Rekayasa Internet

Susmini I. Lestariningati, M.T

Pengantar Kriptografi

Pengantar Kriptografi

- Message (Pesan) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya.
  - Nama lain : **Plainteks** (*plaintext*) atau **teks-jelas** (*cleartext*)
- Bentuk/rupa pesan : teks, gambar, audio, musik, video, dan lain-lain
- Pesan ada yang:
  - dikirim (via pos, kurir, saluran telekomunikasi, dan lain-lain)
  - disimpan didalam media penyimpanan/storage berupa disk, kaset, dan lain-lain.

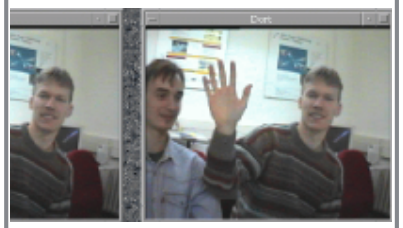
Teks

"Kita semua bersaudara"

Gambar

Audio

Video



Terminologi

- **Pengirim (sender)** : pihak yang mengirim pesan
- **Penerima (receiver)** : pihak yang menerima pesan
- Pengirim dan penerima bisa berupa orang, komputer, mesin, dan lain-lain
- Pengirim ingin pesan yang dikirim secara aman, dimana pihak lain tidak dapat membaca/ memanipulasi pesan
- Contoh: pengirim = Alice , penerima = Bob

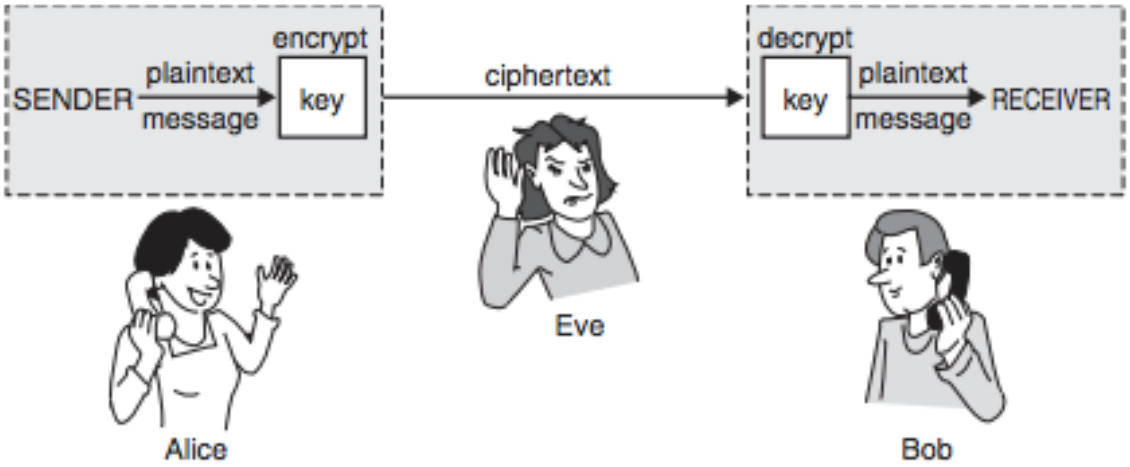
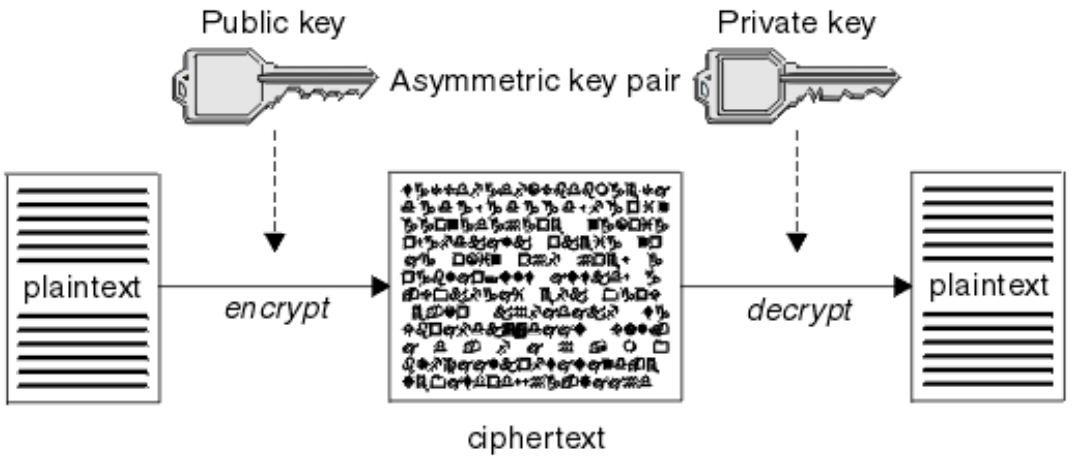


FIGURE 5.6 Standard cryptographic scenario. Alice wants to send a message to Bob. She encrypts it using a secret key. Bob decrypts it using his copy of the key. Eve is an eavesdropper. She intercepts the coded message in transit, and tries to decrypt it.

- **Cipherteks (ciphertext)**: pesan yang telah disandikan sehingga tidak bermakna lagi.
  - Tujuan: agar pesan tidak dapat dibaca oleh pihak yang tidak berhak.
  - Nama lain: kriptogram (cryptogram)
- Cipherteks harus dapat dikembalikan menjadi plainteks semula



plaintext	ciphertext
culik anak itu jam 11 siang	`t^$gfUi89rewoFpfdWqL:p[uTcxZ`

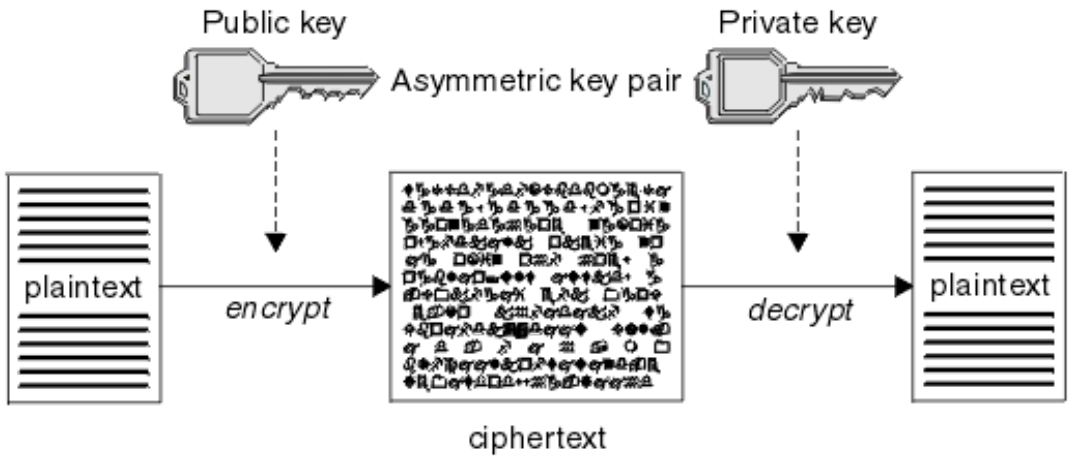
```
Ketika saya berjalan-jalan
di pantai, saya menemukan
banyak sekali kepiting yang
merangkak menuju laut.
Mereka adalah anak-anak
kepiting yang baru menetas
dari dalam pasir. Naluri
mereka mengatakan bahwa laut
adalah tempat kehidupan
mereka.
```

(a) Plainteks (teks)

```
Ztâxzp/épêp/qtüyp{p}<yp{p}/sx/ p}âpx;
  épêp/|t}t|äzp}/qp}êpz/étzp{x/zt xâx
}v  êp}v/|tüp}vzpz/|t}äyä/{päâ=/\tütz
p  psp{pw/p}pz<p}pz/zt xâx}v/êp}
v/qpüä  |t}tâpé/spüx/sp{p|/ péxü=/]
p{äüx  |ttüzp/|t}vpâpzp}/qpwåp/{päâ
/psp{pw  ât| pâ/ztwxsä p}/|tützp=
```

(b) Cipherteks dari (a)

Terminologi



- **Enkripsi (encryption)**: proses menyandikan plainteks menjadi cipherteks.
  - Nama lain: enciphering
- **Dekripsi (decryption):** Proses mengembalikan cipherteks menjadi plainteks semula.
  - Nama lain: deciphering

Notasi Matematis

- Misalkan:

  C = chiperteks

  P = plainteks

- Fungsi enkripsi E memetakan P ke C,

  E(P) = C

- Fungsi dekripsi D memetakan C ke P,

  D(C) = P

- Fungsi enkripsi dan dekripsi harus memenuhi sifat:

