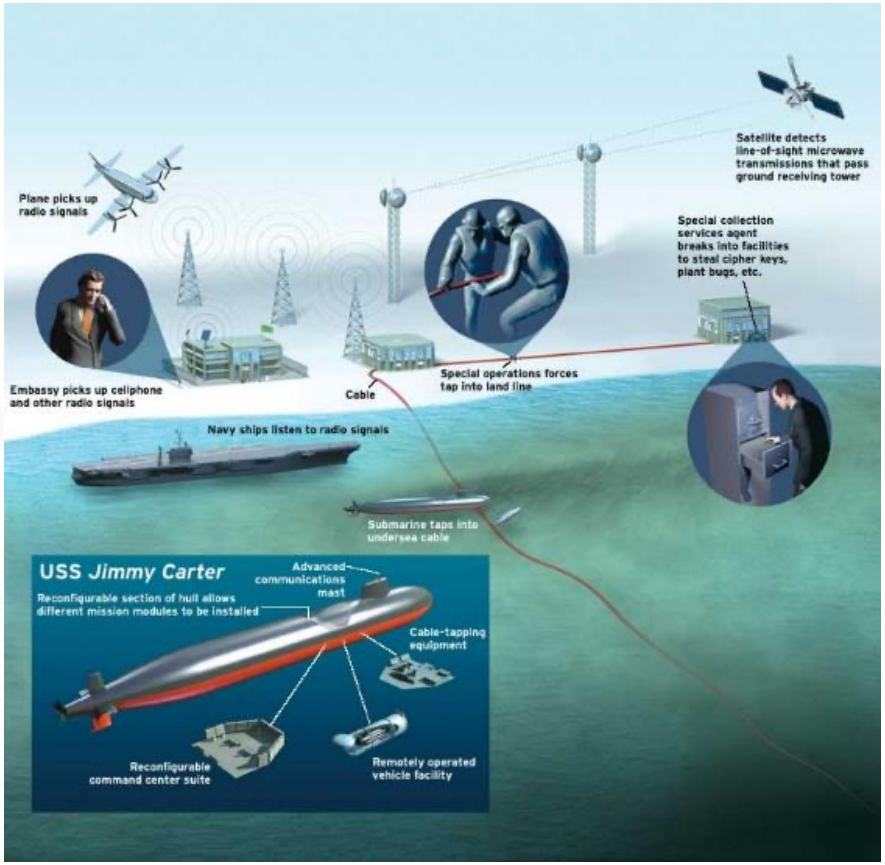
- Signal Intelligence
  - Interception & Direction-Finding
  - Traffic Analysis
  - Cryptanalysis
- Electronic Intelligence
  - Electronic reconnaissance (eavesdroping on radar emission)
  - Countermeasures (jamming, false radar echoes)

Source: David Kahn, The Code Breakers

Keamanan Negara

- Kemampuan mengamankan data dan menangkap data merupakan kepentingan negara
  - Privacy vs keamanan negara?
  - Spy vs spy?

Penyadapan Internasional



Sumber: IEEE Spectrum, April 2003

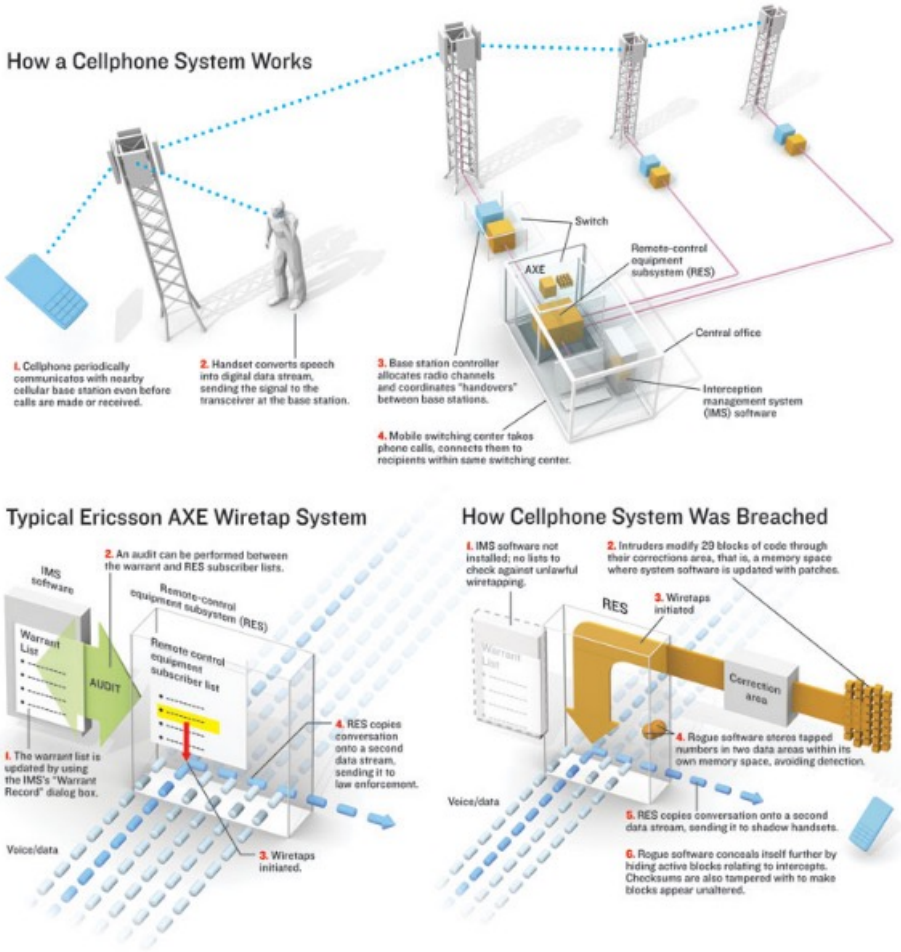
Sadap, Filter, Simpan

Sumber: IEEE Spectrum April 2003

The Athens Affair

- 9 March 2005, Costas Tsalikidis (38 thn) bunuh diri
- Besoknya diberitakan telepon PM Yunani disadap (+ 100 orang lainnya)
- Pelanggan Vodafone-Panafon (Vodafone Greek)

http://www.spectrum.ieee.org/print/5280/

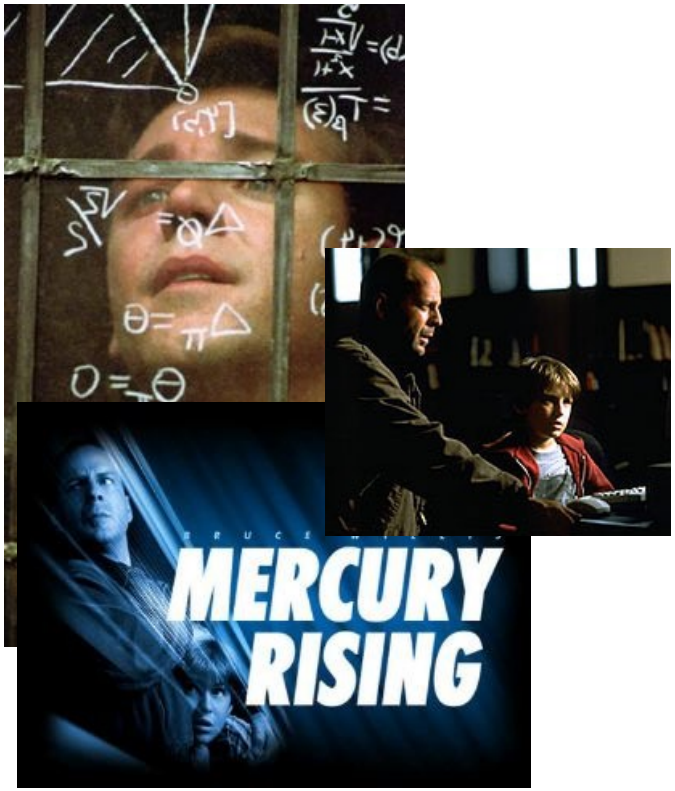

How a Cellphone System Works
1. Cellphone periodically communicates with nearby cellular base station even before calls are made or received.
2. Handset converts speech into digital data stream, sending the signal to the transceiver at the base station.
3. Base station controller allocates radio channels and coordinates "handovers" between base stations.
4. Mobile switching center takes phone calls, connects them to recipients within same switching center.
Switch
AXE
Remote-control equipment subsystem (RES)
Central office
Interception management system (IMS) software
Typical Ericsson AXE Wiretap System
IMS software
Warrant List
AUDIT
2. An audit can be performed between the warrant and RES subscriber lists.
Remote-control equipment subsystem (RES)
Remote control equipment subscriber list
1. The warrant list is updated by using the IMS's "Warrant Record" dialog box.
4. RES copies conversation onto a second data stream, sending it to law enforcement.
Voice/data
3. Wiretaps initiated.
How Cellphone System Was Breached
1. IMS software not installed; no lists to check against unlawful wiretapping.
2. Intruders modify 29 blocks of code through their corrections area, that is, a memory space where system software is updated with patches.
RES
3. Wiretaps initiated
Correction area
4. Rogue software stores tapped numbers in two data areas within its own memory space, avoiding detection.
Voice/data
5. RES copies conversation onto a second data stream, sending it to shadow handsets.
6. Rogue software conceals itself further by hiding active blocks relating to intercepts. Checksums are also tampered with to make blocks appear unaltered.


JAMES BOND
007


THE STAR OF
BEAN
IS NOW
HER MAJESTY'S
MOST TRUSTED
SECRET
AGENT
ROWAN ATKINSON
JOHNNY ENGLISH
He knows no Fear. He knows no Danger.
He knows Nothing.

