1

Pengantar Kriptografi

Kehidupan kita saat ini dilingkupi oleh kriptografi. Mulai dari transaksi di mesin ATM, transaksi di bank, transaksi dengan kartu kredit, percakapan melalui telepon genggam, mengakses internet, sampai mengaktifkan peluru kendali pun menggunakan kriptografi. Begitu pentingnya kriptografi untuk keamanan informasi (*information security*), sehingga jika berbicara mengenai masalah keamanan yang berkaitan dengan penggunaan komputer, maka orang tidak bisa memisahkannya dengan kriptografi. Bab satu ini memperkenalkan kriptografi dan terminologi yang berkaitan dengannya. Dibahas pula mengenai sejarah, tujuan yang ingin dicapai dengan kriptografi, dan beberapa contoh penggunaan kriptografi.

1.1 Definisi dan Terminologi

Jika anda bertukar pesan (misalnya surat) dengan orang lain, maka anda tentu ingin pesan yang anda kirim sampai ke pihak yang dituju dengan aman. Pengertian aman di sini sangat luas. Aman bisa berarti bahwa selama pengiriman pesan tentu anda berharap pesan tersebut tidak dibaca oleh orang yang tidak berhak. Sebab, mungkin saja pesan yang anda kirim berisi sesuatu yang rahasia sehingga jika pesan rahasia dibaca oleh pihak lawan atau pihak yang tidak berkepentingan, maka bocorlah kerahasiaan pesan yang anda kirim. Ini adalah masalah keamanan pesan yang dinamakan **kerahasiaan** (*confidentiality* atau *privacy*).

Aman bisa juga berarti bahwa anda ingin pesan yang dikirim sampai dengan utuh ke tangan penerima, artinya isi pesan tidak diubah atau dimanipulasi selama pengiriman oleh pihak ketiga. Di sisi penerima pesan, ia tentu ingin memastikan bahwa pesan yang ia terima adalah pesan yang masih asli, bukan pesan yang sudah ditambah-tambah atau dikurangi. Ini adalah masalah keamanan pesan yang disebut **integritas data** (*data integrity*). Selain itu, penerima yakin bahwa pesan tersebut memang benar berasal dari anda, bukan dari orang lain yang menyamar seperti anda, dan anda pun yakin bahwa orang yang anda kirimi pesan adalah orang yang sesungguhnya. Ini adalah masalah keamanan pesan yang dinamakan **otentikasi** (*auhentication*).

Jika anda sebagai penerima pesan, anda pun tidak ingin kelak pengirim pesan membantah pernah mengirim pesan kepada anda. Ini adalah masalah keamanan yang disebut **penyangkalan** (*repudiaton*). Zaman sekarang banyak orang yang membantah telah mengirim atau menerima pesan. Padahal anda yakin bahwa anda memang menerima pesan dari orang tersebut. Jika pengirim membantah telah mengirim pesan, maka anda perlu membuktikan ketidakbenaran penyangkalan tersebut (*non-repudiation*).

Keempat masalah keamanan yang disebutkan di atas, yaitu kerahasiaan, integritas data, otentikasi, dan penyangkalan dapat diselesaikan dengan menggunakan kriptografi. Kriptografi tidak hanya menyediakan alat untuk keamanan pesan, tetapi juga sekumpulan teknik yang berguna.

Kriptografi (*cryptography*) berasal dari Bahasa Yunani: "*cryptós*" artinya "*secret*" (rahasia), sedangkan "*gráphein*" artinya "*writing*" (tulisan). Jadi, kriptografi berarti "*secret writing*" (tulisan rahasia). Ada beberapa definisi kriptografi yang telah dikemukakan di dalam berbagai literatur. Definisi yang dipakai di dalam buku-buku yang lama (sebelum tahun 1980-an) menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Definisi ini mungkin cocok pada masa lalu di mana kriptografi digunakan untuk keamanan komunikasi penting seperti komunikasi di kalangan militer, diplomat, dan mata-mata. Namun saat ini kriptografi lebih dari sekadar *privacy*, tetapi juga untuk tujuan *data integrity*, *authentication*, dan *non-repudiation*.

Definisi yang kita pakai di dalam buku ini mengutip definisi yang dikemukakan di dalam [SCH96]:

> **Kriptografi** adalah ilmu dan seni untuk menjaga keamanan pesan
> (*Cryptography is the art and science of keeping messages secure*)

Sebagai pembanding, selain definisi tersebut di atas, terdapat pula definisi yang dikemukakan di dalam [MEN96]:

> **Kriptografi** adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi

Kata "seni" di dalam definisi di atas berasal dari fakta sejarah bahwa pada masa-masa awal sejarah kriptografi, setiap orang mungkin mempunyai cara yang unik untuk merahasiakan pesan. Cara-cara unik tersebut mungkin berbeda-beda pada setiap pelaku kriptografi sehingga setiap cara menulis pesan rahasia pesan mempunyai nilai estetika tersendiri

sehingga kriptografi berkembang menjadi sebuah seni merahasiakan pesan (kata "*graphy*" di dalam "*cryptography*" itu sendiri sudah menyiratkan sebuah seni). Anda akan melihat di dalam bab 3 contoh-contoh teknik keriptografi dari zaman dahulu hingga zaman sekarang sehingga anda dapat mamahami bahwa kriptografi dapat dipandang sebagai sebuah seni merahasiakan pesan. Pada perkembangan selanjutnya, kriptografi berkembang menjadi sebuah disiplin ilmu sendiri karena teknik-teknik kriptografi dapat diformulasikan secara matematik sehingga menjadi sebuah metode yang formal.