  D(E(P)) = P

Kriptografi

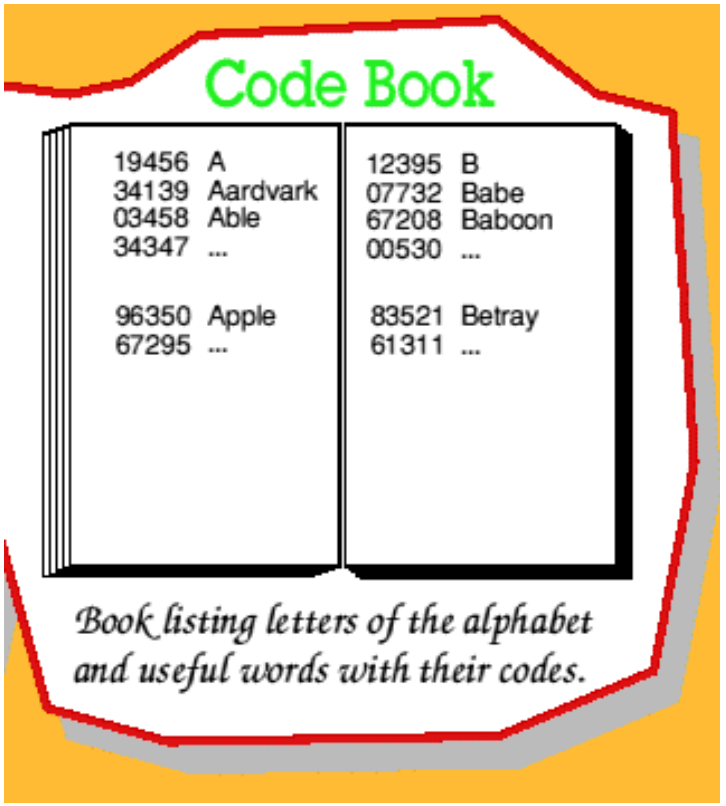
- Kata cryptography berasal dari bahasa Yunani: κρυπτο (hidden atau secret) dan γραφη (writing)
  - Artinya “secret writing”
- **Definisi lama:**
  - Kriptografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya.
- **Definisi baru:**
  - Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (message) [Schneier, 1996].

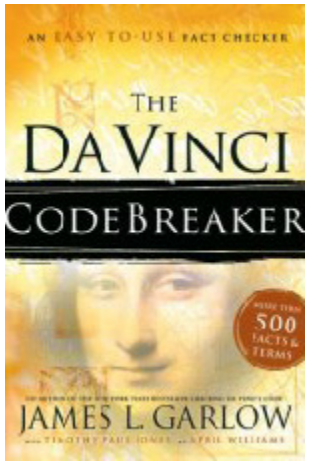
“art and science to keep message secure”

- Algoritma kriptografi (cipher)
  - aturan untuk enchipering dan dechipering, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi pesan.

Encoding vs Decoding

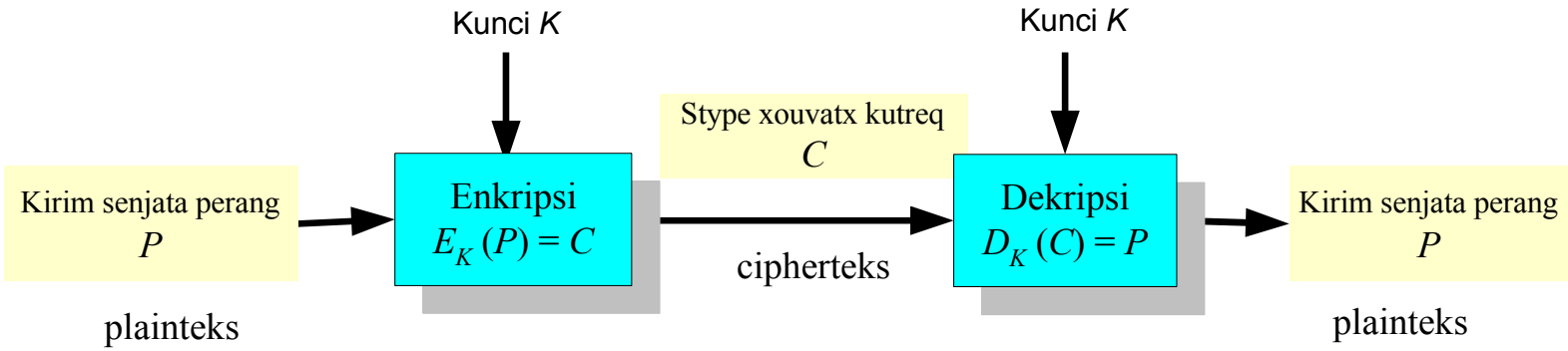
- Encoding: Transformasi dari plainteks menjadi kode
- Decoding: transformasi kebalikan dari kode menajdi plainteks.
- Buku kode (codebook): dokumen yang digunakan untuk mengimplementasikan suatu kode
- Buku kode terdiri dari tabel lookup (lookup table) untuk encoding dan decodingCodebreaker:
- Orang yang memecahkan kode (untuk menemukan plainteks)





Terminologi Kunci (Key)

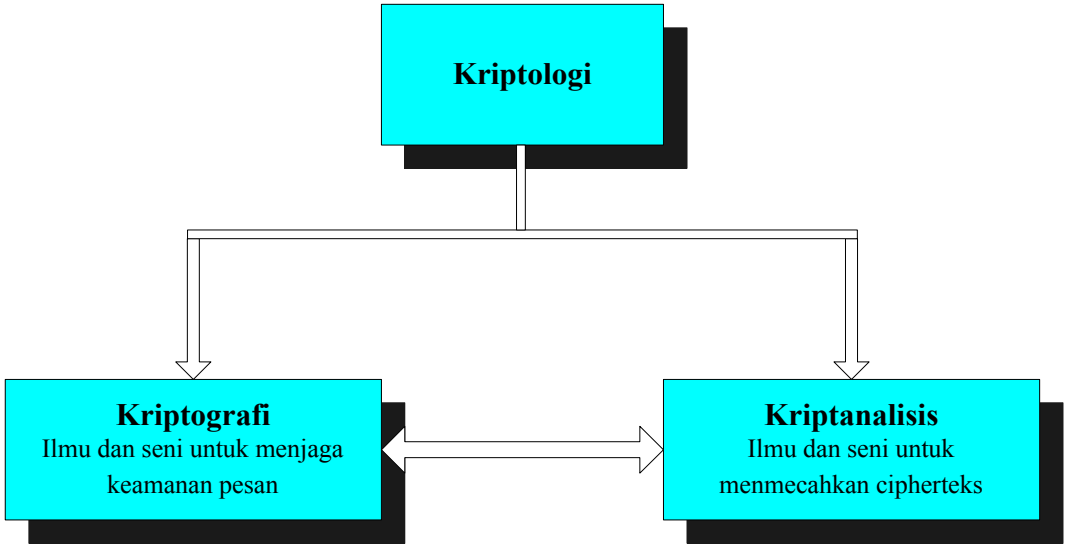
- Kunci: parameter yang digunakan untuk transformasi enciphering dan dechipering
- Jika kekuatan kriptografi ditentukan dengan menjaga kerahasiaan algoritmanya, maka algoritma kriptografinya dinamakan algoritma restricted
- Algoritma resricted tidak cocok lagi saat ini
- Kriptografi modern mengatasi masalah ini dengan menggunakan kunci.
- Kunci bersifat rahasia (secret), sedangkan algoritma kriptografi tidak rahasia (public)



- Enkripsi dan dekripsi dengan kunci:
  - Enkripsi: $E_K(P) = C$
  - Dekripsi: $D_K(C) = P$
  - Harus dipenuhi: $D_K(E_K(P)) = P$

Kriptologi

- **Kriptologi (cryptology):** studi mengenai kriptografi dan kriptanalisis.



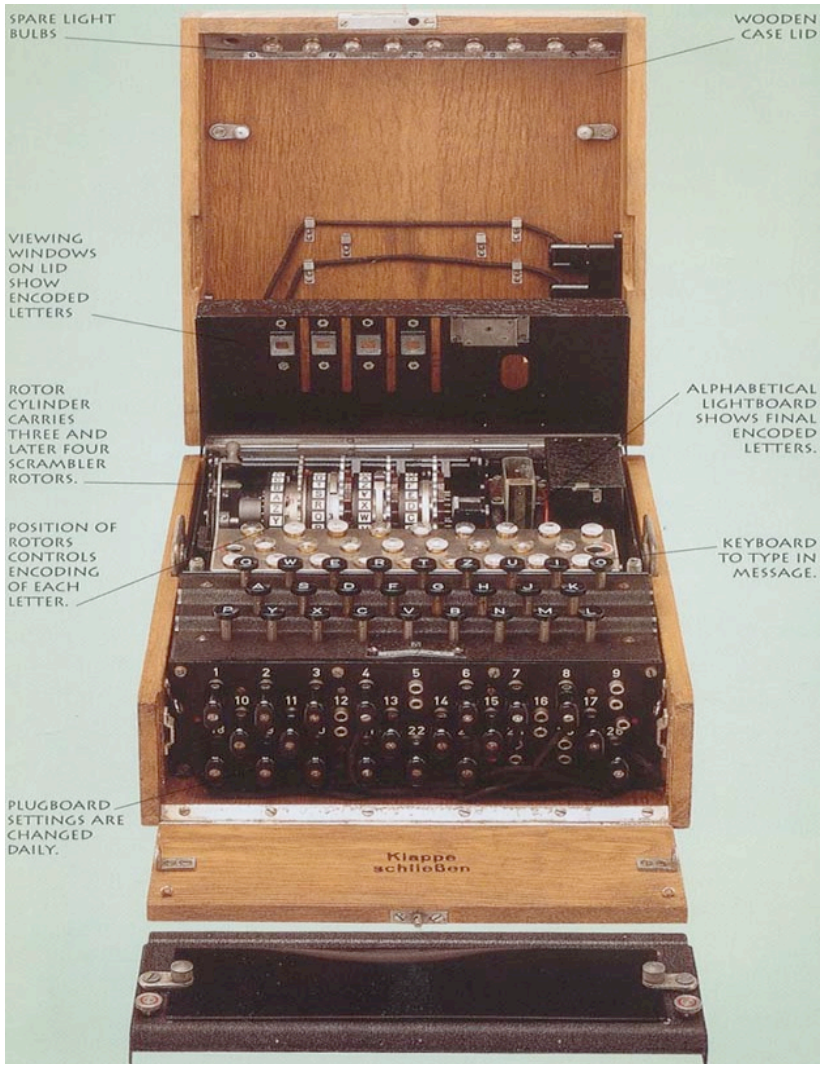
- Persamaan kriptografer dan kriptanalis:
  - Keduanya sama-sama menerjemahkan cipherteks menjadi plainteks
- Perbedaan kriptografer dan kriptanalis:
  - Kriptografer bekerja atas legitimasi pengirim atau penerima pesan
  - Kriptanalis bekerja tanpa legitimasi pengirim atau penerima pesan

