Bagian 4
Kriptografi

Sub Capaian Pembelajaran Mata Kuliah

SubCPMK 08.02.01 Mampu merancang dan mengimplementasikan solusi keamanan informasi yang mencakup teknik enkripsi, mekanisme pengendalian akses, serta strategi pengelolaan ancaman siber

Referensi

- Whitman, M. E., & Mattord, H. J. (2022). Principles of information security (Seventh edition). Cengage.
- Mitnick, K. D., & Vamosi, R. (2019). The art of invisibility: The world's most famous hacker teaches you how to be safe in the age of Big Brother and big data. Little, Brown and Company
- Danturthi, R. S. (2024). Database and application security: A practitioner's guide ([First edition]). Addison-Wesley Professional.
- ISO 27001:2013
- ISO 27002:2013
- Munir, R. (2019). Kriptografi (Edisi Kedua). Bandung-Indonesia: Penerbit Informatika


1
AVAILABILITY
INFORMATION SECURITY
2
INTEGRITY
3
CONFIDENTIALITY

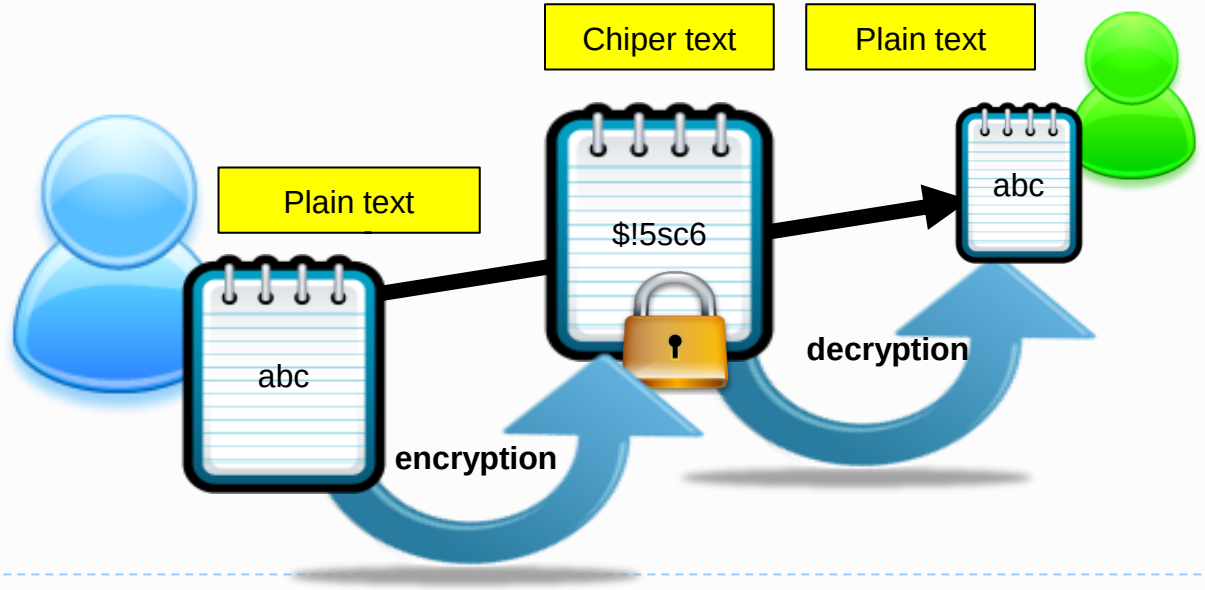
Kriptografi??

Sumber: https://jabar.tribunnews.com/

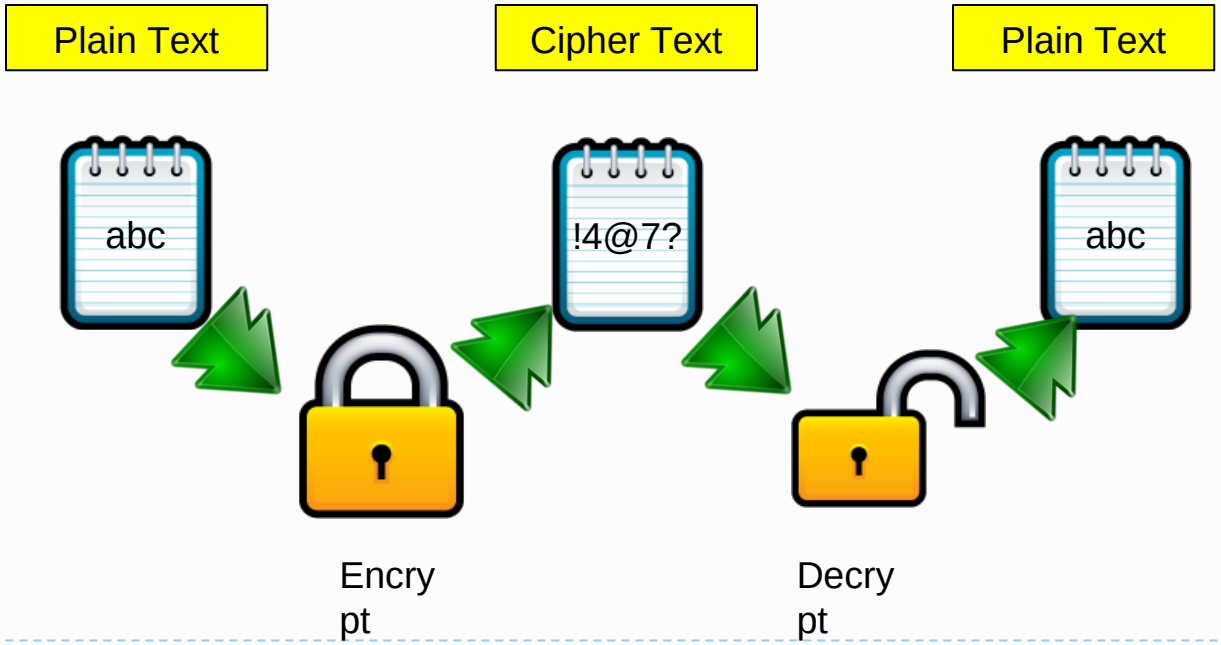
Definisi

- Kata cryptography berasal dari bahasa Yunani: cryptos (rahasia) dan graphia (tulisan).
- Artinya "tulisan rahasia".
- Kriptografi merupakan ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya kedalam bentuk yang tidak dapat dimengerti lagi maknanya.

Kriptografi?



Enkripsi dan Dekripsi



TERMINOLOGI

- Plaintext adalah pesan yang hendak dikirim (berita data asli).
- Ciphertext adalah pesan terenkripsi (tersandi) yang merupakan hasil enkripsi.
- Algoritma adalah aturan untuk enkripsi dan dekripsi, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi
- Kunci adalah parameter yang digunakan untuk transformasi enkripsi dan dekripsi.
- Kunci bersifat rahasia (secret), sedangkan algoritma kriptografi tidak rahasia (publik).

TUJUAN KRIPTOGRAFI

Confidentiality

Authentication

Integrity

Non Repudiation

KONSEP KRIPTOGRAFI

Keacakan (Randomness)

- Keacakan dalam kriptografi mengacu pada penggunaan nilai atau data yang tidak dapat diprediksi.
- Keacakan sangat penting untuk memastikan bahwa hasil enkripsi tidak dapat ditebak oleh penyerang.
- **Tujuan:** Menghindari pola yang dapat dieksploitasi oleh penyerang.

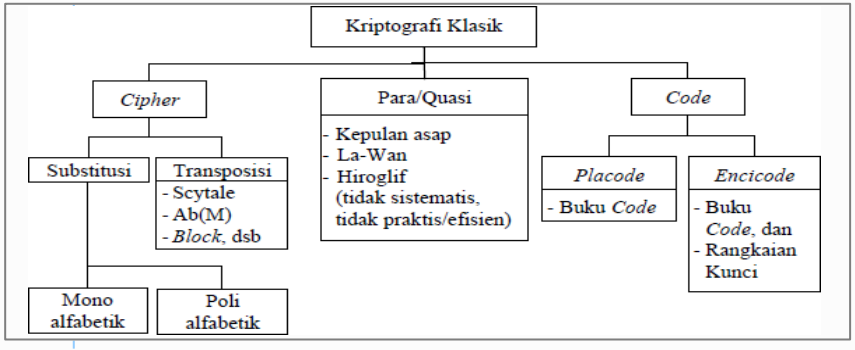
Difusi (Diffusion)

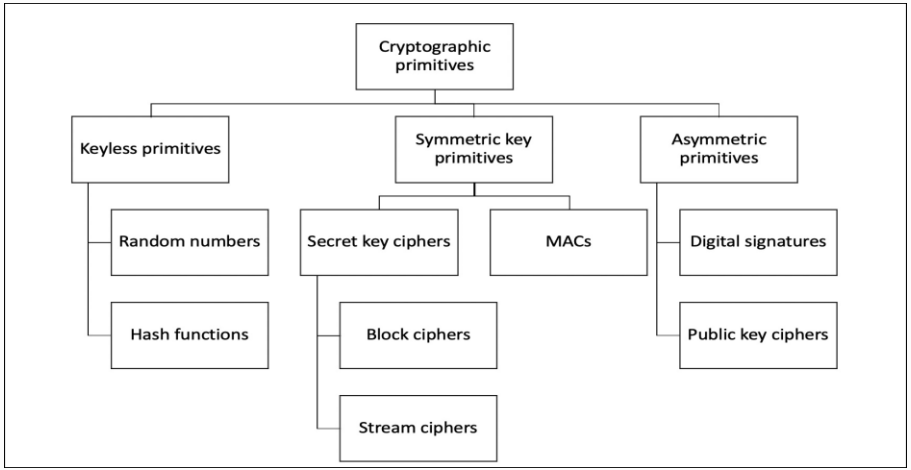
- Difusi adalah konsep di mana perubahan kecil pada teks asli (*plaintext*) menyebabkan perubahan besar yang menyebar di seluruh *ciphertext*.
- **Tujuan:** Menyulitkan penyerang dalam menemukan hubungan langsung antara *plaintext* dan *ciphertext*. Dengan adanya difusi, mengubah satu bit pada *plaintext* akan mengubah banyak bit pada *ciphertext*, sehingga pola di *plaintext* tidak mudah dikenali.

Konfusi (Cofusion)

- Konfusi adalah konsep yang bertujuan untuk membuat hubungan antara kunci kriptografi dan *ciphertext* menjadi sekompleks mungkin.
- **Tujuan:** Mengaburkan keterkaitan langsung antara plaintext, ciphertext, dan kunci kriptografi. Hal ini membuat analisis kriptografi, seperti analisis diferensial atau serangan kunci, menjadi lebih sulit dilakukan oleh penyerang.

Kriptografi Klasik v Kriptografi Modern



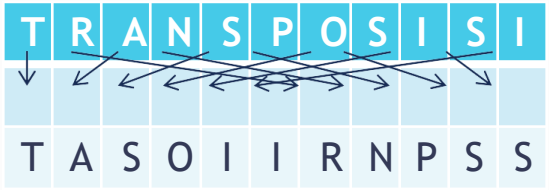


Kriptografi Klasik

Kriptografi Klasik

- Caesar Cipher
- Shift Cipher
- Vignere Cipher
- Hill Cipher
- Polyalphabetics Cipher
- Autokey Cipher
- dll..

TEKNIK DASAR KRIPTOGRAFI

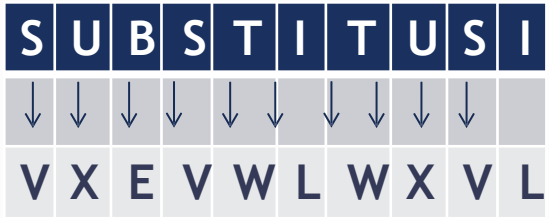


Transposisi

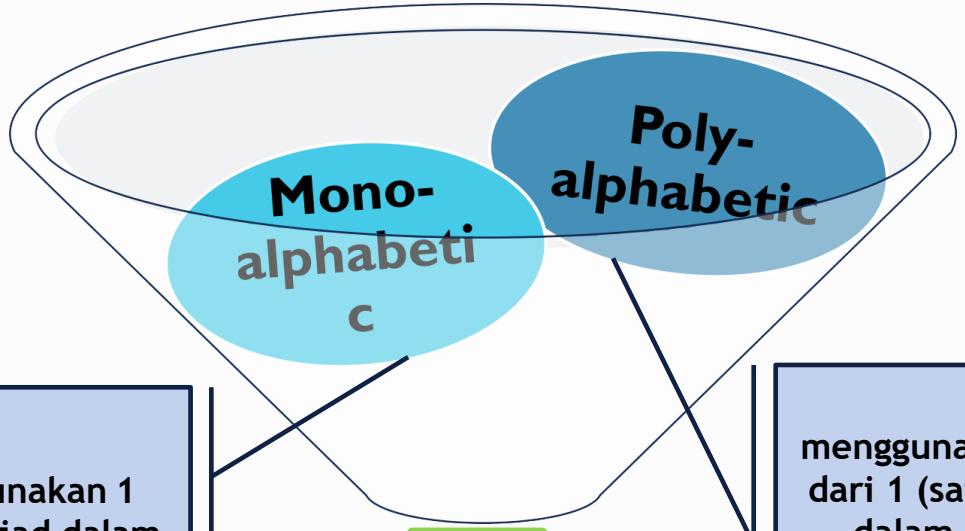
(Merubah posisi huruf terang)

Subtitusi

(Mengganti huruf terang dengan huruf lain / angka / kode, tanpa merubah posisinya)



SUBSTITUSI ALFABETIS



menggunakan 1 (satu) abjad dalam proses penyandian.

1 huruf terang = 1 Huruf sandi

menggunakan lebih dari 1 (satu) abjad dalam proses penyandian.

1 huruf terang = >1 Huruf sandi

MONOALPHABETIC SUBSTITUTION

- CAESAR (QEL)
- 4PHS (FOUR PART HOMOPHONIC SUBSTITUTION)
- MACD (MEXICAN ARMY CIPHER DISK)
- BILLINEAR SUBSTITUTION (BIL-I)
- BILLINEAR HOMOPHONIC SUBSTITUTION (BIL-II)

PERIODIC POLYALPHABETIC SUBSTITUTION

- VIGENERE
- BEAUFORT (UPPER BEAUFORT AND LOWER BEAUFORT)

POLYALPHABETIC SUBSTITUTION

- **RUNNING KEY**
- **ONE TIME PAD / ONE TIME KEY**

Caesar Cipher

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

- Enkripsi
  - C = E (P) = (P + K) mod (26)
  - C = E (P) = (P + 3) mod (26)

Deskripsi

- P = D (C) = (C - K) mod 26
- P = D (C) = (C – 3) mod 26

VIGENÈRE CIPHER

- Ditemukan oleh Blaise de Vigenère, seorang diplomat Prancis pada tahun 1568.
- A method of encrypting alphabetic text by using a series of different mono-alphabet ciphers selected based on the letters of a keyword.