Evolusi pengamanan data

- Steganography
  - Membuat seolah-olah pesan tidak ada
  - Film: “Mercury rising”, “Beautiful mind”
- Cryptography
  - Transposition (letters arranged)
  - Substitution (letters substituted with other letters)



Steganography

Steganography

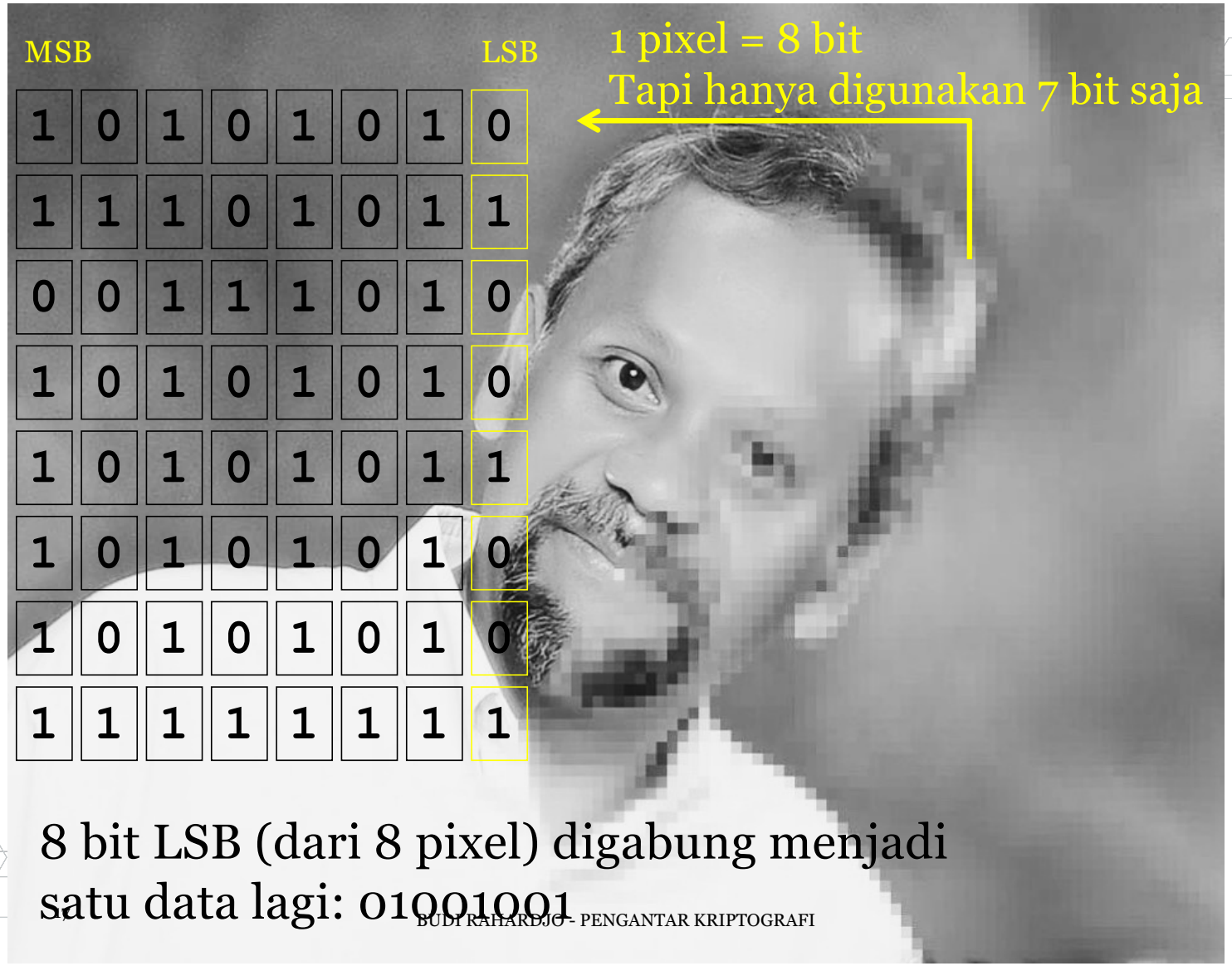
- Yunani (Greek) vs Persia
  - Pesan disembunyikan di meja yang dilapisi lilin

Steganography

- Histiaeus secret message
  - Pesan ditato di kepala budak yang telah digunduli

Steganography saat ini

- Digital watermarking
  - Menandai kepemilikan gambar digital, misalnya dengan menggunakan LSB (*least significant bit*) dari pixel sebagai bagian dari pesan
  - Bisa juga diterapkan di audio (MP3), video, dan format digital lainnya untuk menjadi bagian dari *Digital Rights Management* (DRM)



8 bit LSB (dari 8 pixel) digabung menjadi satu data lagi: 01001001

http://www.randomhouse.com/doubleday/davinci/

While in Paris on business, Harvard symbologist Robert Langdon receives an urgent late-night phone call. The elderly curator of the Louvre has been murdered inside the museum, a baffling cipher found near the body. As Langdon and a gifted French cryptologist, Sophie Neveu, sort through the bizarre riddles, they are stunned to discover a trail of clues hidden in the works of Da Vinci—clues visible for all to see and yet ingeniously disguised by the painter.

The stakes are raised when Langdon uncovers a startling link: The late curator was involved in the Priory of Sion—an actual secret society whose members included Sir Isaac Newton, Botticelli, Victor Hugo, and Da Vinci, among others. Langdon suspects they are on the hunt for a breathtaking historical secret, one that has proven through the centuries to be as enlightening as it is dangerous. In a frantic race through Paris, and beyond,

(continued on back flap)

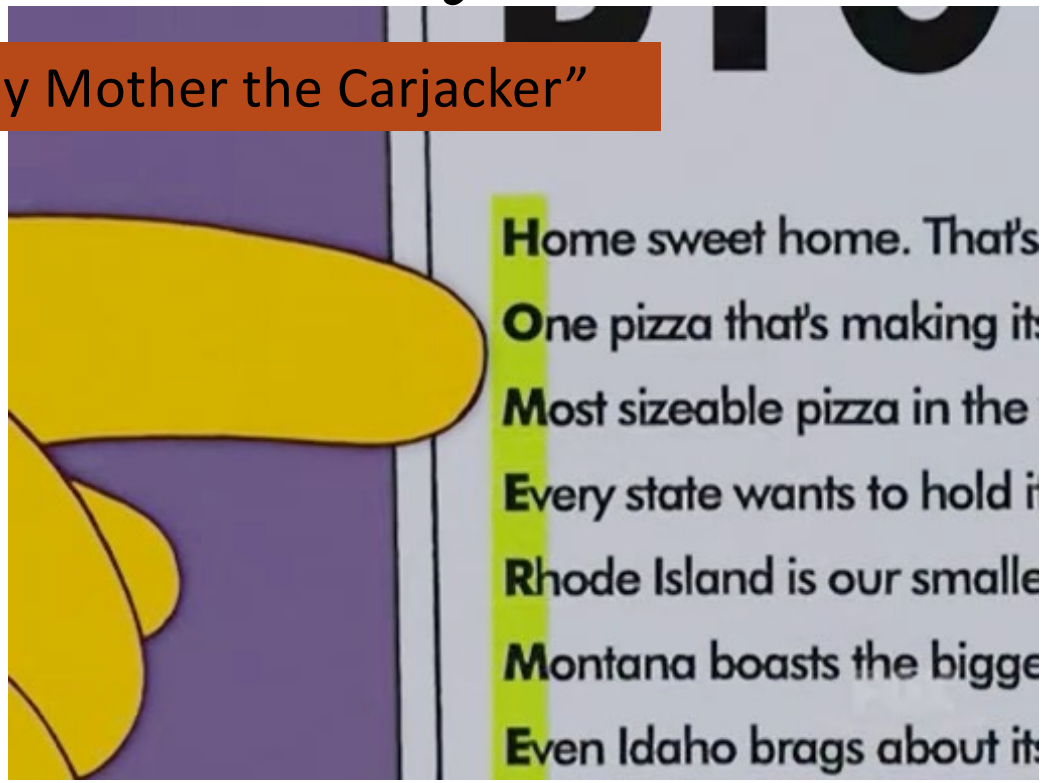
Langdon and Neveu find themselves matching wits with a faceless powerbroker who appears to anticipate their every move. Unless they can decipher the labyrinthine puzzle, the Priory's secret—and an explosive ancient truth—will be lost forever.

Breaking the mold of traditional suspense novels, *The Da Vinci Code* is simultaneously lightning-paced, intelligent, and intricately layered with remarkable research and detail. From the opening pages to the unpredictable and stunning conclusion, bestselling author Dan Brown proves himself a master storyteller.

Contoh Tugas Steganography

- Tugas dari Nur Alimah
  - Setelah engkau rasakan apa nikmatnya gula, hisap aroma rokok ini sampai engkau nyaman ingin nambah.