Sejarah Kriptografi

- Kriptografi mempunyai sejarah yang panjang.
- Tercatat Bangsa Mesir 4000 tahun yang lalu menggunakan hieroglyph yang tidak standard untuk menulis pesan

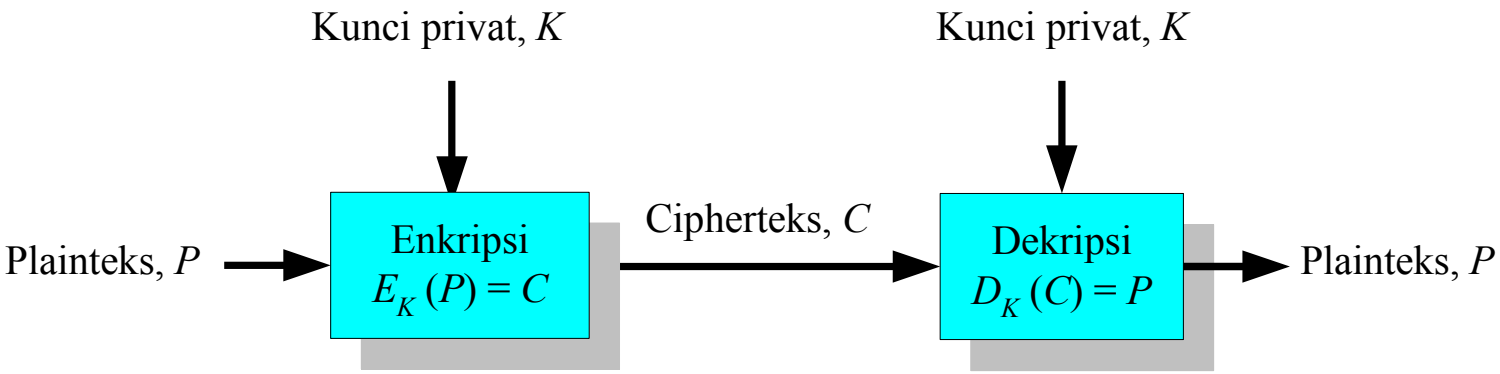
Sejarah Kriptografi

- Perang Dunia ke II, Pemerintah Nazi Jerman membuat mesin enkripsi yang dinamakan Enigma.
- Enigma cipher berhasil dipecahkan oleh pihak Sekutu.
- Keberhasilan memecahkan Enigma sering dikatakan sebagai faktor yang memperpendek perang dunia ke-2



Kriptografi Kunci-Simetri

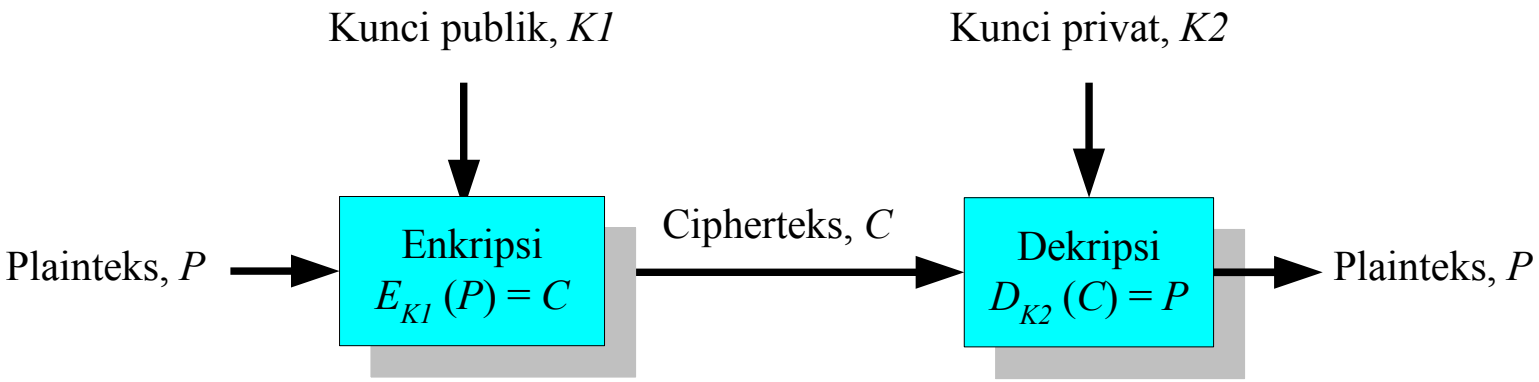
- Symmetric-key cryptography
  - Kunci enkripsi = kunci dekripsi
- Istilah lainnya: kunci simetri, kunci privat, kunci rahasia (secret key)
- Algoritma kriptografinya disebut algoritma simetri
- Istilah lainnya: algoritma konvensional



- Contoh algoritma simetri: DES (Data Encryption Standard), Rijndael, Blowfish, IDEA, GOST, Serpent, RC2, RC4, RC5, dan lain sebagainya.

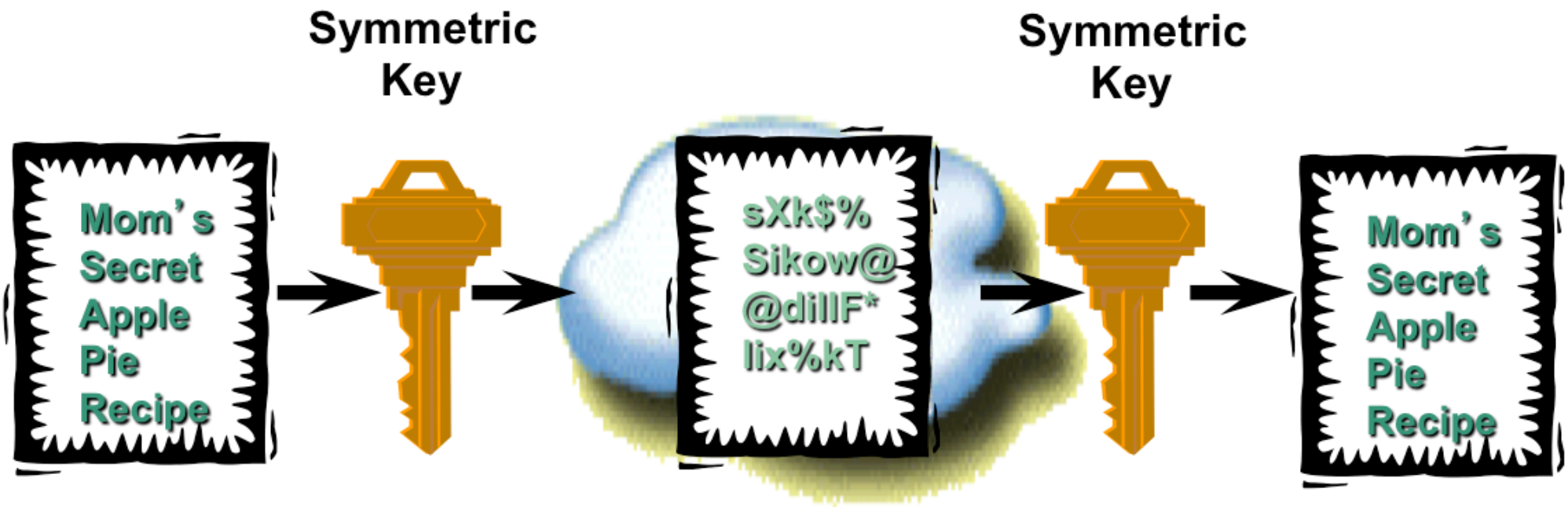
Kriptografi Kunci Asimetri

- Asymmetric-key cryptography
  - Kunci enkripsi ≠ kunci dekripsi
- Nama lain: kriptografi kunci-publik
  - karena kunci enkripsi bersifat publik (**public key**) sedangkan kunci dekripsi bersifat rahasia (**secret key** atau **private key**).