VignerCipher

VIGENERE TABEL

PLAIN TEXT

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

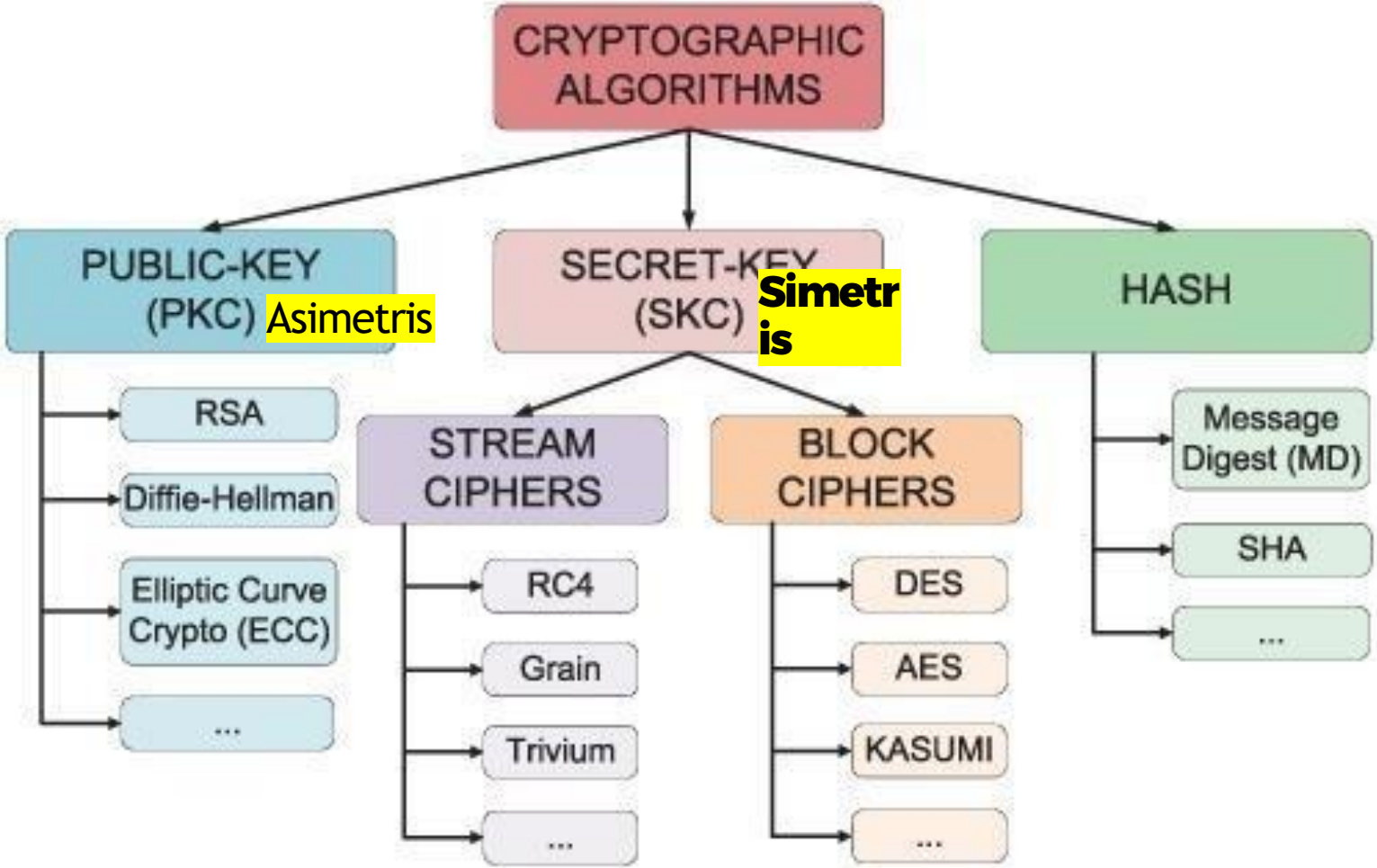
Vignere Cipher

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Pilih huruf kunci. Misal HURT,
- Misal, enkripsikan YOUARE

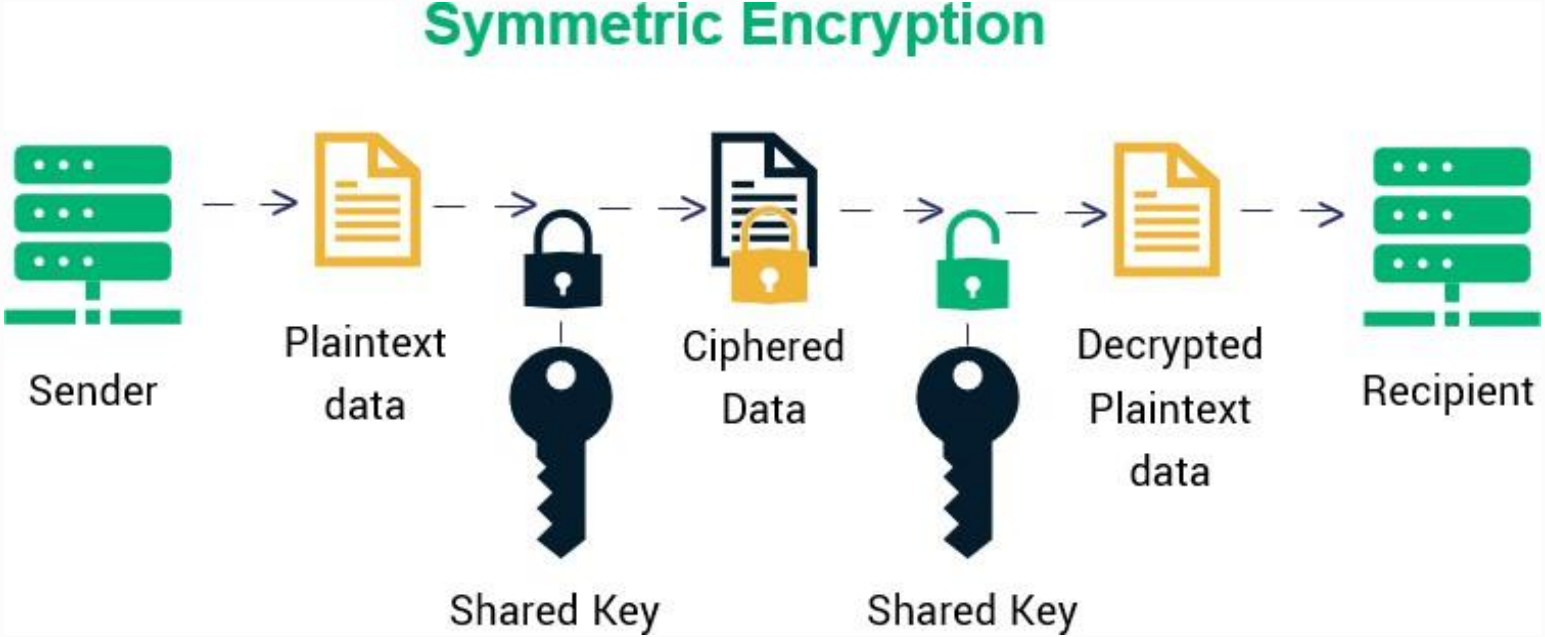
Y	O	U	A	R	E
h	u	r	t	h	u

Maka, hasil enkripsinya?


CRYPTOGRAPHIC ALGORITHMS
PUBLIC-KEY (PKC)
Asimetris
SECRET-KEY (SKC)
Simetris
HASH
RSA
Diffie-Hellman
Elliptic Curve Crypto (ECC)
...
STREAM CIPHERS
RC4
Grain
Trivium
...
BLOCK CIPHERS
DES
AES
KASUMI
...
Message Digest (MD)
SHA
...

Metode Simetris

Source : https://sectigostore.com/blog/types-of-encryption-what-to-know-about-symmetric-vs-asymmetric-encryption/



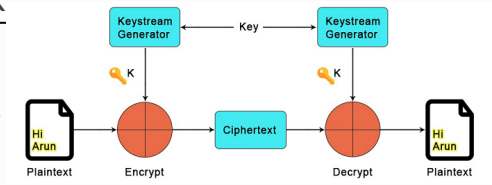
KUNCI ENKRIPSI = KUNCI DEKRIPSI

Block Cipher Vs. Stream Cipher

There are two types of symmetric algorithms:

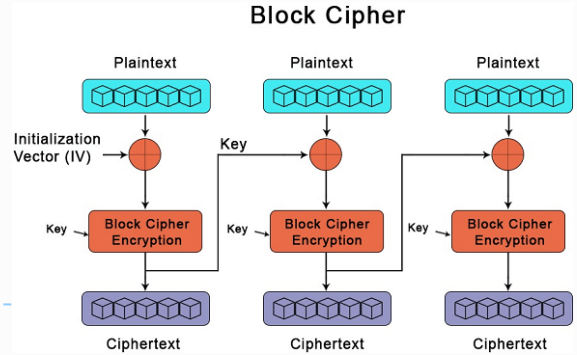
BLOCK CIPHER

- Encrypts the data in blocks. 64-bit blocks are quite common, although some algorithms (like AES) use larger blocks.
- For example, AES uses a 128-bit block



STREAM CIPHER

- encrypt the data as a stream, one bit at a time.



CIRI-CIRI ENKRIPSI SIMETRIS

Kunci yang Sama untuk Enkripsi dan Dekripsi

- Kunci enkripsi (kunci simetris) yang digunakan untuk mengenkripsi pesan juga digunakan untuk mendekripsi pesan tersebut.

Kecepatan

- Algoritma enkripsi simetris umumnya lebih cepat dibandingkan algoritma enkripsi asimetris. Ini membuatnya ideal untuk enkripsi data dalam jumlah besar.

Keamanan Kunci

- Keamanan enkripsi simetris sangat tergantung pada kerahasiaan kunci. Jika kunci diketahui oleh pihak ketiga, mereka dapat dengan mudah mendekripsi pesan yang dienkripsi dengan kunci tersebut.

ALGORITMA UMUM ENKRIPSI SIMETRIS

AES (Advanced Encryption Standard)

- **Deskripsi:** AES adalah standar enkripsi yang digunakan secara luas dan dianggap sangat aman.AES mendukung ukuran kunci 128-bit, 192-bit, dan 256-bit.
- Penggunaan: Digunakan dalam banyak aplikasi dan protokol, termasuk HTTPS,VPN, dan enkripsi file.

DES (Data Encryption Standard)

- **Deskripsi:** DES adalah algoritma enkripsi yang lebih tua dengan ukuran kunci 56-bit. DES dianggap tidak aman untuk kebanyakan aplikasi modern karena panjang kunci yang terlalu pendek.
- **Penggunaan:** Pernah digunakan secara luas tetapi sekarang telah digantikan oleh algoritma yang lebih aman seperti AES.

3DES (Triple DES)

- **Deskripsi:** 3DES memperpanjang keamanan DES dengan menerapkan algoritma DES tiga kali berturut-turut menggunakan dua atau tiga kunci yang berbeda.
- **Penggunaan:** Masih digunakan dalam beberapa aplikasi yang memerlukan kompatibilitas dengan DES tetapi secara bertahap digantikan oleh AES.

Blowfish

- **Deskripsi:** Blowfish adalah algoritma enkripsi simetris yang dirancang untuk memberikan keamanan tinggi dan efisiensi dengan panjang kunci yang dapat bervariasi hingga 448 bit.
- **Penggunaan:** Digunakan dalam berbagai aplikasi, termasuk enkripsi file dan sistem operasi tertentu.

RC4

- **Deskripsi:** RC4 adalah algoritma stream cipher yang sangat cepat tetapi telah ditemukan memiliki kelemahan keamanan.
- **Penggunaan:** Pernah digunakan dalam protokol seperti SSL dan WEP tetapi sekarang sudah jarang digunakan karena kelemahan keamanannya.

Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES)

- Perlu diusulkan standard algoritma baru sebagai modifikasi dari DES.
- National Institute of Standards and Technology (NIST) mengusulkan kepada Pemerintah Federal AS untuk sebuah standard kriptografi kriptografi yang baru.
- NIST mengadakan lomba membuat standard algoritma kriptografi yang baru. Standard tersebut kelak diberi nama Advanced Encryption Standard (AES).

singkat cerita...

- Pada bulan Oktober 2000, NIST mengumumkan untuk memilih Rijndael (dibaca: Rhine-doll)
- Pada bulan November 2001, Rijndael ditetapkan sebagai AES
- Diharapkan Rijndael menjadi standard kriptografi yang dominan paling sedikit selama 10 tahun.

Algoritma Rijndael

- Tidak seperti DES yang berorientasi bit, Rijndael beroperasi dalam orientasi byte.
- Setiap putaran mengunakan kunci internal yang berbeda (disebut round key).
- Enkripsi melibatkan operasi substitusi dan permutasi.

KELEBIHAN DAN KEKURANGAN

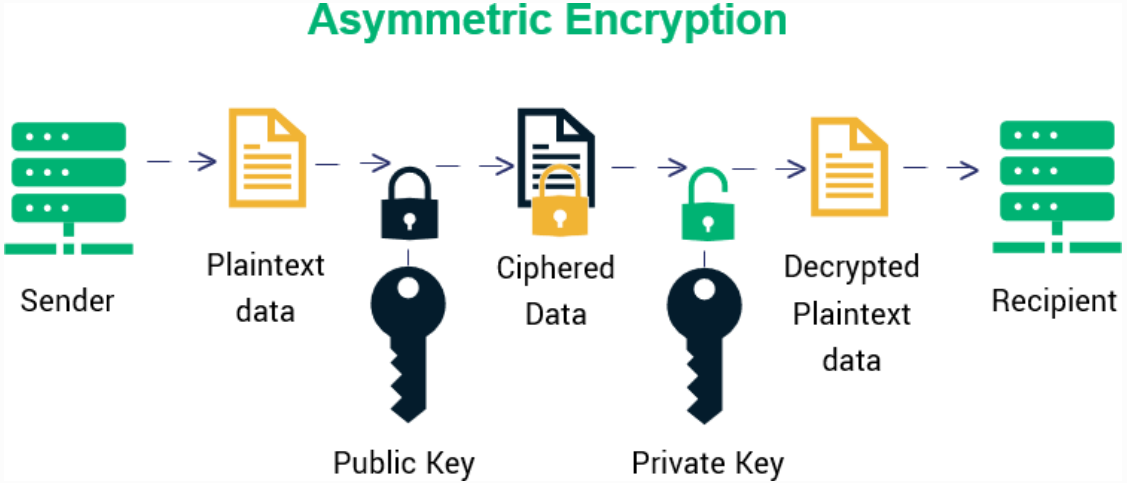
Kelebihan

- **Kecepatan:** Lebih cepat daripada enkripsi asimetris, cocok untuk enkripsi data dalam jumlah besar.
- **Efisiensi:** Memerlukan lebih sedikit sumber daya komputasi dibandingkan dengan enkripsi asimetris.

Kekurangan

- **Distribusi Kunci:** Mengamankan dan mendistribusikan kunci enkripsi kepada semua pihak yang berkomunikasi bisa menjadi tantangan.
- **Skalabilitas:** Kurang skalabel dibandingkan dengan enkripsi asimetris karena setiap pasangan pengguna memerlukan kunci yang berbeda.

Source : https://sectigostore.com/blog/types-of-encryption-what-to-know-about-symmetric-vs-asymmetric-encryption/



KUNCI ENKRIPSI ≠ KUNCI DEKRIPSI

Proses

- Proses pengiriman dan penerimaan data melalui kriptografi asimetris ini biasanya terdiri dari lima langkah, yaitu:
  - Generasi kunci (Key generation) : setiap individu akan menghasilkan public key dan private key.
  - Pertukaran kunci (Key exchange) : pengirim dan penerima akan saling bertukar public key.
  - Enkripsi (Encryption) : data pengirim dienkripsi menggunakan public key penerima.
  - Mengirim data terenkripsi (Sending encrypted data) : data yang sudah terenkripsi kemudian dikirim ke penerima.
  - Dekripsi (Decryption) : penerima mendekripsi pesan menggunakan kunci pribadi mereka sendiri.

ALGORITMA UMUM ENKRIPSI ASIMETRIS

RSA (Rivest-Shamir-Adleman): Salah satu algoritma asimetris yang paling umum digunakan. RSA didasarkan pada kesulitan faktorisasi bilangan besar.

- Digunakan dalam banyak protokol keamanan, termasuk HTTPS/TLS dan untuk menandatangani sertifikat digital.

ECC (*Elliptic Curve Cryptography*): Algoritma yang lebih efisien daripada RSA dalam hal ukuran kunci dan kinerja, berdasarkan pada aljabar eliptik kurva.

- Digunakan dalam banyak aplikasi modern termasuk TLS/SSL, Bitcoin, dan perangkat *mobile* karena efisiensinya.

DSA (*Digital Signature Algorithm*): Digunakan terutama untuk tanda tangan digital dan tidak untuk enkripsi data.

- Digunakan dalam berbagai protokol untuk verifikasi identitas dan integritas data.

ElGamal: algoritma kriptografi asimetris yang dapat digunakan untuk enkripsi dan tanda tangan digital.Algoritma ini didasarkan pada masalah logaritma diskret dalam grup siklik, yang membuatnya aman terhadap serangan brute force.

- Fleksibel dan dapat digunakan untuk enkripsi asimetris dan tanda tangan digital.

DH (Diffie-Hellman): protokol pertukaran kunci yang memungkinkan dua pihak untuk secara aman berbagi kunci kriptografi melalui saluran komunikasi yang tidak aman. Ini adalah salah satu algoritma pertama yang memungkinkan pertukaran kunci secara aman di internet.

- Digunakan untuk pertukaran kunci secara aman dalam berbagai protokol seperti TLS/SSL.