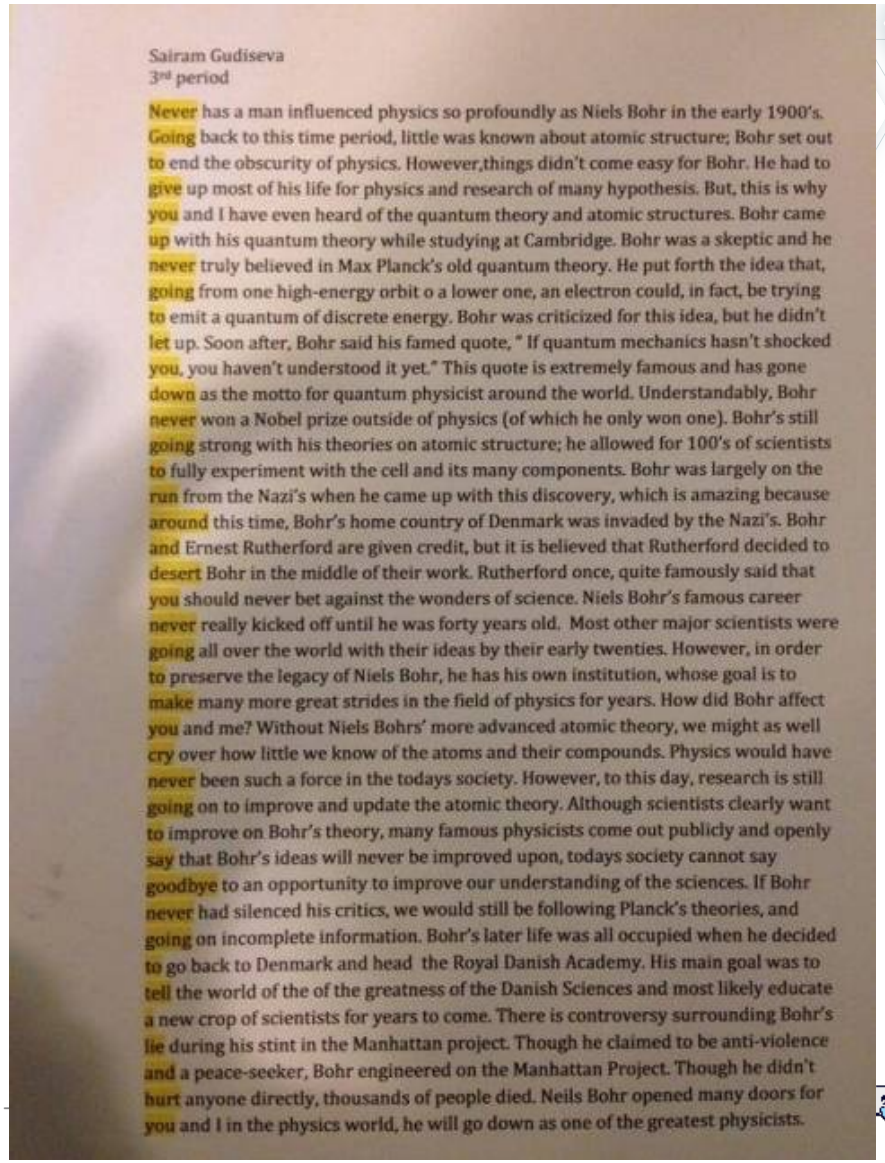
Pesan untuk (Homer) Simpson dari ibunya (Mona)



Dalam buku

- Lirik dari lagu
  Rick Astley –
  Never Gonna Give You Up

https://rhollick.wordpress.com/2017/10/07/never-going-to-give-you-up/



Sairam Gudiseva
3rd period

Never has a man influenced physics so profoundly as Niels Bohr in the early 1900's. Going back to this time period, little was known about atomic structure; Bohr set out to end the obscurity of physics. However,things didn't come easy for Bohr. He had to give up most of his life for physics and research of many hypothesis. But, this is why you and I have even heard of the quantum theory and atomic structures. Bohr came up with his quantum theory while studying at Cambridge. Bohr was a skeptic and he never truly believed in Max Planck's old quantum theory. He put forth the idea that, going from one high-energy orbit o a lower one, an electron could, in fact, be trying to emit a quantum of discrete energy. Bohr was criticized for this idea, but he didn't let up. Soon after, Bohr said his famed quote, " If quantum mechanics hasn't shocked you, you haven't understood it yet." This quote is extremely famous and has gone down as the motto for quantum physicist around the world. Understandably, Bohr never won a Nobel prize outside of physics (of which he only won one). Bohr's still going strong with his theories on atomic structure; he allowed for 100's of scientists to fully experiment with the cell and its many components. Bohr was largely on the run from the Nazi's when he came up with this discovery, which is amazing because around this time, Bohr's home country of Denmark was invaded by the Nazi's. Bohr and Ernest Rutherford are given credit, but it is believed that Rutherford decided to desert Bohr in the middle of their work. Rutherford once, quite famously said that you should never bet against the wonders of science. Niels Bohr's famous career never really kicked off until he was forty years old. Most other major scientists were going all over the world with their ideas by their early twenties. However, in order to preserve the legacy of Niels Bohr, he has his own institution, whose goal is to make many more great strides in the field of physics for years. How did Bohr affect you and me? Without Niels Bohrs' more advanced atomic theory, we might as well cry over how little we know of the atoms and their compounds. Physics would have never been such a force in the todays society. However, to this day, research is still going on to improve and update the atomic theory. Although scientists clearly want to improve on Bohr's theory, many famous physicists come out publicly and openly say that Bohr's ideas will never be improved upon, todays society cannot say goodbye to an opportunity to improve our understanding of the sciences. If Bohr never had silenced his critics, we would still be following Planck's theories, and going on incomplete information. Bohr's later life was all occupied when he decided to go back to Denmark and head the Royal Danish Academy. His main goal was to tell the world of the of the greatness of the Danish Sciences and most likely educate a new crop of scientists for years to come. There is controversy surrounding Bohr's lie during his stint in the Manhattan project. Though he claimed to be anti-violence and a peace-seeker, Bohr engineered on the Manhattan Project. Though he didn't hurt anyone directly, thousands of people died. Neils Bohr opened many doors for you and I in the physics world, he will go down as one of the greatest physicists.

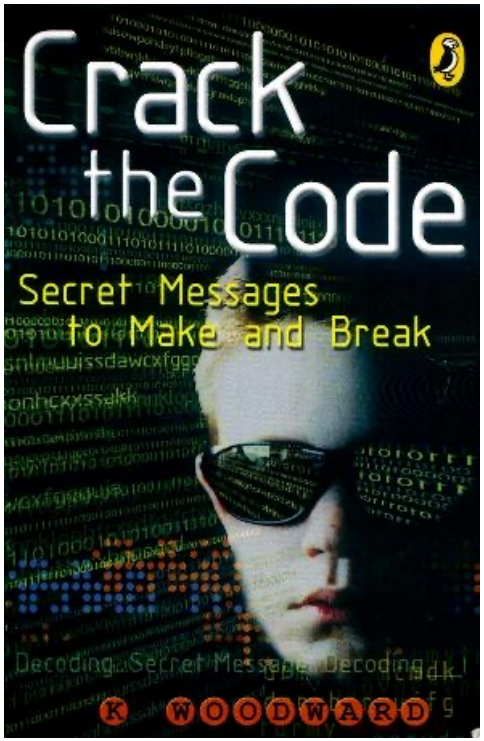
Kriptografi

Cryptography

- ***Cryptography*** *(or cryptology; derived from Greek κρύπτω kryptó "hidden" and the verb γράφω gráfo "to write" or λέγειν legein "to speak") is the practice and study of hiding information. In modern times, cryptography is considered to be a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security, and engineering.*

[sumber: wikipedia]

www.nsa.gov/kids



- How to make crypto more **fun**?

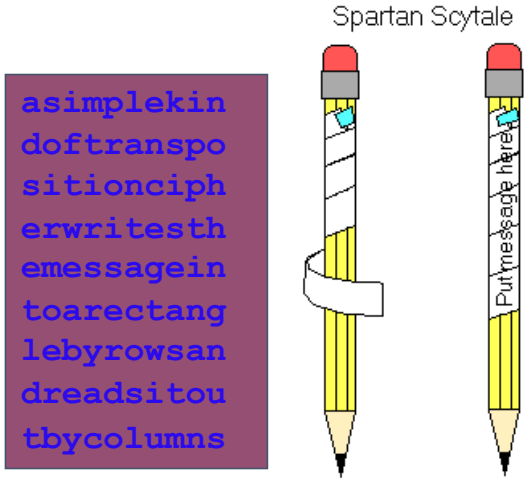
Kripto penentu hidup mati

- Mary, Queen of Scots dipancung
  - Menggunakan cipher messages untuk mengirimkan berita kepada kelompok anti Queen Elizabeth I
  - Dituduh merencanakan pembunuhan Queen Elizabeth I
  - Lawannya: Walsingham yang menggunakan Thomas Phelippes, seorang pakar pemecah kode
  - Dihukum mati 8 Februari 1587

Kriptografi: Transposition

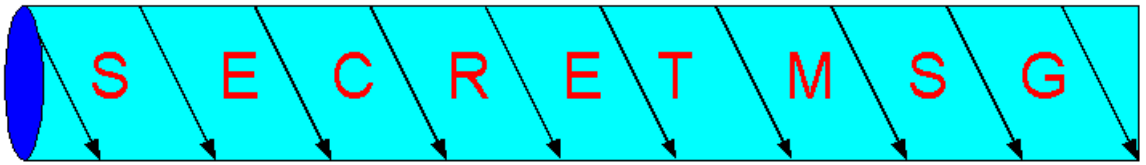
- Contoh transposition
  - Rail fence
  - Simple transposition:
    pesan ditulis mendatar dikirimkan vertikal
  - Spartan Scytale (5 BC)

http://www.unmuseum.org/excoded.htm



http://en.wikibooks.org/wiki/Cryptography:Transposition_ciphers

http://www.ccisource.com/content/resources/articles/Jan01/symmetric.htm



Kriptografi: Substitution

- **Caesar cipher** (geser 3 huruf)

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

d e f g h i j k l m n o p q r s t u v w x y z a b c

BUDI = exgl

Tabel dapat digeser *n* huruf ke kiri
atau ke kanan. *n* dan arah menjadi kunci

- **Monoalphabetical cipher**, satu huruf selalu digantikan oleh huruf yang sama
  Dalam contoh di atas, huruf "B" selalu menjadi "e"

Pemecahan Caesar Cipher

- Al Kindi menggunakan statistik untuk memecahkan Caesar Cipher
  - Cari huruf yang paling sering muncul dalam *ciphertext* dan luruskan (align) dengan huruf yang paling sering muncul dalam *plaintext*
  - Huruf apa yang sering muncul dalam
    - Bahasa Inggris
    - Bahasa Indonesia
    - Bahasa Daerah lainnya?