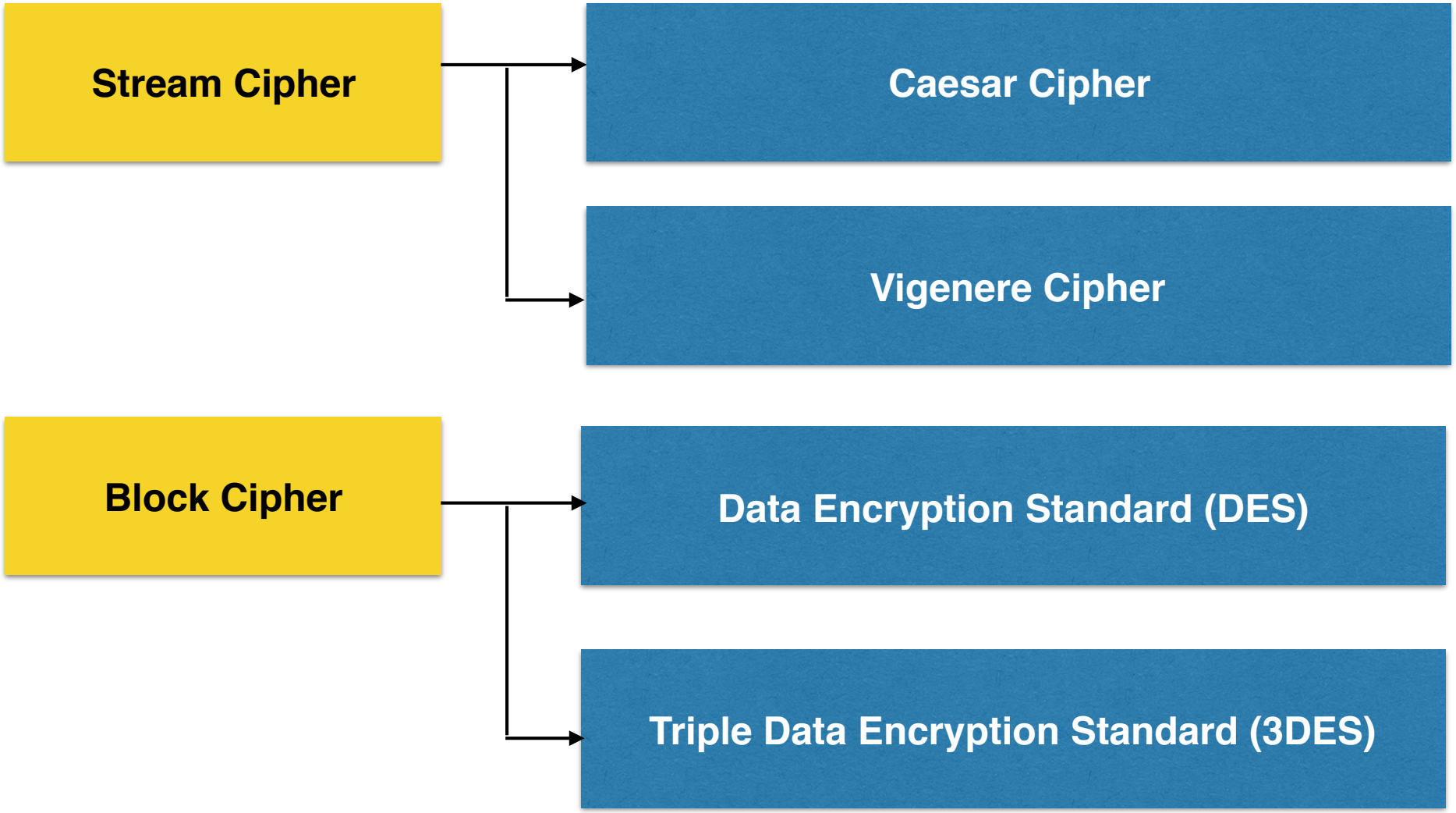
Symmetric v/s Asymmetric

Characteristic	Symmetric Key Cryptography	Asymmetric Key Cryptography
Key used for encryption / decryption	Same key is used for encryption and decryption	One key used for encryption and another, different key is used for decryption
Speed of encryption / decryption	Very fast	Slower
Size of resulting encrypted text	Usually same as or less than the original clear text size	More than the original clear text size
Key agreement / exchange	A big problem	No problem at all
Number of keys required as compared to the number of participants in the message exchange	Equals about the square of the number of participants, so scalability is an issue	Same as the number of participants, so scales up quite well
Usage	Mainly for encryption and decryption (confidentiality), cannot be used for digital signatures (integrity and non-repudiation checks)	Can be used for encryption and decryption (confidentiality) as well as for digital signatures (integrity and non-repudiation checks)



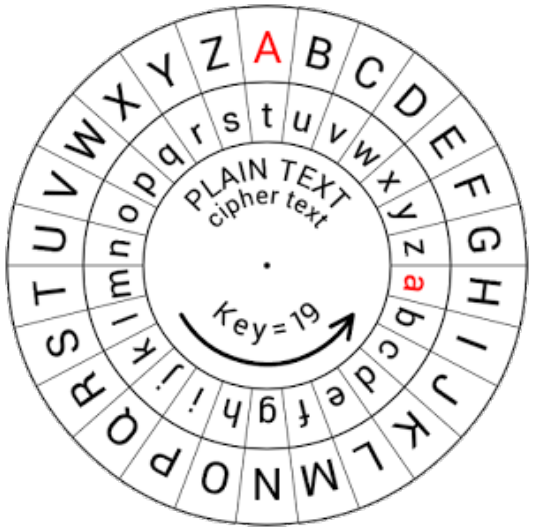
SYMMETRIC KEY ALGORITHM

Symmetric Key Algorithm



Caesar Cipher

- Dalam kriptografi, sandi Caesar, atau sandi geser, kode Caesar atau Geseran Caesar adalah salah satu teknik enkripsi paling sederhana dan paling terkenal. Sandi ini termasuk sandi substitusi dimana setiap huruf pada teks terang (plaintext) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet.
- Algoritma cipher substitusi yang menggunakan konsep pergeseran huruf dengan modulo 26. Secara matematis dapat dirumuskan sebagai:
  - **C = E(M) = (M+K) mod 26**
  - M = Message, K = Key



Caesar Cipher

$$c_i = E(p_i) = p_i + 3$$

A full translation chart of the Caesar cipher is shown here.

Plaintext	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
Ciphertext	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

Using this encryption, the message

TREATY IMPOSSIBLE

would be encoded as

T	R	E	A	T	Y		I	M	P	O	S	S	I	B	L	E
w	u	h	d	w	b		l	p	s	r	v	v	l	e	o	h

Vigenere Cipher

- **Vigenere Cipher** adalah suatu algoritma kriptografi klasik yang ditemukan oleh Giovan Battista Bellaso. Beliau menuliskan metodenya tersebut pada bukunya yang berjudul La Cifra del. Sig. Giovan Battista Bellaso pada tahun 1553.
- Nama vigenere sendiri diambil dari seorang yang bernama Blaise de Vigenere. Nama vigenere diambil sebagai nama algoritma ini karena beliau menemukan kunci yang lebih kuat lagi untuk algoritma ini dengan metode autokey cipher meskipun algoritma dasarnya telah ditemukan lebih dahulu oleh Giovan Battista Bellaso.
- Teknik ini menggunakan tabel bujur sangkat yang berisi kombinasi dari plaintext pada kolom, serta kunci pada baris. Kombinasi keduanya akan menghasilkan cipher pada baris dan kolom

Tabel Vigenere

	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	D
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	C
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	B
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

Cara Kerja Vignere Cipher

1. Langkah awal adalah tuliskan plainteks yang ingin di enkripsi dengan menghilangkan spasi antar kata, hal ini untuk mempersulit orang untuk menebak dari plaintext tersebut.

   contoh :

   - plaintext: BELAJAR REKAYASA INTERNET
   - dengan menghilangkan spasi: BELAJARREKAYASAINTERNET

2. Pilih kunci (key) yang akan disepakati oleh pengirim serta penerima

   contoh :

   - Key: TEKKOM

3. Susunlah plaintext dengan kunci sebagaimana berikut:

PLAINTEXT	B	E	L	A	J	A	R	R	E	K	A	Y	A	S	A	I	N	T	E	R	N	E	T
KEY	T	E	K	K	O	M	T	E	K	K	O	M	T	E	K	K	O	M	T	E	K	K	O

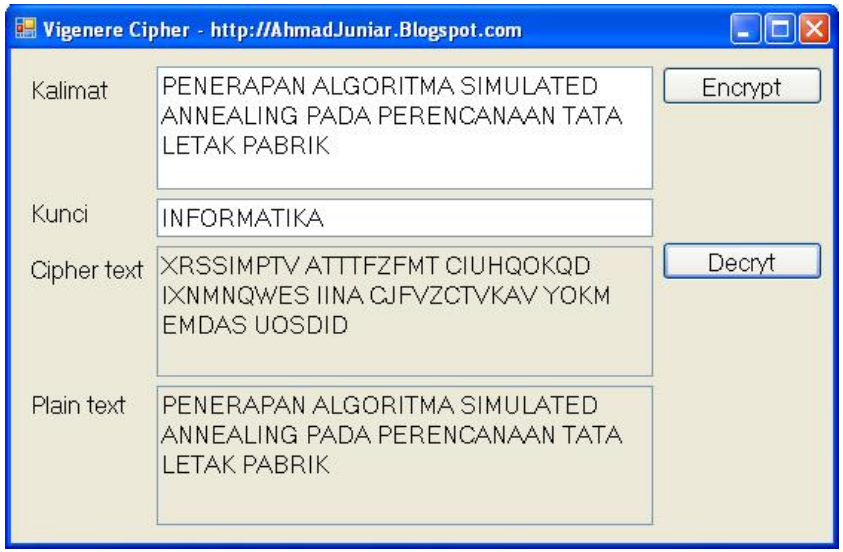
4. Dengan menggunakan tabel Vigenere maka kita akan mendapatkan hasil ciphertext sebagaimana berikut:

