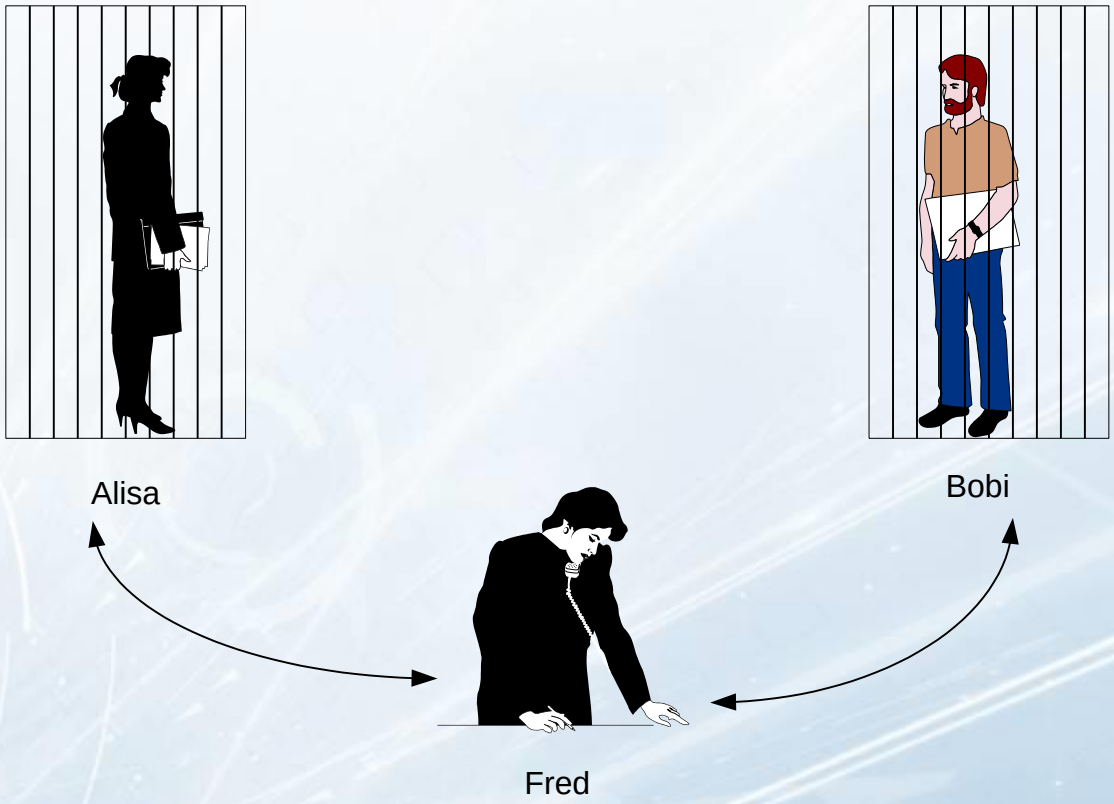
Dasar-Dasar Keamanan

(Steganografi dan Kriptografi)

Muhammad Izzuddin Mahali, M.Cs.
Izzudin@uny.ac.id / m.Izzuddin.m@gmail.com
Program Studi Pendidikan Teknik Informatika
Jurusan Pendidikan Teknik Elektronika
Fakultas Teknik
Universitas Negeri Yogyakarta

Steganografi

Pengantar: *Prisoner's Problem*



Pesan rahasia: "Lari jam satu"

- Alternatif 2: menyembunyikannya di dalam pesan lain

  Lupakan asal rumor itu jangan ambil manfaatnya setelah aku tutup usia

  Fred tidak akan curiga!

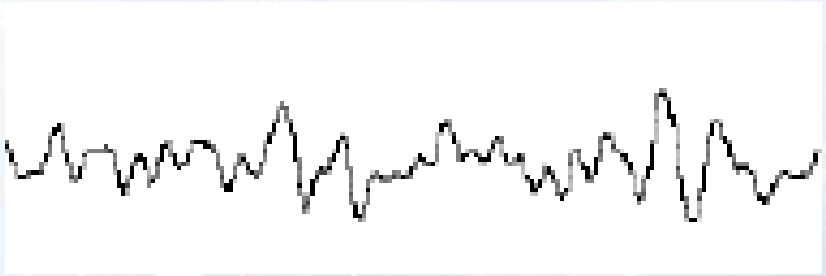
Information hiding dengan steganografi!