ROT13

- Menggeser huruf sebanyak 13 huruf
- Karena jumlah huruf ada 26, maka algoritma (geser13) bisa digunakan untuk enkripsi dan dekripsi
- Lihat situs http://www.rot13.com
- Dapat digunakan untuk tebak-tebakan

Contoh ROT13

Apa bedanya handphone dan monyet?

Jawaban:
Xnynh unaqcubar, abxvn. Xnynh zbalr, ah xvrh

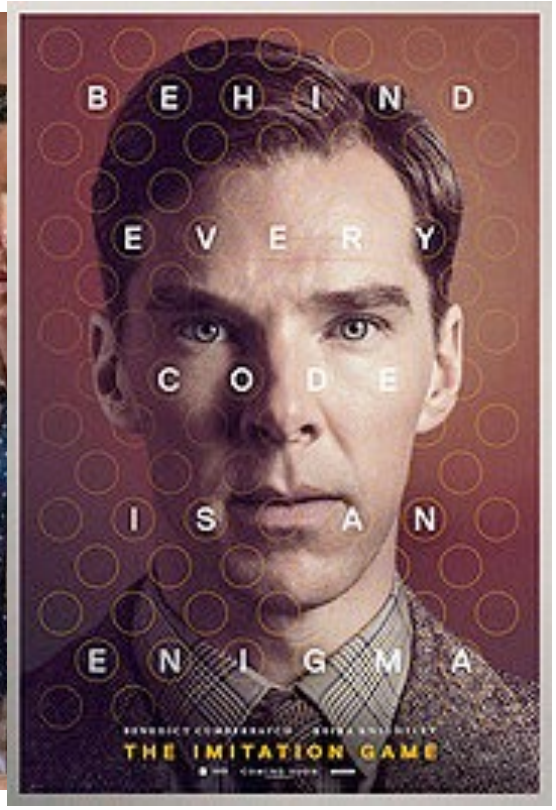
Cipher dengan banyak tabel

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

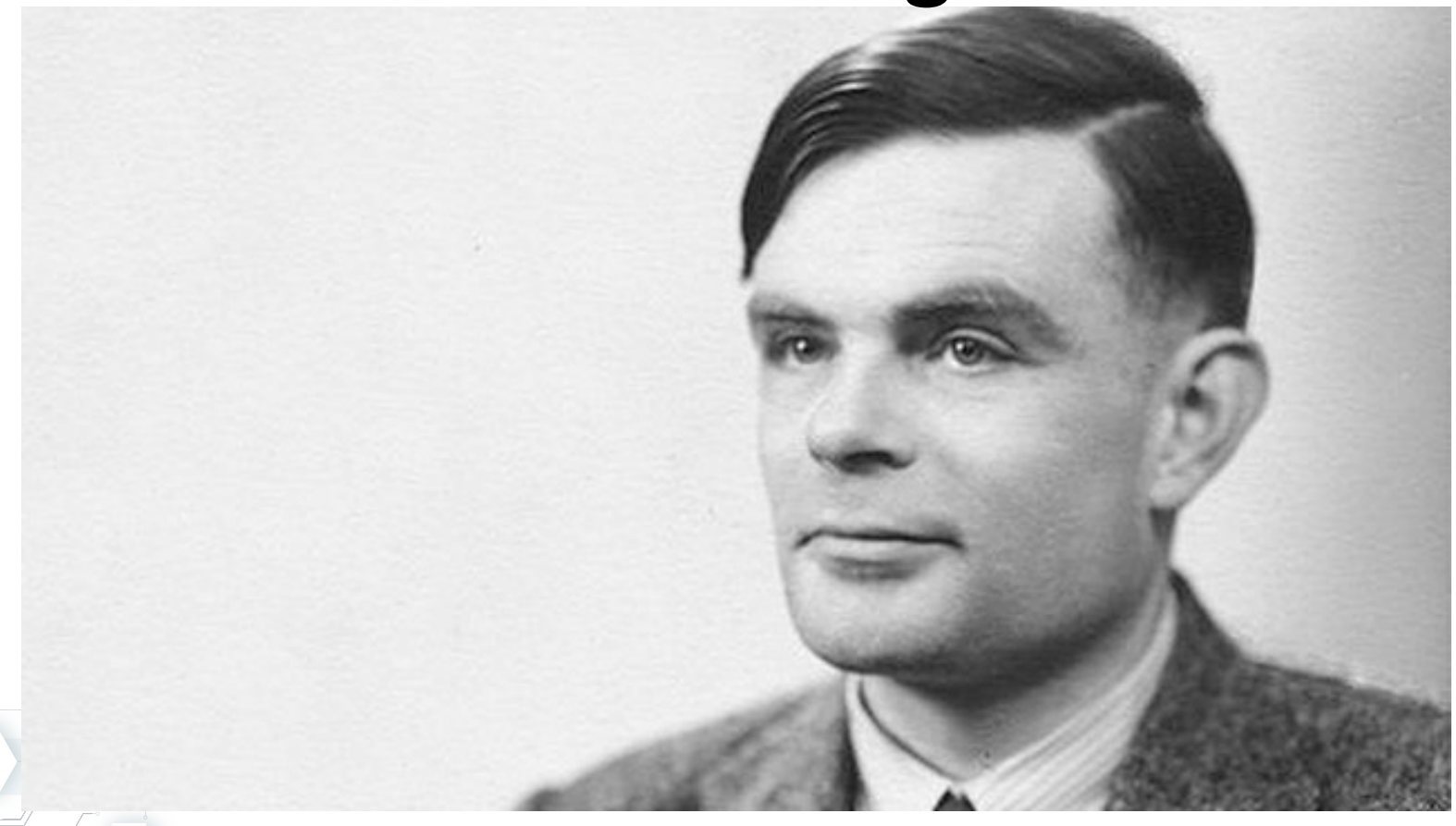
d e f g h i j k l m n o p q r s t u v w x y z a b c
g h i j k l m n o p q r s t u v w x y z a b c d e f
m n o p q r s t u v w x y z a b c d e f g h i j k l

- Huruf pertama dengan tabel pertama
- Huruf kedua dengan tabel kedua
- Huruf ketiga dengan tabel ketiga
- Huruf keempat dengan tabel pertama
- ... dan seterusnya ...

Film tentang Enigma ...



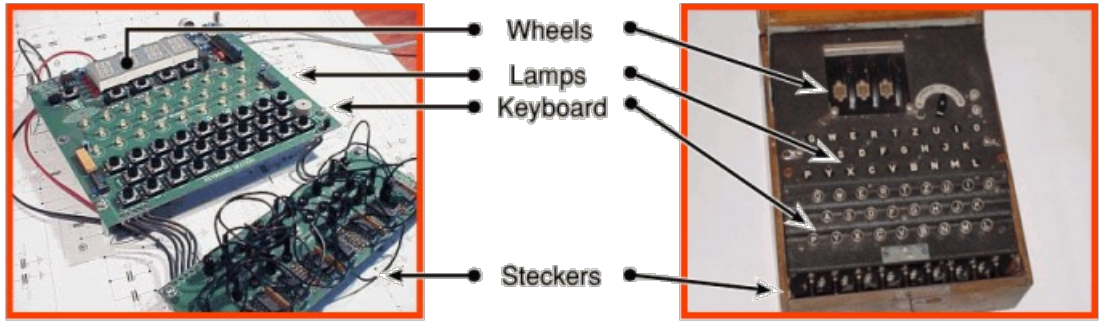
Alan Turing



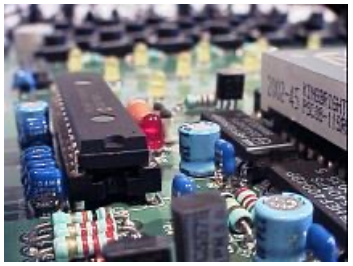
Enigma Rotor

- Digunakan Jerman pada Perang Dunia 2
- Memiliki rotor yang berubah posisinya setelah setiap huruf dikirim
- Posisi awal dari rotor merupakan kunci
- Dipecahkan oleh pihak Sekutu dengan bantuan **Alan Turing** dan komputer

