Bahan Kuliah ke-1

IF5054 Kriptografi

Pengantar Kriptografi

Disusun oleh:

Ir. Rinaldi Munir, M.T.

Departemen Teknik Informatika
Institut Teknologi Bandung
2004

1. Pengantar Kriptografi

1.1 Terminologi

(a) Pengirim dan Penerima pesan

- Seorang pengirim pesan (*sender*) ingin mengirim pesan kepada seorang penerima (*receiver*).

- Pengirim menginginkan pesan dapat dikirim secara aman, yaitu ia yakin bahwa pihak lain tidak dapat membaca isi pesan.

(b) Pesan, Plainteks, dan Cipherteks

- Pesan adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah **plainteks** (*plaintext*) atau teks-jelas (*cleartext*).

- Pesan dapat berupa data atau informasi yang dikirim (melalui kurir, saluran komunikasi data, dsb) atau yang disimpan di dalam media perekaman (kertas, storage, dsb).

- Agar pesan tidak dapat dimengerti maknanya oleh pihak lain, maka pesan disandikan ke bentuk lain. Bentuk pesan yang tersandi disebut **cipherteks** (*ciphertext*) atau **kriptogram** (**cryptogram**).

- Cipherteks harus dapat ditransformasi kembali menjadi plainteks.

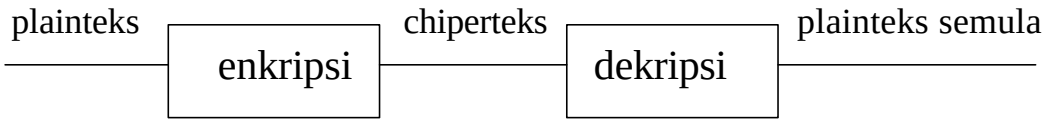
Contoh:

Plainteks: `uang disimpan di balik buku X`
Cipherteks: `j&kloP#d$gkh*7h^”tn%6^klp..t@`

(c) Enkripsi dan Dekripsi

- Proses menyandikan plainteks menjadi cipherteks disebut enkripsi (*encryption*) atau *enciphering* (standard nama menurut ISO 7498-2).

- Proses mengembalikan cipherteks menjadi plainteksnya disebut dekripsi (decryption) atau *deciphering* (standard nama menurut ISO 7498-2).



Gambar 1.1 Enkripsi dan dekripsi

(d) Kriptografi

- **Kriptografi** adalah ilmu sekaligus seni untuk menjaga keamanan pesan (*message*) [Schneier, 1996].

- Praktisi (pengguna kriptografi) disebut **kriptografer** (*cryptographer*).

(e) Algoritma kriptografi dan Kunci

- **Algoritma kriptografi** adalah:
  - aturan untuk *enchipering* dan *dechipering*
  - fungsi matematika yang digunakan untuk enkripsi dan dekripsi.
- **Kunci** adalah parameter yang digunakan untuk transformasi *enciphering* dan *dechipering*.

(f) Sistem Kriptografi

- **Sistem kriptografi (**atau ***cryptosystem*****)** adalah algoritma kriptografi, plainteks, cipherteks, dan kunci.

(g) Penyadap

- **Penyadap** (*eavesdropper*) adalah orang yang mencoba menangkap pesan selama ditransmisikan.

  Nama lain: *enemy*, *adversary*, *intruder*, *interceptor*, *bad guy*

(h) Kriptanalisis dan kriptologi

- **Kriptanalisis** (*cryptanalysis*) adalah ilmu dan seni untuk memecahkan chiperteks menjadi plainteks tanpa mengetahui *kunci* yang diberikan. Pelakunya disebut **kriptanalis**.

- **Kriptologi** (*cryptology*) adalah 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 atas nama penyadap yang tidak berhak.

1.2 Sejarah Kriptografi

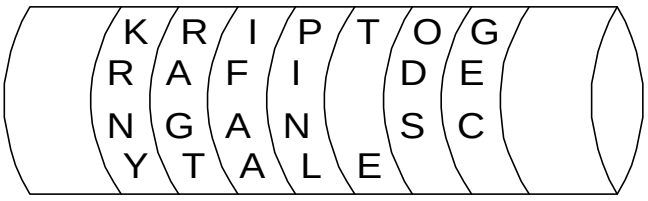
- Kriptografi sudah lama digunakan oleh tentara Sparta di Yunani pada permulaan tahun 400 SM. Mereka menggunakan alat yang namanya *scytale*.

- *Scytale*: pita panjang dari daun *papyrus* + sebatang silinder

  Pesan ditulis horizontal (baris per baris).

  Bila pita dilepaskan, maka huruf-huruf di dalamnya telah tersusun membentuk pesan rahasia.

  Untuk membaca pesan, penerima melilitkan kembali silinder yang diameternya sama dengan diameter silinder pengirim.