Pesan (*message*)

1. Teks

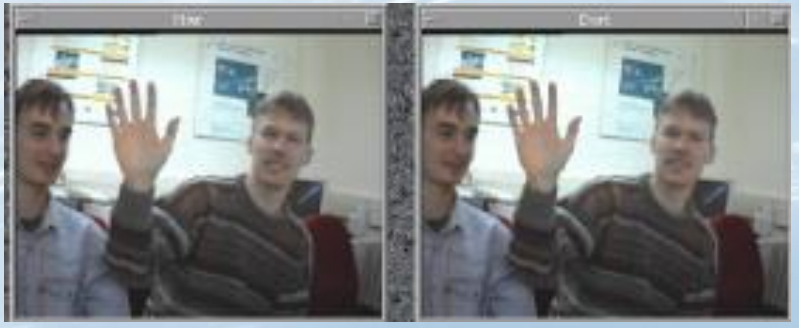
   “Torang semua bersodara”

2. Audio



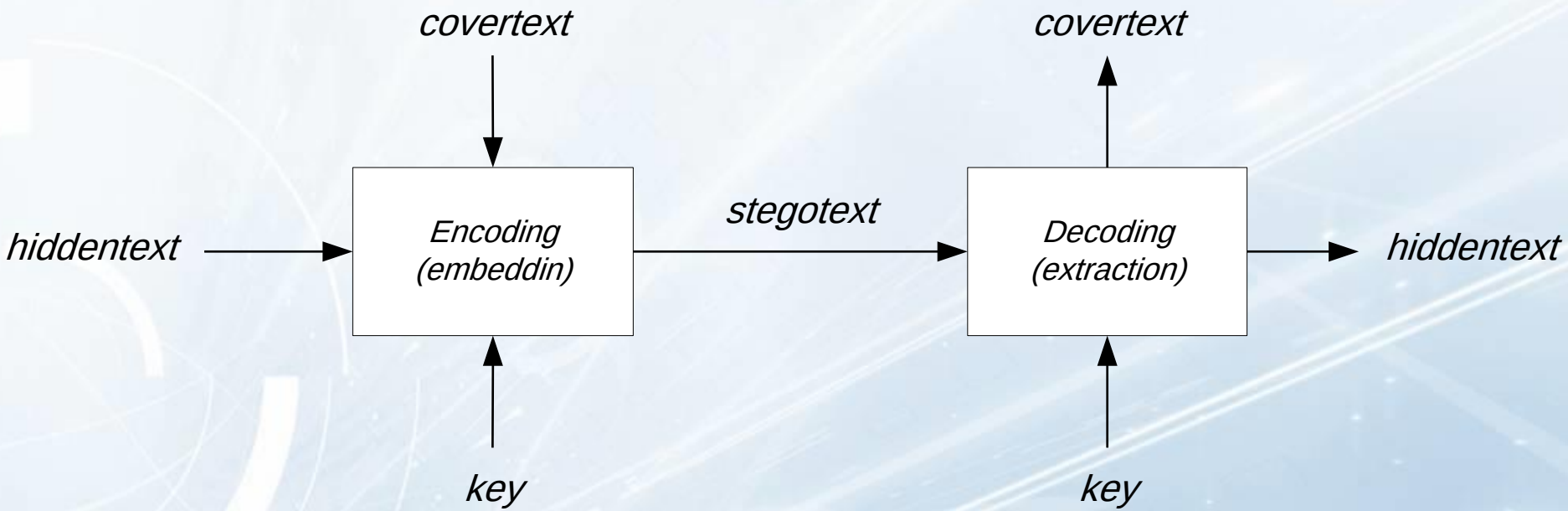
3. Gambar (*image*)

4. Video



Properti Steganografi

1. *Embedded message* (*hiddentext)*: pesan yang disembunyikan.
2. *Cover-object* (*covertext):* pesan yang digunakan untuk menyembunyikan *embedded message*.
3. *Stego-object* (*stegotext):* pesan yang sudah berisi pesan *embedded message*.


covertext
covertext
hiddentext
Encoding
(embeddin)
stegotext
Decoding
(extraction)
hiddentext
key
key

Contoh-contoh:

Lupakan asal rumor itu jangan ambil manfaatnya setelah aku tutup usia

Covertext:

upakan sal umor tu angan mbil anfaatnya etelah ku utup sia

Hiddentext:

Lari jam satu

Stegotext:

Lupakan asal rumor itu jangan ambil manfaatnya setelah aku tutup usia

Pengertian Steganografi

- Steganografi (steganography) adalah teknik menyembunyikan data rahasia di dalam wadah (media) digital, sehingga keberadaan data rahasia tersebut tidak diketahui oleh orang.
- Steganografi membutuhkan dua properti : wadah penampung dan data rahasia yang akan disembunyikan.

- Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya citra suara (audio), teks, dan video.
- Data rahasia yang disembunyikan juga dapat berupa citra, suara, teks, atau video.
- Penggunaan steganografi antara lain bertujuan untuk menyamarkan eksistensi (keberadaan) data rahasia, sehingga sulit dideteksi, dan melindungi hak cipta suatu produk.

- Steganografi dapat dipandang sebagai kelanjutan kriptografi. Jika pada kriptografi data yang telah disandikan (*chipertext*) tetap tersedia, maka dengan steganografi chiperteks dapat disembunyikan sehingga pihak ketiga tidak mengetahui keberadaannya.
- Data rahasia yang disembunyikan dapat diekstraksi kembali persis sama seperti keadaan aslinya.

Sejarah Steganografi

- Steganografi dengan media kepala budak (Herodatus, penguasa Yunani).

  Kepala budak dibotaki, ditulisi pesan, rambut budak dibiarkan tumbuh, budak dikirim.

- Penggunaan tinta tak-tampak (*invisible ink*).

