
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

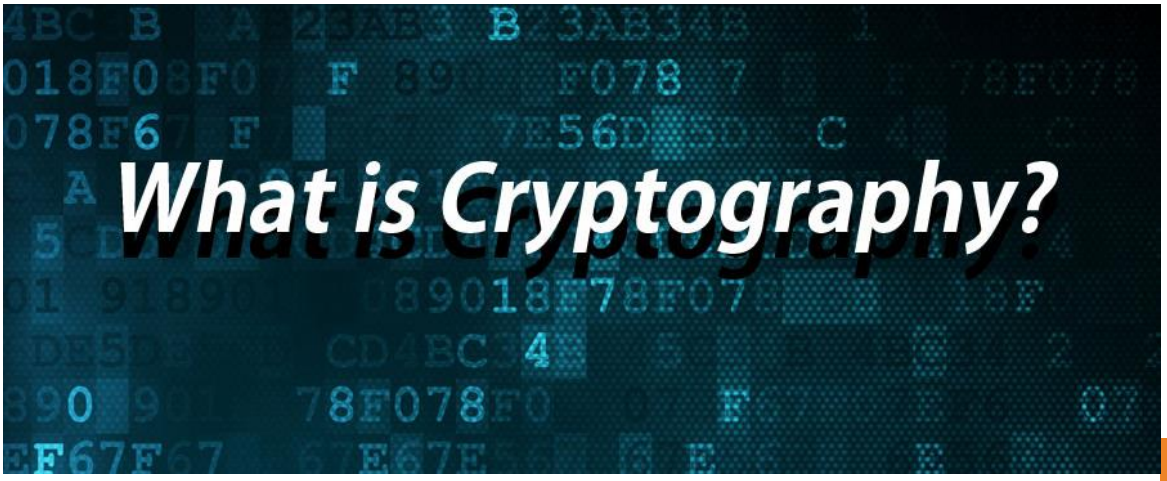
- Mahasiswa memahami konsep dasar kriptografi
- Mahasiswa memahami komponen-komponen kriptografi

Agenda.

- Cryptograpy
  - Encryption & Decryption
  - Secret key cryptography
  - Public key cryptography
- Conventional cryptography and clasification
- 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

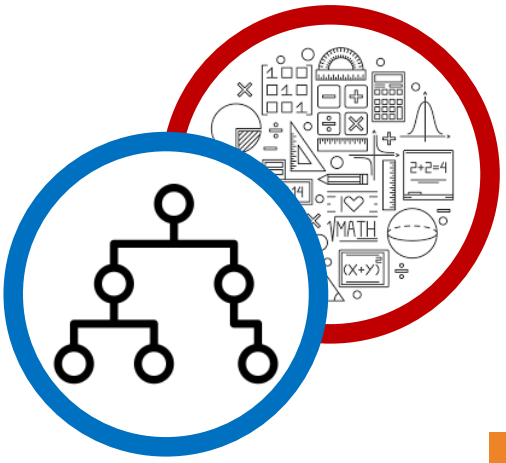
CRYPTOGRAPHY

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

8

CRYPTOGRAPHY

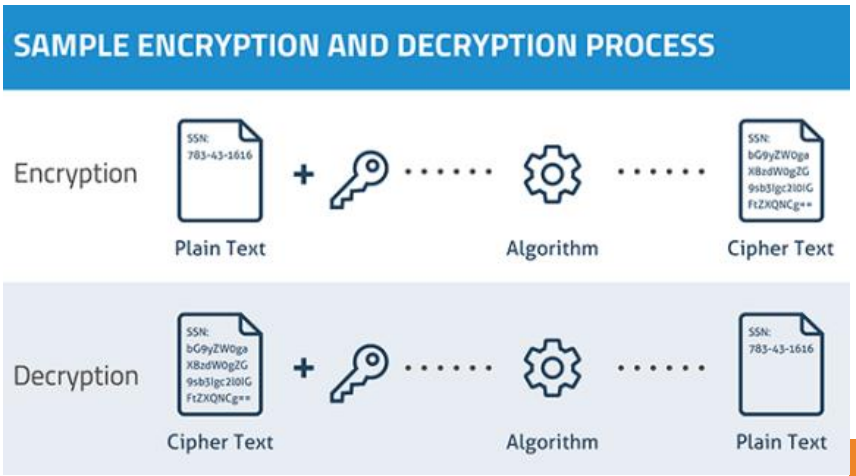
- Metode kriptografi berasal dari konsep matematika
- Menggunakan algoritma atau aturan perhitungan dasar (tambah kurang bagi kali)
- Algoritma tersebut akan membentuk sebuah ***cryptographic key*** yang mengendalikan penanda digital dan verifikasi untuk menjaga kerahasiaan data pengguna.