PLAINTEXT	B	E	L	A	J	A	R	R	E	K	A	Y	A	S	A	I	N	T	E	R	N	E	T
KEY	T	E	K	K	O	M	T	E	K	K	O	M	T	E	K	K	O	M	T	E	K	K	O
CIPHERTEXT	U	I	V	K	X	M	K	V	O	U	O	K	T	W	K	S	B	F	X	V	X	O	H

Maka hasilnya adalah sebagaimana berikut:

- plaintext : BELAJAR REKAYASA INTERNET
- Key : TEKKOM
- ciphertext : UIVKXMK VOUOKTWK SBFXVXOH

Contoh Aplikasi Simulasi Vigenere Cipher Menggunakan Visual Basic



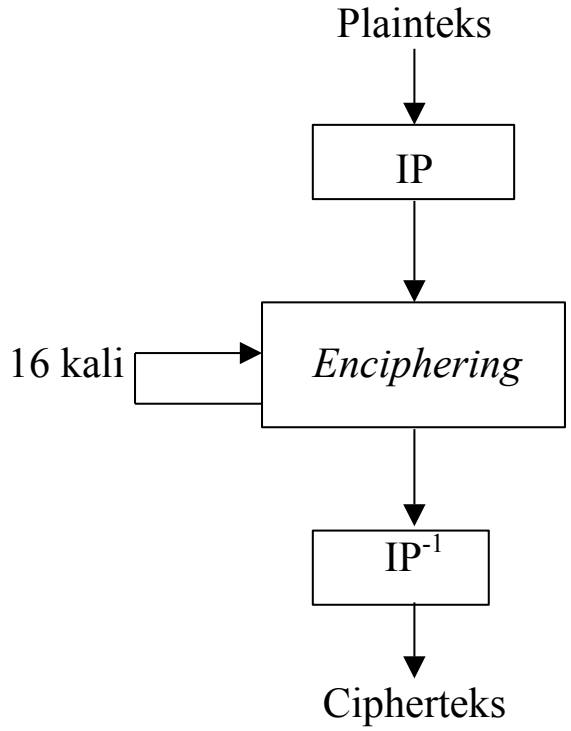

```
Dim vigenere(25, 25) As Char
Dim i, j, plain, cipher, key As Integer
Dim plainChar, cipherChar, keyChar As Char
Dim kunci, plainText, cipherText As String

Private Sub ButtonEncrypt_Click(ByVal sender As System.Object, ByVal
    If (TextBoxPlain.TextLength > 0 And TextBoxKunci.TextLength > 0)
        TextBoxPlain.Text = UCase(TextBoxPlain.Text)
        TextBoxKunci.Text = UCase(TextBoxKunci.Text)
        cipherText = ""
        aturKunci()
        ' copyright (c) AhmadJuniar.Blogspot.com
        For i = 0 To TextBoxPlain.TextLength - 1
            plain = getAscIndex(TextBoxPlain.Text.Substring(i, 1))
            key = getAscIndex(kunci.Substring(i, 1))
            If (plain = 32) Then
                cipherChar = Chr(32)
            Else
                cipherChar = vigenere(key, plain)
            End If
            ' copyright (c) AhmadJuniar.Blogspot.com
            cipherText = String.Concat(cipherText, cipherChar)
        Next i
        TextBoxCipher.Text = cipherText
    End If
End Sub
```

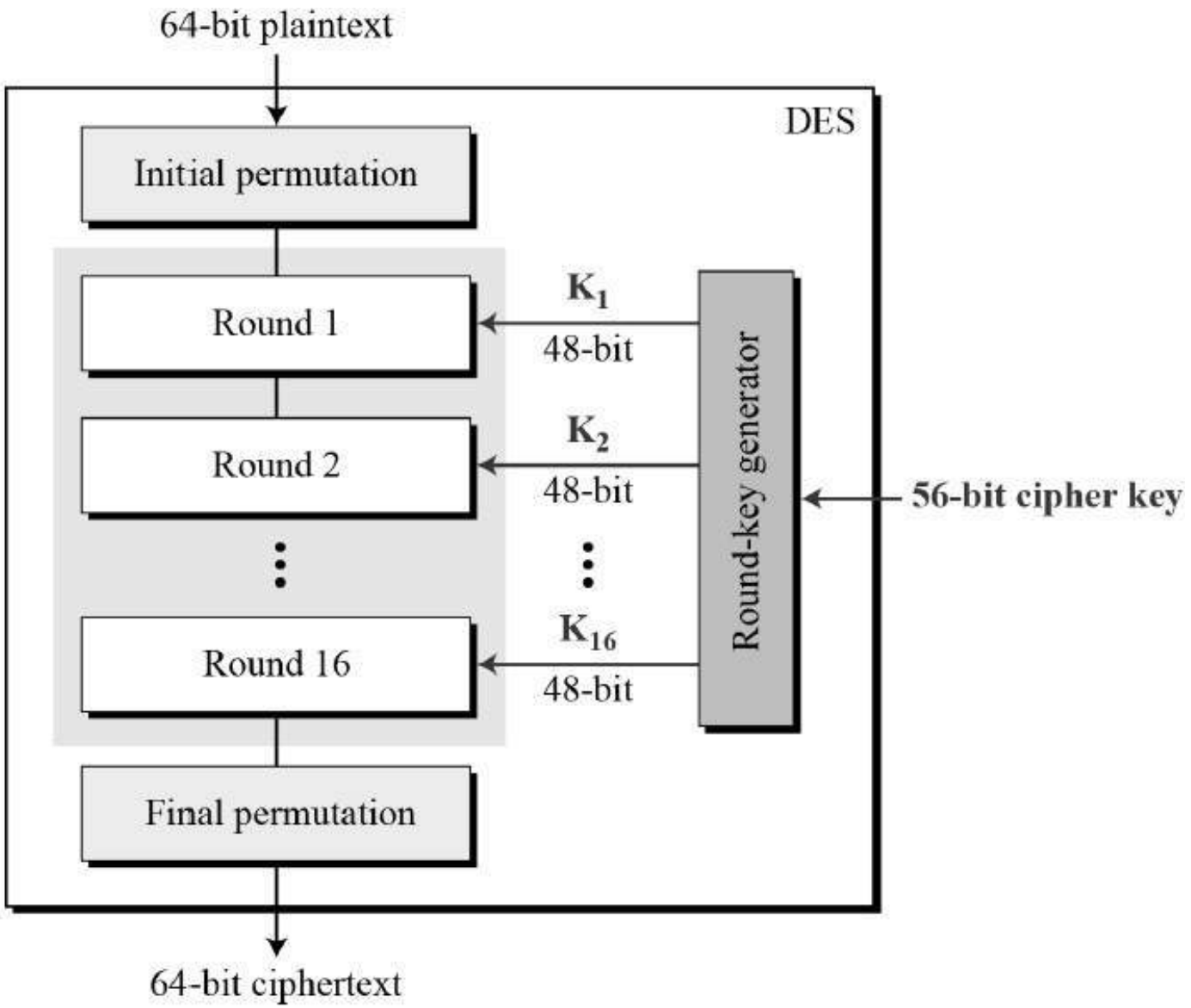
Data Encryption Standard (DES)

- Dikembangkan di IBM pada tahun 1972.
- Berdasarkan pada algoritma Lucifer yang dibuat oleh Horst Feistel.
- Disetujui oleh National Bureau of Standard (NBS) setelah penilaian kekuatannya oleh National Security Agency (NSA) Amerika Serikat.
- DES termasuk ke dalam kriptografi kunci-simetri dan tergolong jenis cipher blok.
- DES beroperasi pada ukuran blok 64 bit.
- Panjang kunci ekternal = 64 bit (sesuai ukuran blok), tetapi hanya 56 bit yang dipakai (8 bit paritas tidak digunakan)

- Setiap blok (plainteks atau cipherteks) dienkripsi dalam 16 putaran.
- Setiap putaran menggunakan kunci internal berbeda.
- Kunci internal (56-bit) dibangkitkan dari kunci eksternal
- Setiap blok mengalami permutasi awal (IP), 16 putaran enciphering, dan inversi permutasi awal (IP-1). (lihat Gambar 9.1)