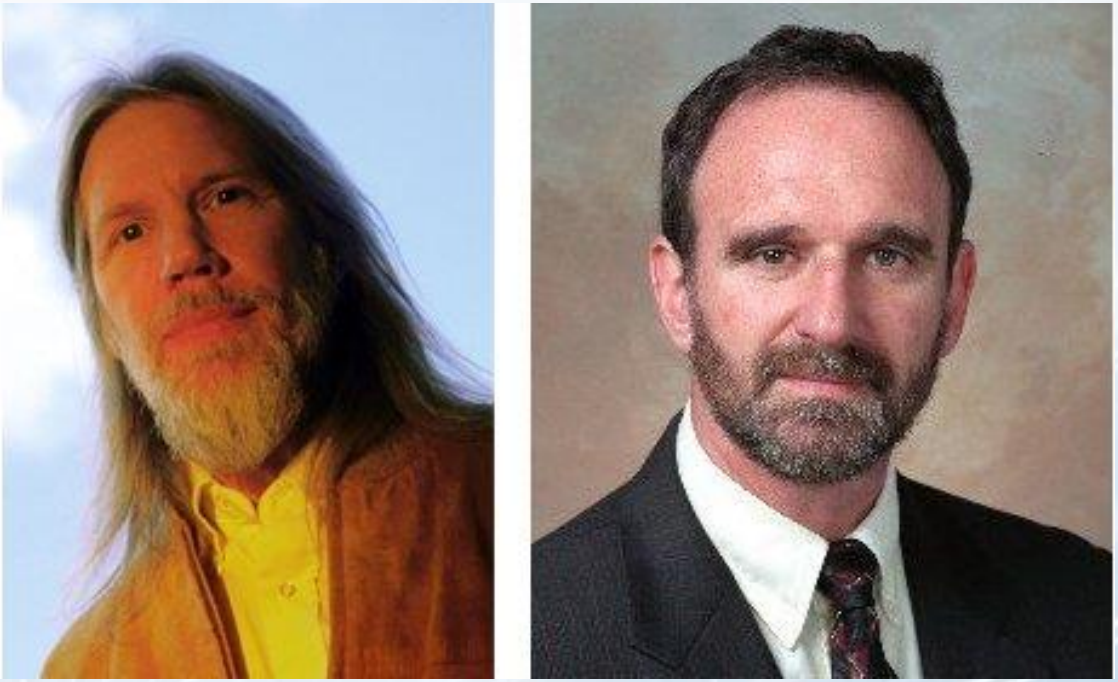
  Tinta dibuat dari campuran sari buah, susu, dan cuka. Tulisan di atas kertas dapat dibaca dengan cara memanaskan kertas tersebut.

Kriptografi

Pendahuluan

- Sampai akhir tahun 1970, hanya ada sistem kriptografi kunci-simetri.
- Satu masalah besar dalam sistem kriptografi: bagaimana mengirimkan kunci rahasia kepada penerima?
- Mengirim kunci rahasia pada saluran publik (telepon, internet, pos) sangat tidak aman.
- Oleh karena itu, kunci harus dikirim melalui saluran kedua yang benar-benar aman.
- Saluran kedua tersebut umumnya lambat dan mahal.

- Ide kriptografi kunci-nirsimetri (*asymmetric-key cryptography*) muncul pada tahun 1976.
- Makalah pertama perihal kriptografi kunci-publik ditulis oleh Diffie-Hellman (ilmuwan dari Stanford University) di IEEE
- Judul makalahnya "*New Directions in Cryptography*".
- Namun pada saat itu belum ditemukan algoritma kriptografi kunci-nirsimetri yang sesungguhnya.



Gambar Whitfield Diffie dan Martin Hellman, penemu kriptografi kunci-publik

KRIPTOGRAFI

Pendahuluan :

- Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga
- Hal ini seiring dengan semakin berkembangnya teknologi jaringan komputer dan internet
- Semakin banyaknya aplikasi yang muncul memanfaatkan teknologi jaringan
- Beberapa aplikasi tersebut menuntut tingkat aplikasi pengiriman data yang aman

Proses Utama pada Kriptografi :

Enkripsi

- adalah proses dimana informasi/data yang hendak
- dikirim diubah menjadi bentuk yang hampir tidak
- dikenali sebagai informasi awalnya dengan
- menggunakan algoritma tertentu

Dekripsi

- adalah kebalikan dari enkripsi yaitu mengubah kembali
- bentuk tersamar tersebut menjadi informasi awal

Istilah dalam Kriptografi :

Berikut adalah istilah-istilah yang digunakan dalam bidang kriptografi :

- **Plaintext** (M) adalah pesan yang hendak dikirimkan (berisi data asli).
- **Ciphertext** (C) adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.
- **Enkripsi** (fungsi E) adalah proses pengubahan *plaintext* menjadi *ciphertext*.
- **Dekripsi** (fungsi D) adalah kebalikan dari enkripsi yakni mengubah *ciphertext* menjadi *plaintext*, sehingga berupa data awal/asli.
- **Kunci** adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.

