
CRYPTOGRAPHY


IN OUR CLASSROOM
WE RESPECT EACH OTHER.
WE TRY OUR BEST.
WE ARE A TEAM.
WE LEARN FROM MISTAKES.
WE CREATE.
WE CELEBRATE EACH OTHER'S SUCCESS.
TEACHFACTORY.COM

AN INTRODUCTION TO CRYPTOGRAPHY

CAPAIAN PEMBELAJARAN

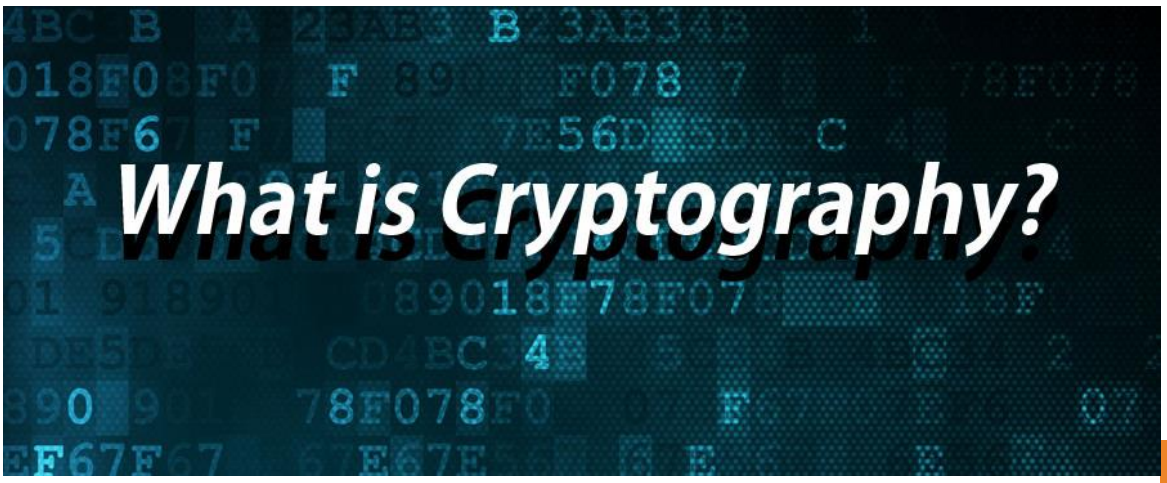
- Mahasiswa memahami konsep dasar kriptografi
- Mahasiswa memahami komponen-komponen kriptografi

Agenda.

- Cryptograpy
  - Encryption & Decryption
  - Secret key cryptography
  - Public key cryptography
- Digital signatures dan certificates
- Validity and trust

4

CRYPTOGRAPHY



5

CRYPTOGRAPHY

- Kriptografi adalah sebuah metode proteksi informasi dan komunikasi ke dalam bentuk kode.
- Kode tersebut memastikan bahwa hanya penerima yang diinginkan dapat membaca dan memproses pesan yang dikirimkan.
- Kriptografi terbagi ke dalam 2 kata; (1) **"crypt" – tersembunyi** dan (2) **"graphy" – tulisan**.

7

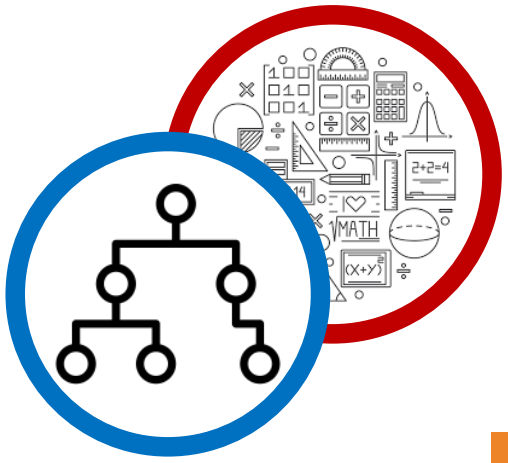
CRYPTOGRAPHY

- Kriptografi modern memiliki 4 standard utama:
  1. **Confidetiality (kerahasiaan)**
  2. **Integrity (menyeluruh)**
  3. **Non-repudiation (tidak dapat disangkal)**
  4. **Authentication (keaslian)**

