Computer and Network Security
- Security Technology Part 2–
VER 2020

What is a digital signature?

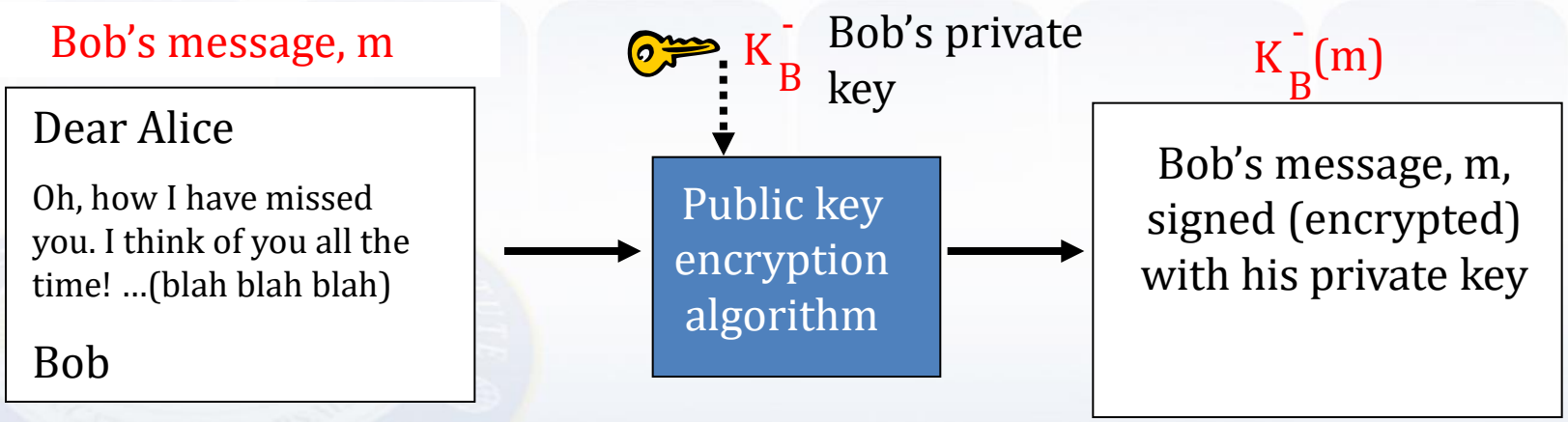
- is an **electronic signature** that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

- is a type of **asymmetric cryptography** used to simulate the security properties of a **signature** in digital, rather than written, form. Digital signature schemes normally give two algorithms, one for signing which involves the user's secret or **private key**, and one for verifying signatures which involves the user's **public key**. The output of the signature process is called the "digital signature.“