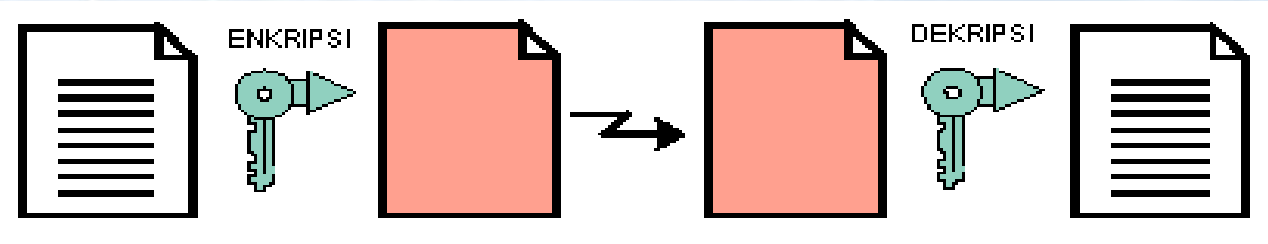
Algoritma Kriptografi :

- Berdasarkan jenis kunci yang digunakan :
  - Algoritma Simetris
  - Algoritma Asimetris
- Berdasarkan besar data yang diolah :
  - Algoritma Block Cipher
  - Algoritma Stream Cipher

Algoritma Simetris

- Algoritma Simetris

Algoritma simetris *(symmetric algorithm)* adalah suatu algoritma dimana kunci enkripsi yang digunakan sama dengan kunci dekripsi sehingga algoritma ini disebut juga sebagai *single-key algorithm.*



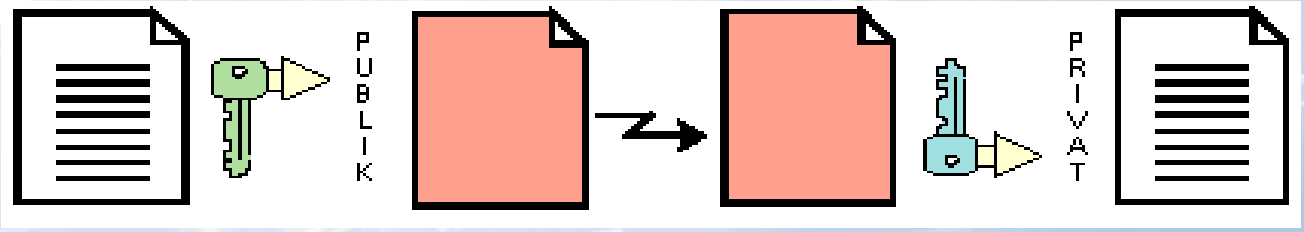
Algoritma Simetris

- Kelebihan algoritma simetris :
  - Kecepatan operasi lebih tinggi bila dibandingkan dengan algoritma asimetrik.
  - Karena kecepatannya yang cukup tinggi, maka dapat digunakan pada sistem *real-time*
- Kelemahan algoritma simetris :
  - Untuk tiap pengiriman pesan dengan pengguna yang berbeda dibutuhkan kunci yang berbeda juga, sehingga akan terjadi kesulitan dalam manajemen kunci tersebut.
  - Permasalahan dalam pengiriman kunci itu sendiri yang disebut *"key distribution problem"*

Algoritma Asimetris

- Algoritma Asimetris

Algoritma asimetris *(asymmetric algorithm)* adalah suatu algoritma dimana kunci enkripsi yang digunakan tidak sama dengan kunci dekripsi. Pada algoritma ini menggunakan dua kunci yakni kunci publik *(public key)* dan kunci privat *(private key).* Kunci publik disebarkan secara umum sedangkan kunci privat disimpan secara rahasia oleh si pengguna. Walau kunci publik telah diketahui namun akan sangat sukar mengetahui kunci privat yang digunakan.



Algoritma Asimetris

- Kelebihan algoritma asimetris :
  - Masalah keamanan pada distribusi kunci dapat lebih baik
  - Masalah manajemen kunci yang lebih baik karena jumlah kunci yang lebih sedikit

- Kelemahan algoritma asimetris :
  - Kecepatan yang lebih rendah bila dibandingkan dengan algoritma simetris
  - Untuk tingkat keamanan sama, kunci yang digunakan lebih panjang dibandingkan dengan algoritma simetris.

Block Cipher dan Stream Ciper

- Block Cipher

  algoritma kriptografi ini bekerja pada suatu data yang berbentuk blok/kelompok data dengan panjang data tertentu (dalam beberapa byte), jadi dalam sekali proses enkripsi atau dekripsi data yang masuk mempunyai ukuran yang sama.

- Stream Cipher

  algoritma yang dalam operasinya bekerja dalam suatu pesan berupa bit tunggal atau terkadang dalam suatu byte, jadi format data berupa aliran dari bit untuk kemudian mengalami proses enkripsi dan dekripsi.