8

CRYPTOGRAPHY

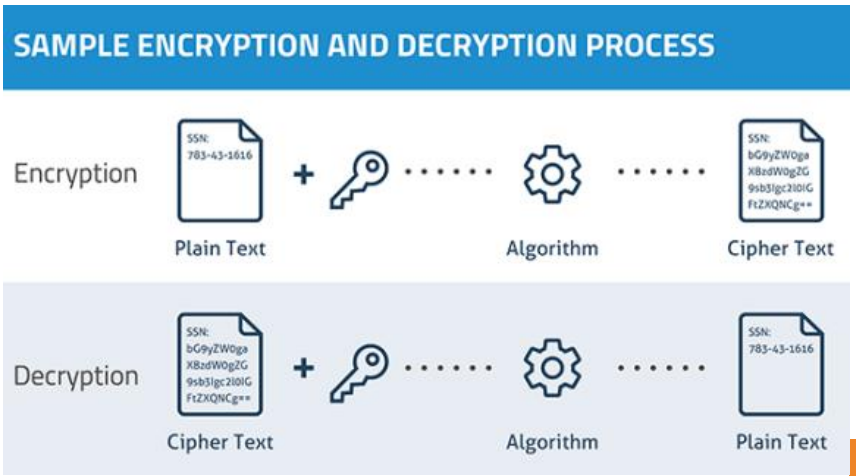
- Metode kriptografi berasal dari konsep matematika
- Menggunakan algoritma atau aturan perhitungan dasar (tambah kurang bagi kali)
- Algoritma tersebut akan membentuk sebuah ***cryptographic key*** yang mengendalikan penanda digital dan verifikasi untuk menjaga kerahasiaan data pengguna.



9

CRYPTOGRAPHY

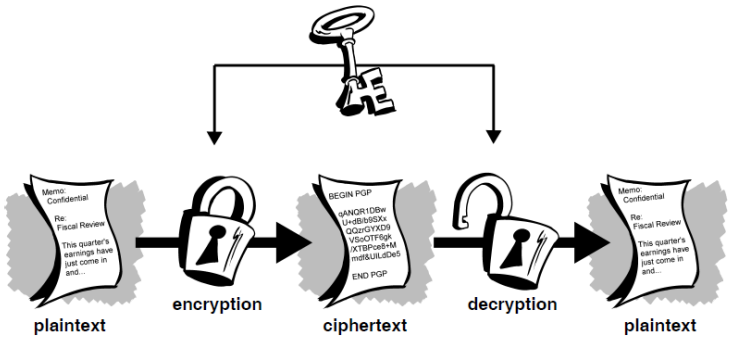
- Kriptografi modern pada dasarnya mengubah sebuah data (***plaintext***) ke dalam bentuk ***unreadable text*** yang disebuh dengan ***chiper text*** kemudian mengbahnay kembali ke dalam bentuk ***plaintext***.



10

CRYPTOGRAPHY

Secret Key Cryptography Algorithmsz



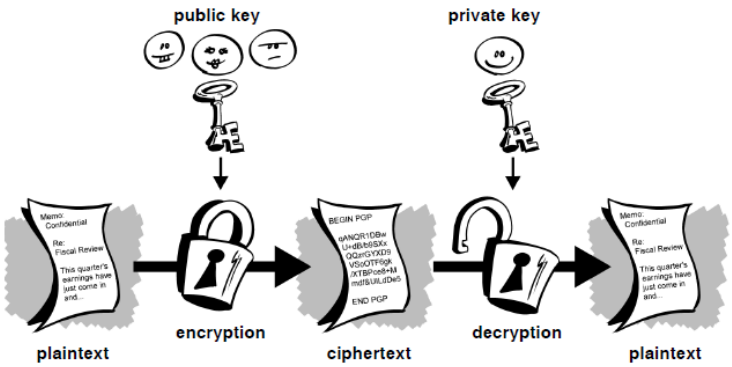
- Eknripsi dan deskripsi menggunakan *key* yang sama
- Digunakan untuk melakukan enkripsi isi pesan