KELEBIHAN DAN KEKURANGAN ASIMETRIS

KELEBIHAN

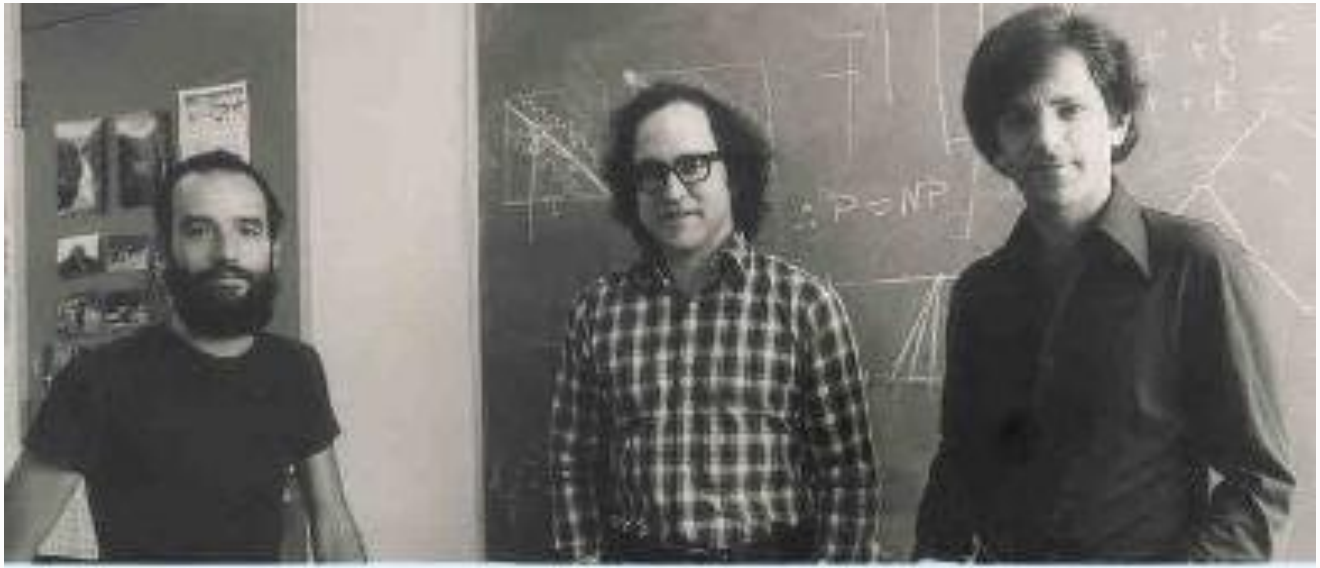
- **Keamanan:** Data yang dienkripsi dengan kunci publik hanya dapat didekripsi dengan kunci privat yang sesuai, sehingga meskipun kunci publik diketahui banyak orang, data tetap aman.
- **Distribusi Kunci yang Mudah:** Tidak perlu mengamankan distribusi kunci publik seperti halnya dengan kunci simetris. Ini mengurangi risiko kunci enkripsi jatuh ke tangan yang salah.
- **Otentikasi:** Penggunaan kunci privat untuk menandatangani data memungkinkan penerima untuk memverifikasi identitas pengirim menggunakan kunci publik mereka.

KEKURANGAN

- **Kecepatan:** Enkripsi asimetris umumnya lebih lambat dibandingkan enkripsi simetris karena kompleksitas matematis yang lebih tinggi.
- **Ukuran Kunci:** Kunci asimetris biasanya lebih panjang daripada kunci simetris untuk mencapai tingkat keamanan yang sama, yang bisa mempengaruhi kinerja.

RSA

- Algoritma kunci-publik yang paling terkenal dan paling banyak aplikasinya.
- Ditemukan oleh tiga peneliti dari MIT (Massachussets Institute of Technology), yaitu Ron Rivest, Adi Shamir, dan Len Adleman, pada tahun 1976.
- Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima.



Source:https://jayani-hewavitharana.medium.com/the-mathematical-beauty-behind-rsa-a7eb2b1e8562

Kekuatan dan Keamanan RSA

- Kekuatan algoritma RSA terletak pada tingkat kesulitan dalam memfaktorkan bilangan menjadi faktor-faktor prima, yang dalam hal ini $n = a \times b$.
- Sekali n berhasil difaktorkan menjadi a dan b, maka $\phi(n) = (a - 1) \times (b - 1)$ dapat dihitung. Selanjutnya, karena kunci enkripsi e diumumkan (tidak rahasia), maka kunci dekripsi d dapat dihitung dari persamaan $ed \equiv 1 \pmod{n}$.

Kelemahan RSA

- RSA lebih lambat daripada algoritma kriptografi kunci-simetri seperti DES dan AES
- Dalam praktek, RSA tidak digunakan untuk mengenkripsi pesan, tetapi mengenkripsi kunci simetri (kunci sesi) dengan kunci publik penerima pesan.
- Pesan dienkripsi dengan algoritma simetri seperti DES atau AES.
- Pesan dan kunci rahasia dikirim bersamaan.
- Penerima mendekripsi kunci simetri dengan kunci privatnya, lalu mendekripsi pesan dengan kunci simetri tersebut.

Proses RSA


Pembangkitan KUNCI Public & Privat
Enkripsi
Menggunakan Kunci Publik
Dekripsi
Menggunakan Kunci Privat

Pembangkitan Sepasang Kunci

- Pilih dua bilangan prima, p dan q (rahasia)
- Hitung n = pq.
- Hitung $\phi(n) = (p - 1)(q - 1)$.
- Pilih sebuah bilangan bulat e untuk kunci publik, sebut, e relatif prima terhadap $\phi(n)$.
- Hitung kunci dekripsi, d, dengan persamaaan
- $ed \equiv 1 \pmod{\phi(n)}$ atau $d \equiv e^{-1} \bmod (\phi(n))$

- Hasil dari algoritma di atas:
- - Kunci publik adalah pasangan (e, n)
- - Kunci privat adalah pasangan (d, n)

Enkripsi

- Nyatakan pesan menjadi blok-blok plainteks: m1, m2, m3, ...
- (syarat: 0 < mi < n – 1)
- Hitung blok cipherteks ci untuk blok plainteks pi
- dengan persamaan
- ci = mie mod n
- yang dalam hal ini, e adalah kunci publik.

Deskripsi

Proses dekripsi dilakukan dengan menggunakan persamaan

$$mi = cid \bmod n,$$

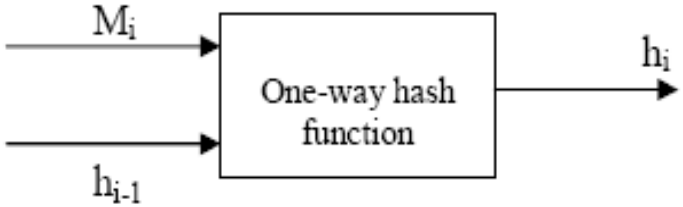
yang dalam hal ini, d adalah kunci privat.

Hash Function

Hash Function

- Hash value biasanya digambarkan sebagai suatu string pendek yang terdiri atas huruf dan angka yang terlihat random (data biner yang ditulis dalam notasi heksadesimal).

Fungsi hash satu arah (one-way hash function) adalah hash function yang bekerja satu arah, yaitu suatu hash function yang dengan mudah dapat menghitung hash value dari pre-image, tetapi sangat sukar untuk menghitung pre-image dari hash value



Secure Hash Algorithm (SHA)

- SHA adalah fungsi hash satu-arah yang dibuat oleh NIST dan digunakan bersama DSS (Digital Signature Standard).
- Oleh NSA, SHA dinyatakan sebagai standard fungsi hash satu-arah.
- SHA didasarkan pada MD4 yang dibuat oleh Ronald L. Rivest dari MIT.
- Algoritma SHA menerima masukan berupa pesan dengan ukuran maksimum 264 bit (2.147.483.648 gigabyte) dan menghasilkan message digest yang panjangnya 160 bit, lebih panjang dari message digest yang dihasilkan oleh MD5.

SHA

- SHA mengacu pada keluarga fungsi hash satu-arah.
- Enam varian SHA: SHA-0, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512.
- SHA-0 sering diacu sebagai SHA saja
- Yang akan dibahas: SHA-1

- Specified by the National Institute of Standards and Technology (NIST) and are used by NSA's Information Assurance Directorate in solutions approved for protecting classified and unclassified National Security Systems (NSS).

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher used for information protection	FIPS Pub 197	Use 256 bit keys to protect up to TOP SECRET
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	Asymmetric algorithm used for key establishment	NIST SP 800-56A	Use Curve P-384 to protect up to TOP SECRET.
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithm used for digital signatures	FIPS Pub 186-4	Use Curve P-384 to protect up to TOP SECRET.
Secure Hash Algorithm (SHA)	Algorithm used for computing a condensed representation of information	FIPS Pub 180-4	Use SHA-384 to protect up to TOP SECRET.
Diffie-Hellman (DH) Key Exchange	Asymmetric algorithm used for key establishment	IETF RFC 3526	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for key establishment	NIST SP 800-56B rev 1	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for digital signatures	FIPS PUB 186-4	Minimum 3072 bit-modulus to protect up to TOP SECRET.

STANDAR NASIONAL INDONESIA (SNI ISO/IEC)
19790:2015
TEKNOLOGI INFORMASI - TEKNIK KEAMANAN - PERSYARATAN KEAMANAN UNTUK MODUL KRIPTOGRAFI

ANNEX C
Approved Security Functions

This annex provides a list of the ISO/IEC approved standards that specify approved security functions applicable to this Standard.
The categories include ***block ciphers, stream ciphers, asymmetric key, message authentication codes, hash functions, entity authentication, key management*** *and* ***random bit generation****.*

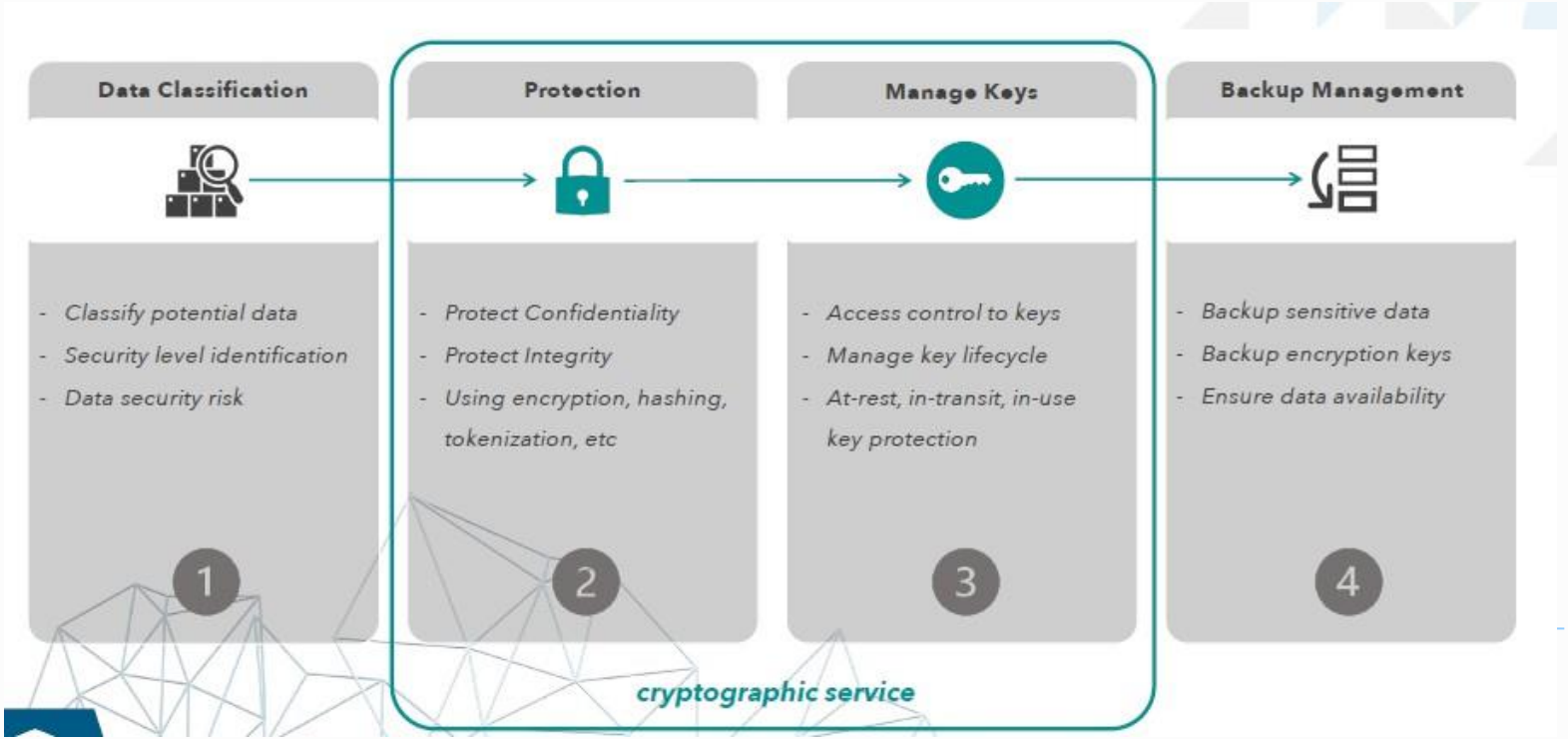
C.1.1 Block Ciphers	ISO/IEC 18033-3 (part 3)
C.1.2 Stream Ciphers	ISO/IEC 18033-4 (part 4)
C.1.3 Asymmetric Algorithm & Techniques	ISO/IEC 9796-2, ISO/IEC 9796-3, ISO/IEC 14888, ISO/IEC 15946, ISO/IEC 18033-2
C.1.4 Message Authentication Codes	ISO/IEC 9797-2 (part 2)
C.1.5 Hash Functions	ISO/IEC 10118-2, ISO/IEC 10118-3, ISO/IEC 10118-4
C.1.6 Entity Authentication	ISO/IEC 9798-2, ISO/IEC 9798-3, ISO/IEC 9798-4, ISO/IEC 9798-5, ISO/IEC 9798-6
C.1.7 Key Management	ISO/IEC 11770-2, ISO/IEC 11770-3, ISO/IEC 11770-4
C.1.8 Random Bit Generation	ISO/IEC 18031

KRIPTOGRAFI UNTUK KEAMANAN INFORMASI

DATA STATES

at rest	in transit	in use
- Passive State - not Currently Accessed, Updated, Or Processed	- Active State - Transmitted Between 2 or More Points - Preparation For Processing	- Active State - Autonomous System - Human Viewing, Updating, or Editing
- at Cloud - at Hard Drive - at Storage - at Database	- Submitting Form - Upload/Download File - Checking Balance - Tracking/Monitoring	- Data Transaction - Data Operation
- Security Access Policy - File Encryption - Full-disk Encryption - Information Rights Management - Data Leak Prevention	- TLS 1.2/1.3 - Security Protocols (https,sftp, etc) - Manage File Transfer	- Identity and Access Management (SSO, 2FA, MFA, etc) - Information Rights Management - Role Based Access Control

PROTECTION PHASE



Layanan *cryptography as a service* milik BSSN yang menyediakan solusi **keamanan data** melalui penerapan fungsi kriptografi yang aman dan terpercaya.

Sandi Data memberikan proteksi **kerahasiaan data** yang ada di dalam aplikasi atau sistem elektronik sebagai bentuk pelindungan terhadap *data breach yang* diwujudkan melalui penyediaan ***key management system*** dan ***cryptographic services***.

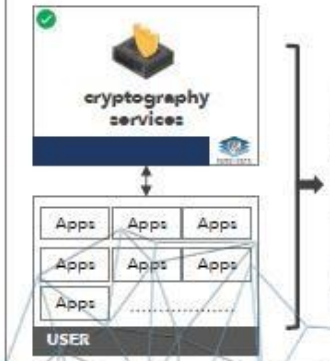
Key Management System	***Cryptographic Services***
Key Security (in use, in transit, at rest)	*Encrypt / Decrypt*
Control Encryption Keys	*Tokenize / Detokenize*
Full Key Management	*Random Number Generator*
Hierarchial Key Protection	*Re-Encrypt*
Backup Protection	*End-to-End Encryption*
Hardware-Based Protection	*Hash / HMAC*

SANDI DATA

Id	First name	Last name	Birth date
43	yoyok	darmanto	24 April 1996
44	yan	hadynoer	12 Februari 1994
45	sofyan	reza	6 Januari 1990
46	dony	irwansyah	1 Januari 2020

DATA TERBUKA

DATA TERLINDUNGI



id	st_nam	last_name	birth_date
Filter	Filter	Filter	Filter
44	yan	eyJ0ZXh0IjoieGs4bW5WY2Q2N0U9IiwibWFjIjoiUTZnc3J2aUJKZE1XTGp...	eyJ0ZXh0IjoiWjI4RUZoWTBoTU82M3VRb3dSYlBkUT09IiwibWFjIjoiV2VCNU0xd...
45	sofyan	eyJ0ZXh0IjoiVXNVTk9nPT0iLCJtYWMiOiJ5UXk5ZlNGXC92RW1aamF5R0...	eyJ0ZXh0IjoiZkMrOWNlQmJRYnB5QVAxRWU0QT0iLCJtYWMiOiJWS0lhWGFoUG...
46	dony	eyJ0ZXh0IjoiS1VhaXhXQzhCQW5xIiwibWFjIjoiaDlpdnpmRWZRK1wvYU...	eyJ0ZXh0IjoidGdvUW53Q1wvbmZmY3ZhYmJlSWc9IiwibWFjIjoicmRqZ0xyODBu...
43	yoyok	eyJ0ZXh0IjoibDF5WnU5YjRcL0pFPSIsIm1hYyI6InNNTGI5dHMyQk1MT3...	eyJ0ZXh0IjoienBReFwvXC9tK0lSeXM0U1l8UkE9PSIsIm1hYyI6IjBVUXU4V25lWE...