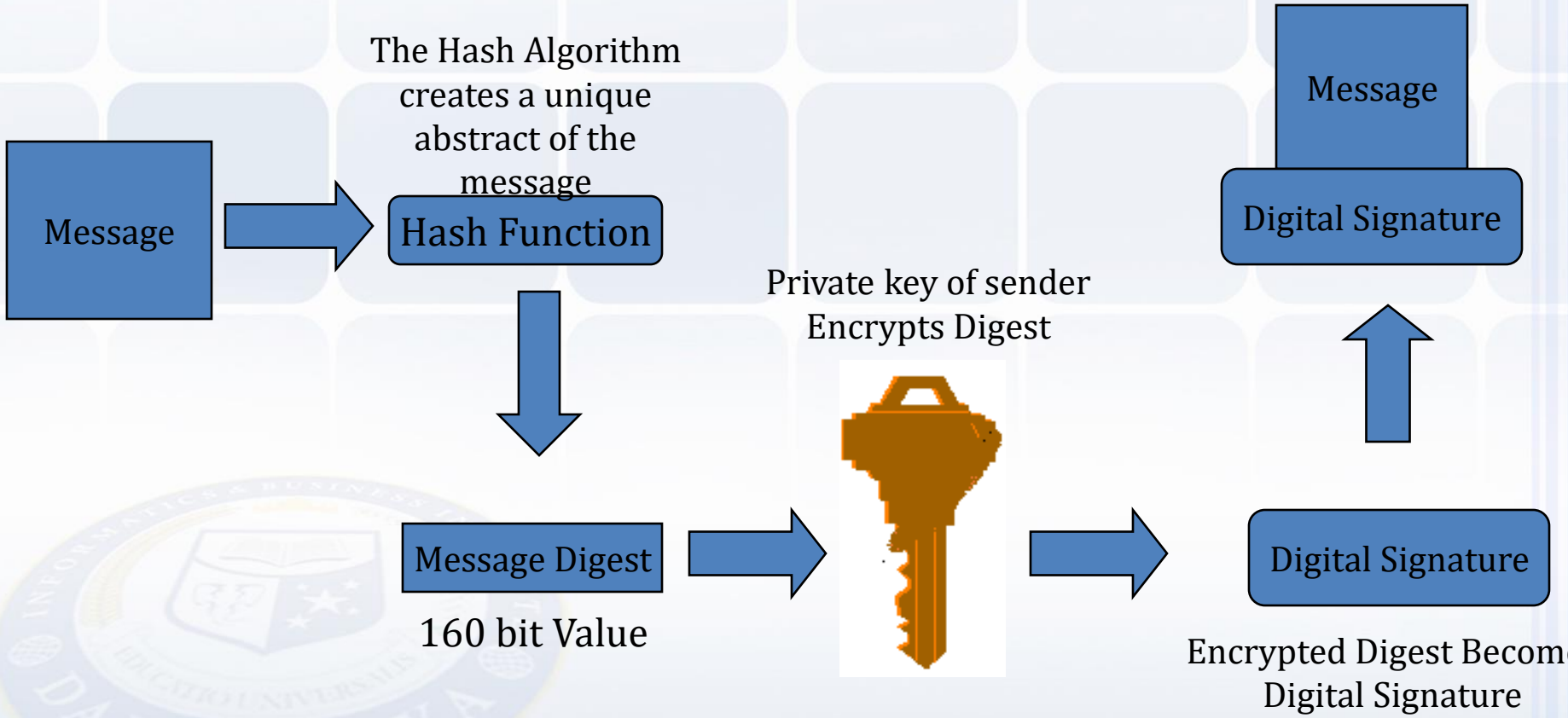
Digital Signature

Example digital signature for message (m):

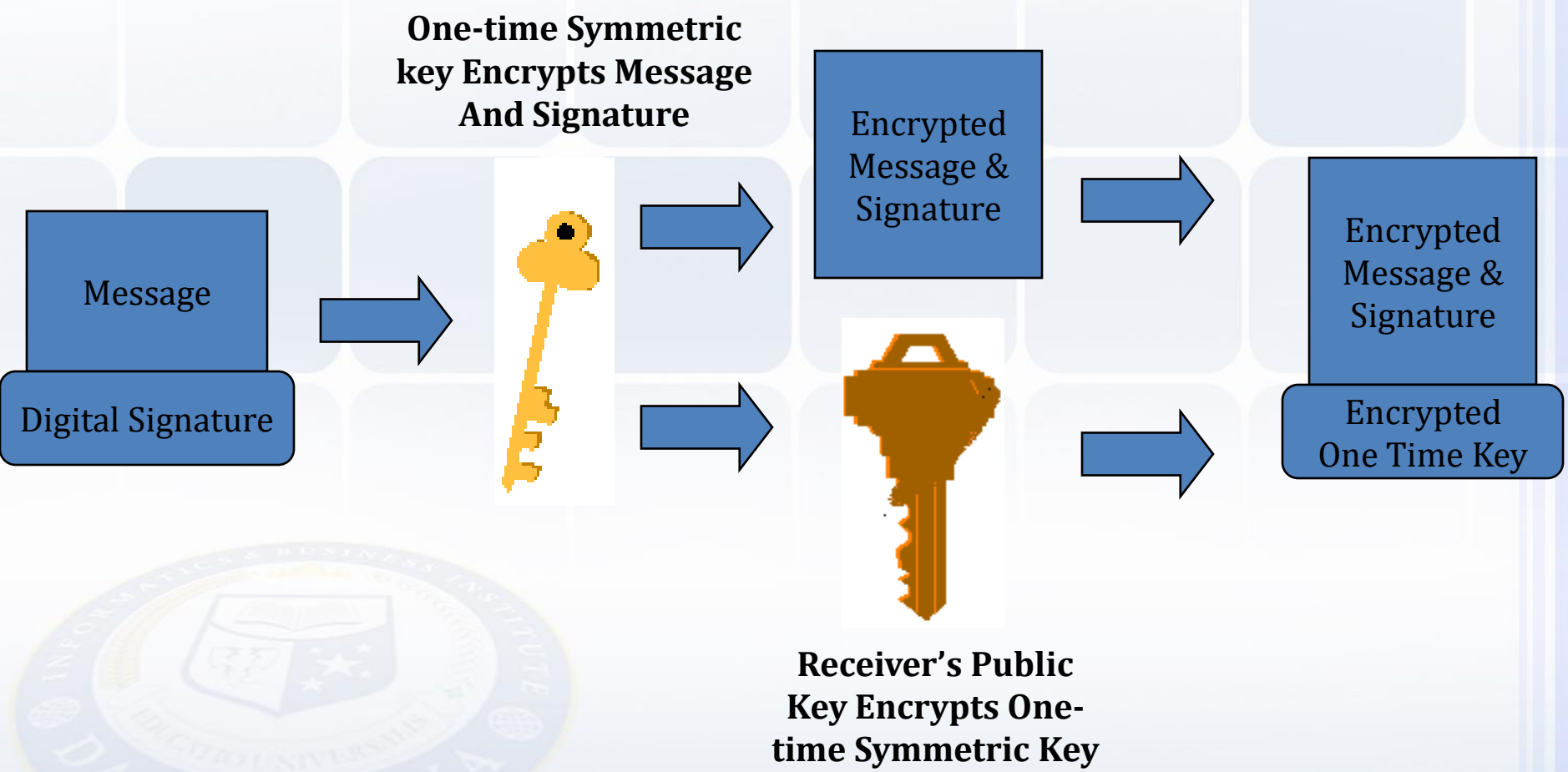
- Bob signs (m) by encrypting it with his private key (K_B^-), to produce signed message ($K_B^-(m)$)