Enigma-E



http://www.xat.nl/enigma-e/desc/index.htm


Komponen dari kriptografi

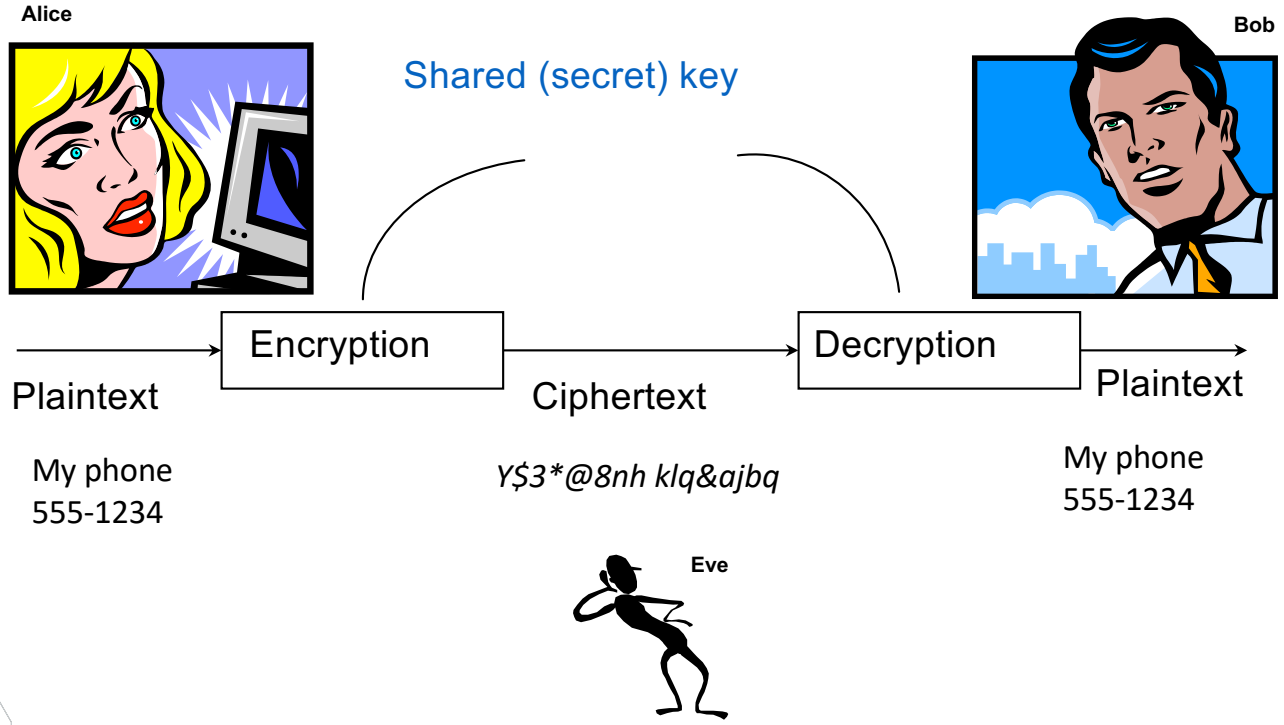
- Plain text
  - Sumber berita/pesan/teks asli
- Cipher text
  - Teks yang sudah diproses (diacak, digantikan)
- Algoritma & kunci
  - Misal: subsitusi (algoritma) & *number of shift* (kunci)
  - Pemisahan algoritma & kunci ditemukan oleh Auguste Kerckhoffs von Niewenhof (1883)

CRYPTOGRAPHY

- ***Private key cryptosystem***
  (Sistem kripto kunci privat)
  - Simetrik (**kunci** untuk mengunci dan membuka **sama/satu**)
- ***Public key cryptosystem***
  (Sistem kripto kunci publik)
  - Asimetrik (**kunci** untuk mengunci dan membuka **berbeda**)

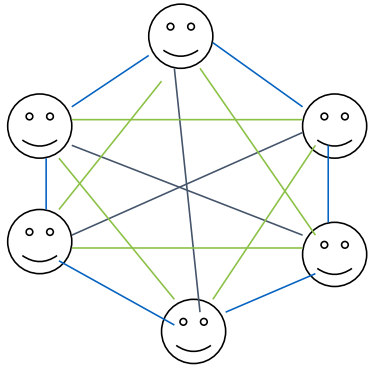
Kripto Kunci Privat

(secret key, symmetric cryptosystem)



Kripto Kunci Privat

- Menggunakan satu kunci
- Masalah dalam distribusi kunci
  - Pengiriman kunci membutuhkan saluran khusus
  - Jumlah kunci meledak secara eksponensial:
    n (n-1)/2: (lihat ilustrasi / gambar di bawah)
- Keuntungan: operasi yang cepat
- Contoh: DES, IDEA, AES

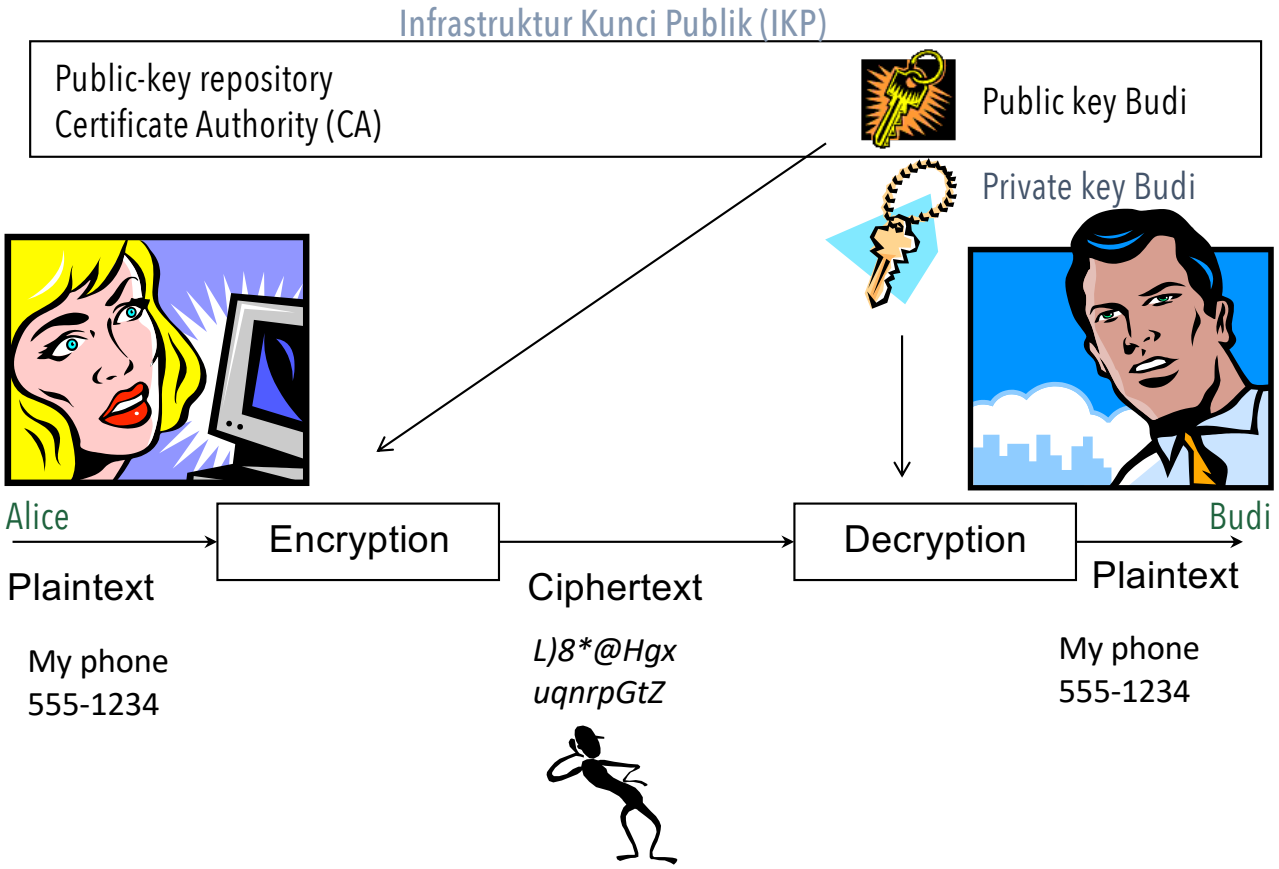


Meledaknya Jumlah Kunci

n (jumlah orang)	$n * (n-1) / 2 \approx n^2/2$ jumlah kunci
10	50
100	5000
1000	500.000
10.000	50.000.000
100.000	5.000.000.000

Jika 1 kunci memiliki ukuran 1 kByte, maka untuk 100.000 orang dibutuhkan 5 TBytes untuk kunci saja

Kriptografi Kunci Publik



Kripto Kunci Publik

- Menggunakan kunci yang berbeda untuk enkripsi dan dekripsi
- Jumlah kunci yang lebih sedikit dibandingkan enkripsi dengan kunci privat
- Membutuhkan komputasi yang tinggi (membutuhkan waktu yang lebih lama)

Kripto Kunci Publik

- Membutuhkan penyimpanan kunci publik (Certificate Authority) yang terpercaya (trusted). Siapa? Verisign?
- Pengelolaan kunci (key management) bisa menjadi kompleks (revocation, pihak ketiga, dll.)
- Contoh algoritma: RSA, ECC

Pionir Kripto Kunci Publik

Amerika

- Whitfield Diffie
- Martin Hellman
- Ralph Merkle
- Ron Rivest
- Adi Shamir
- Len Adleman
- ...