Symmetric cryptography algorithms

11

CRYPTOGRAPHY

Public Key Cryptography Algorithms



- Eknripsi dan deskripsi menggunakan *key* yang berbeda, *public key* dan *private key*
- Digunakan untuk melakukan enkripsi *digital certification* dan pengelolaan key (*key menagement*)

Asymmetric cryptography algorithms

12

DIGITAL SIGNATURES & CERTIFICATE

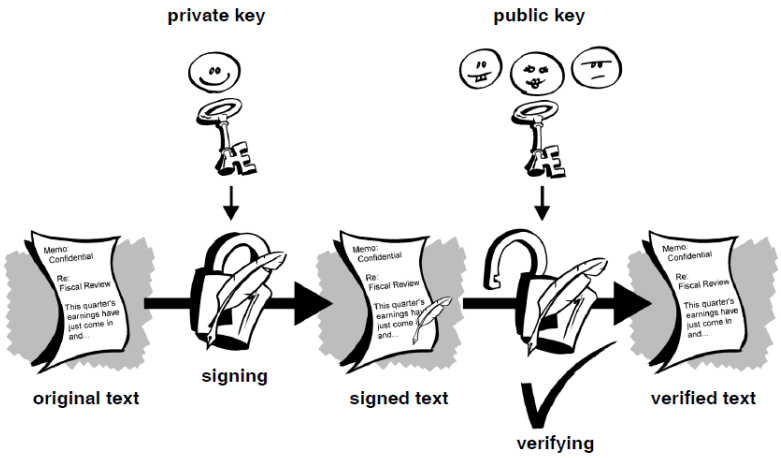
Digital Signatures.

- Tujuan dari tanda tangan digital pada sertifikat adalah untuk menyatakan bahwa informasi sertifikat telah dibuktikan oleh beberapa orang atau entitas lain.
- Keuntungan utama dari *public key cryptography* adalah menyediakan metode untuk *digital signatures* (tanda tangan digital).
- *Digital signatures* memungkinkan penerima informasi melakukan verifikasi keaslian asal informasi dan memastikan bahwa pesan tidak diubah saat dalam perjalanan.
- *Digital signatures* memberikan pencegahan dari penyangkalan (*non-repudiation*) pengirim untuk mengklaim bahwa pengirim tidak benar-benar mengirimkan informasi.

13

DIGITAL SIGNATURES & CERTIFICATE

- Serupa tapi tak sama dengan tanda tangan dengan tulisan tangan.



14

DIGITAL SIGNATURES & CERTIFICATE

Digital Certificate.

- Satu masalah dengan *cryptosystem* kunci publik adalah bahwa pengguna harus selalu waspada memastikan pengirim mengenkripsi kunci yang sesuai yang dimiliki penerima.
- Menyederhanakan tugas menetapkan apakah kunci publik benar-benar milik pemilik yang diklaim.
- *Digital certificate* terdiri atas 3 hal:
  1. Sebuah kunci publik
  2. Informasi mengenai sertifikat (identitas)
  3. Satu atau lebih *digital signatures*

15

DIGITAL SIGNATURES & CERTIFICATE

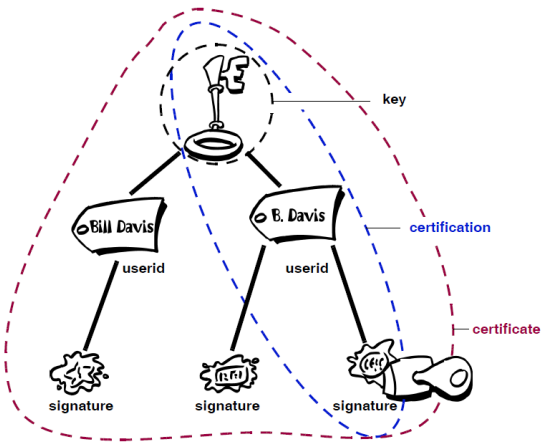
Digital Certificate.