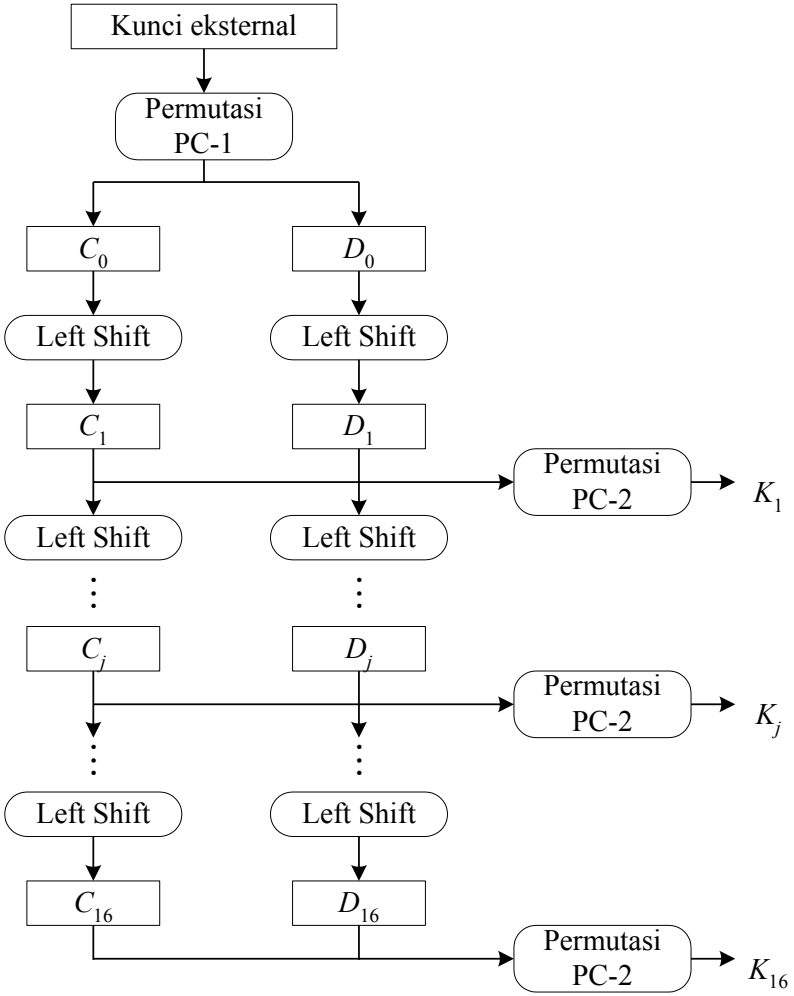


Gambar 9.1 Skema Global Algoritma DES


64-bit plaintext
DES
Initial permutation
Round 1
Round 2
Round 16
Final permutation
K1
48-bit
K2
48-bit
K16
48-bit
Round-key generator
56-bit cipher key
64-bit ciphertext

Pembangkitan Kunci Internal

- Kunci internal = kunci setiap putaran
- Ada 16 putaran, jadi ada 16 kunci internal: K1, K2, …, K16
- Dibangkitkan dari kunci eksternal (64 bit) yang diberikan oleh pengguna.
- Gambar 9.2 memperlihatkan proses pembangkitan kunci internal.



Implementasi DES

- DES sudah diimplementasikan dalam bentuk perangkat keras.
- Dalam bentuk perangkat keras, DES diimplementasikan di dalam chip.
- Setiap detik chip ini dapat mengenkripsikan 16,8 juta blok (atau 1 Gigabit per detik).
- Implementasi DES ke dalam perangkat lunak dapat melakukan enkripsi 32.000 blok per detik (pada komputer mainframe IBM 3090).