Digital Signature?

mathematical scheme for demonstrating the authenticity of a digital message or document.

DIGITAL SIGNATURE

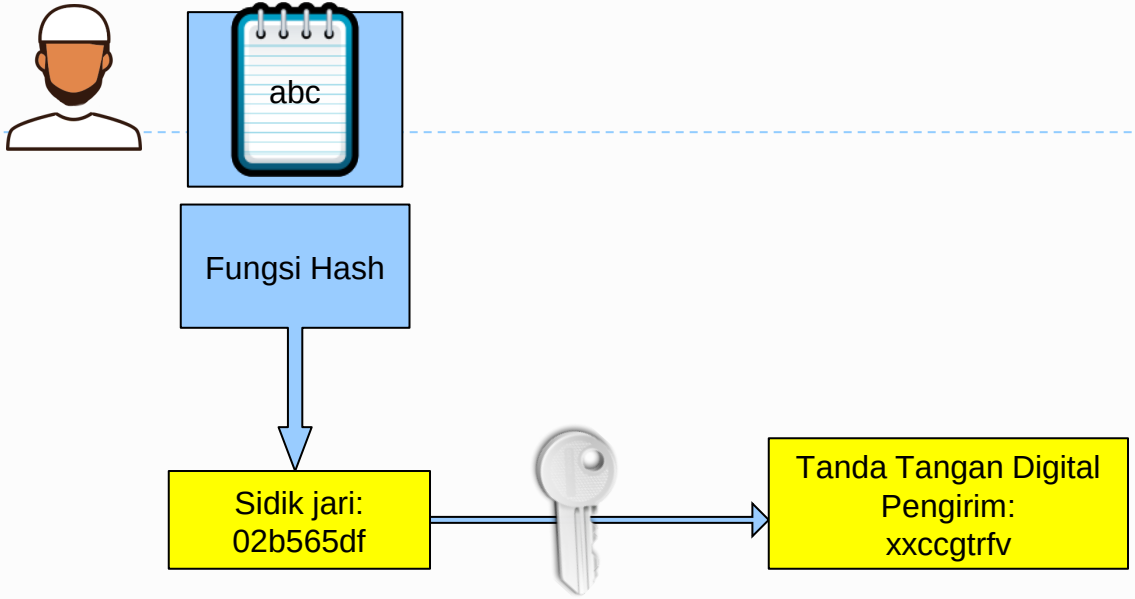
Sejak berabad-abad lamanya, tanda tangan digunakan untuk membuktikan otentikasi dokumen kertas (misalnya surat, piagam, ijazah, buku, karya seni, dan sebagainya)

Tanda-tangan mempunyai karakteristik sebagai berikut:

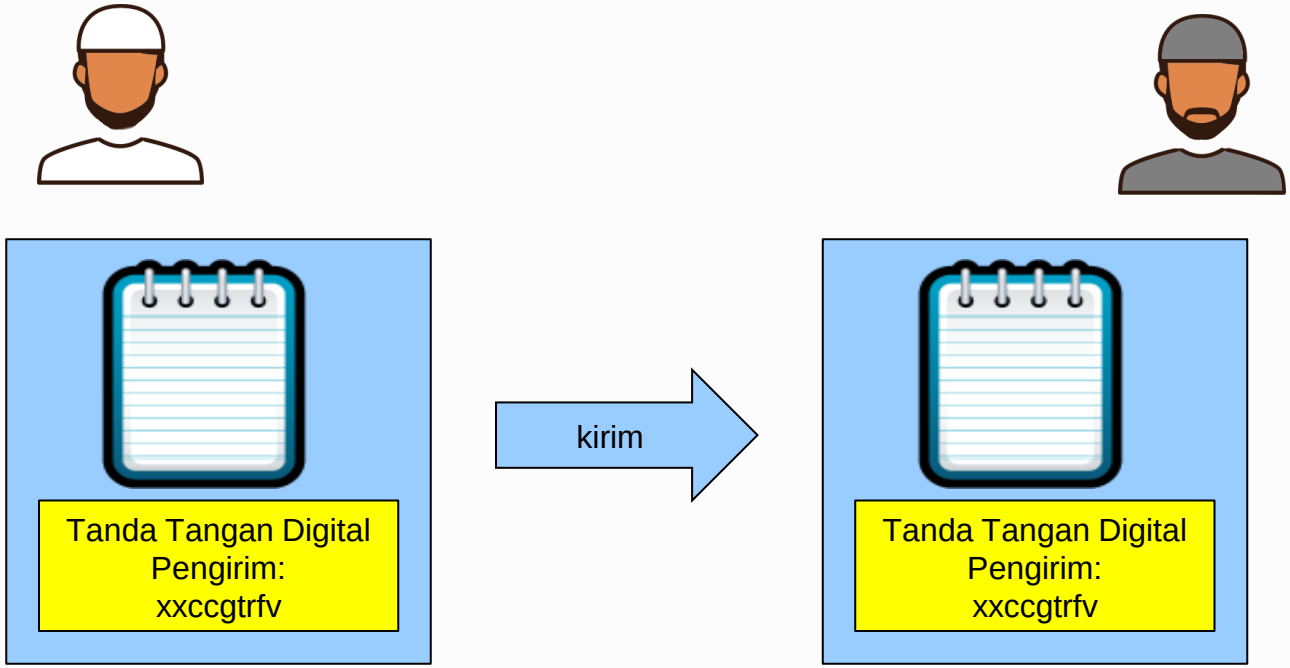
1. 1. Tanda-tangan adalah bukti yang otentik.
2. 2. Tanda tangan tidak dapat dilupakan.
3. 3. Tanda-tangan tidak dapat dipindah untuk digunakan ulang.
4. 4. Dokumen yang telah ditandatangani tidak dapat diubah.
5. 5. Tanda-tangan tidak dapat disangkal (repudiation).

DIGITAL SIGNATURE

- Tanda tangan digital adalah mekanisme kriptografi yang digunakan untuk memverifikasi keaslian dan integritas sebuah pesan, perangkat lunak, atau dokumen digital.
- Tanda tangan digital memberikan jaminan bahwa pesan tersebut benar-benar berasal dari pengirim yang diklaim dan tidak mengalami perubahan selama proses pengiriman.
- Tanda Tangan Elektronik adalah tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi (Pasal 1 (12) UU ITE).
- Berdasarkan Pasal 60 Ayat (2) PP 71/2019 Tanda Tangan Elektronik dibagi menjadi 2 yaitu :
  - Tanda Tangan Elektronik tersertifikasi, yaitu yang dibuat dengan menggunakan jasa penyelenggara sertifikasi elektronik, dan dibuktikan dengan Sertifikat Elektronik; dan
  - Tanda Tangan Elektronik tidak tersertifikasi, yang dibuat tanpa menggunakan jasa penyelenggara sertifikasi elektronik.
- List PSrE di Indonesia : https://tte.kominfo.go.id/listpsrenew.


abc
Fungsi Hash
Sidik jari:
02b565df
Tanda Tangan Digital
Pengirim:
xxccgtrfv

Proses Pengiriman



Proses Pengecekan

Tanda Tangan Digital
Pengirim:
xxccgtrfv

Dekripsi dengan kunci publik

Fungsi Hash

Sidik jari:
02b565df

Sama?

Sidik jari:
02b565df

Ya!
Data Utuh/Sama

Tidak!
Data Sudah Mengalami
Modifikasi

Permasalahan

- Proses transfer kunci publik bisa terjadi pemalsuan
- Misal (A) PbA → PbA(B)
- (A) PbA → PbA (H) PbH → PbH (B)

- Untuk Itulah Diperlukan pihak ketiga yang bisa dipercaya:
- Public Key Infrastructure

Public Key Infrastructure (PKI)

- Infrastruktur Kunci Publik (PKI) memungkinkan pengguna untuk bertransaksi dengan aman melalui penggunaan kriptografi kunci publik.
- Pasangan kunci diperoleh dari otoritas tepercaya pihak ketiga yang disebut Certificate Authority (CA)

Dari Permasalahan Sebelumnya

- Guna mengatasi masalah kemanan pendistribusian kunci publik
- Pada kunci publik direkatkan sertifikat digital
- Sertifikat digital selain berisi kunci publik juga berisi informasi mengenai jati diri pemilik kunci tersebut
- Sertifikat digital Ditanda tangani oleh lembaga yang mengeluarkannya (Certification Authorities)

Certificate Authorities

https://idcloudhost.com/ssl-certificate/

Harga SSL Certificates

IDCloudHost menyediakan layanan SSL Certificates Indonesia untuk mengamankan pertukaran informasi Website / Aplikasi Anda

Comodo PositiveSSL

Rp 100.000 / Tahun

- **Domain** Validation
- **2048 bit**
- **Securing** Domain / Subdomain
- **Compatible** All Servers

Beli Sekarang

Comodo PositiveSSL Multi-Domain

Rp 280.000 / Tahun

- **Domain** Validation
- **2048 bit**
- **Securing** Domain / Subdomain
- **Compatible** All Servers

Beli Sekarang

Comodo Wild Card

Rp 900.000 / Tahun

- **Domain** Validation
- **2048 bit**
- **Securing** Domain / Subdomain
- **Compatible** All Servers

Beli Sekarang

https://www.rumahweb.com/ssl-murah/

SSL STARTER

Rp 8.250/Bulan

☐ Wildcard (*.domain)

Mengamankan website personal, website kecil, dan UKM.

★☆☆☆☆

Pesan Sekarang

SSL BISNIS

Rp 40.833/Bulan

☐ Wildcard (*.domain)

Mengamankan dan menambah kepercayaan website bisnis/perusahaan.

★★★★☆

Pesan Sekarang

SSL ENTERPRISE

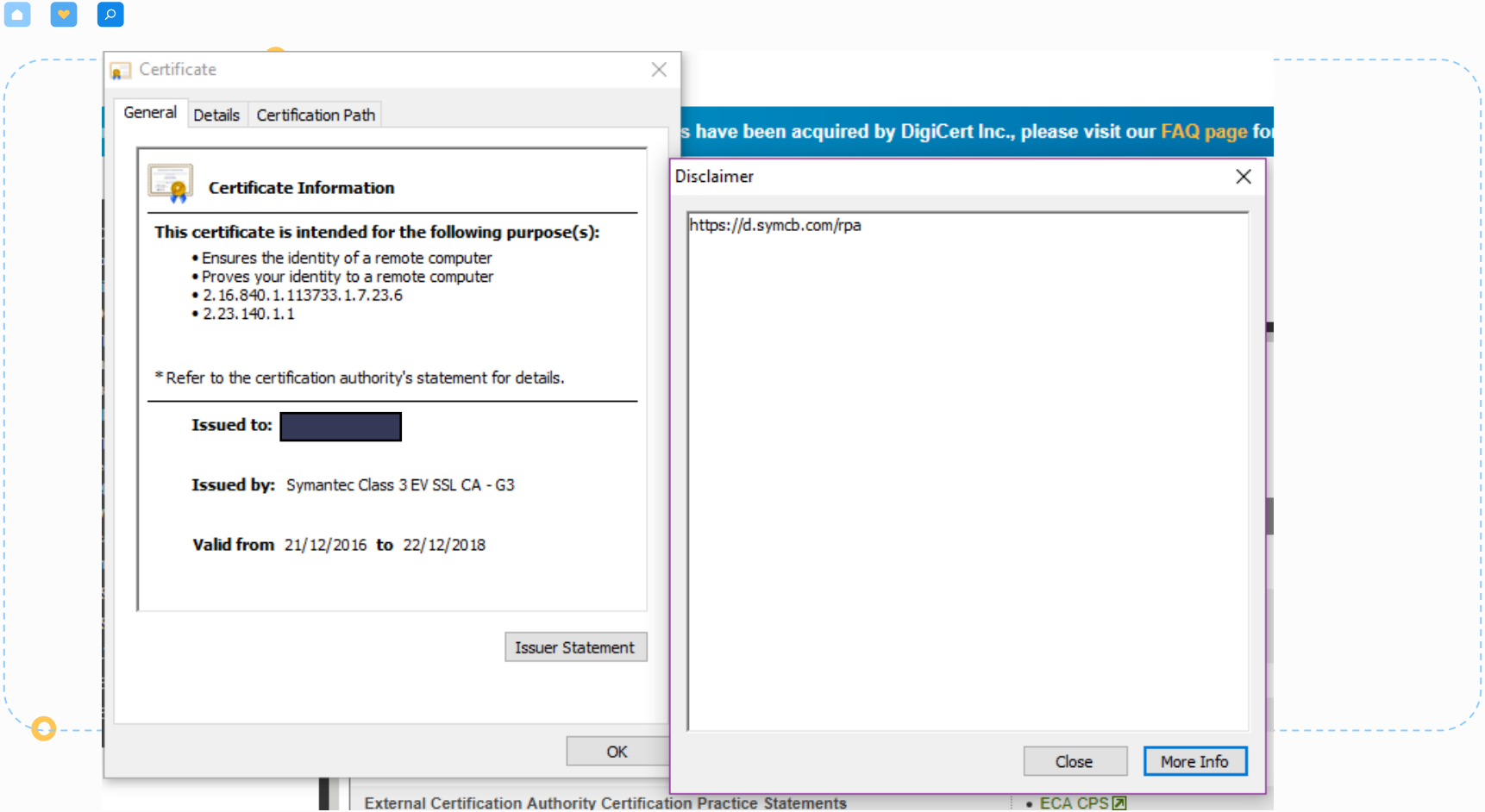
166.583/Bulan

☐ ~~Wildcard (*.domain)~~

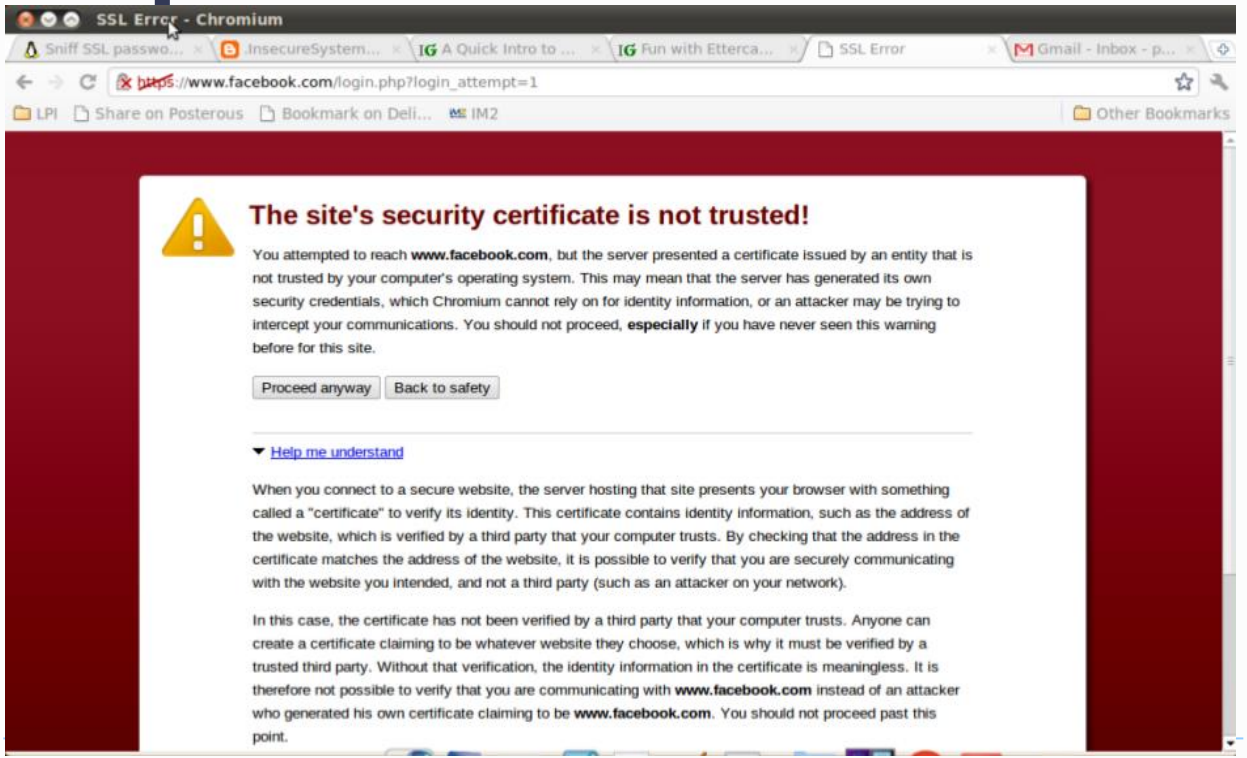
Mengamankan dan menambah kepercayaan website enterprise dengan Green Bar.