9

CRYPTOGRAPHY

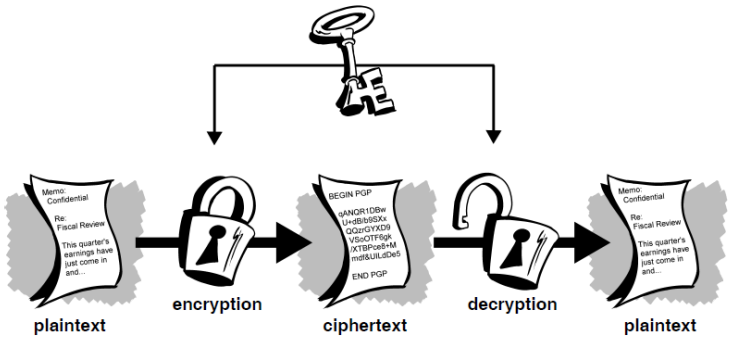
- Kriptografi modern pada dasarnya mengubah sebuah data (***plaintext***) ke dalam bentuk ***unreadable text*** yang disebuh dengan ***chiper text*** kemudian mengbahnay kembali ke dalam bentuk ***plaintext***.



10

CRYPTOGRAPHY

Secret Key Cryptography Algorithmsz



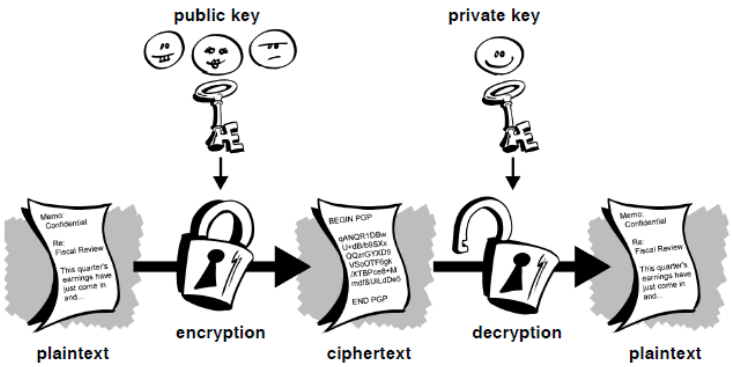
- Eknripsi dan deskripsi menggunakan *key* yang sama
- Digunakan untuk melakukan enkripsi isi pesan