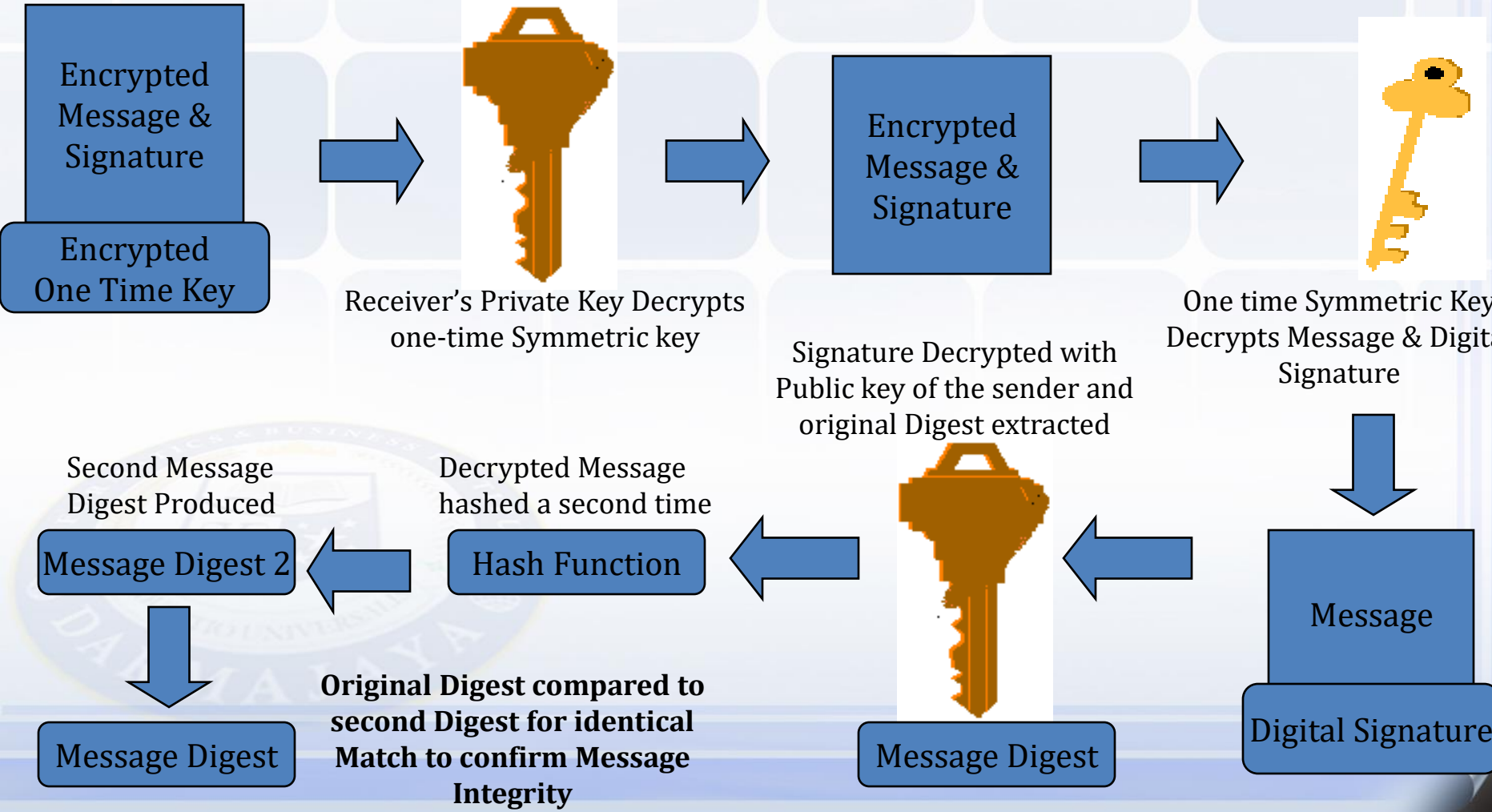
Digital Signature Process



Encryption Process



Decryption and Verification Process



Benefits of digital signatures

These are common reasons for applying a digital signature to communications:

- **Authentication**

  → Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages.

  → When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user.

  → The importance of high confidence in sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.

Benefits of digital signatures

- **Integrity**

→ In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to *change* an encrypted message without understanding it.

→However, if a message is digitally signed, any change in the message will invalidate the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions.

Another Issue

- in-person" verification can be done in a matter of seconds, and becomes a routine affair. However, replicating this procedure on-line is more difficult. The on-line version can't visually compare your face to your ID, nor compare your signature to the previously approved government-sanctioned version of your signature.