Pendahuluan

- Algoritma kriptografi klasik berbasis karakter
- Menggunakan pena dan kertas saja, belum ada komputer
- Termasuk ke dalam kriptografi kunci-simetri
- Algoritma kriptografi klasik:
  - *Cipher* Substitusi (*Substitution Ciphers*)
  - *Cipher* Transposisi (*Transposition Ciphers*)

1. Cipher Substitusi

- Monoalfabet : setiap karakter chipertext menggantikan satu macam karakter plaintext
- Polyalfabet : setiap karakter chipertext menggantikan lebih dari satu macam karakter plaintext
- Monograf /unilateral: satu enkripsi dilakukan terhadap satu karakter plaintext
- Polygraf /multilateral: satu enkripsi dilakukan terhadap lebih dari satu karakter plaintext

Cipher Substitusi - Caesar Cipher

- Tiap huruf alfabet digeser 3 huruf ke kanan

p_i : 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
c_i : **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**

- Contoh:

  Plainteks: AWASI ASTERIX DAN TEMANNYA OBELIX

  Cipherteks: **DZDVL DVWHULA GDQ WHPDQQBA REHOLA**

Cipher Substitusi - Caesar Cipher

- Dalam praktek, cipherteks dikelompokkan ke dalam kelompok n-huruf, misalnya kelompok 4-huruf:

  DZDV LDVW HULA GDQW HPDQ QBAR EHOL A

- Atau membuang semua spasi:

  DZDVLDVWHULAGDQWHPDQQBAREHOLA

- Tujuannya agar kriptanalisis menjadi lebih sulit

Cipher Substitusi - *Vigènere Cipher*

- Termasuk ke dalam cipher abjad-majemuk (polyalpabetic substitution cipher).
- Algoritma tersebut baru dikenal luas 200 tahun kemudian yang oleh penemunya cipher tersebut kemudian dinamakan Vigènere Cipher.
- Vigènere Cipher menggunakan Bujursangkar Vigènere untuk melakukan enkripsi.
- Setiap baris di dalam bujursangkar menyatakan huruf-huruf cipherteks yang diperoleh dengan Caesar Cipher.

Cipher Substitusi - *Vigènere Cipher*

Kunci \ Plainteks	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

Gambar 4.2 Bujursangkar *Vigènere*

Cipher Substitusi - *Vigènere Cipher*

- Contoh penerapan Vigènere Cipher :

  Plainteks : THIS PLAINTEXT

  Kunci : sony sonysonys

  Cipherteks : **LVVQ HZNGFHRVL**

- Jika panjang kunci lebih pendek daripada panjang plainteks, maka kunci diulang secara periodik. Dalam hal ini Kunci "sony" diulang sebanyak panjang plaintext-nya
- Pada dasarnya, setiap enkripsi huruf adalah *Caesar cipher* dengan kunci yang berbeda-beda.

  c('T') = ('T' + 's') mod 26 = L

  T = 20 dan s= 19 → (20+19)%26=13 → L

  c('H') = ('H' + 'o') mod 26 = V, dst

- INDONESIA TANAH AIR BETA
- INDON
- ESIAT
- ANAHA
- IRBET
- A

- IEAIANSNRDIABOAHENTAT
- I N
- E
- A
- I
- A

Plainteks

Kunci	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

Gambar 4.2 Bujursangkar *Vigènere*

Cipher Transposisi

- Cipherteks diperoleh dengan mengubah posisi huruf di dalam plainteks.
- Dengan kata lain, algoritma ini melakukan *transpose* terhadap rangkaian huruf di dalam plainteks.
- Nama lain untuk metode ini adalah **permutasi**, karena *transpose* setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut.

Cipher Transposisi (Contoh)

Contoh: Misalkan plainteks adalah

PENDIDIKAN TEKNIK ELEKTRONIKA UNIVERSITAS NEGERI YOGYAKARTA

Enkripsi:

PENDIDI
KANTEKN
IKELEKT
RONIKAU
NIVERSI
TASNEGE
RIYOGYA
KARTA

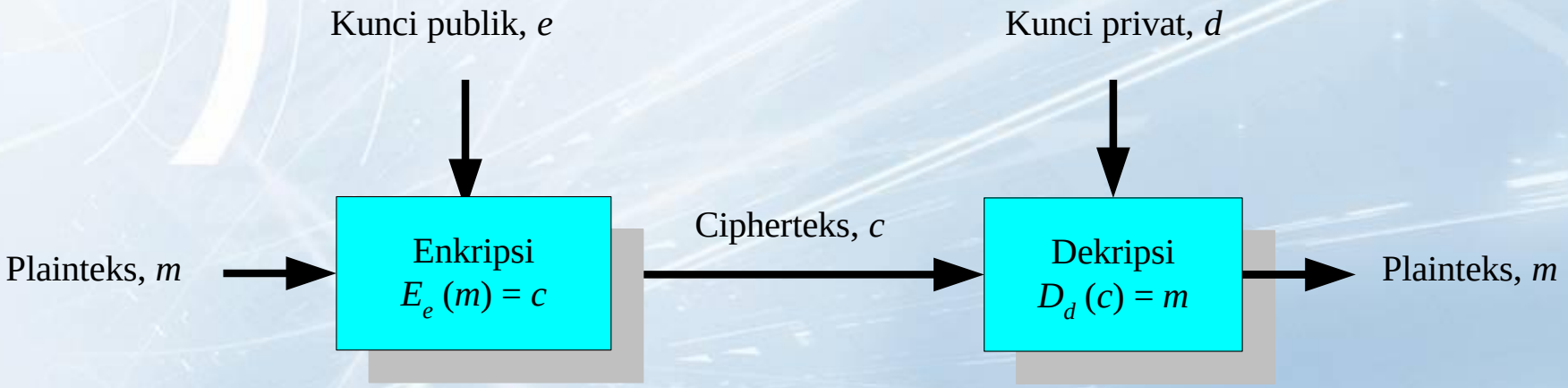
Cipherteks: (baca secara vertikal)