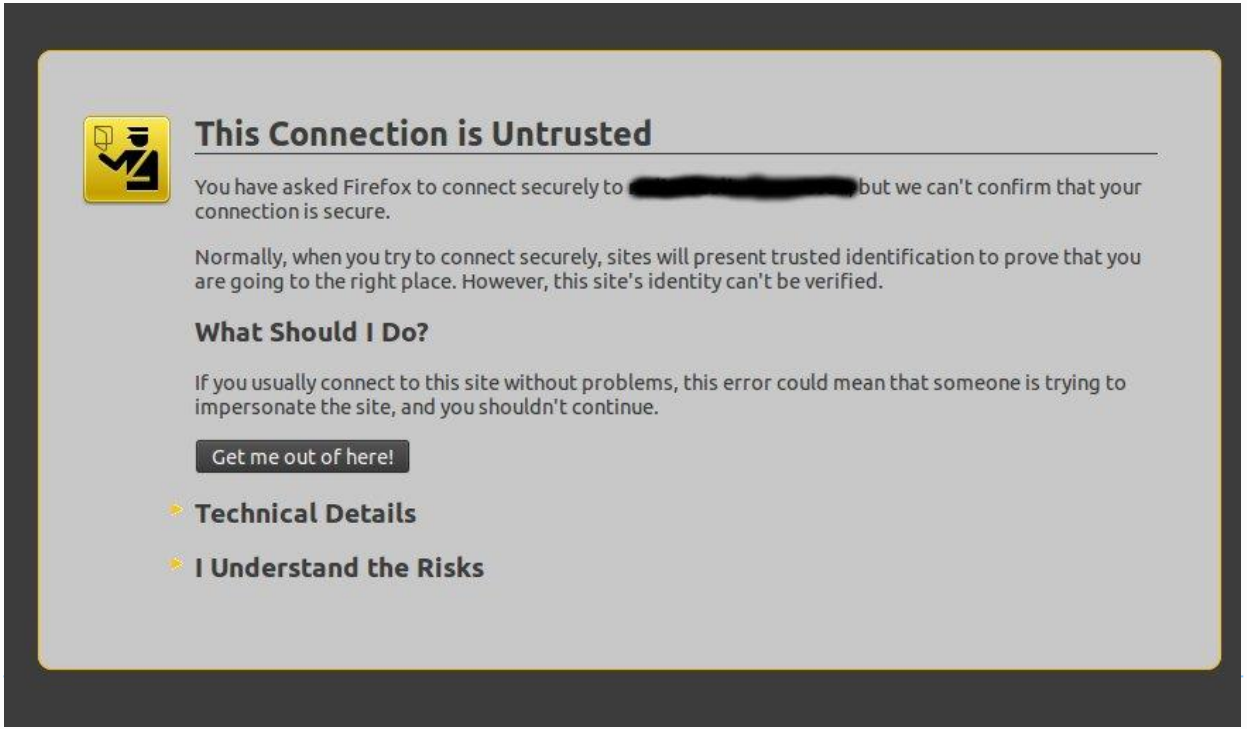
★★★★★

Pesan Sekarang


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
• Proves your identity to a remote computer
• 2.16.840.1.113733.1.7.23.6
• 2.23.140.1.1
* Refer to the certification authority's statement for details.
Issued to:
Issued by: Symantec Class 3 EV SSL CA - G3
Valid from 21/12/2016 to 22/12/2018
Issuer Statement
OK
s have been acquired by DigiCert Inc., please visit our FAQ page fo
Disclaimer
https://d.symcb.com/rpa
Close
More Info
External Certification Authority Certification Practice Statements
• ECA CPS

Https Tanpa Sertifikasi




This Connection is Untrusted
You have asked Firefox to connect securely to [redacted] but we can't confirm that your connection is secure.
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.
What Should I Do?
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.
Get me out of here!
Technical Details
I Understand the Risks

IMPLEMENTASI : SSL/TLS, DIGITAL SIGNATURE DAN PENGGUNAAN SECURE EMAIL

SSL/TLS

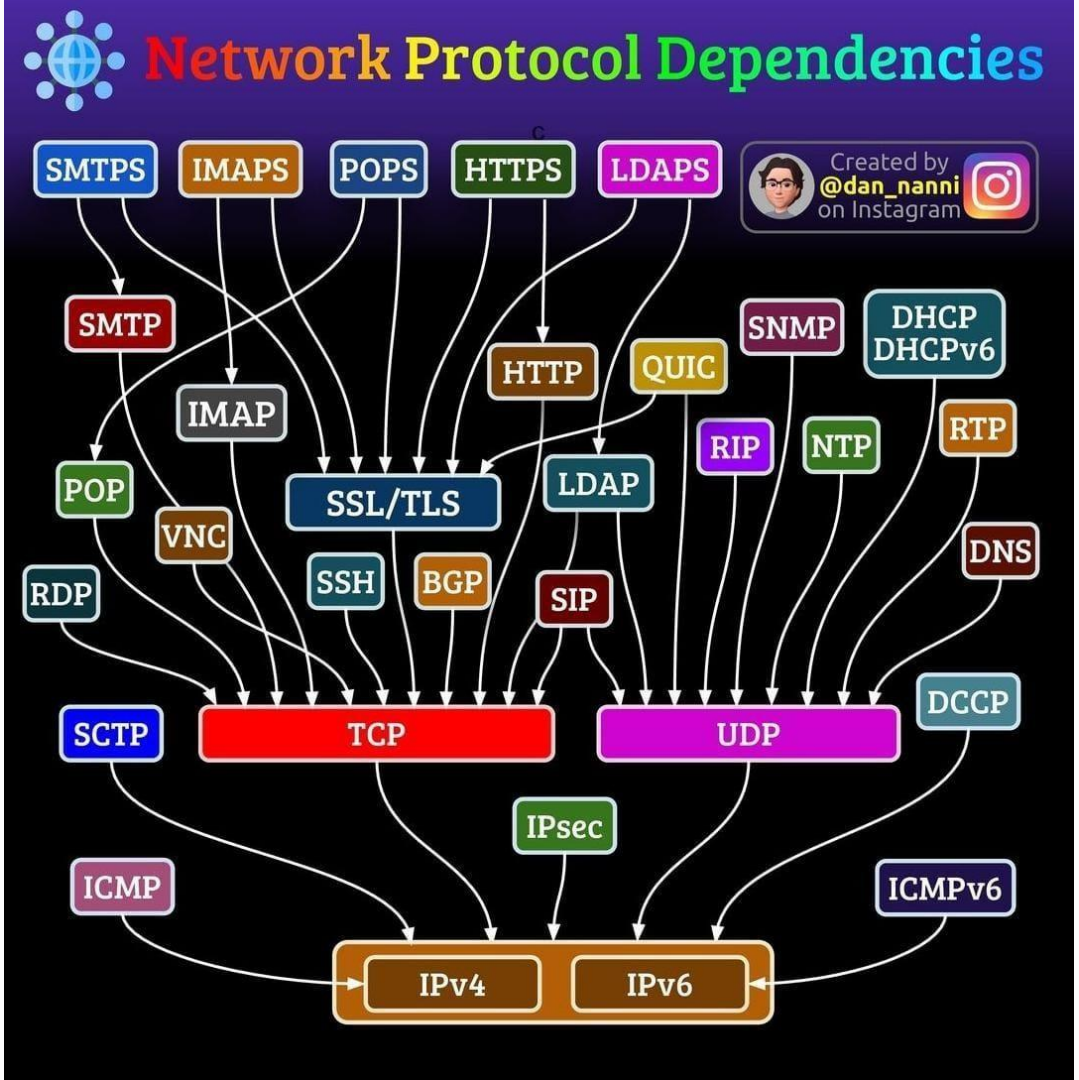
Sejarah

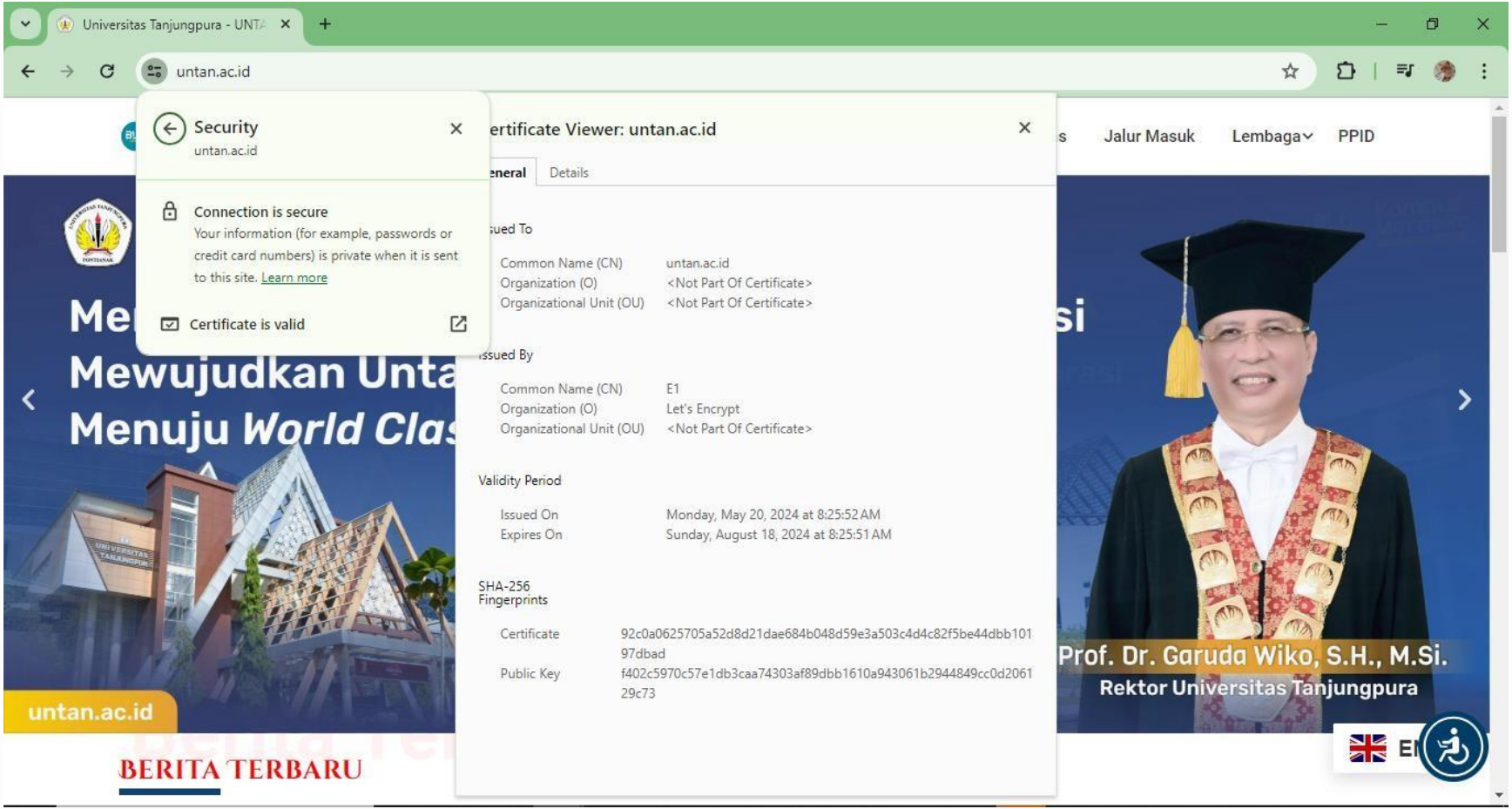
- The first usable version of SSL—SSL 2.0—was designed by Netscape, 1995
- SSL 3.0, 1996, was still widely used until 2014, Google's teams found a major issue in 2014 called POODLE
- TLS was first designed as another protocol upgrade of SSL 3.0 in 1999, TLS 1.0 -> SSL 3.1, IETF
- TLS 1.1 was released in 2006
- TLS 1.2 was released in 2008
- TLS 1.3 was approved in March 2018

PENGERTIAN

- *Secure Socket Layer* (SSL) adalah protokol yang digunakan untuk browsing web secara aman.
- SSL bertindak sebagai protokol yang mengamankan komunikasi antara client dan server.
- *Transport Layer Security* (*T*LS) dapat dianggap sebagai *SSL* versi 3.1.TLS dijelaskan dala RFC 2246.
- Untuk informasi lebih lanjut perihal *TLS*, kunjungi situs *IETF* di *www.ietf.org/rfc/rfc22*.