- So what is needed is an on-line mechanism that provides a similar sort of assurance from an authority that can say, essentially "you don't know this guy, but I do, and he's okay by me".

How To Overcome

- That authority in the on-line environment is known as a “certificate authority” (CA), an agency whose integrity must be beyond reproach.
- A certificate authority establishes protocols to ascertain the identity of registrants, and supports on-line verification that the identity has been proven to the CA. The Certificate Authority essentially says “I checked this person out, and verified that he is who he says he is, you have my word on it”.
- To acquire a digital certificate, an individual or organization registers with a certificate authority and presents proof of identity. The CA requests specific information of the registrant, investigates it, and then issues a digital certificate that confirms that the CA has verified the information independently.

Digital Certificate

The certificate would typically include the following information:

- The registrant's name
- Additional personal information such as an e-mail address for a person or a URL for a web server
- A unique registration number
- The name of the certificate authority
- The public key of the registrant
- Dates that reflect certificate validity (start and expiration dates)
- A digital signature "seal" from the CA that verifies authenticity of the certificate

Certification Authority

- Kriptografi kunci publik dapat digunakan untuk mengenkripsi data yang dikomunikasikan antara dua pihak. Ini biasanya terjadi ketika pengguna log on ke situs yang mengimplementasikan protokol HTTP yang aman (HTTPS).
- Dalam contoh ini mari kita anggap bahwa pengguna log on ke situs bank-nya www.bank.example untuk melakukan online banking. Ketika pengguna membuka situs www.bank.example, ia menerima kunci publik bersama dengan semua data yang menampilkan web-browser-nya.
- Kunci publik dapat digunakan untuk mengenkripsi data dari klien ke server
- Hanya server bank yang memiliki kunci pribadi untuk membacanya.