Terminologi

Di dalam kriptografi kita akan sering menemukan berbagai istilah atau terminologi. Beberapa istilah yang penting untuk diketahui diberikan di bawah ini.

(a) ***Pesan, Plainteks, dan Cipherteks***

Pesan (*message*) 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 telekomunikasi, dsb) atau yang disimpan di dalam media perekaman (kertas, *storage*, dsb). Pesan yang tersimpan tidak hanya berupa teks, tetapi juga dapat berbentuk citra (*image*), suara/bunyi (audio), dan video, atau berkas biner lainnya.

Agar pesan tidak dapat dimengerti maknanya oleh pihak lain, maka pesan perlu disandikan ke bentuk lain yang tidak dapat dipahami. Bentuk pesan yang tersandi disebut **cipherteks** (*ciphertext*) atau **kriptogram** (*cryptogram*). Cipherteks harus dapat ditransformasikan kembali menjadi plainteks semula agar pesan yang diterima bisa dibaca. Gambar 1.1 memperlihatkan contoh-contoh dua buah plainteks, masing-masing berupa teks dan gambar, serta cipherteks yang berkoresponden. Perhatikan bahwa plainteks dapat dibaca dengan jelas, tetapi cipherteks sudah tidak dapat lagi dimengerti maknanya. Melalui proses yang berkebalikan, cipherteks dapat ditransformasikan kembali menjadi plainteks semula.

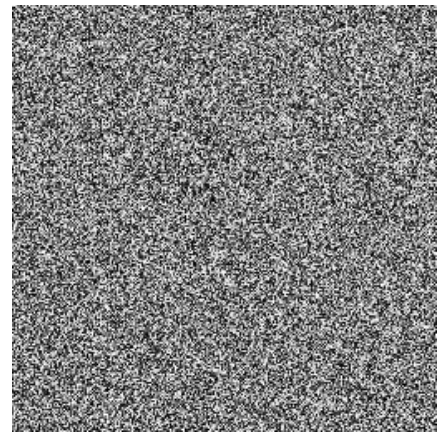
```
Ketika saya berjalan-jalan di
pantai, saya menemukan banyak
sekali kepiting yang merangkak
menuju laut. Mereka adalah
anak-anak kepiting yang baru
menetas dari dalam pasir.
Naluri mereka mengatakan bahwa
laut adalah tempat kehidupan
mereka.
```

(a) Plainteks (teks)

```
Ztâxzp/épêp/qtüyp{p}<yp{p}/sx/•p}
âpx;
  épêp/|t}t|äzp}/qp}êpz/étzp{x/
•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/{p
ää
/psp{pw ât|•pâ/ztwxsä•p}/|tützp=
```

(b) Cipherteks dari (a)

(c) Plainteks (citra)



(d) Cipherteks dari (c)

Gambar 1.1. Contoh-contoh plainteks dan cipherteksnya.

(b) ***Pengirim dan penerima***

Komunikasi data melibatkan pertukaran pesan antara dua entitas. **Pengirim** (*sender*) adalah entitas yang mengirim pesan kepada entitas lainnya. **Penerima** (*receiver*) adalah entitas yang menerima pesan. Entitas di sini dapat berupa orang, mesin (komputer), kartu kredit, dan sebagainya. Jadi, orang bisa bertukar pesan dengan orang lainnya (contoh: Alice berkomunikasi dengan Bob), sedangkan di dalam jaringan komputer mesin (komputer) berkomunikasi dengan mesin (contoh: mesin ATM berkomunikasi dengan komputer *server* di bank).

Pengirim tentu menginginkan pesan dapat dikirim secara aman, yaitu ia yakin bahwa pihak lain tidak dapat membaca isi pesan yang ia kirim. Solusinya adalah dengan cara menyandikan pesan menjadi cipherteks.

(c) ***Enkripsi dan dekripsi***

Proses menyandikan plainteks menjadi cipherteks disebut **enkripsi** (*encryption*) atau *enciphering* (standard nama menurut ISO 7498-2). Sedangkan proses mengembalikan cipherteks menjadi plainteks semula dinamakan **dekripsi** (*decryption*) atau *deciphering* (standard nama menurut ISO 7498-2). Enkripsi dan dekripsi dapat diterapkan baika pada pesan yang dikirim maupun pada pesan tersimpan. Istilah *encryption of data in motion* mengacu pada enkripsi pesan yang ditransmisikan melalui saluran komunikasi, sedangkan istilah *enrypton of data at-rest* mengacu pada enkripsi dokumen yang disimpan di dalam *storage*. Contoh *encryption of data in motion* adalah pengiriman nomor PIN dari mesin ATM ke komputer *server* di kantor bank pusat. Contoh *encryption of data at-rest* adalah enkripsi *file* basis data di dalam hard *disk*. Gambar 1.2 memperlihatkan enkripsi *file* basis data, di mana enkripsi hanya dilakukan terhadap *field-field* tertentu saja (`Nama`, `Tinggi`, dan `Berat`).

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

Gambar 1.2. Enkripsi data tertentu di dalam arsip basisdata.

(d) ***Cipher dan kunci***

Algoritma kriptografi disebut juga *cipher* yaitu aturan untuk *enchipering* dan *dechipering*, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Beberapa *cipher* memerlukan algoritma yang berbeda untuk *enciphering* dan *deciphering*.