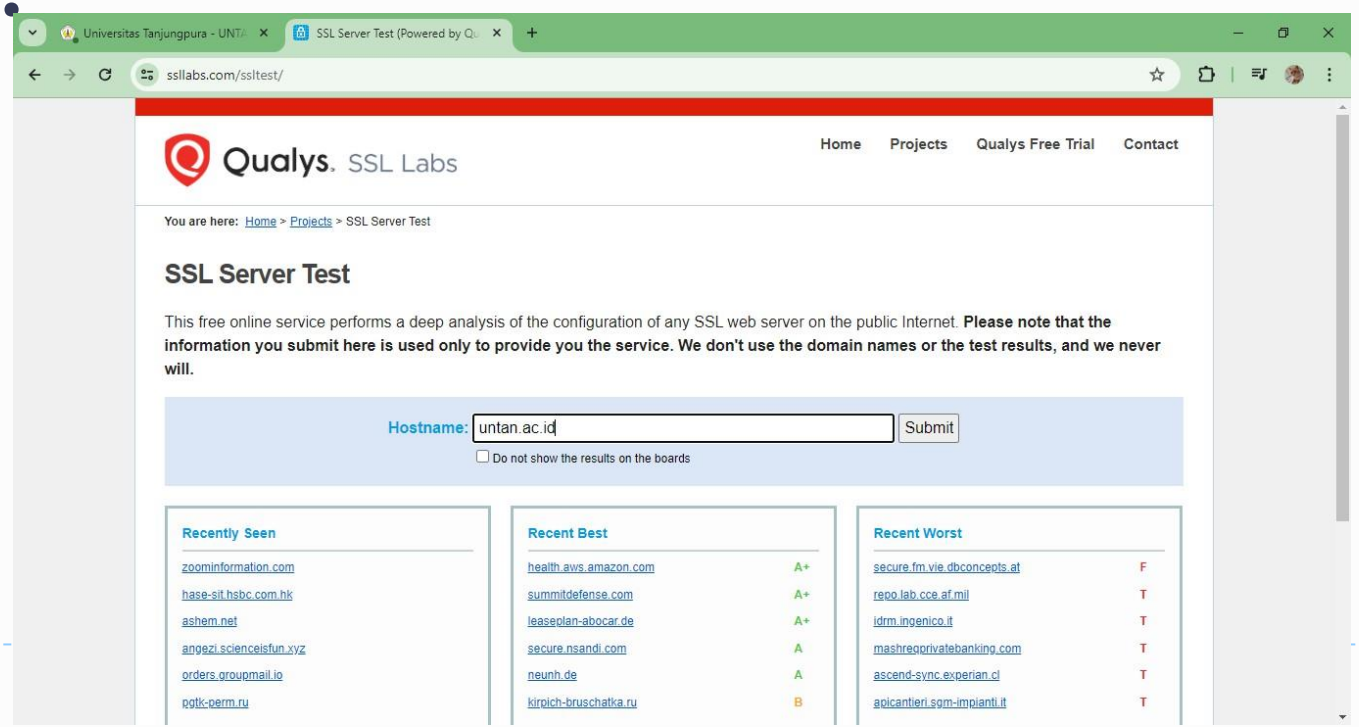
Network Protocol Dependencies



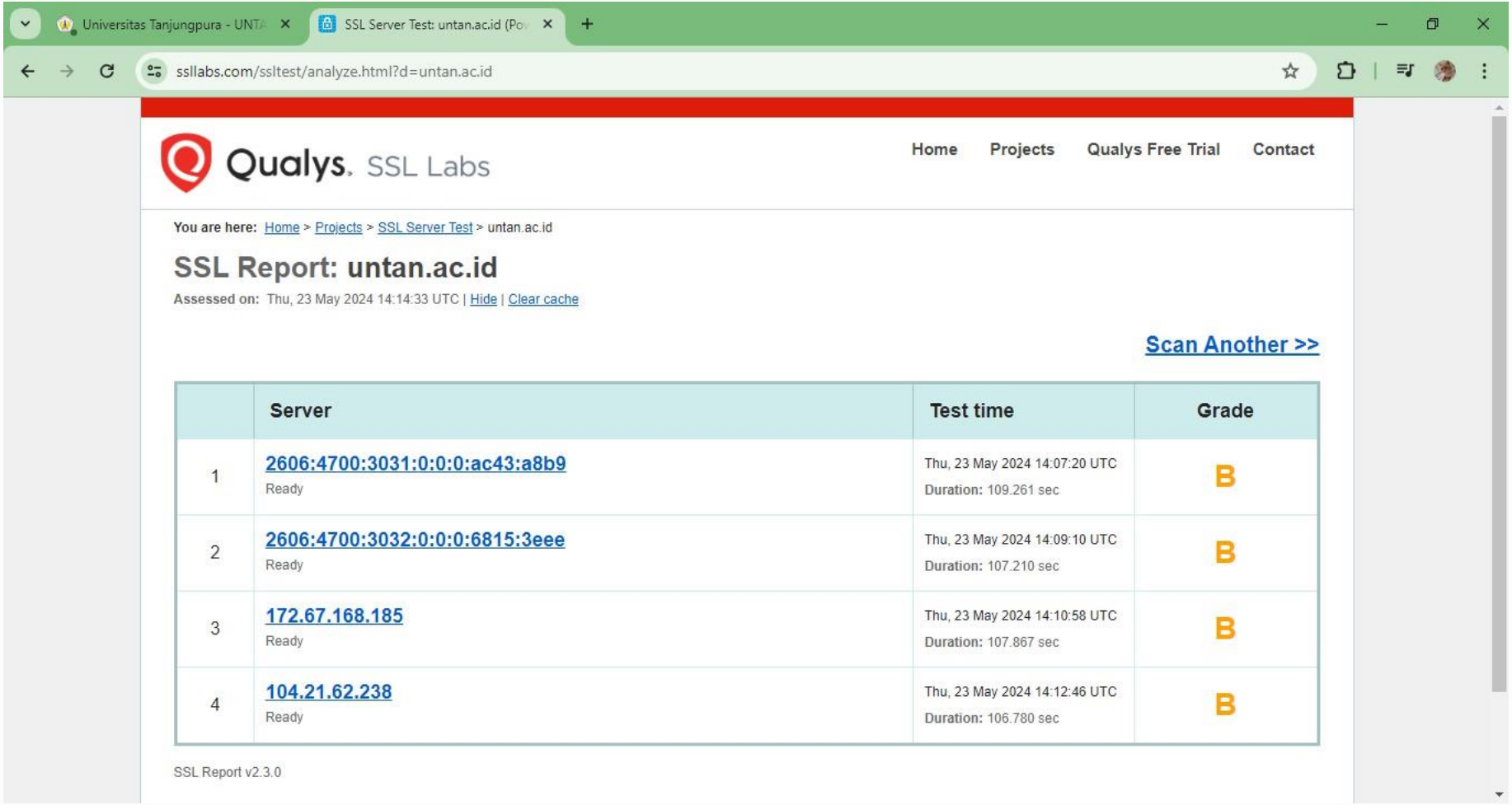

Universitas Tanjungpura - UNTA
untan.ac.id
Security
untan.ac.id
Connection is secure
Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more
Certificate is valid
ertificate Viewer: untan.ac.id
eneral
Details
sued To
Common Name (CN) untan.ac.id
Organization (O) <Not Part Of Certificate>
Organizational Unit (OU) <Not Part Of Certificate>
ssued By
Common Name (CN) E1
Organization (O) Let's Encrypt
Organizational Unit (OU) <Not Part Of Certificate>
Validity Period
Issued On Monday, May 20, 2024 at 8:25:52 AM
Expires On Sunday, August 18, 2024 at 8:25:51 AM
SHA-256 Fingerprints
Certificate 92c0a0625705a52d8d21dae684b048d59e3a503c4d4c82f5be44dbb10197dbad
Public Key f402c5970c57e1db3caa74303af89dbb1610a943061b2944849cc0d206129c73
Jalur Masuk
Lembaga
PPID
Mewujudkan Unta
Menuju World Clas
si
untan.ac.id
Prof. Dr. Garuda Wiko, S.H., M.Si.
Rektor Universitas Tanjungpura
BERITA TERBARU

SSL LAB :

https://www.ssllabs.com/ssltest/



https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide


Universitas Tanjungpura - UNTA
SSL Server Test: untan.ac.id (Po
ssllabs.com/ssltest/analyze.html?d=untan.ac.id
Qualys. SSL Labs
Home
Projects
Qualys Free Trial
Contact
You are here: Home > Projects > SSL Server Test > untan.ac.id
SSL Report: untan.ac.id
Assessed on: Thu, 23 May 2024 14:14:33 UTC | Hide | Clear cache
Scan Another >>
Server
Test time
Grade
1
2606:4700:3031:0:0:0:ac43:a8b9
Ready
Thu, 23 May 2024 14:07:20 UTC
Duration: 109.261 sec
B
2
2606:4700:3032:0:0:0:6815:3eee
Ready
Thu, 23 May 2024 14:09:10 UTC
Duration: 107.210 sec
B
3
172.67.168.185
Ready
Thu, 23 May 2024 14:10:58 UTC
Duration: 107.867 sec
B
4
104.21.62.238
Ready
Thu, 23 May 2024 14:12:46 UTC
Duration: 106.780 sec
B
SSL Report v2.3.0

Universitas Tanjungpura - UNTA | SSL Server Test: untan.ac.id (Po

ssllabs.com/ssltest/analyze.html?d=untan.ac.id&s=2606%3a4700%3a3031%3a0%3a0%3a0%3aac43%3aa8b9

Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > untan.ac.id > 2606:4700:3031:0:0:0:ac43:a8b9

SSL Report: untan.ac.id (2606:4700:3031:0:0:0:ac43:a8b9)

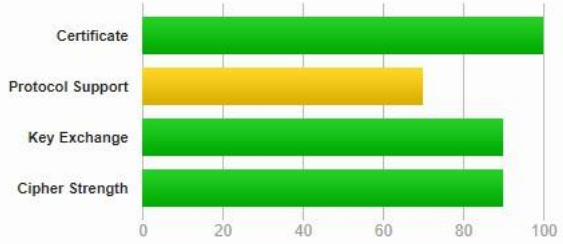
Assessed on: Thu, 23 May 2024 14:14:33 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

B



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »

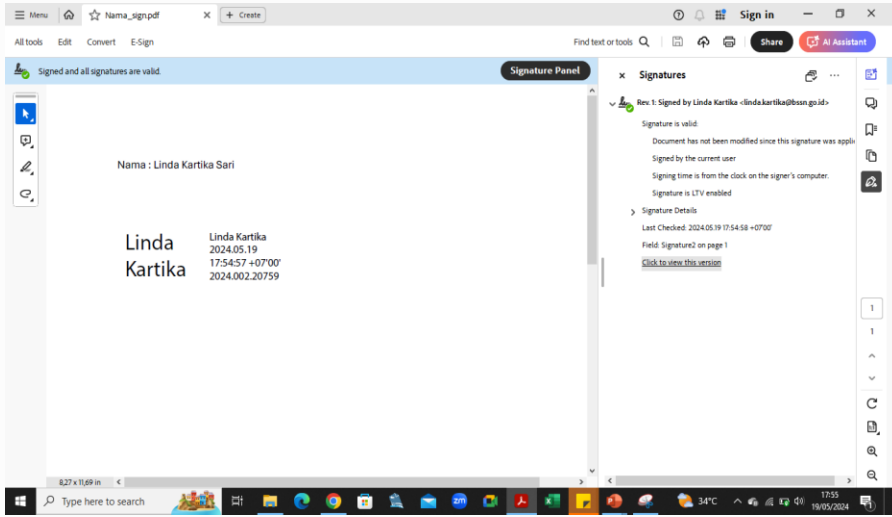
This site works only in browsers with SNI support.

MANFAAT TANDA TANGAN DIGITAL

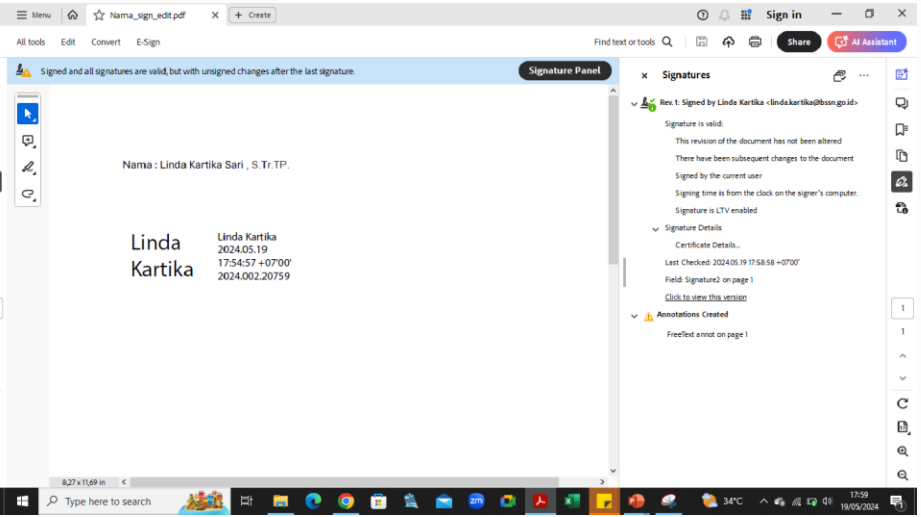
Keaslian (Authenticity):Tanda tangan digital memastikan bahwa pesan benar-benar berasal dari pengirim yang diklaim, karena hanya pemilik kunci privat yang dapat menghasilkan tanda tangan tersebut.

Integritas (Integrity):Tanda tangan digital menjamin bahwa pesan tidak telah diubah selama proses pengiriman. Setiap perubahan pada pesan akan menghasilkan nilai hash yang berbeda, sehingga tanda tangan digital tidak valid.

Non-repudiation: Pengirim tidak dapat menyangkal telah mengirim pesan tersebut, karena tanda tangan digital terkait erat dengan kunci privat pengirim yang unik.