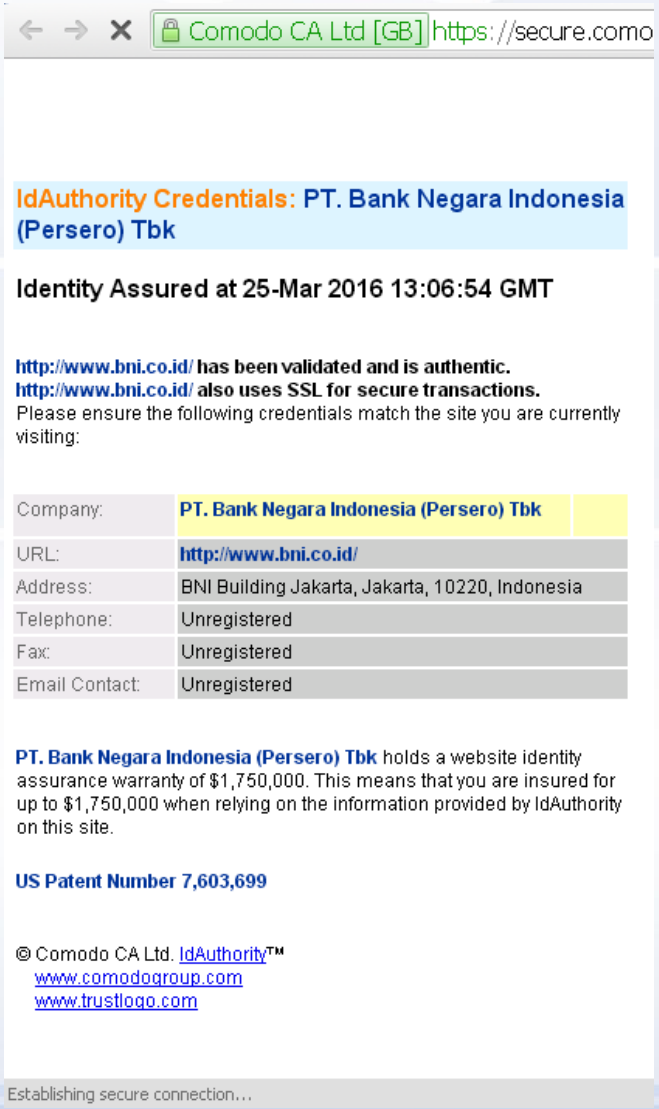
Certificate Authority

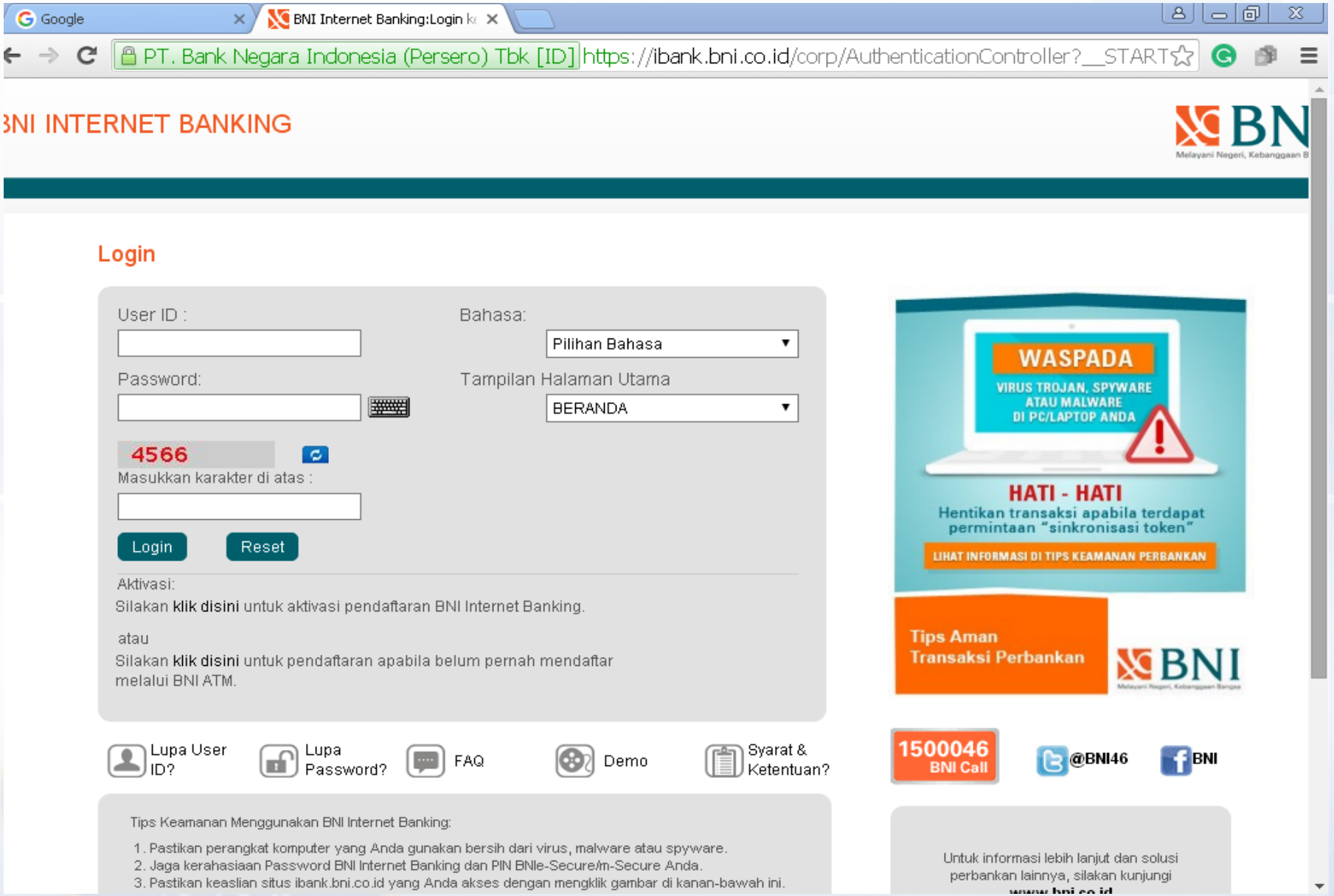
- Komunikasi berikutnya akan menggunakan kunci simetris baru (sekali pakai)
  - jadi ketika pengguna memasukkan beberapa informasi ke halaman bank mengirimkan informasi kembali ke bank maka data pengguna telah masuk ke halaman akan dienkripsi oleh web browsernya . Oleh karena itu, bahkan jika seseorang dapat mengakses (dienkripsi) data yang dikomunikasikan dari pengguna untuk www.bank.example, eavesdropper seperti tidak bisa membaca atau memahaminya.
- www.bank.example yang palsu dpat menggunakan kunci public yang sama, tetapi tidak akan mengetahui pasangan kunci privatenya,. Sehingga tidak dapat menghasilkan “signature” yang sesuai untuk proses autentikasi.