Konsep matematis yang mendasari algoritma kriptografi adalah relasi antara dua buah himpunan yaitu himpunan yang berisi elemen-elemen plainteks dan himpunan yang berisi cipherteks. Enkripsi dan dekripsi merupakan fungsi yang memetakan elemen-elemen antara kedua himpunan tersebut. Misalkan P menyatakan plainteks dan dan C menyatakan chiperteks, maka fungsi enkripsi E memetakan P ke C,

$$E(P) = C$$

Dan 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,

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

Keamanan algoritma sering kriptografi diukur dari banyaknya kerja (*work*) yang dibutuhkan untuk memecahkan chiperteks menjadi plainteksnya tanpa mengetahui kunci yang digunakan. Kerja ini dapat diekivalenkan dengan waktu, memori, uang, dan lain-lain. Semakin banyak kerja yang diperlukan, yang berarti juga semakin lama waktu yang dibutuhkan, maka semakin kuat algoritma kriptografi tersebut, yang berarti semakin aman digunakan untuk menyandikan pesan.

Jika keamanan kriptografi ditentukan dengan menjaga kerahasiaan algoritmanya, maka algoritma kriptografinya dinamakan algoritma *restricted*. Algoritma *restricted* mempunyai sejarah tersendiri di dalam kriptografi. Algoritma *restricted* biasanya digunakan oleh sekelompok orang untuk bertukar pesan satu sama lain. Mereka membuat suatu algoritma enkripsi dan algoritma enkripsi tersebut hanya diketahui oleh anggota kelompok itu saja. Tetapi, algoritma *restricted* tidak cocok lagi saat ini, sebab setiap kali ada anggota kelompok keluar, maka algoritma kriptografi harus diganti lagi.

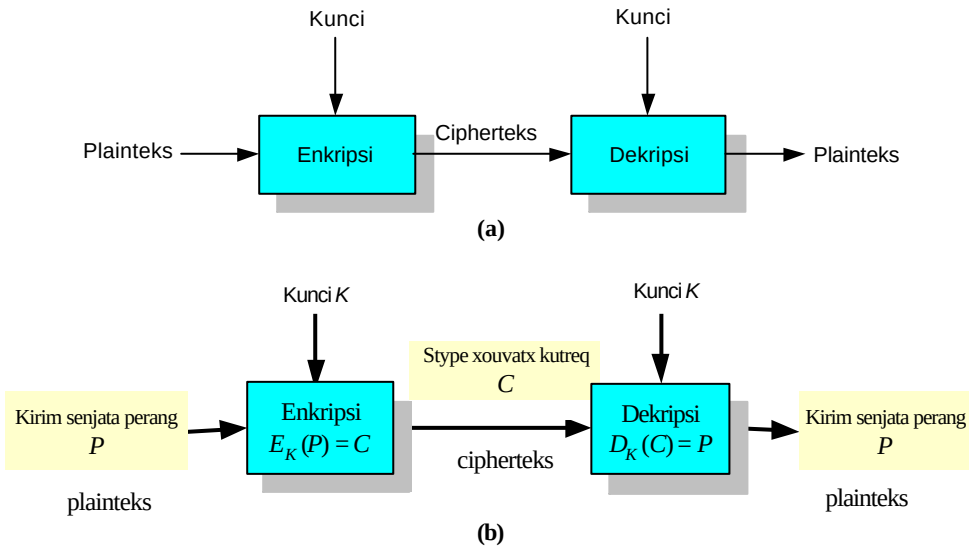
Kriptografi modern mengatasi masalah di atas dengan penggunaan kunci, yang dalam hal ini algoritma tidak lagi dirahasiakan, tetapi kunci harus dijaga kerahasiaannya. **Kunci** (*key*) adalah parameter yang digunakan untuk transformasi *enciphering* dan *dechipering*. Kunci biasanya berupa *string* atau deretan bilangan. Dengan menggunakan kunci K, maka fungsi enkripsi dan dekripsi dapat ditulis sebagai

$$E_K(P) = C \text{ dan } D_K(C) = P$$

dan kedua fungsi ini memenuhi

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

Gambar 1.3(a) memperlihatkan skema enkripsi dan dekripsi dengan menggunakan kunci, sedangkan Gambar 1.3(b) mengilustrasikan enkripsi dan dekripsi terhadap sebuah pesan.



Gambar 1.3. (a) Skema enkripsi dan dekripsi, (b) contoh ilustrasi enkripsi dan dekripsi pesan.

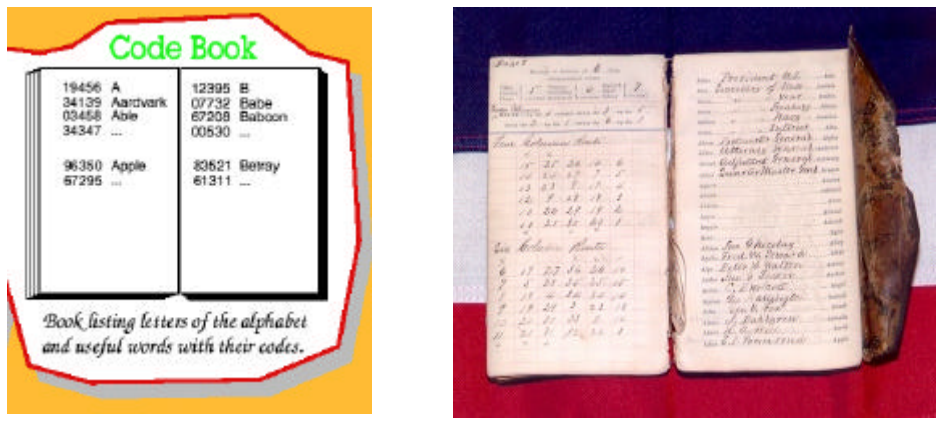
Istilah "*cipher*" sering disamakan dengan **kode** (*code*). Kode mempunyai sejarah tersendiri di dalam kriptografi. Sebenarnya kedua istilah ini tidak sama pengertiannya. Jika *cipher* adalah transformasi karakter-ke-karakter atau bit-ke-bit tanpa memperhatikan struktur bahasa pesan, maka kode sering diacu sebagai prosedur yang mengganti setiap plainteks dengan kata kode, misalnya