Gambar 1.2 *Scytale*

1.3 Aplikasi Kriptografi

- Aplikasi kriptografi:
  1. Pengiriman data melalui saluran komunikasi
  2. Penyimpanan data di dalam *disk storage*.

- Data ditransmisikan dalam bentuk cipherteks. Di tempat penerima cipherteks dikembalikan lagi menjadi plainteks.

- Data di dalam media penyimpanan komputer (seperti *hard disk*) disimpan dalam bentuk cipherteks. Untuk membacanya, hanya orang yang berhak yang dapat mengembalikan chiperteks menjadi plainteks.

- Contoh-contoh enkripsi dan dekripsi pada data tersimpan:

  1. Dokumen teks

     Plainteks (`plain.txt`):

```
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.
```

     Cipherteks (`cipher.txt`):

```
Ztâxzp/épêp/qtüyp{p}<yp{p}/sx/•p}âpx;
  épêp/|t}t|äzp}/qp}êpz/étzp{x/zt•x
}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=
```

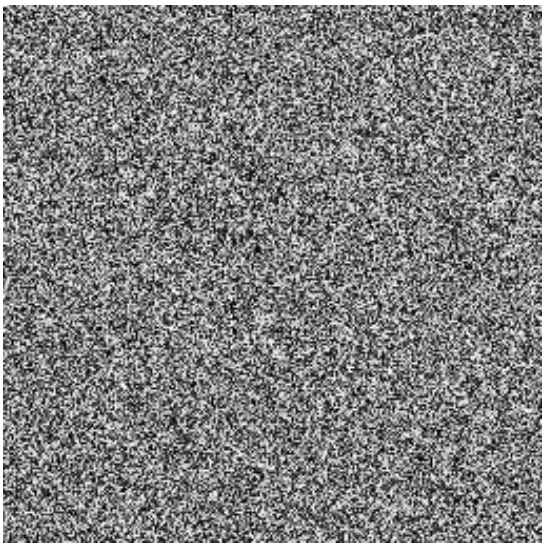
     Hasil dekripsi terhadap berkas `cipher.txt`:

```
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.
```

2. Dokumen gambar

Plainteks (`lena.bmp`):

Cipherteks (`lena2.bmp`):



Hasil dekripsi terhadap berkas `lena2.bmp` menghasilkan gambar yang sama seperti `lena.bmp`.

3. Dokumen basisdata

Plainteks (`siswa.dbf`):

NIM	Nama	Tinggi	Berat
000001	Elin Jamilah	160	50
000002	Fariz RM	157	49
000003	Taufik Hidayat	176	65
000004	Siti Nurhaliza	172	67
000005	Oma Irama	171	60
000006	Aziz Burhan	181	54
000007	Santi Nursanti	167	59
000008	Cut Yanti	169	61
000009	Ina Sabarina	171	62

Cipherteks (`siswa2.dbf`):

NIM	Nama	Tinggi	Berat
000001	tüp}vzpz/|t}äyä/{ää	|äzp}	épêp
000002	|t}tâpé/spüx/	péxü=	ztwxsä•
000003	ât|•pâ/ztwxsä•p}	}/|tü	spüx/
000004	épêp/|t}t|äzp}/qpêpz	qp}êpz	wxsä
000005	étzp{x/zt•xâx}v êp}	päâ/psp	étzp{
000006	spüx/sp{p|/•péxü=/]	xâx}v	ttüzp/|
000007	Ztâxzp/épêp/qtüypp}<	äzp}	}äyä/{
000008	qpwåp/{päâ/psp{pw	Ztwxs	xâx}v
000009	}t|äzp}/qp}êpz/ép{	qp}êp	äzp}/qp

Keterangan: hanya *field* Nama, Berat, dan Tinggi yang dienkripsi.

Hasil dekripsi terhadap berkas `siswa2.dbf` menghasilkan berkas yang sama seperti `siswa.dbf`.

- Kehidupan saat ini dikelilingi oleh kriptografi, mulai:
  - ATM tempat mengambil uang,
  - Telepon genggam (HP),
  - Komputer di lab/kantor,
  - Internet,
  - Gedung-gedung bisnis,
  - sampai ke pangkalan militer

1.5 Kegunaan Kriptografi

- Selain untuk menjaga kerahasiaan (confidentiality) pesan, kriptografi juga digunakan untuk menangani masalah keamanan yang mencakup dua hal berikut:

  1. Keabsahan pengirim (*user authentication*).
     Hal ini berkaitan dengan keaslian pengirim. Dengan kata lain, masalah ini dapat diungkapkan sebagai pertanyaan: "Apakah pesan yang diterima benar-benar berasal dari pengirim yang sesungguhnya?"

  2. Keaslian pesan (*message authentication*).
     Hal ini berkaitan dengan keutuhan pesan (*data integrity*). Dengan kata lain, masalah ini dapat diungkapkan sebagai pertanyaan: "Apakah pesan yang diterima tidak mengalami perubahan (modifikasi)?"