PKIRNTRKEAKOIAIANNENVSYRDTLIENOTIEEKREGADKKASGYINTUIEA

PKIRN TRKEA KOIAI ANNEN VSYRD TLIEN OTIEE KREGA DKKAS GYINT UIEA

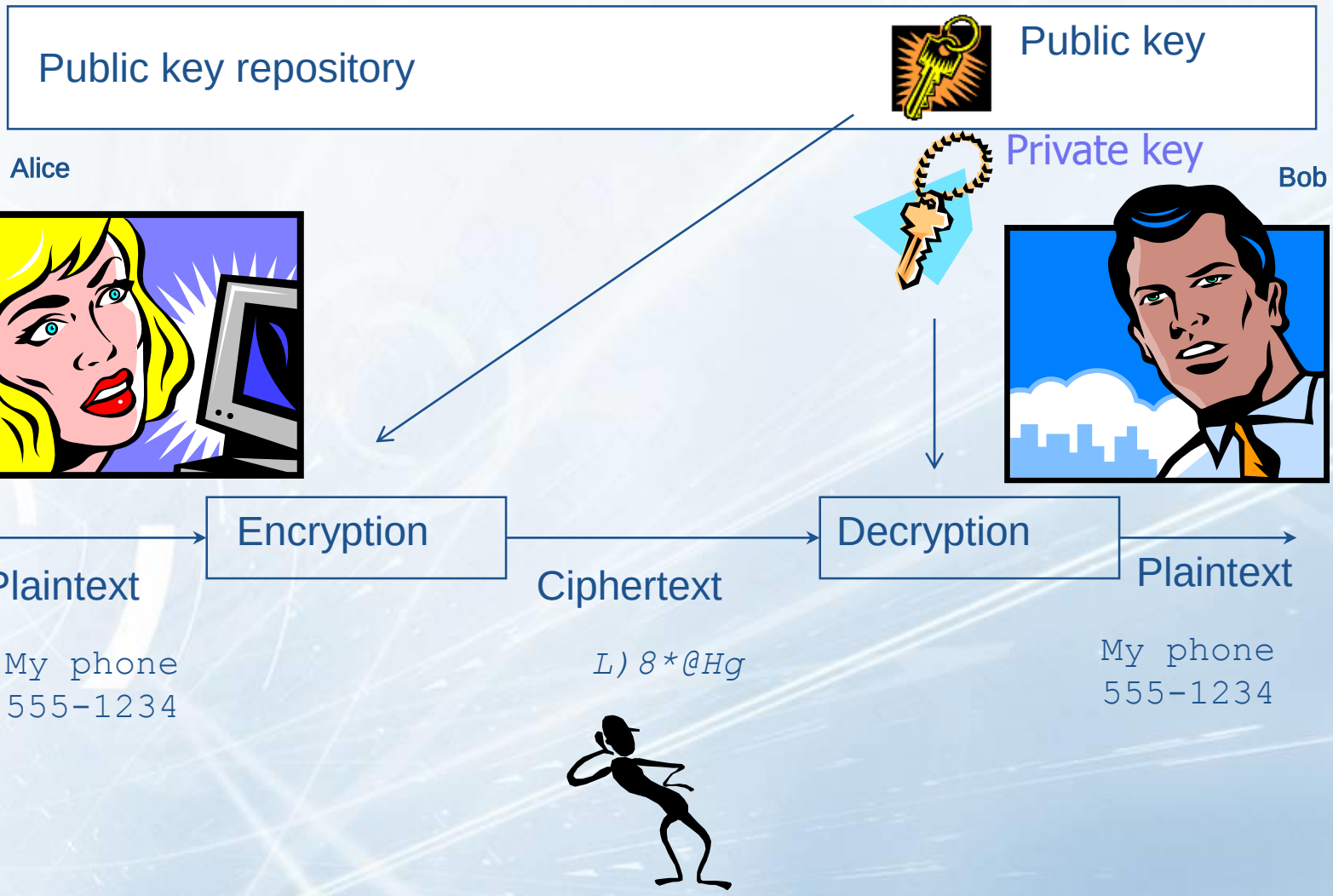
Kunci Private dan Kunci Publik

- Kriptografi kunci-nirsimtri disebut juga kriptografi kunci-publik
- Pada kriptografi kunci-publik, masing-masing pengirim dan penerima mempunyai sepasang kunci:
  1. Kunci publik: untuk mengenkripsi pesan
  2. Kunci privat: untuk mendekripsi pesan.
- $E_e(m) = c$ dan $D_d(c) = m$