Digital Certificate

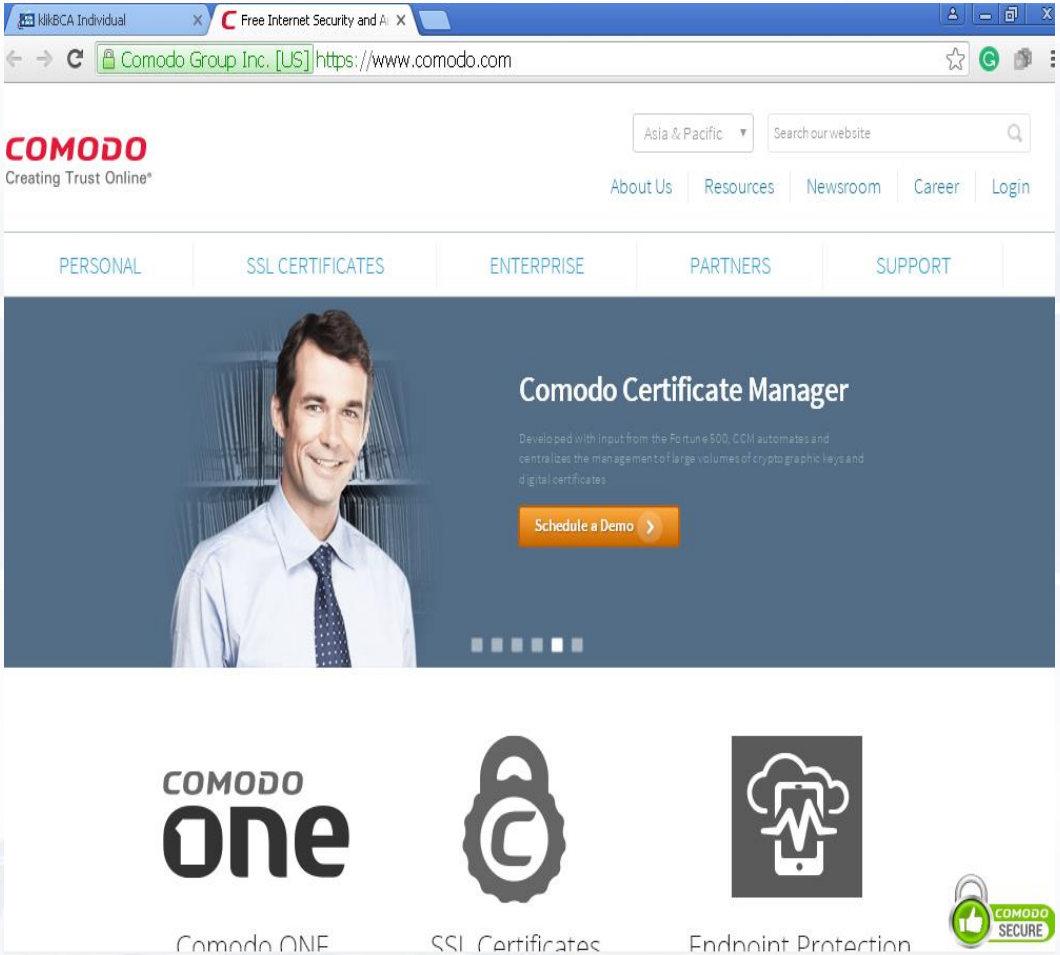
malware atau spyware.
cure/m-Secure Anda.
ngklik gambar di kanan-bawah ini.
finansial atau perubahan data.
a menemukan hal-hal yang

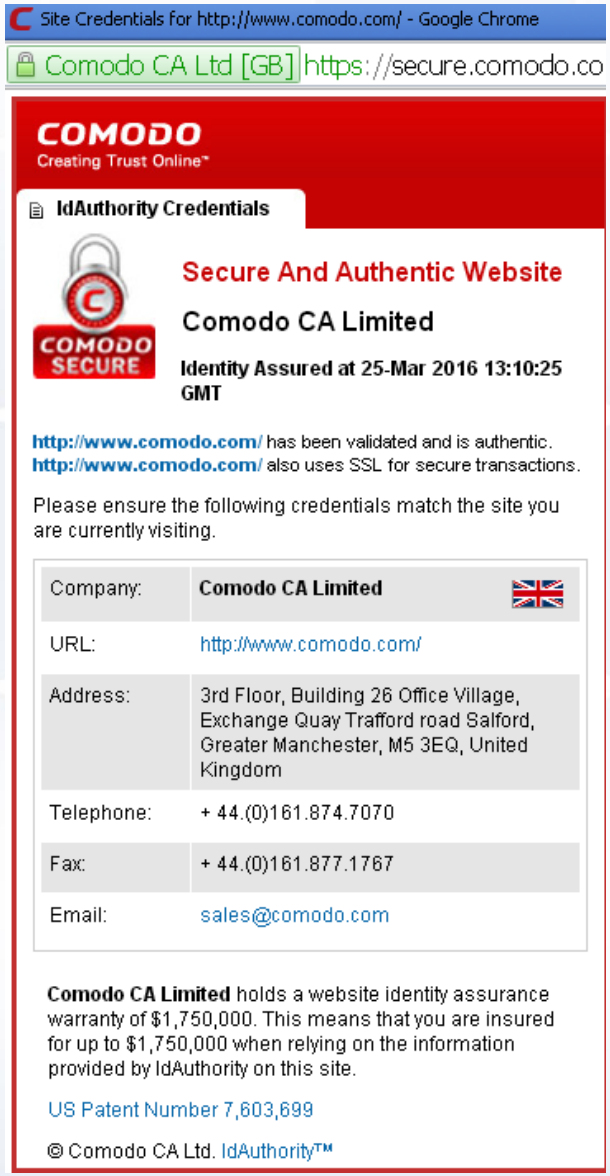
g saat meninggalkan komputer.