`kapal api datang` dikodekan menjadi `hutan bakau hancur`

Kode juga dapat berupa deretan angka dan huruf yang tidak bermakna, seperti

`kapal api datang` dikodekan menjadi `xyztvq bkugbf hjqpot`

Transformasi dari plainteks menjadi kode sering disebut *encoding*, sedangkan transformasi kebalikannya sering disebut *decoding*. Di dalam kriptografi, **buku kode** (*codebook*) – contohnya seperti pada Gambar 1.4 – adalah dokumen yang digunakan untuk mengimplemntasikan suatu kode. Buku kode terdiri dari tabel *lookup* (*lookup table*) untuk *encoding* dan *decoding*. Untuk melakukan enkripsi dan dekripsi pesan, buku kode yang sama harus tersedia di sisi pengirim dan penerima pesan. Penyebaran buku kode menimbulkan masalah tersendiri menyangkut keamanannya, sehingga penggunaan kode di dalam kriptografi tidak mempunyai umur yang panjang dan *cipher* menjadi teknik yang dominan. Pihak lawan yang mencoba mentransformasikan kode menajdi plainteks dinamakan **pemecah kode** (*codebreaker*).



(a) **(b)**

Gambar 1.4. (a) Buku kode, (b) Sebuah buku kode yang digunakan untuk korespondensi telegraf (Sumber: www.mathdaily.com/ lessons/Codebook)

(f) ***Sistem Kriptografi***

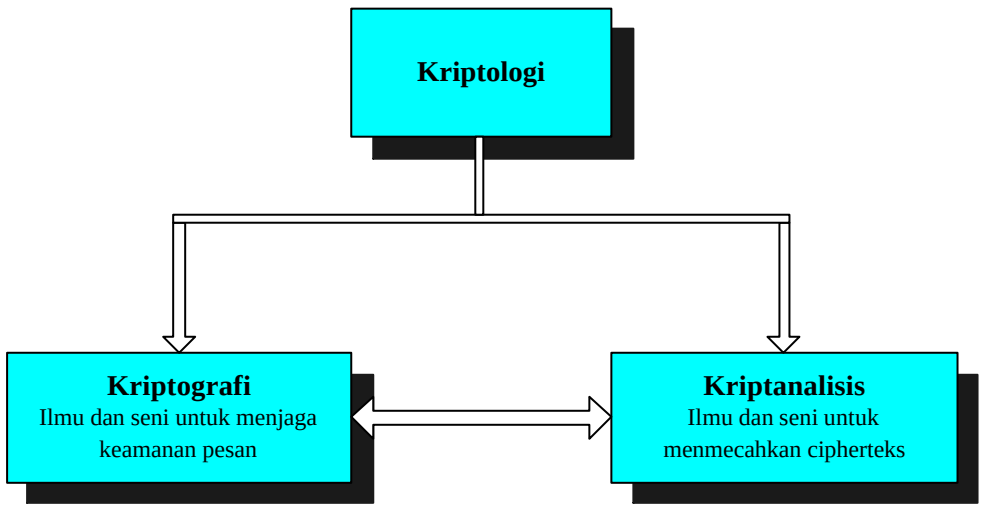
Kriptografi membentuk sebuah sistem yang dinamakan sistem kriptografi. **Sistem kriptografi** (*cryptosystem*) adalah kumpulan yang terdiri dari algoritma kriptografi, semua plainteks dan cipherteks yang mungkin, dan kunci [SCH96]. Di dalam sistem kriptografi, *cipher* hanyalah salah satu komponen saja.

(g) ***Penyadap***

Penyadap (*eavesdropper*) adalah orang yang mencoba menangkap pesan selama ditransmisikan. Tujuan penyadap adalah untuk mendapatkan informasi sebanyak-banyaknya mengenai sistem kriptografi yang digunakan untuk berkomunikasi dengan maksud untuk memecahkan cipherteks. Nama lain penyadap: *enemy*, *adversary*, *intruder*, *interceptor*, *bad guy*. Ron Rivest, seorang pakar kriptografi, menyatakan bahwa *cryptography is about communication in the presence of adversaries* (Kriptografi adalah perihal berkomunikasi dengan keberadaan pihak musuh) [WIK06].

(h) ***Kriptanalisis dan kriptologi***

Kriptografi berkembang sedemikian rupa sehingga melahirkan bidang yang berlawanan yaitu kriptanalisis. **Kriptanalisis** (*cryptanalysis*) adalah ilmu dan seni untuk memecahkan chiperteks menjadi plainteks tanpa mengetahui *kunci* yang digunakan. Pelakunya disebut **kriptanalis**. Jika seorang **kriptografer** (*cryptographer*) mentransformasikan plainteks menjadi cipherteks dengan suatu algoritma dan kunci maka sebaliknya seorang kriptanalis berusaha untuk memecahkan cipherteks tersebut untuk menemukan plainteks atau kunci. **Kriptologi** (*cryptology*) adalah studi mengenai kriptografi dan kriptanalisis. Baik kriptografi maupun kriptanalisis keduanya saling berkaitan. Gambar 1.5 memperlihatkan pohon kriptologi.



Gambar 1.5. Kriptografi dan kriptanalisis adalah cabang bidang ilmu kriptologi.

Sebagian para parktisi sering menggunakan istilah kriptografi dan kriptologi secara bergantian, sebagian lagi membedakan bahwa kriptografi mengacu pada penggunaan praktis teknik-tekink kriptografi, sedangkan kriptologi mengacu pada subjek sebagai bidang studi (seperti halnya biologi, geologi, antropologi, dan sebagainya) [WIK06].