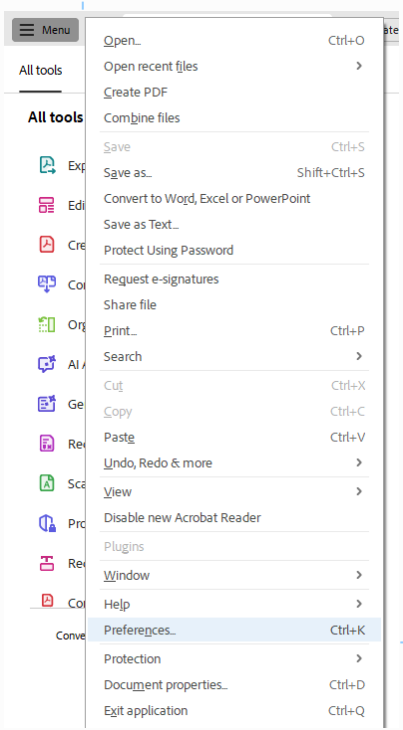


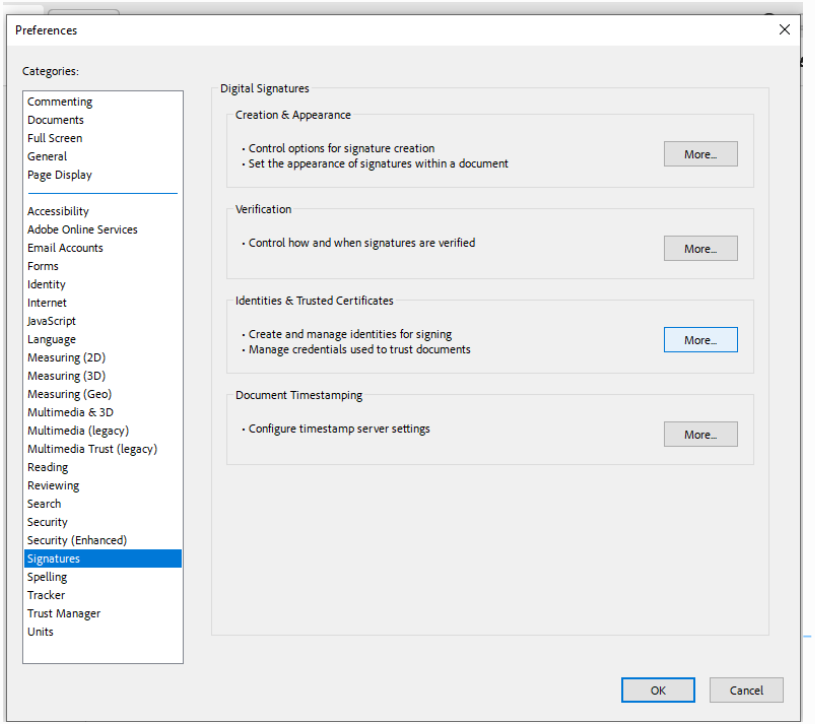
Asli

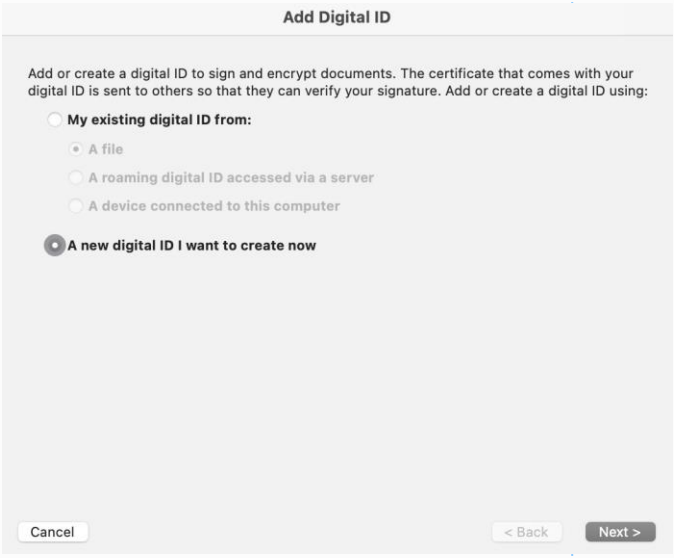


Modifikasi

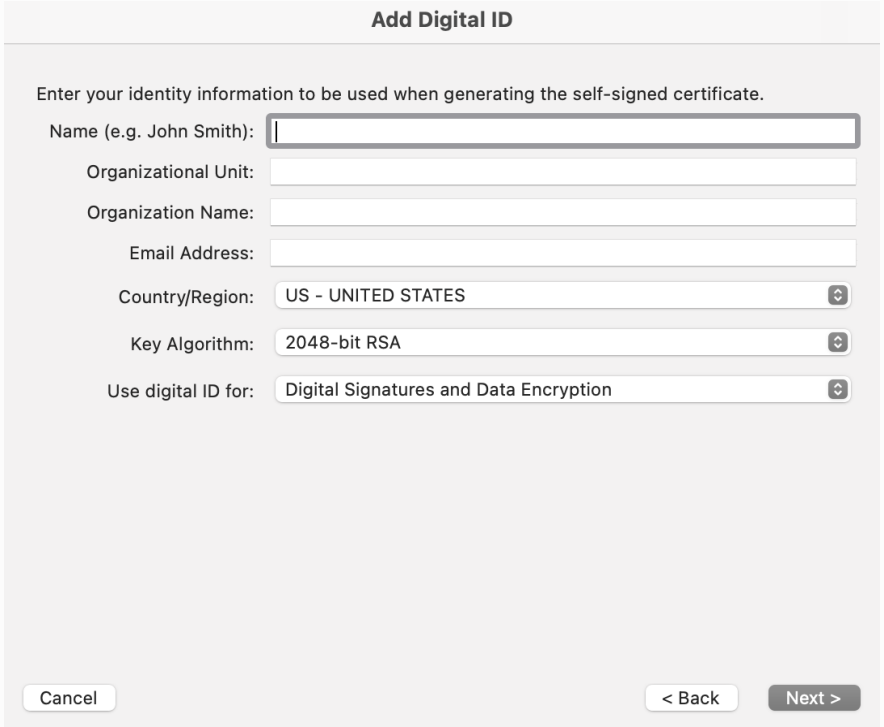
PENGGUNAAN DIGITAL SIGNATURE – ADOBE ACROBAT DC



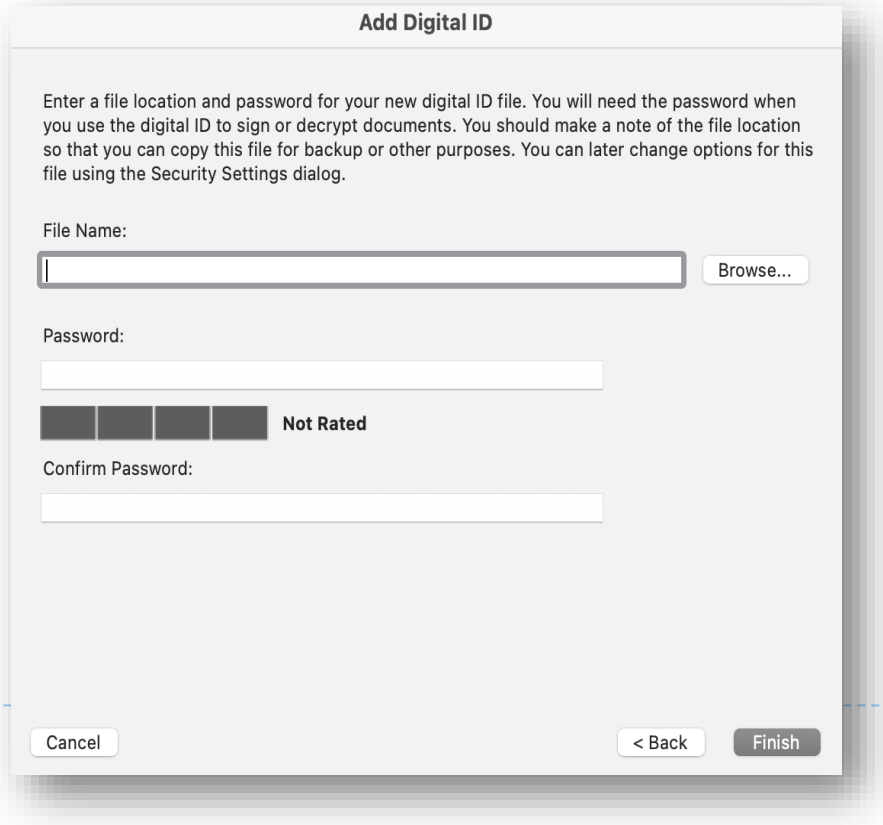




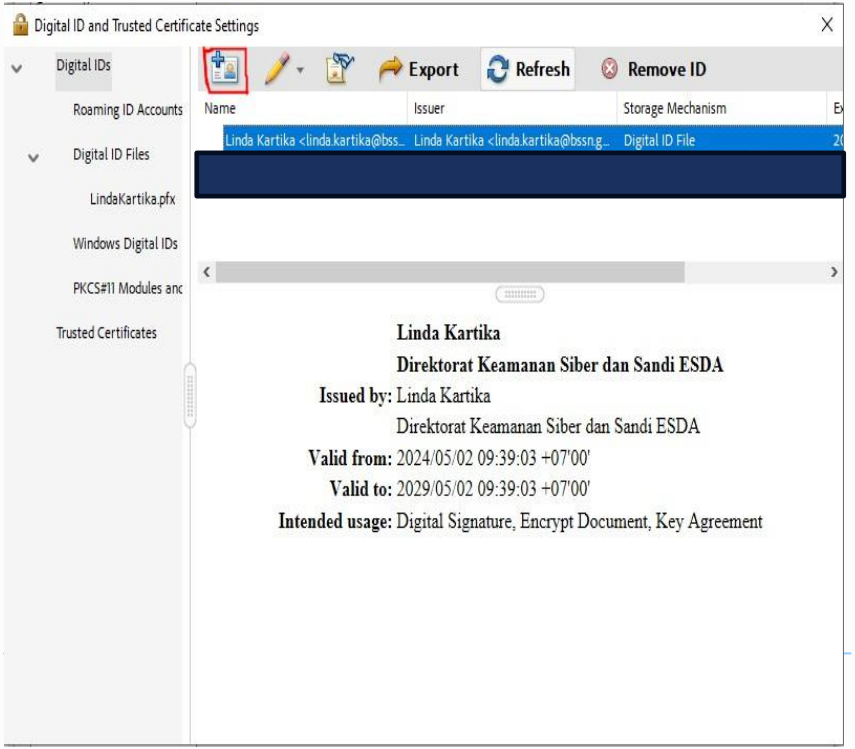
Masukkan beberapa data yang dibutuhkan

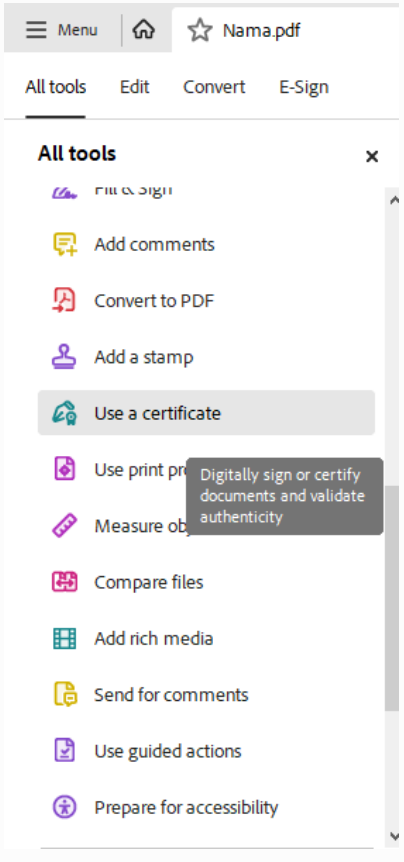


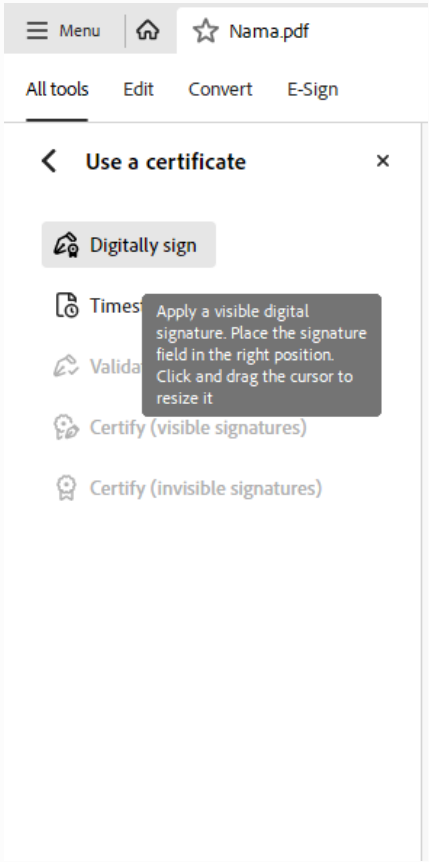
Masukkan lokasi file .p12 akan disimpan dan tentang password/passphrase untuk menggunakan .p12 tersebut

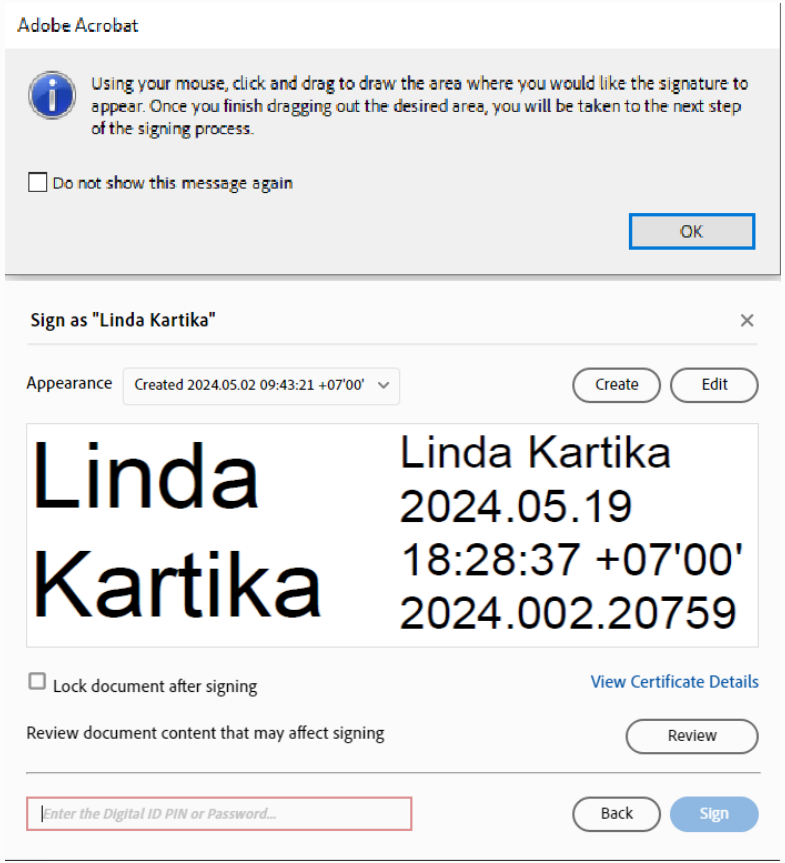


Sertifikat siap digunakan.




Menu
Nama.pdf
All tools
Edit
Convert
E-Sign
All tools
Add comments
Convert to PDF
Add a stamp
Use a certificate
Use print pr
Digitally sign or certify documents and validate authenticity
Measure ob
Compare files
Add rich media
Send for comments
Use guided actions
Prepare for accessibility


Menu
Nama.pdf
All tools
Edit
Convert
E-Sign
Use a certificate
Digitally sign
Times
Valida
Apply a visible digital signature. Place the signature field in the right position. Click and drag the cursor to resize it
Certify (visible signatures)
Certify (invisible signatures)


Adobe Acrobat
Using your mouse, click and drag to draw the area where you would like the signature to appear. Once you finish dragging out the desired area, you will be taken to the next step of the signing process.
Do not show this message again
OK
Sign as "Linda Kartika"
Appearance
Created 2024.05.02 09:43:21 +07'00'
Create
Edit
Linda Kartika
Linda Kartika
2024.05.19
18:28:37 +07'00'
2024.002.20759
Lock document after signing
View Certificate Details
Review document content that may affect signing
Review
Enter the Digital ID PIN or Password...
Back
Sign

Contoh File yang Memiliki Digital Signature

- https://drive.google.com/file/d/1qSD5O-976gG27INoZU3s6ya9tARPs_Am/view?usp=sharing

PRETTY GOOD PRIVACY (PGP)

- Pretty Good Privacy (PGP) adalah suatu pogram komputer yang dikembangkan oleh Phil Zimmermann pada pertengahan tahun 1980 yang memungkinkan seseorang untuk saling bertukar pesan melalui email dan juga file dengan memberikan perlindungan kerahasiaan berupa enkripsi dan otentikasi berupa digital signature.
- PGP mengikuti standar RFC 4880.
- PGP Key yang merupakan pasangan kunci publik dan privat dapat dibangkitkan secara mandiri oleh pengguna dengan menggunakan aplikasi komputer maupun aplikasi berbasis web.

SALT

- Hash akan merubah sebuah input string menjadi nilai hash yang selalu sama
- Misal fox ="DFCD3454"
- Selama menggunakan metode hash yang sama maka hash value akan sama
- Jika terdapat 2 user yang menggunakan password yang sama maka di dalam database akan terlihat hash value yang sama
- Maka perlu ditambahkan salt ke dalam kata sebelum dilakukan hash function, misal 01fox untuk user dengan id=01 dan 23fox untuk user dengan id 23
- Hasilnya hash akan berbeda

Watermarking & Steganography

Perbedaan Steganografi dan Watermarking

Steganografi

- Tujuan: mengirim pesan rahasia apapun tanpa menimbulkan kecurigaan
- Persyaratan: aman, sulit dideteksi, sebanyak mungkin menampung pesan (large capacity)
- Komunikasi: point-to-point
- Media penampung tidak punya arti apa-apa (meaningless)

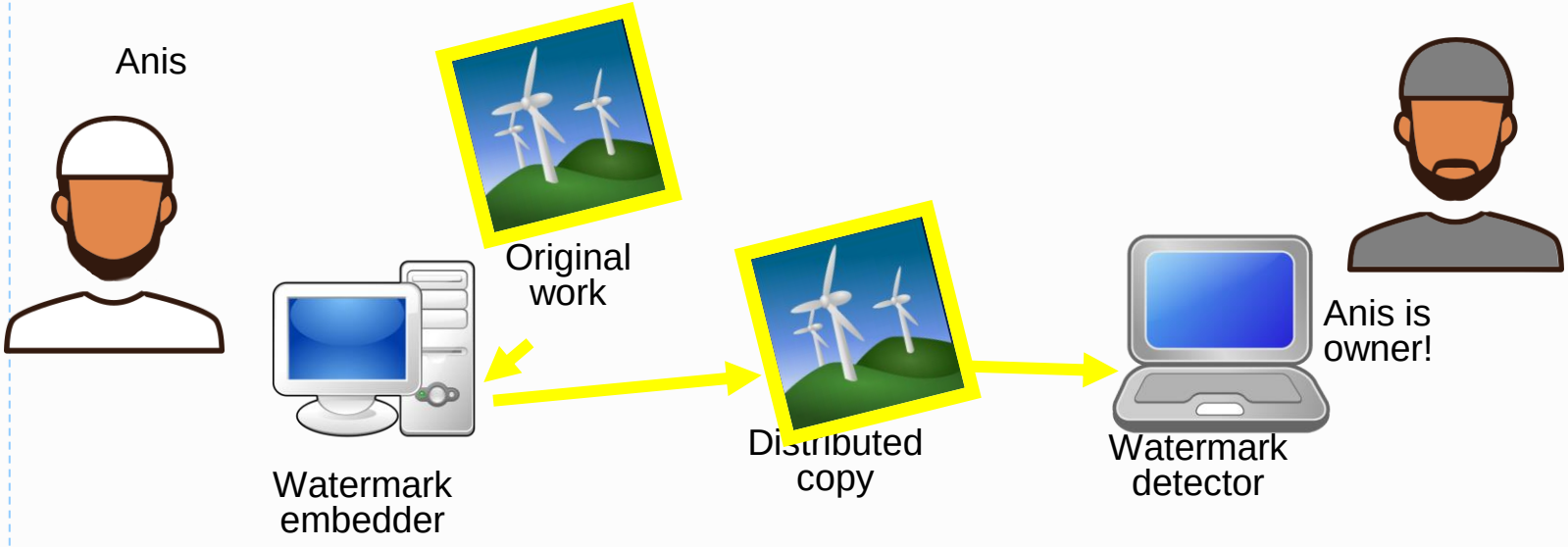
Watermarking:

- Tujuan: perlindungan copyright, pembuktian kepemilikan (ownership), fingerprinting
- Persyaratan: robustness, sulit dihapus (remove)
- Komunikasi: one-to-many
- Komentar lain: media penampung justru yang diberi proteksi, watermark tidak rahasia, tidak mementingkan kapasitas watermark

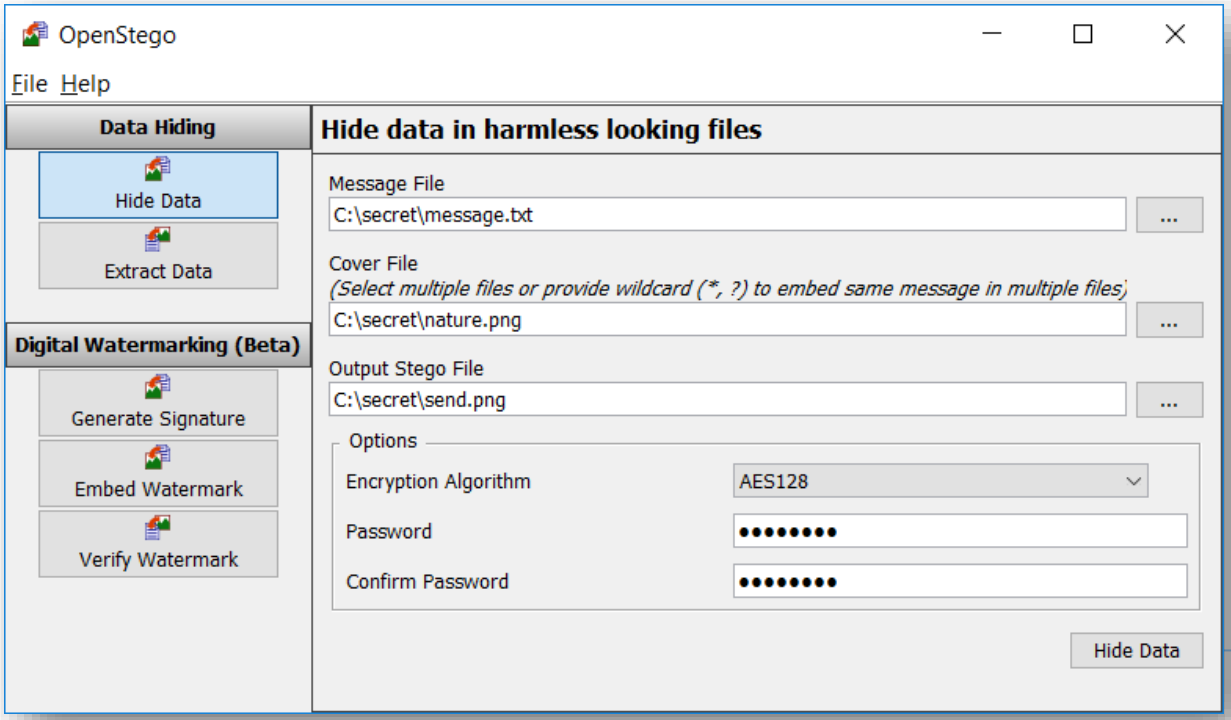
Aplikasi Watermark

- Identifikasi kepemilikan (ownership identification)
- Bukti kepemilikan (proof of ownership)
- Memeriksa keaslian isi karya digital (tamper proofing) ➔ Content authentication
- User authentication/fingerprinting/transaction tracking: mengotentikasi pengguna spesifik. Contoh: distribusi DVD
- Piracy protection/copy control: mencegah penggandaan yang tidak berizin.
- Broadcast monitoring

Owner identification



Contoh Software Watermark



Steganografi

Sejarah Steganografi

- Steganografi dengan media kepala budak (dikisahkan oleh Herodatus, penguasa Yunani pada tahun 440 BC di dalam buku: Histories of Herodatus).
- Kepala budak dibotaki, ditulisi pesan, rambut budak dibiarkan tumbuh, budak dikirim. Di tempat penerima kepala budak digunduli agar pesan bsia dibaca.
- Penggunaan tinta tak-tampak (invisible ink).
- Tinta dibuat dari campuran sari buah, susu, dan cuka. Tulisan di atas kertas dapat dibaca dengan cara memanaskan kertas tersebut.