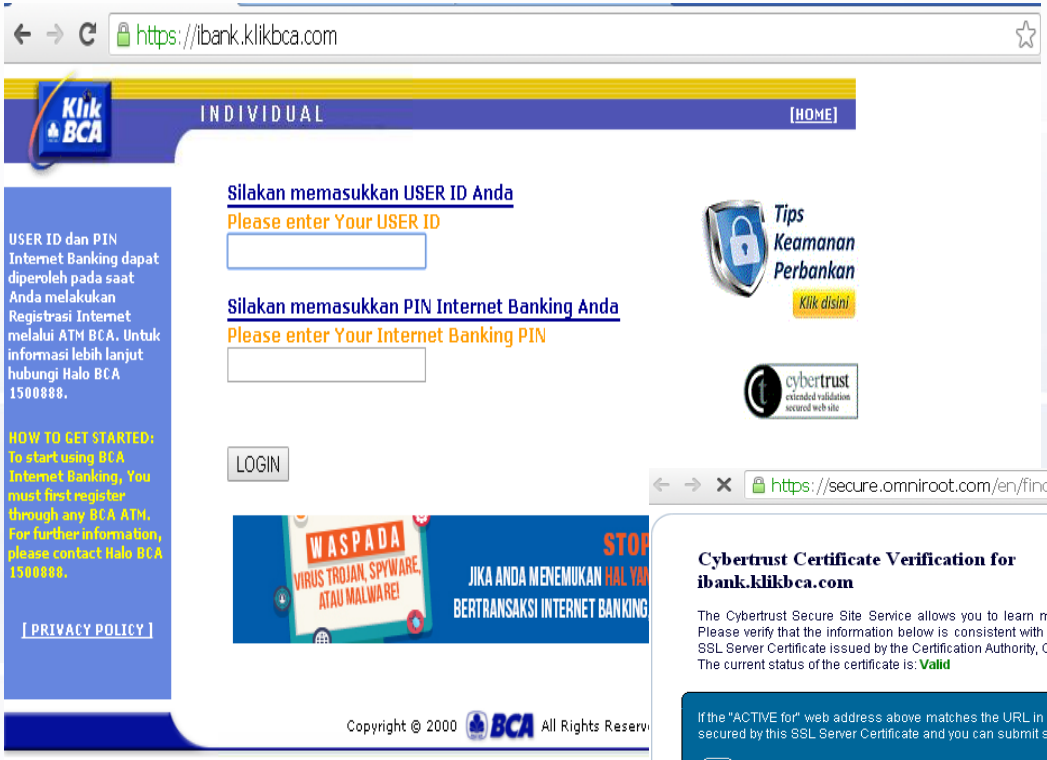



Google
BNI Internet Banking:Login k
PT. Bank Negara Indonesia (Persero) Tbk [ID]
https://ibank.bni.co.id/corp/AuthenticationController?__START
BNI INTERNET BANKING
Login
User ID :
Password:
Bahasa:
Pilihan Bahasa
Tampilan Halaman Utama
BERANDA
4566
Masukkan karakter di atas :
Login
Reset
Aktivasi:
Silakan klik disini untuk aktivasi pendaftaran BNI Internet Banking.
atau
Silakan klik disini untuk pendaftaran apabila belum pernah mendaftar melalui BNI ATM.
WASPADA
VIRUS TROJAN, SPYWARE ATAU MALWARE DI PC/LAPTOP ANDA
HATI - HATI
Hentikan transaksi apabila terdapat permintaan "sinkronisasi token"
LIHAT INFORMASI DI TIPS KEAMANAN PERBANKAN
Tips Aman Transaksi Perbankan
Lupa User ID?
Lupa Password?
FAQ
Demo
Syarat & Ketentuan?
1500046 BNI Call
@BNI46
BNI
Tips Keamanan Menggunakan BNI Internet Banking:
1. Pastikan perangkat komputer yang Anda gunakan bersih dari virus, malware atau spyware.
2. Jaga kerahasiaan Password BNI Internet Banking dan PIN BNIe-Secure/m-Secure Anda.
3. Pastikan keaslian situs ibank.bni.co.id yang Anda akses dengan mengklik gambar di kanan-bawah ini.
Untuk informasi lebih lanjut dan solusi perbankan lainnya, silakan kunjungi

Token


klikBCA Individual
Free Internet Security and A
Comodo Group Inc. [US] https://www.comodo.com
COMODO
Creating Trust Online®
Asia & Pacific
Search our website
About Us
Resources
Newsroom
Career
Login
PERSONAL
SSL CERTIFICATES
ENTERPRISE
PARTNERS
SUPPORT
Comodo Certificate Manager
Developed with input from the Fortune 500, CCM automates and centralizes the management of large volumes of cryptographic keys and digital certificates
Schedule a Demo
COMODO
one
Comodo ONE
SSL Certificates
Endpoint Protection
COMODO
SECURE