1.2 Tujuan Kriptografi

Dari paparan awal di dalam upabab 1.1, kita dapat merangkum bahwa kriptografi bertujuan untuk memberi layanan keamanan (yang juga dinamakan sebagai aspek-aspek keamanan) sebagai berikut [SCH96][MEN96][WIK06]:

1. **Kerahasiaan** (*confidentiality*), adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak. Di dalam kriptografi, layanan ini direalisasikan dengan menyandikan pesan menjadi cipherteks. Misalnya pesan "Harap datang pukul 8" disandikan menjadi "TrxC#45motyptre!%". Istilah lain yang senada dengan *confidentiality* adalah *secrecy* dan *privacy*. Lebih jauh mengenai metode penyandian akan dibahas di dalam bab-bab selanjutnya.

2. **Integritas data** (*data integrity*), adalah layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman. Dengan kata lain, aspek keamanan ini dapat diungkapkan sebagai pertanyaan: "Apakah pesan yang diterima masih asli atau tidak mengalami perubahan (modifikasi)?". Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi pesan oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam pesan yang sebenarnya. Di dalam kriptografi, layanan ini direalisasikan dengan menggunakan tanda-tangan digital (*digital signature*). Pesan yang telah ditandatangani menyiratkan bahwa pesan yang dikirim adalah asli. Lebih jauh mengenai tanda-tangan digital akan dibahas di dalam Bab Tanda-tangan Digital.

3. **Otentikasi** (*authentication*), adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication* atau *entity authentication*) maupun mengidentifikasi kebenaran sumber pesan (*data origin authentication*). Dua pihak yang saling berkomunikasi harus dapat mengotentikasi satu sama lain sehingga ia dapat memastikan sumber pesan. Pesan yang dikirim melalui saluran komunikasi juga harus diotentikasi asalnya. Dengan kata lain, aspek keamanan ini dapat diungkapkan sebagai pertanyaan: "Apakah pesan yang diterima benar-benar berasal dari pengirim yang benar?". Otentikasi sumber pesan secara implisit juga memberikan kepastian integritas data, sebab jika pesan telah dimodifikasi berarti sumber pesan sudah tidak benar. Oleh karena itu, layanan integritas data selalu dikombinasikan dengan layanan otentikasi umber pesan. Di dalam kriptografi, layanan ini direalisasikan dengan menggunakan tanda-tangan digital (*digital signature*). Tanda-tangan digital menyatakan sumber pesan.

4. **Nirpenyangkalan** (*non-repudiation*), adalah layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan. Sebagai contoh misalkan pengirim pesan memberi otoritas kepada penerima pesan untuk melakukan pembelian, namun kemudian ia menyangkal telah memberikan otoritas tersebut. Contoh lainnya, misalkan seorang pemilik emas mengajukan tawaran kepada toko mas bahwa ia akan menjual emasnya. Tetapi, tiba-tiba harga emas turun drastis, lalu ia membantah telah mengajukan tawaran menjual emas. Dalam hal ini, pihak toko emas perlu prosedur nirpenyangkalan untuk membuktikan bahwa pemilik emas telah melakukan kebohongan.

1.3 Sejarah Kriptografi

Kriptografi mempunyai sejarah yang panjang. Informasi yang lengkap mengenai sejarah kriptografi dapat ditemukan di dalam buku David Kahn yang berjudul *The Codebreakers*. Buku yang tebalnya 1000 halaman ini menulis secara rinci sejarah kriptografi mulai dari penggunaan kriptografi oleh Bangsa Mesir 4000 tahun yang lalu (berupa *hieroglyph* yang tidak standard pada priamid) hingga penggunaan kriptografi pada abad ke-20. Secara historis ada empat kelompok orang yang berkontribusi terhadap perkembangan kriptografi, dimana mereka menggunakan kriptografi untuk menjamin kerahasiaan dalam komunikasi pesan penting, yaitu kalangan militer (termasuk intelijen dan mata-mata), kalangan diplomatik, penulis buku harian, dan pencinta (*lovers*). Di antara keempat kelompok ini, kalangan militer yang memberikan kontribusi paling penting penting karena pengiriman pesan di dalam suasana perang membutuhkan teknik enkripsi dan dekripsi yang rumit.

Sejarah kriptografi sebagian besar merupakan sejarah kriptografi klasik, yaitu metode enkripsi yang menggunakan kertas dan pensil atau mungkin dengan bantuan alat mekanik sederhana. Secara umum algoritma kriptografi klasik dikelompokkan menjadi dua kategori, yaitu algoritma transposisi (*transposition cipher*) dan algoritma substitusi (*substitution cipher*). *Cipher* transposisi mengubah susunan huruf-huruf di dalam pesan, sedangkan cipher substitusi mengganti setiap huruf atau kelompok huruf dengan sebuah huruf atau kelompok huruf lain. Sejarah kriptografi klasik mencatat penggunaan *cipher* transposisi oleh tentara Sparta di Yunani pada permulaan tahun 400 SM. Mereka menggunakan alat yang namanya *scytale* (Gambar 1.6(a)). *Scytale* terdiri dari sebuah kertas panjang dari daun *papyrus* yang dililitkan pada sebuah silinder dari diameter tertentu (diameter silender menyatakan kunci penyandian). Pesan ditulis secara horizontal, baris per baris (lihat Gambar 1.6(b)). Bila pita dilepaskan, maka huruf-huruf di dalamnya telah tersusun secara acak membentuk pesan rahasia. Untuk membaca pesan, penerima pesan harus melilitkan kembali melilitkan kembali kertas tersebut ke silinder yang diameternya sama dengan diameter silinder pengirim. Sedangkang algoritma substitusi paling awal dan paling sederhana adalah *Caesar cipher*, yang digunakan oleh raja Yunani kuno, Julius Caesar. Caranya adalah dengan mengganti setiap karakter di dalam alfabet dengan karakter yang terletak pada tiga posisi berikutnya di dalam susunan alfabet.