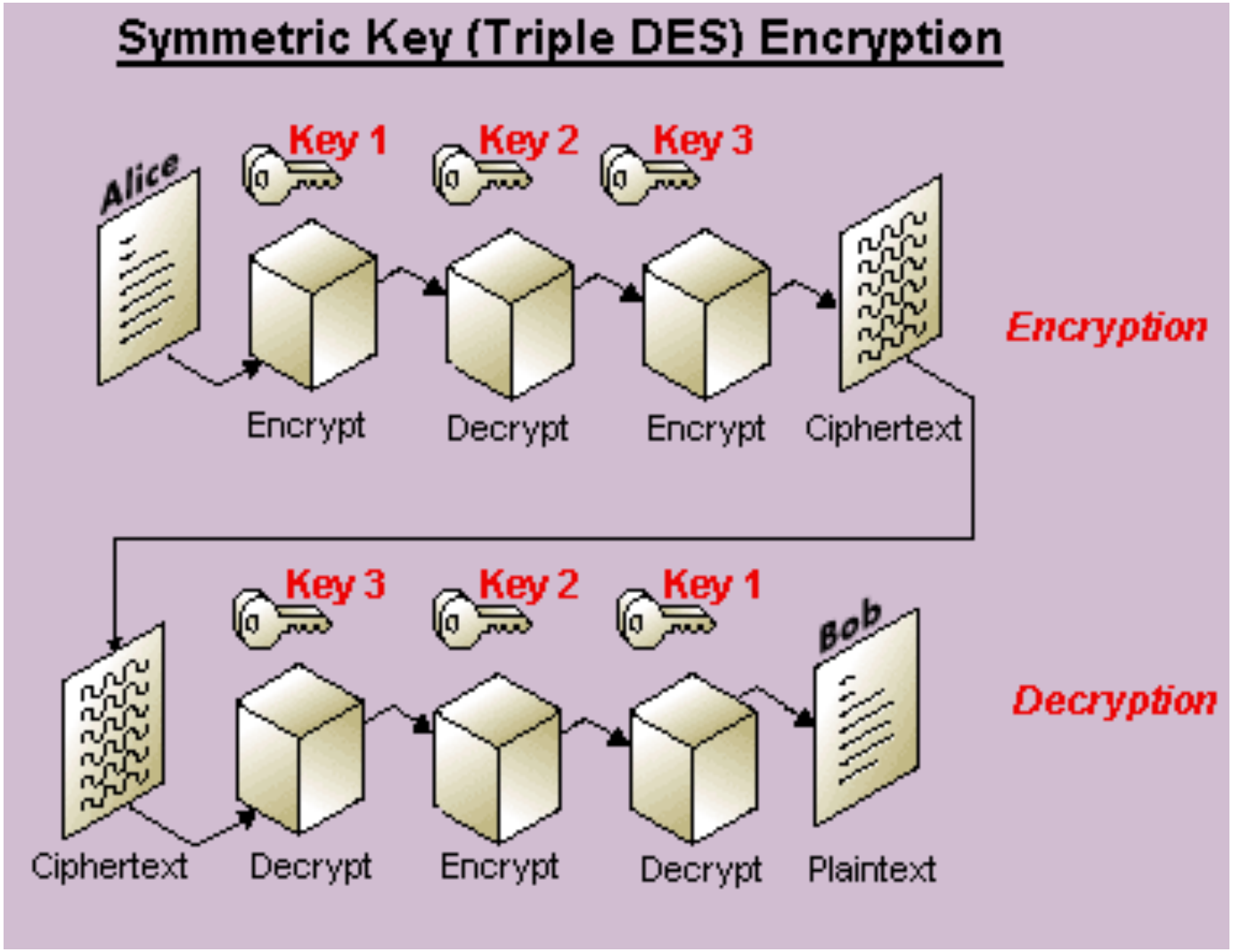
Keamanan DES

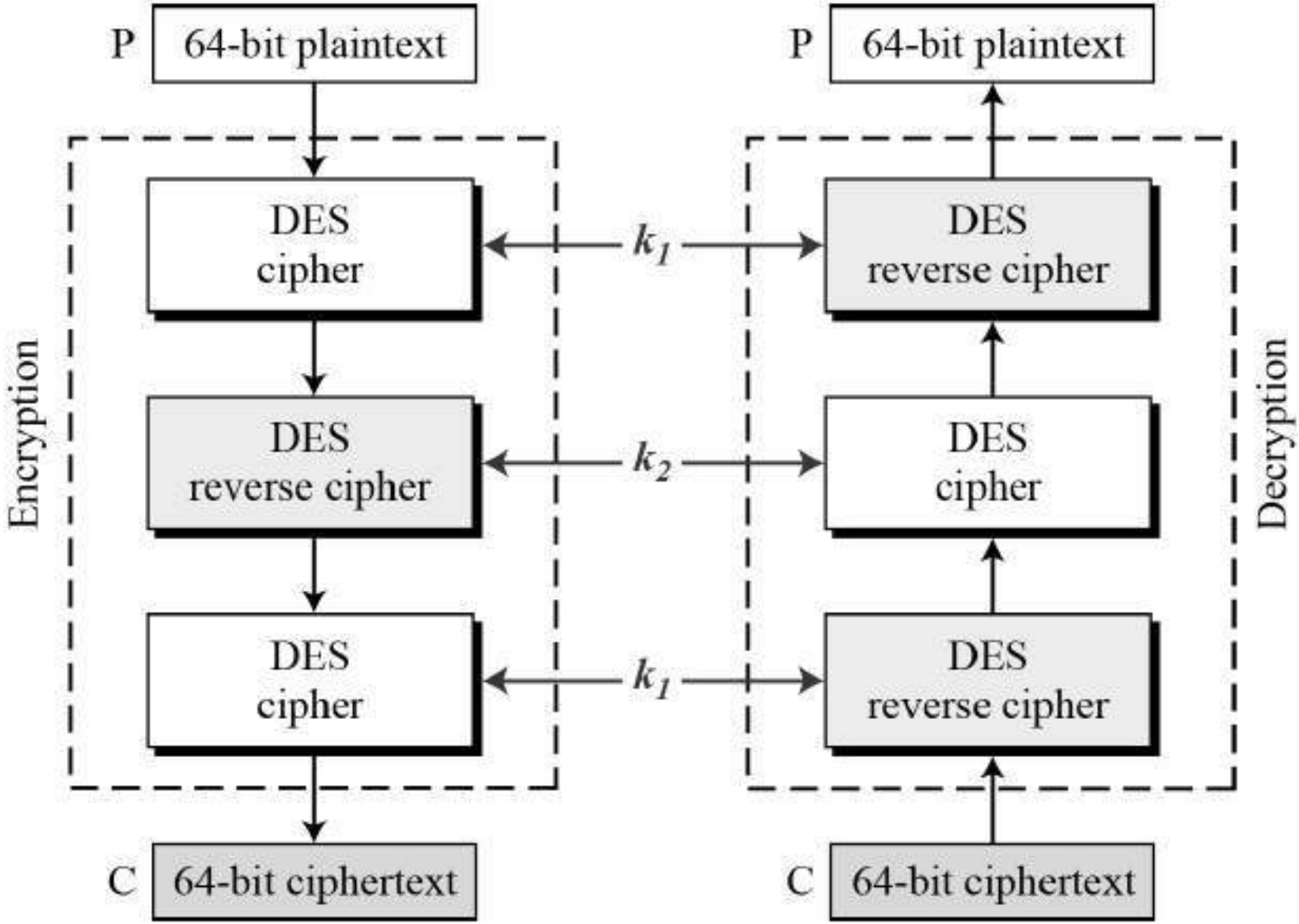
- Keamanan DES ditentukan oleh kunci.
- Panjang kunci eksternal DES hanya 64 bit, tetapi yang dipakai hanya 56 bit.
- Pada rancangan awal, panjang kunci yang diusulkan IBM adalah 128 bit, tetapi atas permintaan NSA, panjang kunci diperkecil menjadi 56 bit.
- Tetapi, dengan panjang kunci 56 bit akan terdapat 256 atau 72.057.594.037.927.936 kemungkinan kunci.
- Jika serangan exhaustive key search dengan menggunakan prosesor paralel, maka dalam satu detik dapat dikerjakan satu juta serangan. Jadi seluruhnya diperlukan 1142 tahun untuk menemukan kunci yang benar.
- Tahun 1998, Electronic Frontier Foundation (EFE) merancang dan membuat perangkat keras khusus untuk menemukan kunci DES secara exhaustive search key dengan biaya $250.000 dan diharapkan dapat menemukan kunci selama 5 hari.
- Tahun 1999, kombinasi perangkat keras EFE dengan kolaborasi internet yang melibatkan lebih dari 100.000 komputer dapat menemukan kunci DES kurang dari 1 hari.

Triple Data Encryption Standard (3DES)

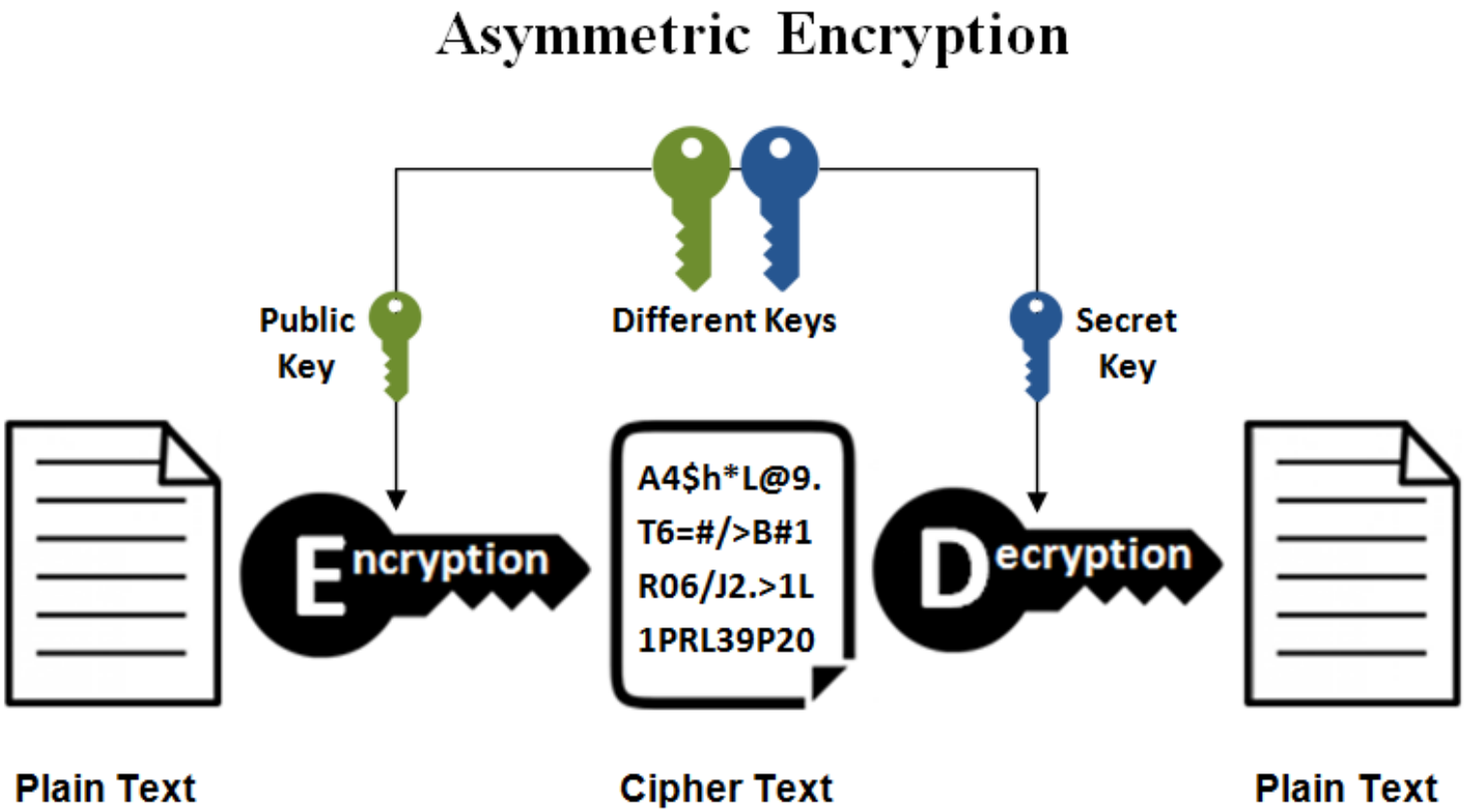
- 3DES (Triple Data Encryption Standard) merupakan salah satu algoritma simetris pada kriptografi yang digunakan untuk mengamankan data dengan cara menyandikan data. Proses yang dilakukan dalam penyandian datanya, yaitu proses enkripsi dan proses dekripsi.
- Algoritma 3DES adalah suatu algoritma pengembangan dari algoritma DES (Data Encryption Standard). Perbedaan DES dengan 3DES terletak pada panjangnya kunci yang digunakan.
- Pada DES menggunakan satu kunci yang panjangnya 56-bit, sedangkan pada 3DES menggunakan 3 kunci yang panjangnya 168-bit (masing-masing panjangnya 56-bit). Pada 3DES, 3 kunci yang digunakan bisa bersifat saling bebas (K1, K2, K3) atau hanya dua buah kunci yang saling bebas dan satu kunci lainnya sama dengan kunci pertama (K1, K2 dan K3=K1).
- Karena tingkat kerahasiaan algoritma 3DES terletak pada panjangnya kunci yang digunakan, maka penggunaan algoritma 3DES dianggap lebih aman dibandingkan dengan algoritma DES.

3DES


Symmetric Key (Triple DES) Encryption
Alice
Key 1
Key 2
Key 3
Encrypt
Decrypt
Encrypt
Ciphertext
Encryption
Key 3
Key 2
Key 1
Bob
Ciphertext
Decrypt
Encrypt
Decrypt
Plaintext
Decryption


P
64-bit plaintext
DES cipher
DES reverse cipher
DES cipher
C
64-bit ciphertext
Encryption
k_1
k_2
k_1
P
64-bit plaintext
DES reverse cipher
DES cipher
DES reverse cipher
C
64-bit ciphertext
Decryption

Factors	AES	3DES	DES
Key Length	128, 192, or 256 bits	(k1,k2 and k3) 168 bits (k1 and k2 is same) 112bits	56 bits
Cipher Type	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher
Block Size	128, 192, or 256 bits	64bits	64 bits
Developed	2000	1978	1977
Cryptanalysis resistance	Strong against differential, truncated differential, linear, interpolation and square attacks	Vulnerable to differential, Brute Force attacker could be analyze plaint text using differential cryptanalysis.	Vulnerable to differential and linear cryptanalysis; weak substitution tables
Security	Considered secure	one only weak which is Exit in DES.	Proven inadequate
Possible Keys	2^{128}, 2^{192}, or 2^{256}	2^{112} or 2^{168}	2^{56}
Possible ASCII printable character keys	95^{16}, 95^{24}, or 95^{32}	95^{14} or 95^{21}	95^{7}
Time required to check all possible keys at 50 billion keys per second**	For a 128-bit key: 5×10^{21} years	For a 112-bit key: 800 Days	For a 56-bit key: 400 Days

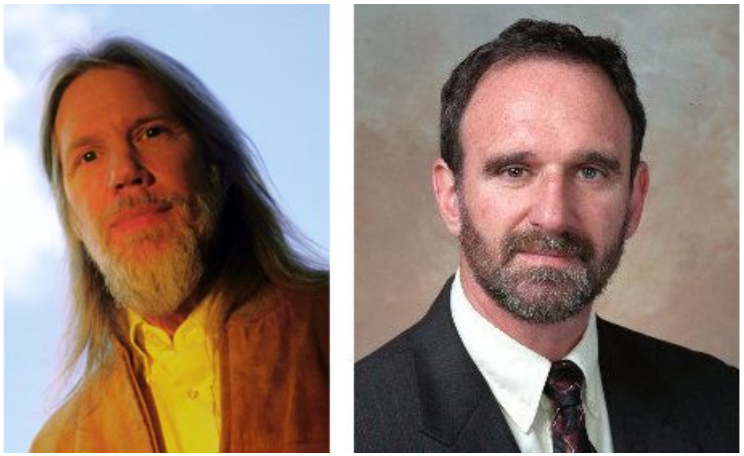


ASYMMETRIC KEY ALGORITHM

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.