Inggris (awal 1970an GCHQ)

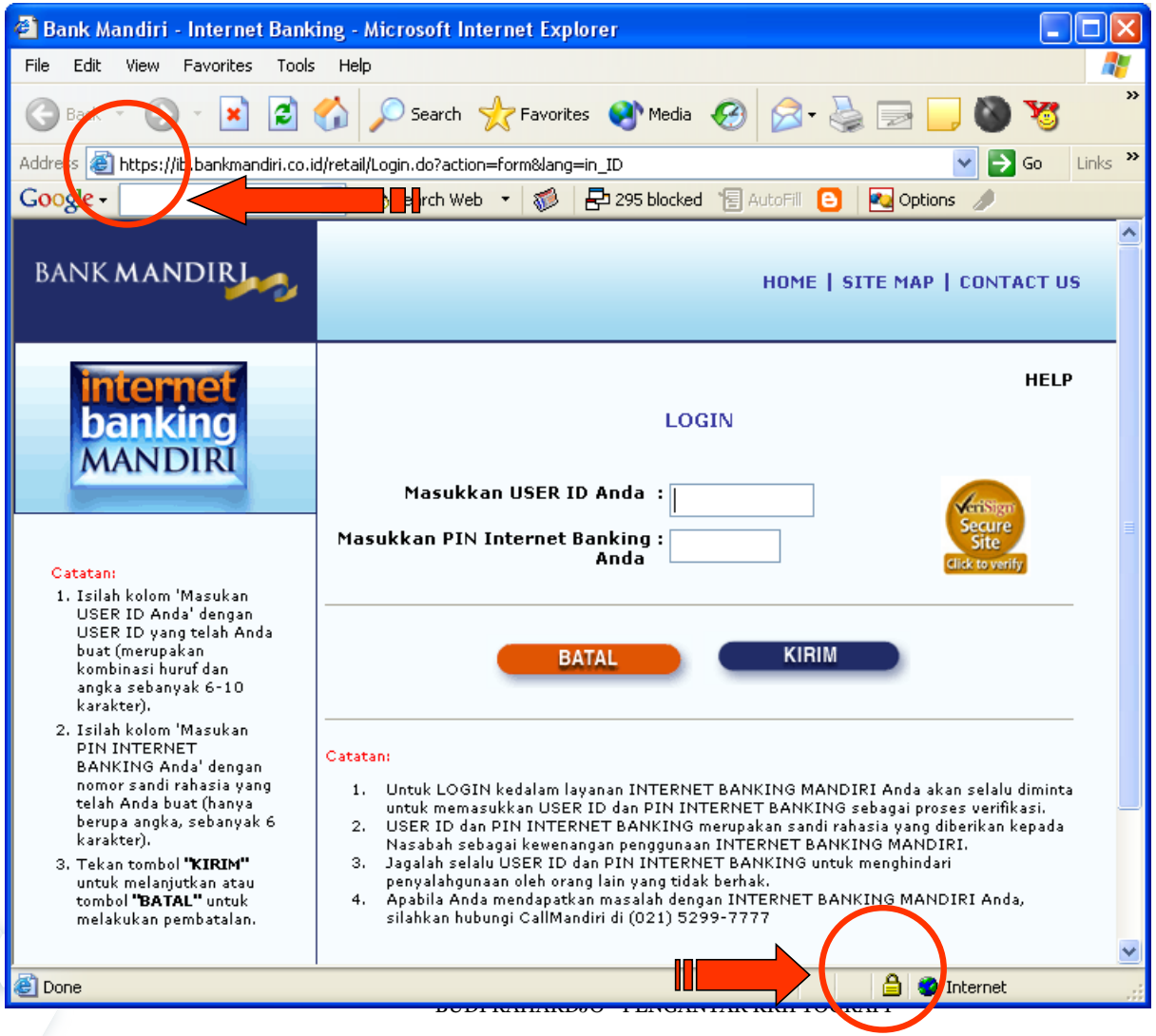
- James Ellis
- Clifford Cocks
- Malcolm Williamson

Contoh Algoritma

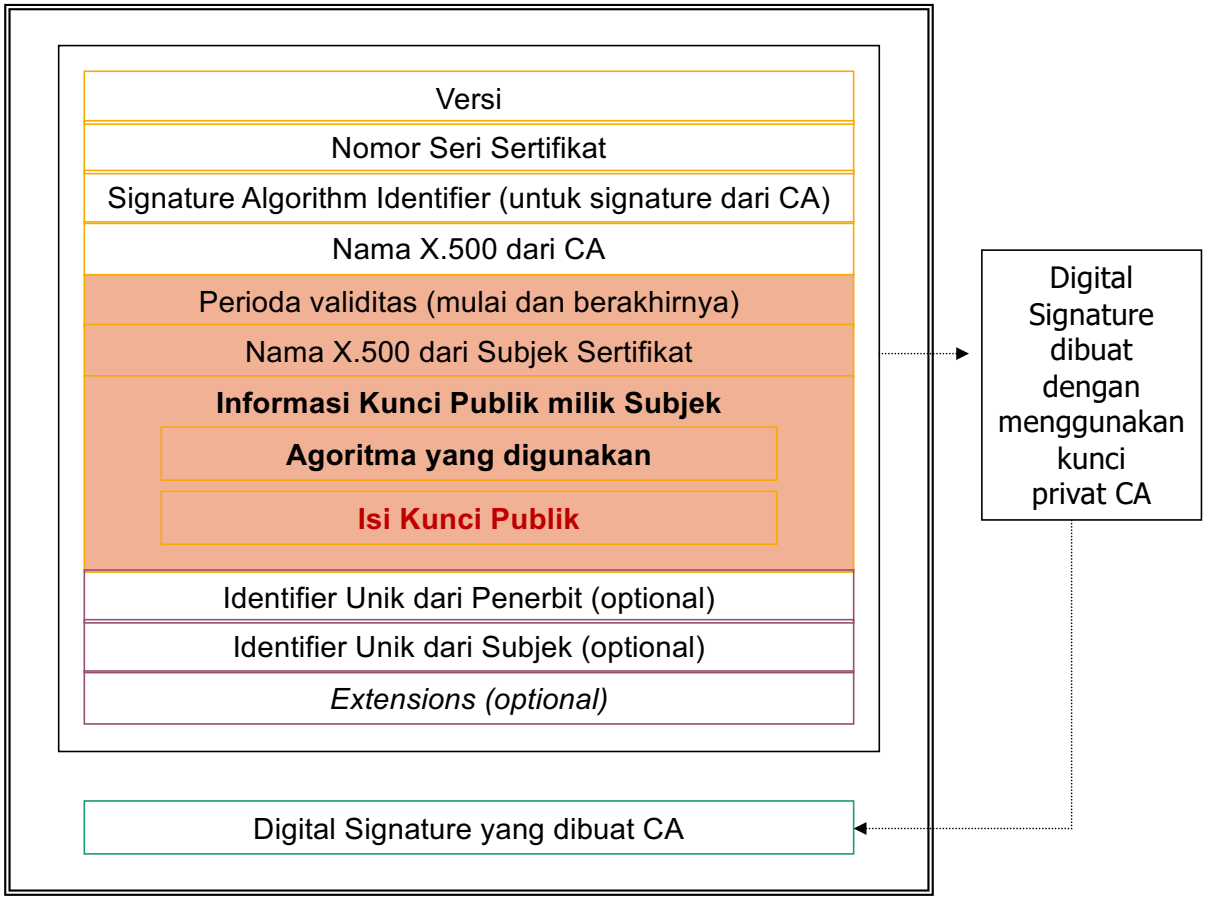
- [Pindah ke slide materi presentasi lain]
- DES
- RSA
- Kekuatan dari Algoritma

Penggunaan Kripto Kunci Publik

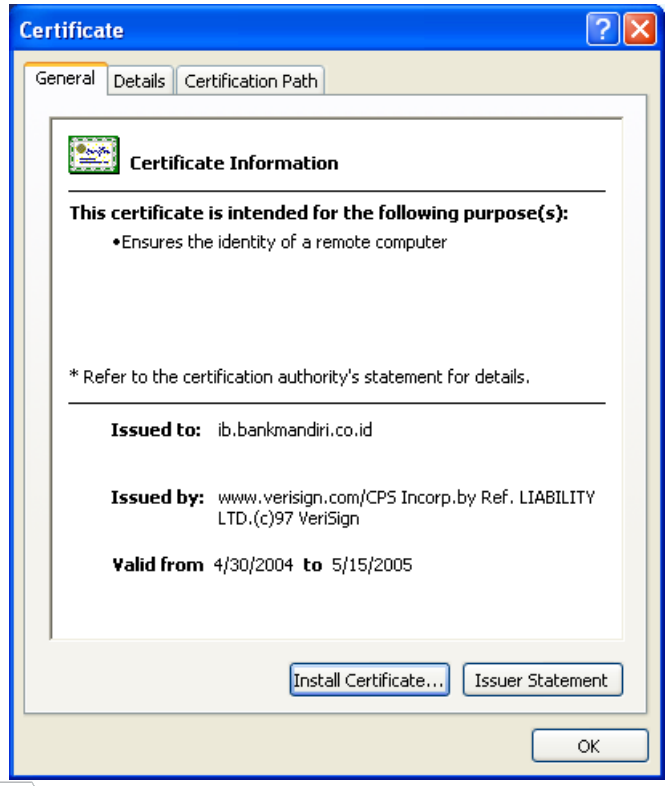
- Secure Socket Layer (SSL)
  - HTTPS
  - SSH
  - STUNNEL
- Pretty Good Privacy (PGP) dan GNU Privacy Guard (GPG)