  3. Anti-penyangkalan (*nonrepudiation*).
     Pengirim tidak dapat menyangkal (berbohong) bahwa dialah yang mengirim pesan.

1.5 Notasi Matematis

- Misalkan:

  C = chiperteks
  P = plainteks dilambangkan

- Fungsi enkripsi E memetakan P ke C,

  $$E(P) = C$$

- Fungsi dekripsi D memetakan C ke P,

  $$D(C) = P$$

- Karena proses enkripsi kemudian dekripsi mengembalikan pesan ke pesan asal, maka kesamaan berikut harus benar,

  $$D(E(P)) = P$$

- Kekuatan algoritma kriptografi diukur dari banyaknya kerja yang dibutuhkan untuk memecahkan data chiperteks menjadi plainteksnya. Kerja ini dapat diekivalenkan dengan waktu.

- Semakin banyak usaha yang diperlukan, yang berarti juga semakin lama waktu yang dibutuhkan, maka semakin kuat algoritma kriptografinya, yang berarti semakin aman digunakan untuk menyandikan pesan.

- Jika kekuatan kriptografi ditentukan dengan menjaga kerahasiaan algoritmanya, maka algoritma kriptografinya dinamakan algoritma *restricted*. Algoritma *restricted* tidak cocok lagi saat ini.

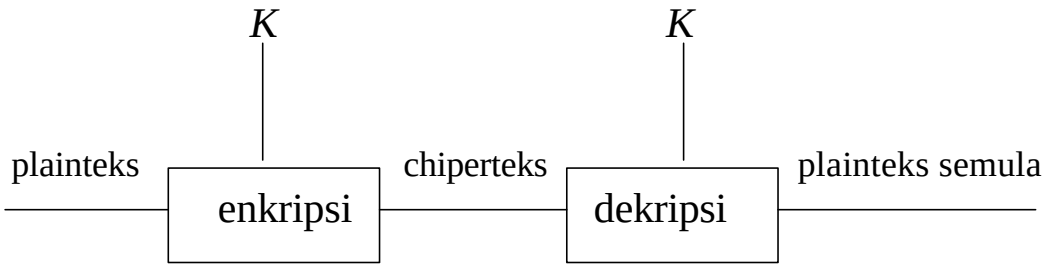
- Pada sistem kriptografi modern, kekuatan kriptografinya terletak pada kunci, yang berupa deretan karakter atau bilangan bulat, dijaga kerahasiaannya.

- Dengan menggunakan kunci *K*, maka fungsi enkripsi dan dekripsi menjadi

$$E_K(P) = C$$
$$D_K(C) = P$$

dan kedua fungsi ini memenuhi

$$D_K(E_K(P)) = P$$



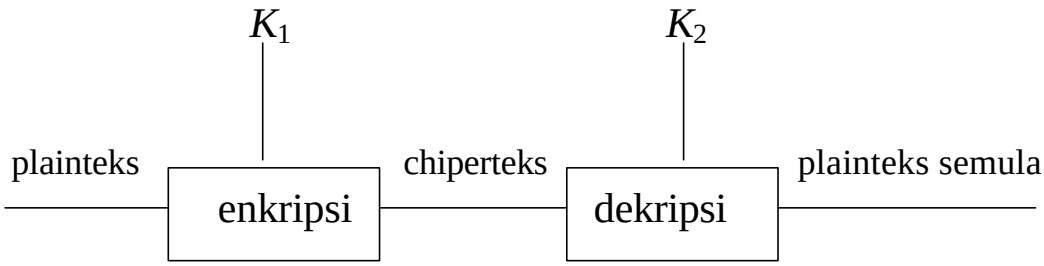
Gambar 1.3 Enkripsi dan dekripsi dengan kunci

- Jika kunci enkripsi sama dengan kunci dekripsi, maka sistem kriptografinya disebut **sistem simetri** atau **sistem konvensional**. Algoritam kriptografinya disebut algoritma simetri atau algoritma konvensional.

  Contoh algoritma simetri: *DES* (*Data Encyption Standard*).

- Beberapa sistem kriptografi menggunakan kunci yang berbeda untuk enkripsi dan dekripsi. Misalkan kunci enkripsi adalah K_1 dan kunci dekripsi yang adalah K_2, yang dalam hal ini $K1 \neq K2$. Sistem kriptograsi semacam ini dinamakan sistem **sistem nirsimetri** atau **sistem kunci-publik**. Algoritam kriptografinya disebut algoritma nirsimetri atau algoritma kunci-publik.

  Contoh algoritma nirsimetri: *RSA* (Rivest-Shamir-Adleman)



Gambar 1.4 Enkripsi dan dekripsi dengan kunci pada sistem nirsimetri