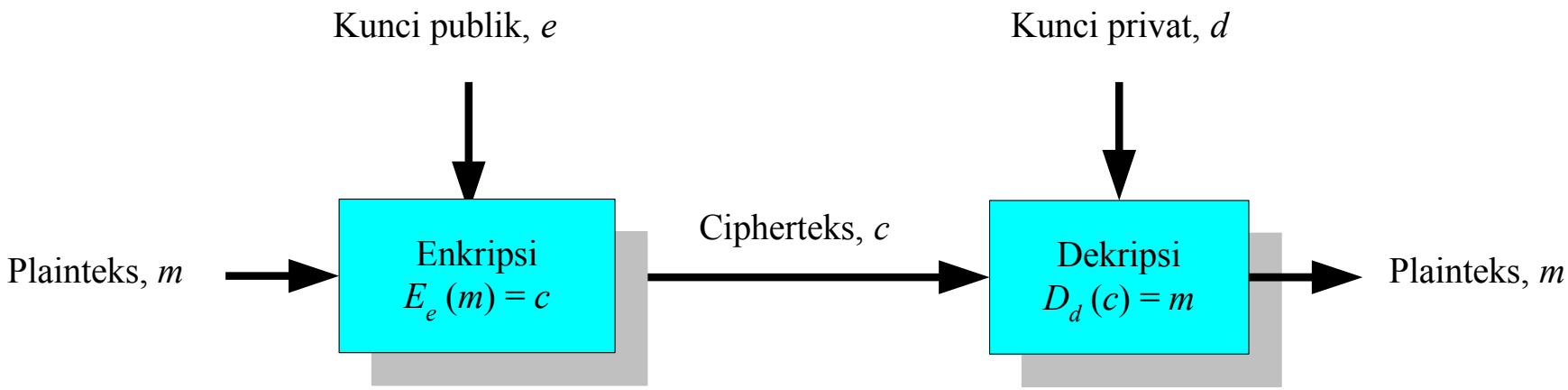
- Ide kriptografi kunci-nirsimetri (*asymmetric-key cryptography*) muncul pada tahun 1976.
- Makalah pertama perihal kriptografi kunci-publik ditulis oleh Diffie-Hellman (ilmuwan dari Stanford University) di IEEE
  - Judul makalahnya “New Directions in Cryptography”.
- Namun pada saat itu belum ditemukan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



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

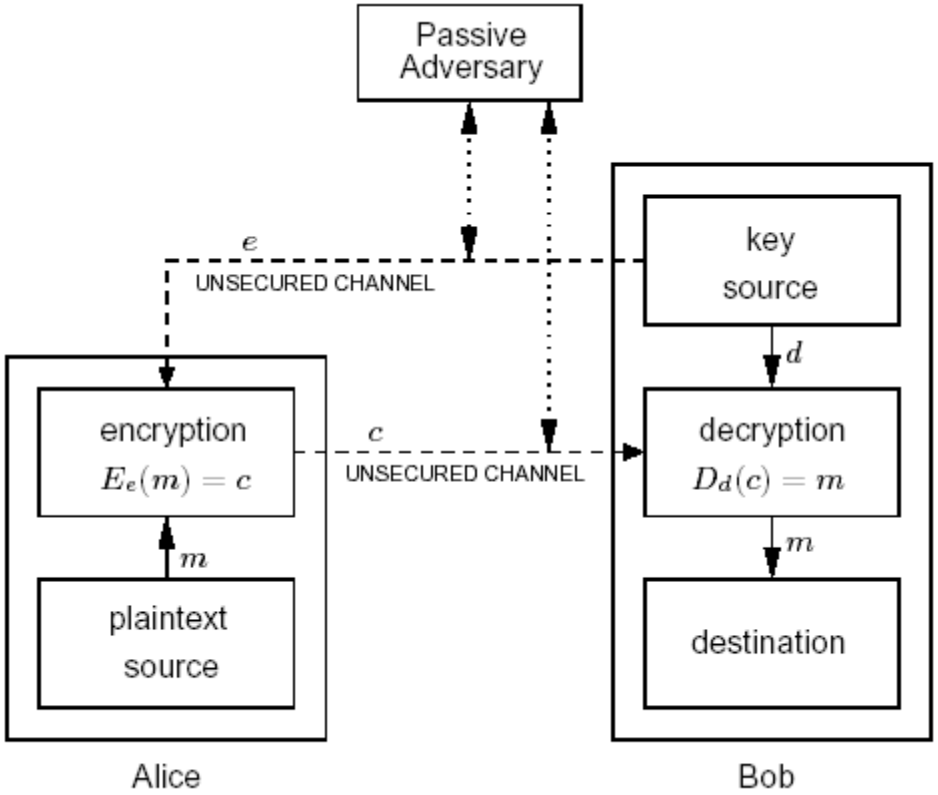
Konsep Asymmetric Algorithm

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



Konsep Asymmetric Algorithm

- 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.



Dua keuntungan kriptografi kunci-publik:

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

Konsep Asymmetric Algorithm

- 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)

Konsep Asymmetric Algorithm

- Pembangkitan sepasang kunci pada kriptografi kunci-publik didasarkan pada persoalan integer klasik sebagai berikut:

1. Pemfaktoran

Diberikan bilangan bulat n. Faktorkan n menjadi faktor primanya

Contoh: 10 = 2 * 5

60 = 2 * 2 * 3 * 5

252601 = 41 * 61 * 101

213 – 1 = 3391 * 23279 * 65993 * 1868569 *

1066818132868207

Semakin besar n, semakin sulit memfaktorkan (butuh waktu sangat lama).

Algoritma yang menggunakan prinsip ini: RSA

2. Logaritma diskrit

Temukan x sedemikian sehingga

$a^x \equiv b \pmod n$ ➔ sulit dihitung

Contoh: jika $3^x \equiv 15 \pmod{17}$ maka x = 6

- Semakin besar a, b, dan n semakin sulit memfaktorkan (butuh waktu lama).
- Algoritma yang menggunakan prinsip ini: ElGamal, DSA
- Catatan:

  Persoalan logaritma diskrit adalah kebalikan dari persoalan perpangkatan modular:

  $a^x \bmod n$ ➔ mudah dihitung

Kriptografi Kunci-Simetri vs Kriptografi Kunci-publik

- **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.

Kriptografi Kunci-Simetri vs Kriptografi Kunci-publik

- **Kelebihan kriptografi kunci-publik:**
  1. Hanya kunci privat yang perlu dijaga kerahasiaannya oleh setiap 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
- **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).
  6. 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

Ron Shamir Adleman (RSA)

- Dari sekian banyak algoritma kriptografi yang pernah dibuat, algoritma yang paling populer adalah algoritma RSA.
- Algoritma RSA dibuat oleh 3 orang peneliti dari MIT (Massachussets Institute of Technology) pada tahun 1976, yaitu: Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman.
- Algorima RSA mendasarkan proses enkripsi dan dekripsinya pada konsep bilangan prima dan aritmatika modulo. Kunci enkripsi maupun kunci dekripsi keduanya harus berupa bilangan bulat.
  - Kunci enkripsi tidak dirahasiakan dan diketahui umum (sehingga dinamakan juga kunci publik), namun kunci untuk dekripsi bersifat rahasia.
  - Kunci dekripsi dibangkitkan dari beberapa buah bilangan prima bersama-sama dengan kunci enkripsi.
  - Untuk menemukan kunci dekripsi, suatu bilangan non prima harus difaktorkan menjadi faktor primanya. Dalam kenyataannya, memfaktorkan bilangan non prima menjadi faktor primanya bukanlah pekerjaan yang mudah. Belum ada algoritma yang secara efisien yang dapat melakukan pemfaktoran tersebut. Semakin besar bilangan non primanya maka semakin sulit pula pemfaktorannya.pemfaktorannya, Semakin sulit pemfaktorannya, semakin kuat pula algoritma RSA.

Key Generation

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption

Ciphertext:	C
Plaintext:	$M = C^d \bmod n$