Site Credentials for http://www.comodo.com/ - Google Chrome
Comodo CA Ltd [GB] https://secure.comodo.co
COMODO
Creating Trust Online®
IdAuthority Credentials
COMODO
SECURE
Secure And Authentic Website
Comodo CA Limited
Identity Assured at 25-Mar 2016 13:10:25 GMT
http://www.comodo.com/ has been validated and is authentic.
http://www.comodo.com/ also uses SSL for secure transactions.
Please ensure the following credentials match the site you are currently visiting.
Company: Comodo CA Limited
URL: http://www.comodo.com/
Address: 3rd Floor, Building 26 Office Village, Exchange Quay Trafford road Salford, Greater Manchester, M5 3EQ, United Kingdom
Telephone: + 44.(0)161.874.7070
Fax: + 44.(0)161.877.1767
Email: sales@comodo.com
Comodo CA Limited holds a website identity assurance warranty of $1,750,000. This means that you are insured for up to $1,750,000 when relying on the information provided by IdAuthority on this site.
US Patent Number 7,603,699
© Comodo CA Ltd. IdAuthority™


https://ibank.klikbca.com
INDIVIDUAL
[HOME]
Silakan memasukkan USER ID Anda
Please enter Your USER ID
Silakan memasukkan PIN Internet Banking Anda
Please enter Your Internet Banking PIN
LOGIN
USER ID dan PIN Internet Banking dapat diperoleh pada saat Anda melakukan Registrasi Internet melalui ATM BCA. Untuk informasi lebih lanjut hubungi Halo BCA 1500888.
HOW TO GET STARTED: To start using BCA Internet Banking, You must first register through any BCA ATM. For further information, please contact Halo BCA 1500888.
[PRIVACY POLICY]
Tips Keamanan Perbankan
Klik disini
cybertrust
extended validation secured web site
WASPADA
VIRUS TROJAN, SPYWARE, ATAU MALWARE!
STOP
JIKA ANDA MENEMUKAN HAL YA
BERTRANSAKSI INTERNET BANKING
Copyright © 2000 BCA All Rights Reserv


https://secure.omniroot.com/en/find/sealct.cfm?cn=ibank.klikbca.com
Cybertrust Certificate Verification for ibank.klikbca.com
cybertrust secured website
The Cybertrust Secure Site Service allows you to learn more about the web sites you visit before submitting sensitive data. Please verify that the information below is consistent with the web site you are visiting. The web site referenced below uses a SSL Server Certificate issued by the Certification Authority, Cybertrust.
The current status of the certificate is: Valid
If the "ACTIVE for" web address above matches the URL in the browser window of the site which you are verifying, then it is being secured by this SSL Server Certificate and you can submit sensitive data such as credit card details with the assurance that:
AN IDENTITY BACKGROUND CHECK HAS TAKEN PLACE
ALL TRANSACTIONS ARE SECURE, PRIVATE AND TAMPER-PROOF
The Registration Authority has verified the organization's name.
This site is legitimately owned by PT. Bank Central Asia Tbk.
For addresses beginning with HTTPS all information sent to this site, is encrypted and protected against disclosure to third parties. This also guarantees the integrity of the data being sent over the Net.
CERTIFICATION DETAILS
Company/Organization Name: PT. Bank Central Asia Tbk.
Website Address: ibank.klikbca.com
Status: Valid
Expiration Date: Dec-26-2016 13:27 GMT
Security Statement
The SSL Server Certificate enables the secure transmission of information between you and this web site and provides an electronic credential for this web site's identity. Before relying upon a SSL Server Certificate, it is important that you understand the practices employed by the Certification Authority Cybertrust in issuing this web site's certificate. You can find these practices in the Cybertrust Certification Practice Statement.
To learn more about SSL Server Certificates and online security visit http://www.cybertrust.com.

Table 11.1 Modern cryptographic security services

Security Services	Cryptographic Mechanism to Achieve the Service
Confidentiality	Symmetric encryption
Authentication	Digital signatures and digital certificates
Integrity	Decryption of digital signature with a public key to obtain the message digest. The message is hashed to create a second digest. If the digests are identical, the message is authentic and the signer's identity is proven.
Nonrepudiation	Digital signatures of a hashed message then encrypting the result with the private key of the sender, thus binding the digital signature to the message being sent.
Nonreplay	Encryption, hashing, and digital signature

Serangan Cryptanalysis

- Replay Attack
  - Mengulangi nilai yang sudah diketahui sebelumnya.
- Social Engineering
  - Manusia adalah “link” terlemah
- Temporary Files
  - Mungin saja terdapat plaintext file

Table 2.1 Types of Attacks on Encrypted Messages

Type of Attack	Known to Cryptanalyst
Ciphertext only	• Encryption algorithm • Ciphertext to be decoded
Known plaintext	• Encryption algorithm • Ciphertext to be decoded • One or more plaintext–ciphertext pairs formed with the secret key
Chosen plaintext	• Encryption algorithm • Ciphertext to be decoded • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen ciphertext	• Encryption algorithm • Ciphertext to be decoded • Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen text	• Encryption algorithm • Ciphertext to be decoded • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Secure Encryption

- An encryption scheme is **computationally secure if the ciphertext generated** by the scheme meets one or both of the following criteria:
  - The cost of breaking the cipher exceeds the value of the encrypted information.
  - The time required to break the cipher exceeds the useful lifetime of the information.

At the end

The mantra of any good security engineer is: **'Security is a not a product, but a process.'** It's more than designing strong cryptography into a system; it's designing the entire system such that all security measures, including cryptography, work together.

by Bruce Schneier

End