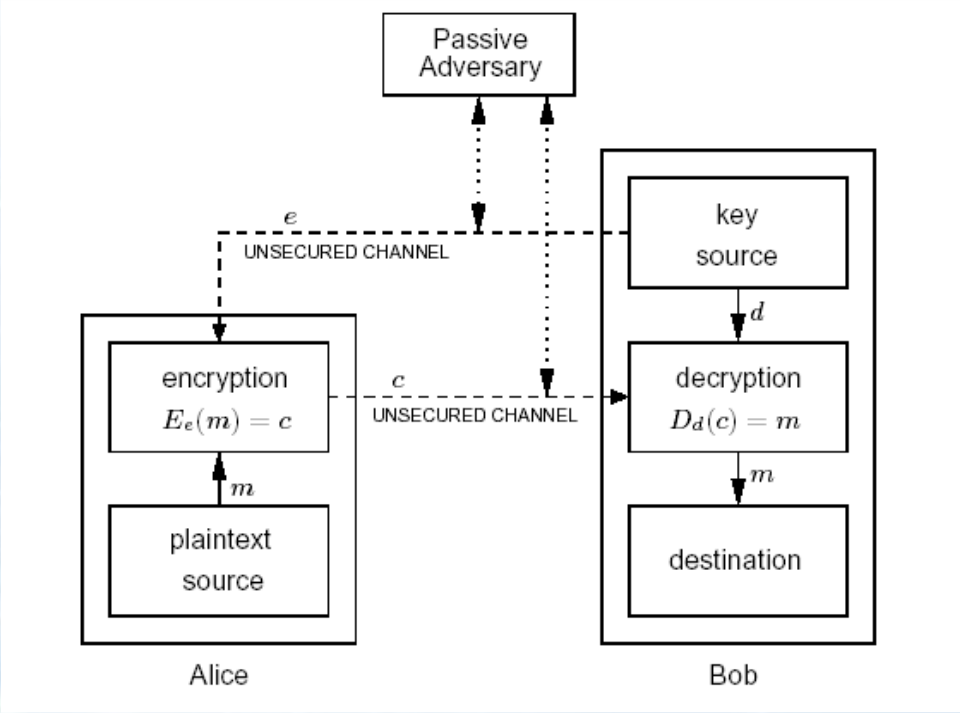


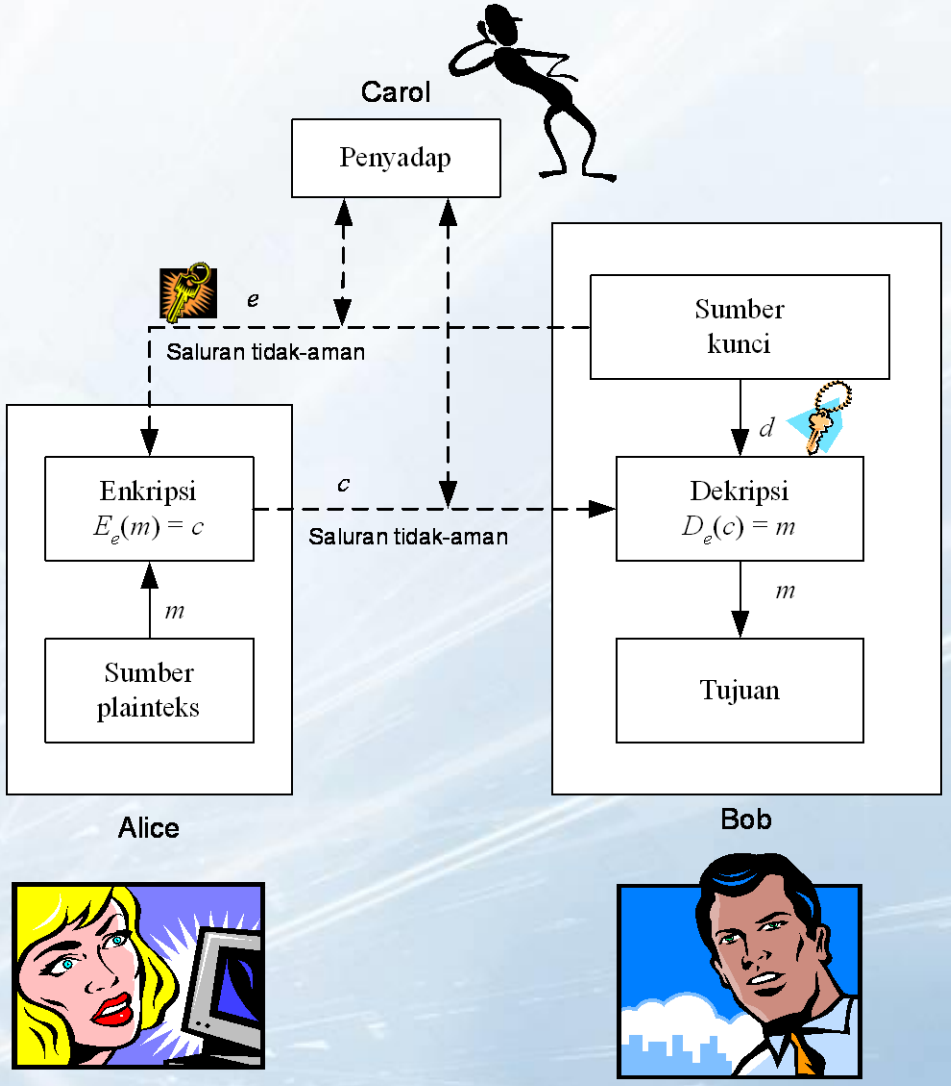
- Misalkan: Pengirim pesan: Alice
  Penerima pesan: Bob
- Alice mengenkripsi pesan dengan kunci publik Bob
- Bob mendekripsi pesan dengan kunci privatnya (kunci privat Bob)
- Sebaliknya, Bob mengenkripsi pesan dengan kunci publik Alice
- Alice mendekripsi pesan dengan kunci privatnya (kunci privat Alice)
- Dengan mekanisme seperti ini, tidak ada kebutuhan mengirimkan kunci rahasia (seperti halnya pada sistem kriptografi simetri