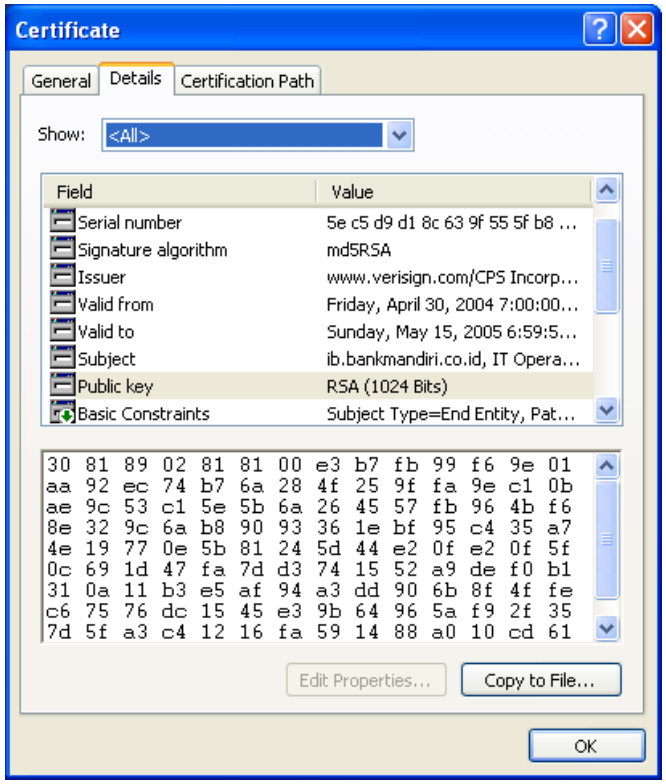

Bank Mandiri - Internet Banking - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Search Favorites Media
https://ib.bankmandiri.co.id/retail/Login.do?action=form&lang=in_ID
Go Links
Google
295 blocked AutoFill Options
BANK MANDIRI
HOME | SITE MAP | CONTACT US
internet banking MANDIRI
HELP
LOGIN
Masukkan USER ID Anda :
Masukkan PIN Internet Banking : Anda
VeriSign Secure Site Click to verify
BATAL
KIRIM
Catatan:
1. Isilah kolom 'Masukan USER ID Anda' dengan USER ID yang telah Anda buat (merupakan kombinasi huruf dan angka sebanyak 6-10 karakter).
2. Isilah kolom 'Masukan 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.
Catatan:
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

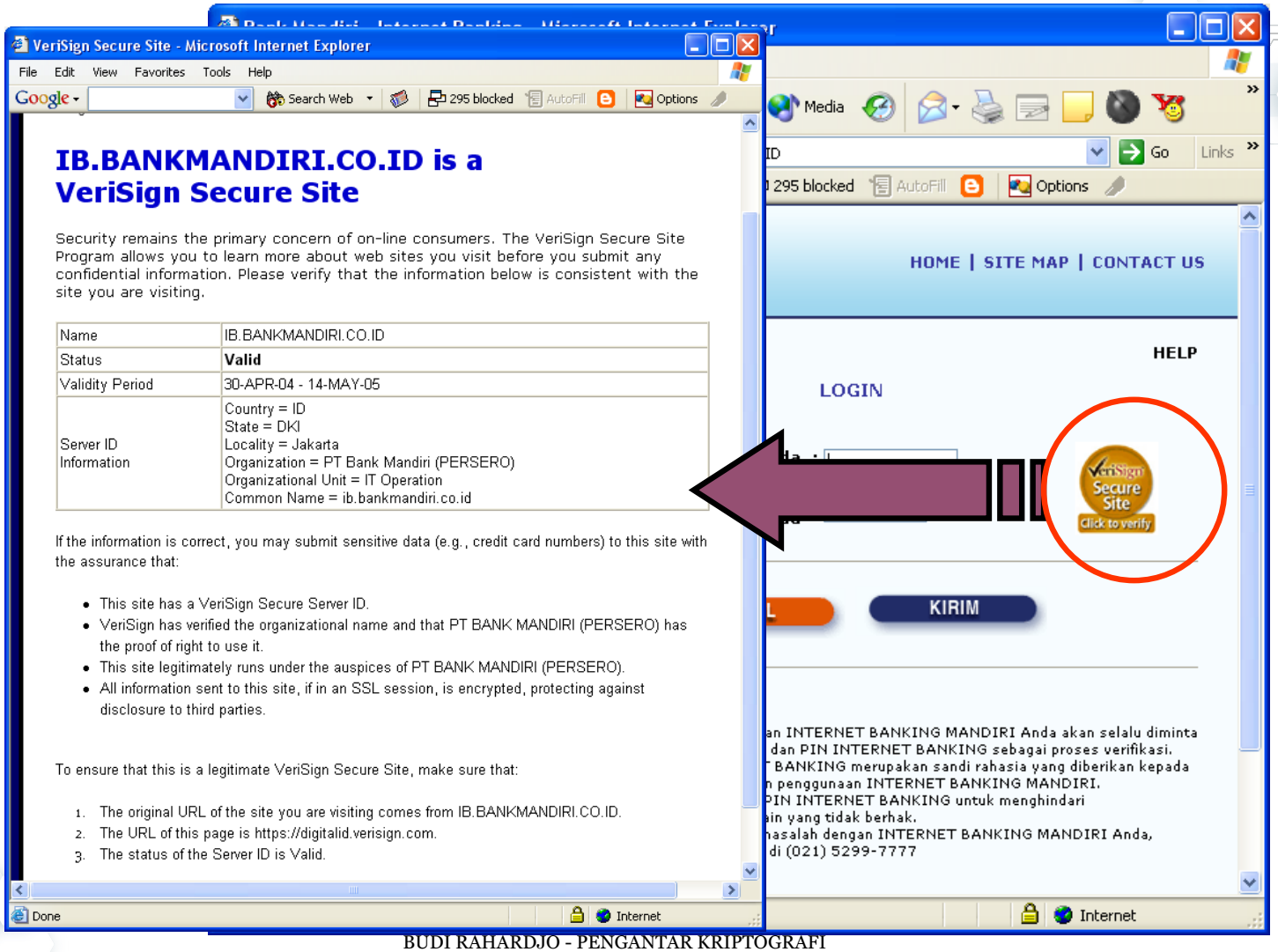
Sertifikat Digital X.509 versi 3



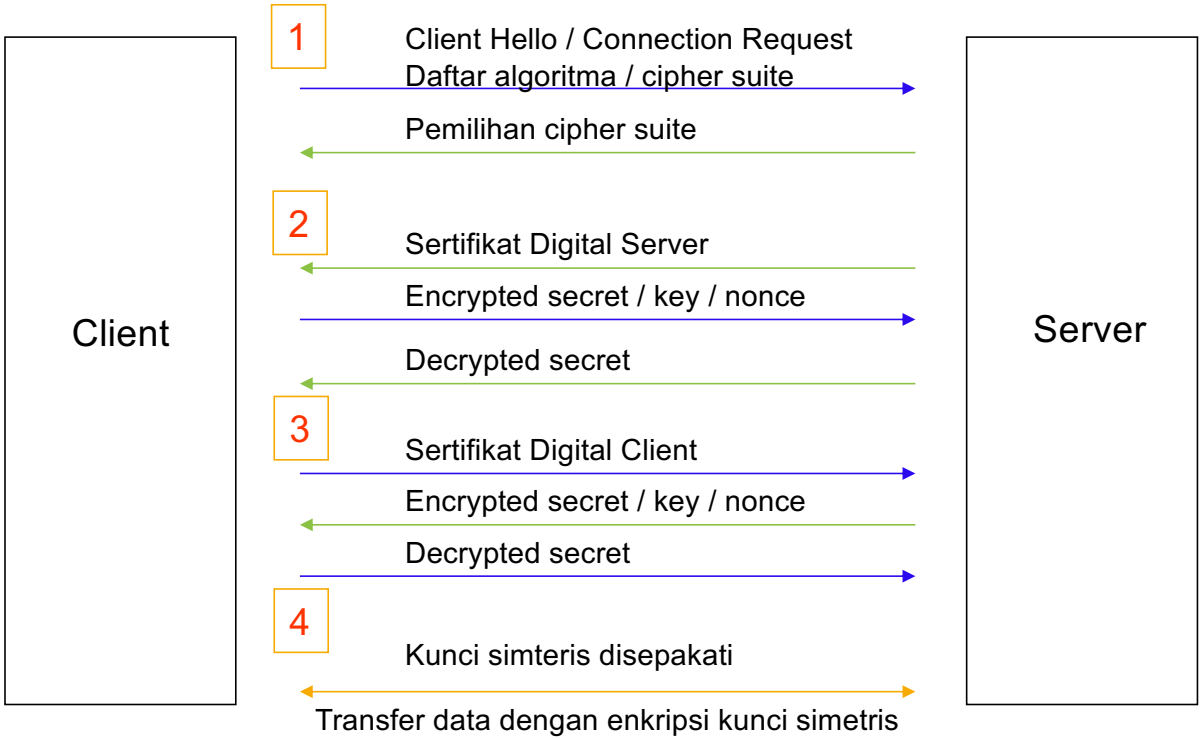
Contoh Sertifikat






VeriSign Secure Site - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Google
Search Web
295 blocked
AutoFill
Options
IB.BANKMANDIRI.CO.ID is a
VeriSign Secure Site
Security remains the primary concern of on-line consumers. The VeriSign Secure Site Program allows you to learn more about web sites you visit before you submit any confidential information. Please verify that the information below is consistent with the site you are visiting.
Name
IB.BANKMANDIRI.CO.ID
Status
Valid
Validity Period
30-APR-04 - 14-MAY-05
Server ID Information
Country = ID
State = DKI
Locality = Jakarta
Organization = PT Bank Mandiri (PERSERO)
Organizational Unit = IT Operation
Common Name = ib.bankmandiri.co.id
If the information is correct, you may submit sensitive data (e.g., credit card numbers) to this site with the assurance that:
This site has a VeriSign Secure Server ID.
VeriSign has verified the organizational name and that PT BANK MANDIRI (PERSERO) has the proof of right to use it.
This site legitimately runs under the auspices of PT BANK MANDIRI (PERSERO).
All information sent to this site, if in an SSL session, is encrypted, protecting against disclosure to third parties.
To ensure that this is a legitimate VeriSign Secure Site, make sure that:
1. The original URL of the site you are visiting comes from IB.BANKMANDIRI.CO.ID.
2. The URL of this page is https://digitalid.verisign.com.
3. The status of the Server ID is Valid.
Done
Internet
Media
Go
Links
295 blocked
AutoFill
Options
HOME | SITE MAP | CONTACT US
HELP
LOGIN
VeriSign Secure Site
Click to verify
KIRIM
an INTERNET BANKING MANDIRI Anda akan selalu diminta
dan PIN INTERNET BANKING sebagai proses verifikasi.
BANKING merupakan sandi rahasia yang diberikan kepada
penggunaan INTERNET BANKING MANDIRI.
PIN INTERNET BANKING untuk menghindari
ain yang tidak berhak.
hasalah dengan INTERNET BANKING MANDIRI Anda,
di (021) 5299-7777
Internet