(a) **(b)**

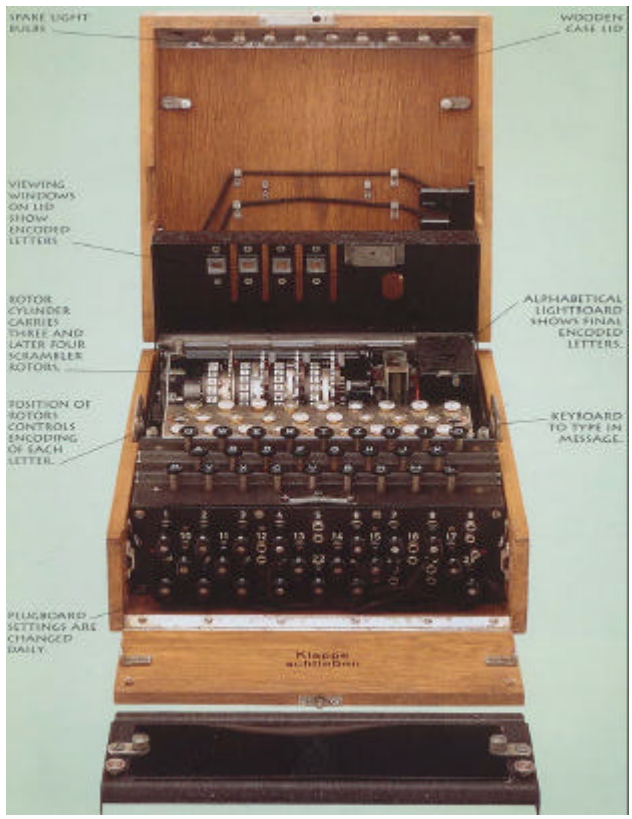
Gambar 1.6. (a) Sebuah *scytale*; (b) Pesan ditulis secara horizontal, baris per baris. Bila kertas dilepaskan, maka pesan yang terbentuk adalah cipherteks.

Kriptografi juga digunakan untuk tujuan keamanan. Kalangan gereja pada masa awal agama Kristen menggunakan kriptografi untuk menjaga tulisan relijius dari gangguan otoritas politik atau budaya yang dominan saat itu. Mungkin yang sangat terkenal adalah "Angka si Buruk Rupa (*Number of the Beast*) di dalam Kitab Perjanjian Baru. Angka "666" menyatakan cara kriptografik (yaitu dienkripsi) untuk menyembunyikan pesan berbahaya; para ahli percaya bahwa pesan tersebut mengacu pada Kerajaan Romawi [WIK06].

Di India, kriptografi digunakan oleh pencinta (*lovers*) untuk berkomunikasi tanpa diketahui orang. Bukti ini ditemukan di dalam buku *Kama Sutra* yang merekomendasikan wanita seharusnya mempelajari seni memahami tulisan dengan *cipher*.

Pada Abad ke-17, sejarah kriptografi mencatat korban ketika ratu Skotlandia, Queen Mary, dipancung setelah surat rahasianya dari balik penjara (surat terenkrpsi yang isinya rencana membunuh Ratu Elizabeth I) berhasil dipecahkan oleh seorang pemecah kode.

Seperti yang telah disebutkan di atas bahwa kriptografi umum digunakan di kalangan militer. Pada Perang Dunia ke II, Pemerintah Nazi Jerman membuat mesin enkripsi yang dinamakan *Enigma*. (Gambar 1.7). Mesin yang menggunakan beberapa buah *rotor* (roda berputar) ini melakukan enkripsi dengan cara yang sangat rumit. Namun *Enigma cipher* berhasil dipecahkan oleh pihak Sekutu dan keberhasilan memecahkan *Enigma* sering dikatakan sebagai faktor yang memperpendek perang dunia ke-2.



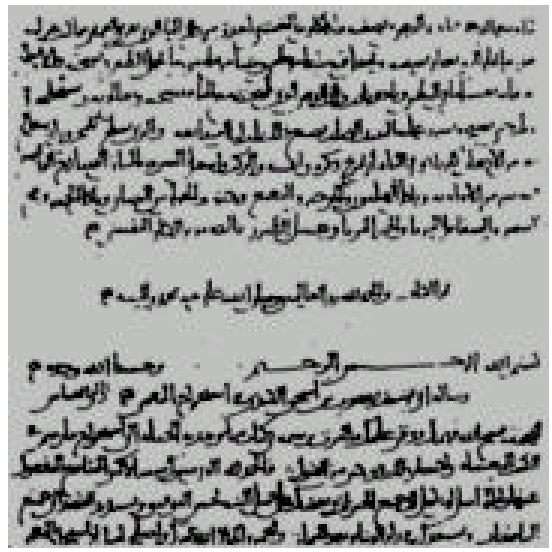
Gambar 1.7. Mesin enkripsi *Enigma* yang digunakan oleh tentara Jerman pada masa Perang Dunia ke-2. *Enigma cipher* berhasil dipecahkan oleh Sekutu.