Symmetric cryptography algorithms

11

CRYPTOGRAPHY

Public Key Cryptography Algorithms

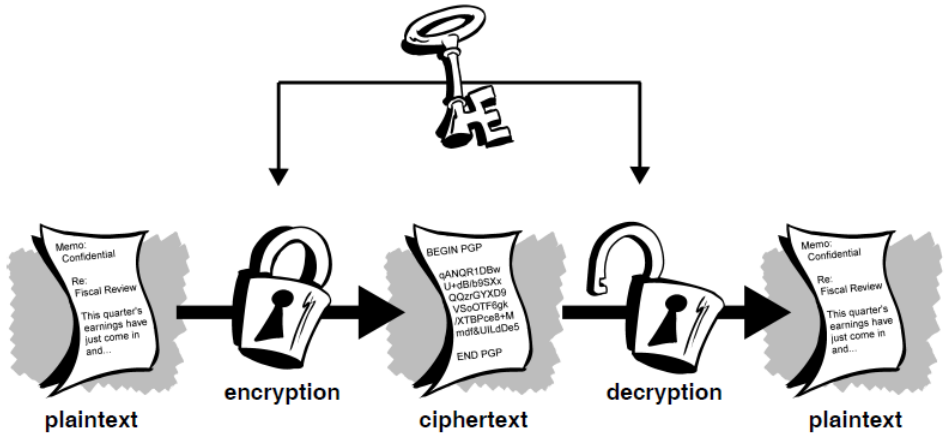


- Eknripsi dan deskripsi menggunakan *key* yang berbeda, *public key* dan *private key*
- Digunakan untuk melakukan enkripsi *digital certification* dan pengelolaan key (*key menagement*)

Asymmetric cryptography algorithms

12

CONVENTIONAL CRYPTOGRAPHY



13

CONVENTIONAL CRYPTOGRAPHY

- Kriptogrfi konvensional terbagi ke dalam 9 klasifikasi
  - Monoalphabetic - Caesar's chiper, ROT13, Four Square chiper
  - Polyalphabetic - Running Key, Vigenere, One Time Pad
  - Polygraphic - Playfair, Tripid
  - Route Transposition - Rail Fence
  - Synchronous Stream - A5/1
  - Asynchronous Stream - Rabbit, Autokey
  - Iterated Block - AES, Blowfish, DES, IDEA, SMS4
  - Fractionated Block - ADFGVX, Stradding Checkboard
  - Steganigraphic - Bacon

14

CONVENTIONAL CRYPTOGRAPHY AND CLASIFICATION

Caesar's Chiper

- **Caesar's chiper** adalah contoh kriptogrfi konvensional **monoalphabetic** yang digunakan oleh Julius Caesar untuk mengirimkan pesan kepada bawahannya dan sekutunya.
- Caesar's chiper dilakukan dengan cara melakukan enkripsi pada setiap huruf alfabet dengan melakukan penggeseran (shifting) urutan alfabet.
- Contoh:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

and sliding everything up by 3, you get

DEFGHIJKLMNOPQRSTUVWXYZABC

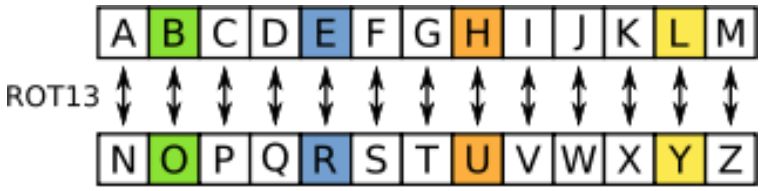
where D=A, E=B, F=C, and so on.

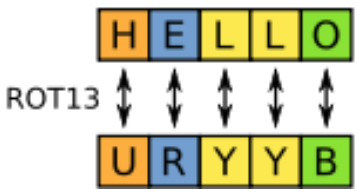
15

CONVENTIONAL CRYPTOGRAPHY AND CLASIFICATION

ROT13 Chiper

- Contoh lainnya dalam penggunaan kriptogrfi konvensional adalah **ROT13** dan **Four Square Chiper**
- **ROT13** menggantikan setiap huruf dengan mitranya 13 karakter lebih jauh di sepanjang alfabet.





16

CONVENTIONAL CRYPTOGRAPHY AND CLASIFICATION

Four Square Chiper

- **Four Square Chiper** menggunakan urutan alfabet yang disajikan dalam bentuk kubus (*square*) berjumlah 4 buah
- Setiap alfabet dalam *plaintext* kemudian digantikan oleh setiap alfabet pada kubus alfabet lainnya.
- Pengaturan huruf dalam kubus dapat diatur sedemikian rupa sesuai kesepakatan antara enkriptor dan dekriptor.

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

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

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

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

17

CONVENTIONAL CRYPTOGRAPHY AND CLASIFICATION

Running Key Chiper

to be continued...

18

AN INTRODUCTION TO CRYPTOGRAPHY