Protokol SSL



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

PENGGUNAAN ENKRIPSI

- Mengamankan data dengan mengacak data sehingga sulit untuk dibaca
  Confidentiality
- Meyakinkan tidak ada perubahan data
  Integrity
- Memastikan identitas seseorang dengan digital signature
  Authentication

Message Digest

- Menghasilkan rangkuman (*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)
  - Mudah dihitung untuk satu arah (forward)
  - Sulit (hard) dihitung inverse-nya
- Perubahan satu bit saja akan mengubah keluaran hash secara drastis
- Digunakan untuk menjamin integritas dan digital signature

Fungsi Hash Sederhana

- Menjumlahkan nilai ASCII dari karakter
- Pesan: **BUDI**

no	Karakter	ASCII	Total
0	B	66	66
1	U	85	151
2	D	68	219
3	I	73	**292**

- Punya masalah dengan *collision*

Hash Function

- Contoh yang lazim digunakan:
  MD5, SHA-1, SHA-256, RIPEMD

```
unix$ md5sum /bin/login
af005c0810eeca2d50f2904d87d9ba1c  /bin/login
unix$ md5sum /etc/passwd
a3eeed3854a930c97a125378785045f9  /etc/passwd
unix$ shasum README.md
75d2ba77c401d7df44b79093db004e358f663db6  README.md
```

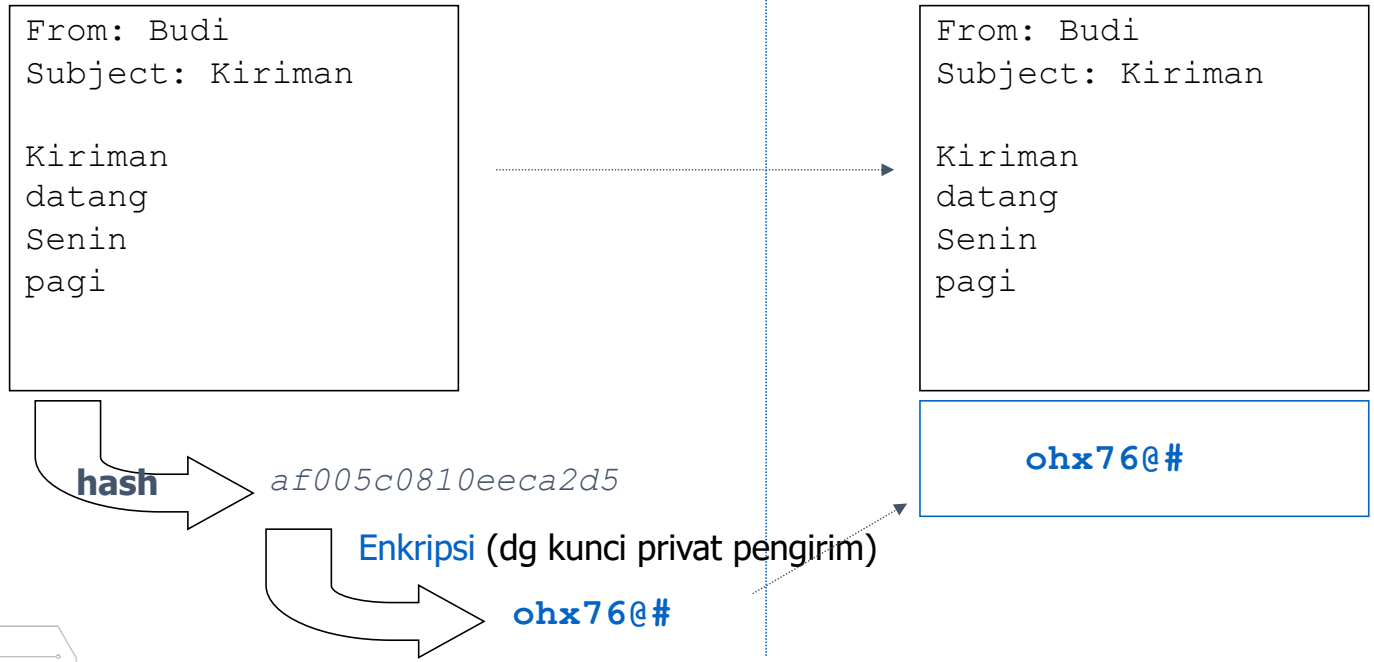

Hash Function & Tools

- Jacksum (a collection of hash functions)
  - http://jacksum.net/en/index.html
- Identify what hash function is being used
  - https://hashes.com/en/tools/hash_identifier
  - https://github.com/psypanda/hashID

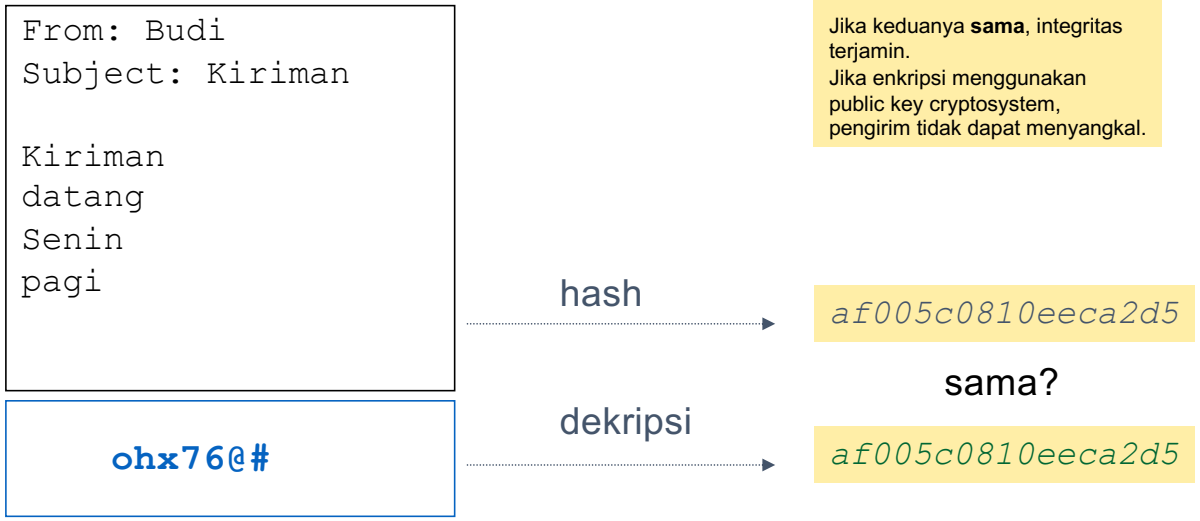
Penggunaan Hash: Pengirim

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

Keduanya disatukan dan dikirimkan



Pada Penerima



Jika keduanya **tidak sama**,
patut dicurigai.
Integritas tidak terjamin.

Jika keduanya **sama**, integritas terjamin.
Jika enkripsi menggunakan public key cryptosystem, pengirim tidak dapat menyangkal.

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)
  - Basis dari konsep *digital signature*
  - Pesan juga dapat dienkripsi jika diinginkan kerahasiaan
- Contoh aplikasi lain: hash encrypted password, blockchain (yang merupakan fondasi dari Bitcoin)

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 nilai hash yang sama

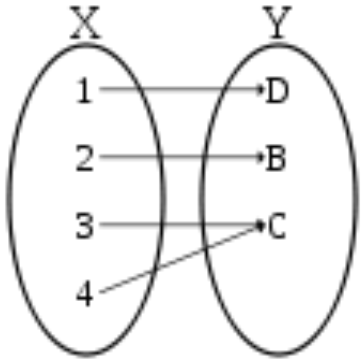


image from wikipedia

Permasalahan Hash

- 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
  - http://shattered.it
- ~~Meskipun dua data yang dipetakan itu tidak mudah dibuat dan kadang-kadang *completely useless*~~
- Pernyataan di atas sudah tidak tepat untuk pemecahan SHA-1

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

Hash & Aplikasi Database

- Bagaimana cara menyimpan pasangan “userid” dan “password” dalam database?
  - Umumnya “password” disimpan dalam bentuk plain text sehingga dapat dilihat oleh DB admin
  - Simpan password dalam bentuk ***hashed***
  - Next level: beri ***salt***

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/