Kriptografi Kunci-publik
(http://budi.insan.co.id/courses/ec7010)



- Kunci enkripsi dapat dikirim melalui saluran yang tidak perlu aman (*unsecure channel*).
- Saluran yang tidak perlu aman ini mungkin sama dengan saluran yang digunakan untuk mengirim cipherteks.




Carol
Penyadap
e
Saluran tidak-aman
Sumber
kunci
d
Enkripsi
$E_e(m) = c$
c
Saluran tidak-aman
Dekripsi
$D_e(c) = m$
m
m
Sumber
plainteks
Tujuan
Alice
Bob

Dua keuntungan kriptografi kunci-publik:

1. Tidak diperlukan pengiriman kunci rahasia
2. Jumlah kunci dapat ditekan

- Kriptografi kunci-publik didasarkan pada fakta:
  1. Komputasi untuk enkripsi/dekripsi pesan mudah dilakukan.
  2. Secara komputasi hampir tidak mungkin (*infeasible*) menurunkan kunci privat, *d*, bila diketahui kunci publik, *e*.

- Analogi kriptografi kunci-simetri dan kriptografi kunci-publik dengan kotak surat yang dapat dikunci dengan gembok.
- Kriptografi kunci-simetri: Alice dan Bob memiliki kunci gembok yang sama
- Kriptografi kunci-publik: Bob mengirimi Alice gembok dalam keadaan tidak terkunci (gembok = kunci publik Bob, kunci gembok = kunci privat Bob).

Kelebihan kriptografi kunci-simetri:

1. Proses enkripsi/dekripsi membutuhkan waktu yang singkat.
2. Ukuran kunci simetri relatif pendek
3. Otentikasi pengirim pesan langsung diketahui dari cipherteks yang diterima, karena kunci hanya diketahui oleh pengirim dan penerima pesan saja.

Kelemahan kriptografi kunci-simetri:

1. Kunci simetri harus dikirim melalui saluran yang aman. Kedua entitas yang berkomunikasi harus menjaga kerahasiaan kunci ini.
2. Kunci harus sering diubah, mungkin pada setiap sesi komunikasi.

Kelebihan kriptografi kunci-publik:

1. Hanya kunci privat yang perlu dijaga kerahasiaannya oleh seiap entitas yang berkomuniaksi. Tidak ada kebutuhan mengirim kunci kunci privat sebagaimana pada sistem simetri.
2. Pasangan kunci publik/kunci privat tidak perlu diubah, bahkan dalam periode waktu yang panjang.
3. Dapat digunakan untuk mengamankan pengiriman kunci simetri.
4. Beberapa algoritma kunci-publik dapat digunakan untuk memberi tanda tangan digital pada pesan (akan dijelaskan pada materi kuliah selanjutnya)

Kelemahan kriptografi kunci-publik:

1. Enkripsi dan dekripsi data umumnya lebih lambat daripada sistem simetri, karena enkripsi dan dekripsi menggunakan bilangan yang besar dan melibatkan operasi perpangkatan yang besar.
2. Ukuran cipherteks lebih besar daripada plainteks (bisa dua sampai empat kali ukuran plainteks).
3. Ukuran kunci relatif lebih besar daripada ukuran kunci simetri.

4. Karena kunci publik diketahui secara luas dan dapat digunakan setiap orang, maka cipherteks tidak memberikan informasi mengenai otentikasi pengirim.
5. Tidak ada algoritma kunci-publik yang terbukti aman (sama seperti *block cipher*).

   Kebanyakan algoritma mendasarkan keamanannya pada sulitnya memecahkan persoalan-persoalan aritmetik (pemfaktoran, logaritmik, dsb) yang menjadi dasar pembangkitan kunci.

Aplikasi Kriptografi Kunci-Publik

- Meskipun masih berusia relatif muda (dibandingkan dengan algoritma simetri), tetapi algoritma kunci-publik mempunyai aplikasi yang sangat luas:
  1. **Enkripsi/dekripsi pesan**

     Algoritma: *RSA*, *Rabin*, *ElGamal*
  2. ***Digital signatures***

     Tujuan: membuktikan otentikasi pesan/pengirim

     Algoritma: *RSA*, *ElGamal*, *DSA, GOST*
  3. **Pertukaran kunci (*key exchange*)**

     Tujuan: mempertukarkan kunci simetri

     Algoritma: Diffie-Hellman