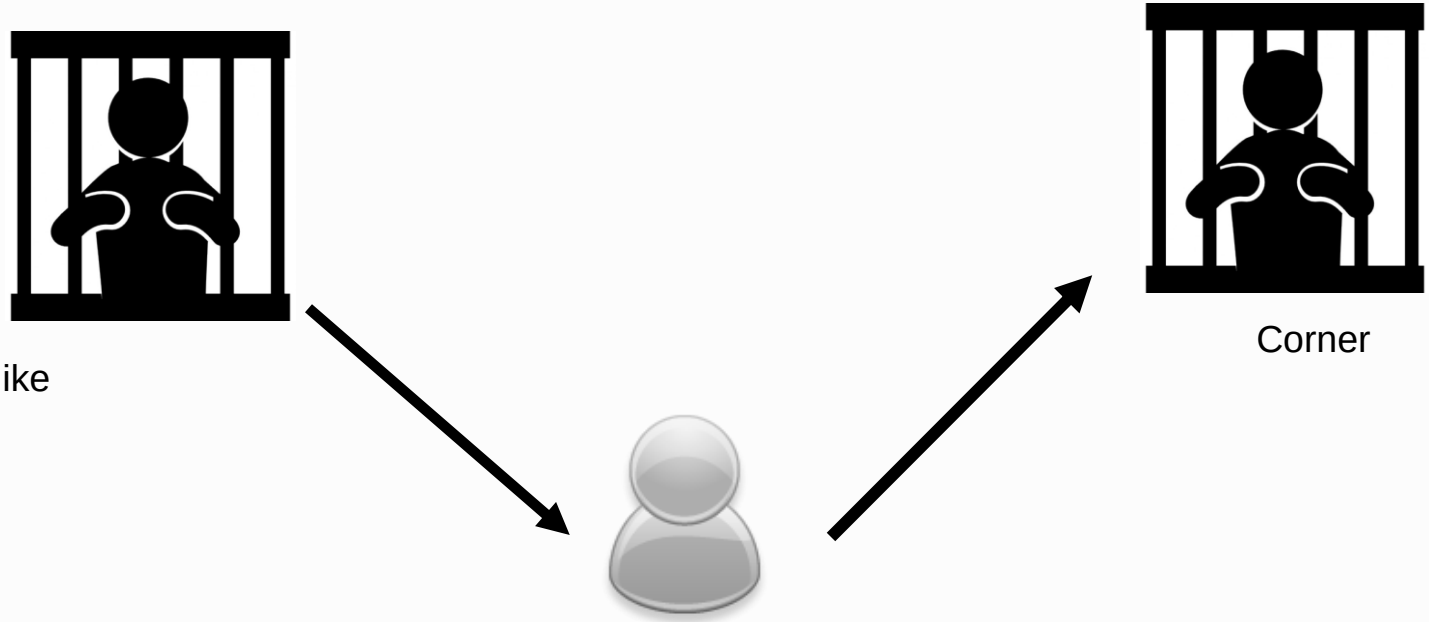
Steganografi vs Kriptografi

- Steganografi dapat dianggap pelengkap kriptografi (bukan pengganti).
- Steganografi: menyembunyikan keberadaan (existence) pesan

  Tujuan: untuk menghindari kecurigaan (conspicuous)
- Kriptografi: menyembunyikan isi (content) pesan

  Tujuan: agar pesan tidak dapat dibaca

Pengantar: Prisoner's Problem



Bagaimana Bob mengirim pesan rahasia kepada Alice tanpa diketahui oleh Sipir?

- Alternatif 1: mengenkripsinya

xjT#9uvmY!rc$

- Sipir pasti curiga!

Alternatif 2: menyembunyikannya di dalam pesan lain

Lupakan asal rumor itu, jaga agar matamu sehat atau turunkan ubanmu

sipir *tidak akan curiga!*

Information hiding dengan steganografi!

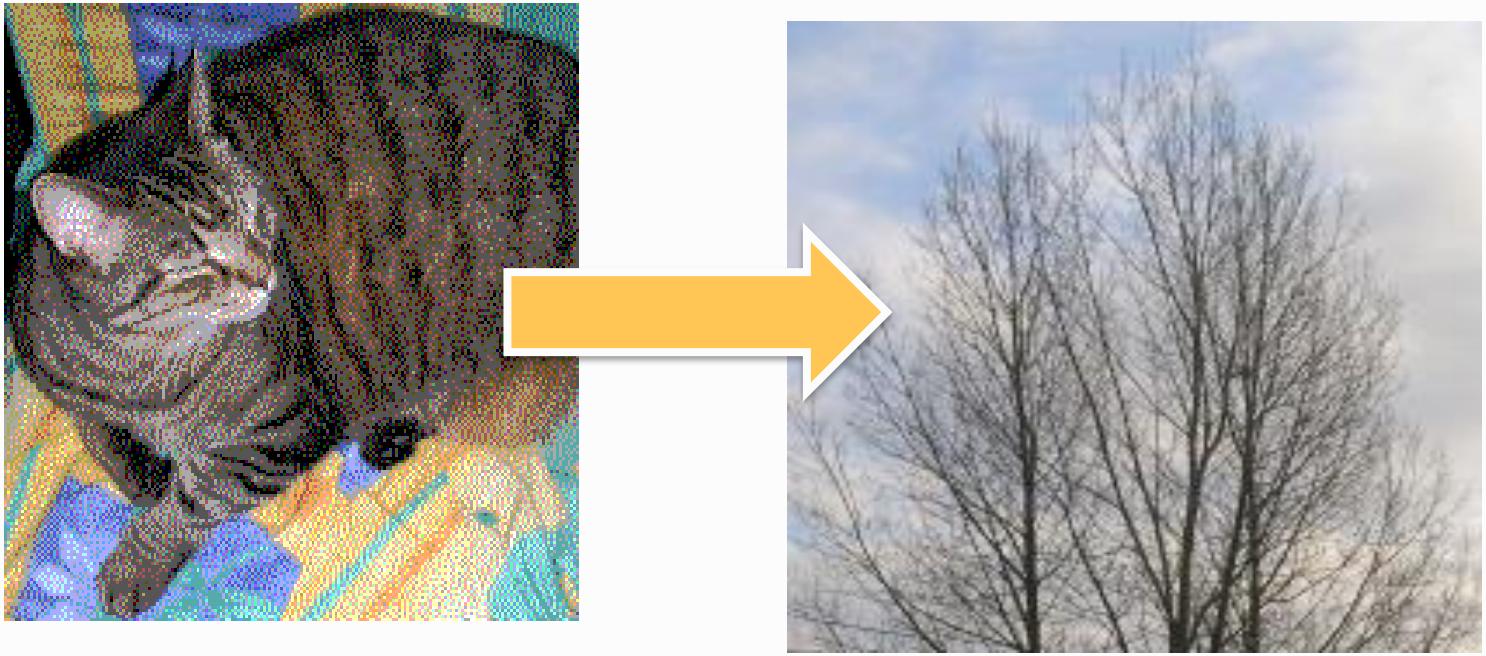
Apa Steganografi itu?

- "steganos" (B.Yunani) ➔ tulisan tersembunyi (covered writing)
- Steganography: ilmu dan seni menyembunyikan (embedded) informasi dengan cara menyisipkan pesan rahasia di dalam pesan lain [1].
- Steganografi digital: steganografi pada data digital dengan menggunakan komputer digital

Contoh: Pesan (teks) disembunyikan ke dalam gambar (citra)

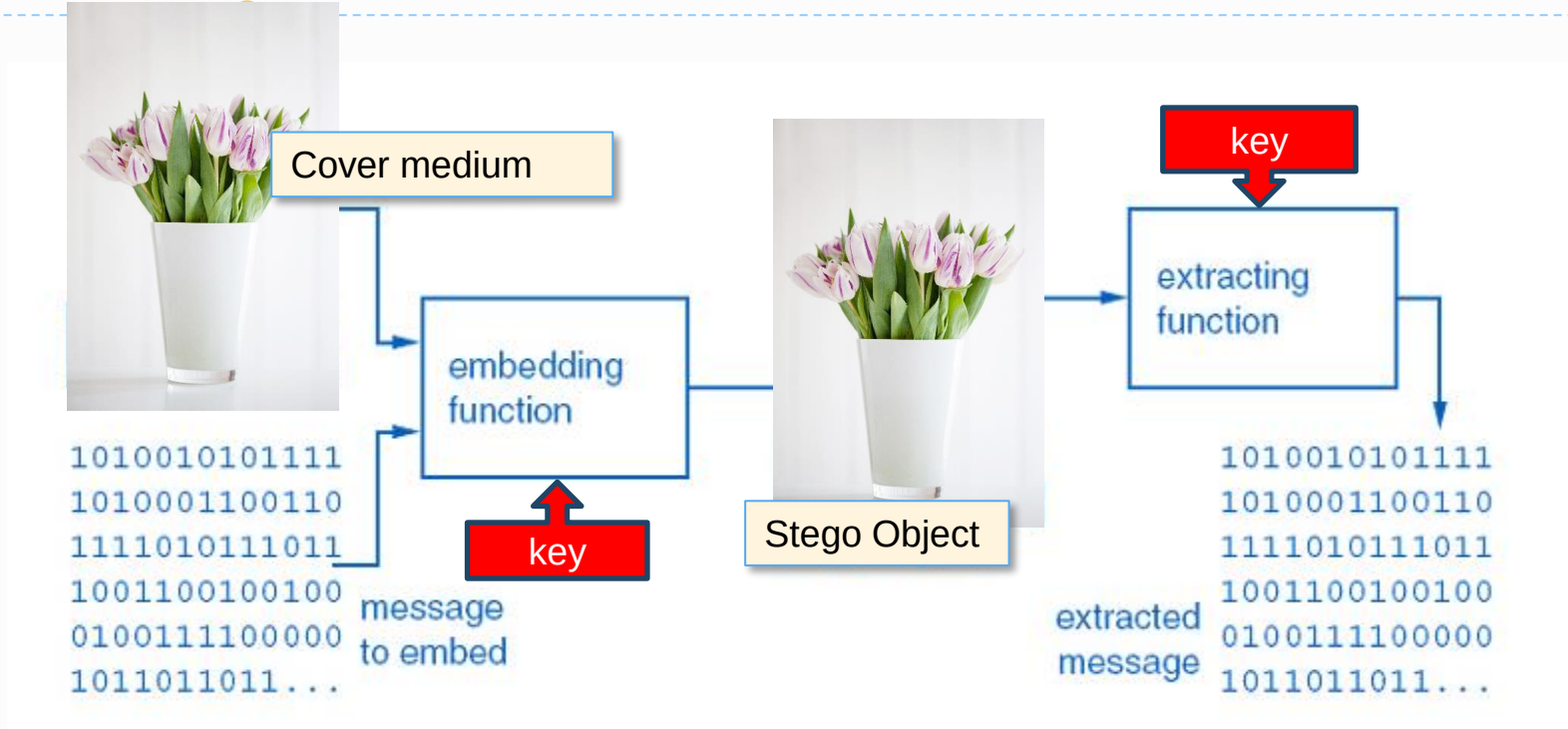
PESAN RAHASIA :
KIRIM BAKWAN PUKUL 13.00!

Contoh: Pesan (citra) disembunyikan ke dalam citra



Properti Steganografi

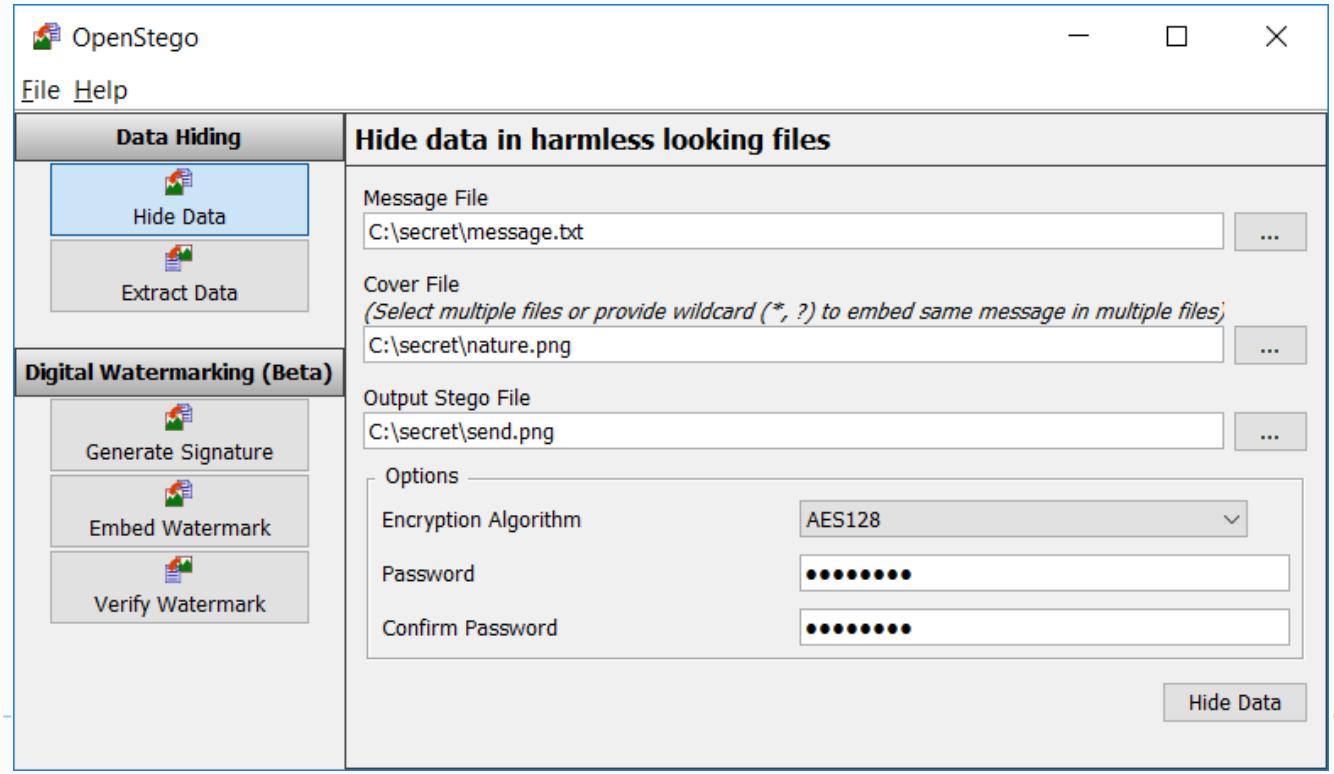
- **Embedded message** (hiddentext): pesan yang disembunyikan.
  - Bisa berupa teks, gambar, audio, video, dll
- **Cover-object (covertext):** pesan yang digunakan untuk menyembunyikan embedded message.
  - Bisa berupa teks, gambar, audio, video, dll
- **Stego-object (stegotext):** pesan yang sudah berisi pesan embedded message.
- **Stego-key:** kunci yang digunakan untuk menyisipan pesan dan mengekstraksi pesan dari stegotext.


Cover medium
embedding function
key
Stego Object
key
extracting function
10100101011111010001100110111101011101110011001001000100111100000101110110...
message to embed
extracted message
10100101011111010001100110111101011101110011001001000100111100000101110110...

Tools Steganography

- Image Steganography: OpenStego
- Document Steganography: Stegostick
- Video Steganography: Stegostick
- Audio Steganography: bitcrypt
- White Space Steganography: snow
- Spam/Email Steganography: Spam Mimic

OpenStego


OpenStego
File Help
Data Hiding
Hide Data
Extract Data
Digital Watermarking (Beta)
Generate Signature
Embed Watermark
Verify Watermark
Hide data in harmless looking files
Message File
C:\secret\message.txt
...
Cover File
(Select multiple files or provide wildcard (*, ?) to embed same message in multiple files)
C:\secret\nature.png
...
Output Stego File
C:\secret\send.png
...
Options
Encryption Algorithm
AES128
Password
Confirm Password
Hide Data