Kriptografi modern dipicu oleh perkembangan peralatan komputer digital. Dengan komputer digital, *cipher* yang lebih kompleks menjadi sangat mungkin untuk dapat dihasilkan. Tidak seperti kriptografi klasik yang mengenkripsi karakter per karakter (dengan menggunakan alfabet tradisionil), kriptografi modern beroperasi pada *string biner*. *Cipher* yang kompleks seperti DES (*Data Encryption Standard*) dan penemuan algoritma RSA adalah algoritma kriptografi modern yang paling dikenal di dalam sejarah kriptografi modern. Kriptografi modern tidak hanya berkaitan dengan teknik menjaga kerahasiaan pesan, tetapi juga melahirkan konsep seperti tanda-tangan digital dan sertifikat digital. Dengan kata lain, kriptografi modern tidak hanya memberikan aspek keamanan *confidentiality*, tetapi juga aspek keamanan lain seperti otentikasi, integritas data, dan nirpenyangkalan sebagaimana sudah dijelaskan di dalam upa-bab 1.2.

1.4 Kriptanalisis

Sejarah kriptografi paralel dengan sejarah kriptanalisis (*cryptanalysis*) , yaitu bidang ilmu dan seni untuk memecahkan cipherteks. Kata "kriptanalisis" sendiri relatif masih baru (pertama kali diungkapkan oleh William Friedman pada tahun 1920), namun sebenarnya teknik kriptanalisis sudah ada sejak abad ke-9. Adalah seorang ilmuwan Arab pada Abad IX bernama Abu Yusuf Yaqub Ibnu Ishaq Ibnu As-Sabbah Ibnu 'Omran Ibnu Ismail Al-Kindi, atau yang lebih dikenal sebagai Al-Kindi yang menulis buku tentang seni memecahkan kode. Dalam buku yang berjudul '*Risalah fi Istikhraj al-Mu'amma* (*Manuscript for the Deciphering Cryptographic Messages*), ia menuliskan naskah untuk menguraikan kode-kode rahasia (Gambar 1.8). Di dalam buku tersebut Al-Kindi memperkenalkan teknik penguraian kode atau atau sandi yang sulit dipecahkan. Ia juga mengklasifikasikan sandi rahasia itu serta menjelaskan ilmu fonetik Arab dan sintaksisnya. Yang paling penting lagi, dalam bukunya ini ia mengenalkan penggunaan beberapa teknik statistika untuk memecahkan kode-kode rahasia (dikutip dari Republika *online*, 16 Juni 2006).

Apa yang dilakukan oleh Al-Kindi didalam kriptanalisis dikenal dengan nama teknik **analisis frekuensi**, yaitu teknik untuk memecahkan cipherteks berdasarkan frekuensi kemunculan karakter di dalam pesan dan kaitannya dengan frekuensi kemunculan karakter di dalam alfabet. Analisis frekuensi dilatarbelakangi oleh fakta bahwa *cipher* gagal menyembunyikan statistik kemunculan karakter di dalam cipherteksnya. Misalnya, di dalam Bahasa Inggris huruf "E" adalah huruf paling sering muncul di dalam kalimat-kalimat berbahas Inggris. Jika di dalam cipherteks terdapat huruf yang paling sering muncul, maka kemungkinan besar huruf tersebut di dalam plainteksnya adalah huruf E (teknik ini akan dijleaskan di dalam Bab 4). Berbagai *cipher* klasik berhasil dipecahkan dengan teknik analisis frekuensi ini.



Gambar 1.8. Halaman pertama buku Al-Kindi, *Manuscript for the Deciphering Cryptographic* (sumber: wikipedia).

Teknik analisis frekuensi masih digunakan di dalam kriptanalisis modern, tetapi karena *cipher* semakin rumit, maka pendekatan matematik masih tetap dominan dalam melakukan kriptanalisis. Perkembangan komputer pun ikut membantu kegiatan kriptanilisis. Sejarah kriptanalissi mencatat hasil gemilang seperti pemecahan Telegram Zimmermann yang membawa Amerika Serikat ke kancah Perang Dunia I, dan pemecahan cipherteks dari mesin *Enigma* ikut andil mengakhiri Perang Dunia II [WIK06].

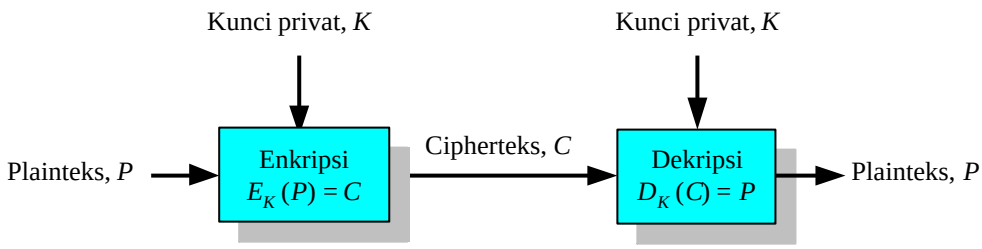
1.5 Kriptografi Kunci-Simetri dan Nirsimetri

Selain berdasarkan sejarah yang membagi kriptografi menjadi kriptografi klasik dan kriptografi modern, maka berdasarkan kunci yang digunakan untuk enkripsi dan dekripsi, kriptografi dapat dibedakan lagi menjadi **kriptografi kunci-simetri** (*symmetric-key cryptography*) dan **kriptografi kunci-nirsimetri** (*asymmetric-key cryptography*).