- Satu masalah dengan *cryptosystem* kunci publik adalah bahwa pengguna harus selalu waspada memastikan pengirim mengenkripsi kunci yang sesuai yang dimiliki penerima.
- Menyederhanakan tugas menetapkan apakah kunci publik benar-benar milik pemilik yang diklaim.
- *Digital certificate* terdiri atas 3 hal:
  1. Sebuah kunci publik
  2. Informasi mengenai sertifikat (identitas)
  3. Satu atau lebih *digital signatures*

16

DIGITAL SIGNATURES & CERTIFICATE

- Tanda tangan digital tidak tidak membuktikan keaslian sertifikat secara keseluruhan
- Menjamin bahwa informasi identitas yang ditandatangani sejalan dengan, atau terikat pada, kunci publik.
- Sertifikat pada dasarnya adalah kunci publik dengan satu atau dua bentuk ID terlampir.



17

VALIDITY & TRUST

Validity.

- *"Is something we calculate from the signatures on the person's key"*
- Validitas adalah sjatu bentuk keyakinan bahwa sertifikat *public key* adalah milik pemiliknya.
- Validitas sangat penting dalam lingkungan *public key* untuk menetapkan apakah sertifikat tertentu asli atau tidak.

18

VALIDITY & TRUST

Trust.

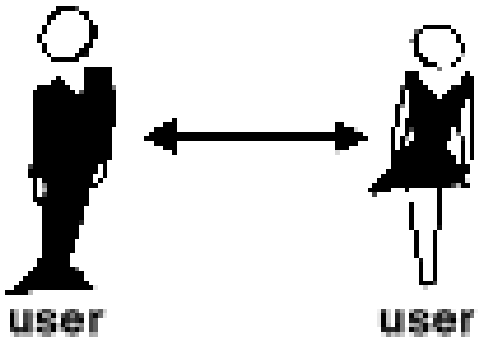
- *"Is something we must assign to each key ourselves in order for it to say something other than **unknown**"*
- Validasi sebuah sertifikat perlu keyakinan bahwa yang melakukan validasi adalah orang yang dipercaya (*trust*)
- Model *trust*:
  - Direct Trust
  - Hierarchical Trust
  - A Web of Trust

19

VALIDITY & TRUST

Direct Trust.

- **Direct trust:** model kepercayaan yang paling sederhana.
- Pengguna percaya bahwa kunci valid karena pengguna mengetahui asal dari suatu kunci.
- Contoh: Browser web mempercayai kunci Otoritas Sertifikasi untuk root karena dikirimkan oleh pabrikan.

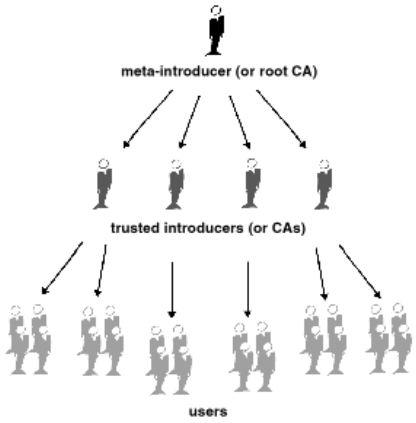


20

VALIDITY & TRUST

Hierarchical Trust.

- **Hierachical trust** memiliki sistem sertifikat "root" hierarkis (berjenjang).
- Sertifikat-sertifikat ini disahkan dalam suatu rantai root.
- Validitas sertifikat "daun" diverifikasi dengan menelusuri mundur dari pengesahnya, ke pengesah lain, hingga ditemukan sertifikat akar yang dipercaya secara langsung.



21

VALIDITY & TRUST

Web of Trust.

- Mencakup kedua model lainnya ditambah gagasan bahwa kepercayaan bergantung kepada pihak yang menentukannya
- Model ini merupakan model kepercayaan kumulatif.
- Sertifikat mungkin dipercaya secara langsung, atau dipercaya dalam suatu rantai yang akan kembali ke sertifikat akar yang dipercaya secara langsung (meta-introduksi), atau oleh beberapa kelompok pengantar.

22

AN INTRODUCTION TO CRYPTOGRAPHY