Pada sistem kriptografi kunci-simetri, kunci untuk enkripsi sama dengan kunci untuk dekripsi, oleh karena itulah dinamakan kriptografi simetri (Gambar 1.9). Istilah lain untuk kriptografi kunci-simetri adalah kriptografi kunci privat (*private-key cryptography*), kriptografi kunci rahasia (*secret-key cryptography*), atau kriptografi konvensional (*conventional cryptography*). Sistem kriptografi kunci-simetri (atau disingkat menjadi "kriptografi simetri" saja), mengasumsikan pengirim dan penerima pesan sudah berbagi kunci yang sama sebelum bertukar pesan. Keamanan sistem kriptografi simetri terletak pada kerahasiaan kuncinya. Kriptografi simetri merupakan satu-satunya jenis kriptografi yang dikenal dalam catatan sejarah hingga tahun 1976. Semua algoritma kriptografi klasik termasuk ke dalam sistem kriptografi simetri. Di sisi lain, ada puluhan algoritma kriptografi modern yang termasuk ke dalam sistem kriptografi simetri, diantaranya adalah

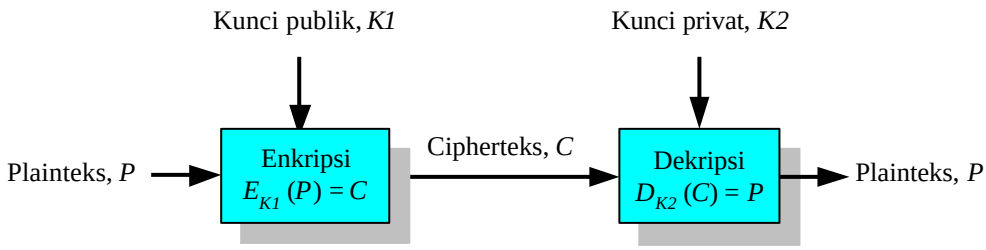
DES (*Data Encryption Standard*), *Blowfish*, *Twofish*, *Triple-DES*, *IDEA*, *Serpent*, dan yang terbaru adalah *AES* (*Advanced Encryption Standard*).

Secara umum, *cipher* yang termasuk ke dalam kriptografi simetri beroperasi dalam mode blok (*block cipher*), yaitu setiap kali enkripsi/dekripsi dilakukan terhadap satu blok data (yang berukuran tertentu), atau beroperasi dalam mode aliran (*stream cipher*), yaitu setiap kali enkripsi/dekripsi dilakukan terhadap satu bit atau satu *byte* data. Aplikasi kriptografi simetri yang utama adalah adalah melindungi kerahasiaan data yang dikirim melalui saluran tidak aman dan melindungi kerahasiaan data yang disimpan pada media yang tidak aman. Kelemahan dari sistem ini adalah baik pengirim maupun penerima pesan harus memiliki kunci yang sama, sehingga pengirim pesan harus mencari cara yang aman untuk memberitahukan kunci kepada penerima pesan.



Gambar 1.9. Skema kriptografi simetri. Kunci enkripsi sama dengan kunci dekripsi, yaitu *K*.

Jika kunci untuk enkripsi tidak sama dengan kunci untuk dekripsi, maka kriptografinya dinamakan sistem kriptografi nirsimetri. Nama lainnya adalah **kriptogarfi kunci-publik** (*public-key cryptography*), sebab kunci untuk enkripsi tidak rahasia dan dapat diketahui oleh siapapun (diumumkan ke publik), sementara kunci untuk dekripsi hanya diketahui oleh penerima pesan (karena itu rahasia). Pada kriptografi jenis ini, setiap orang yang berkomunikasi mempunyai sepasang kunci, yaitu kunci privat dan kunci publik. Pengirim mengenkripsi pesan dengan menggunakan kunci publik si penerima pesan (*receiver*). Hanya penerima pesan yang dapat mendekripsi pesan karena hanya ia yang mengetahui kunci privatnya sendiri (Gambar 1.10). Contoh algoritma kriptografi kunci-publik diantaranya *RSA*, *Elgamal*, *DSA*, dan sebagainya.



Gambar 1.10. Skema kriptografi nirsimetri. Kunci enkripsi tidak sama dengan kunci dekripsi. Kunci enkripsi bersifat publik (tidak rahasia), sedangkan kunci dekripsi privat (rahasia).

Kriptografi kunci-publik dapat dapat dianalogikan seperti kotak surat yang terkunci dan memiliki lubang untuk memasukkan surat. Setiap orang dapat memasukkan surat ke dalam kotak surat tersebut, tetapi hanya pemilik kotak yang dapat membuka kotak dan membaca surat di dalamnya karena ia yang memiliki kunci. Keuntungan sistem ini ada dua. Pertama, tidak ada kebutuhan untuk mendistribusikan kunci privat sebagaimana pada sistem kriptografi simetri. Kunci publik dapat dikirim ke penerima melalui saluran yang sama dengan saluran yang digunakan untuk mengirim pesan. Saluran untuk mengirim pesan umumnya tidak aman.

Kedua, jumlah kunci dapat ditekan. Untuk berkomunikasi secara rahasia dengan banyak orang tidak perlu kunci rahasia sebanyak jumlah orang tersebut, cukup membuat dua buah kunci, yaitu kunci publik bagi para koresponden untuk mengenkripsi pesan, dan kunci privat untuk mendekripsi pesan. Berbeda dengan kriptografi kunci-simetris dimana jumlah kunci yang dibuat adalah sebanyak jumlah pihak yang diajak berkorespondensi. Contoh penggunaan, misalkan jaringan komputer menghubungkan komputer karyawan di kantor cabang dengan komputer menejer di kantor pusat. Seluruh kepala cabang diberitahu bahwa kalau mereka mengirim laporan ke menejer di kantor pusat, mereka harus mengenkripsi laporan tersebut dengan kunci publik menejer (kunci publik menejer diumumkan kepada seluruh kepala cabang). Untuk mengembalikan laporan tersandi ke laporan semula, hanya menejer yang dapat melakukan dekripsi, karena hanya dialah yang memegang kunci privat. Selama proses transmisi cipherteks dari kantor cabang ke kantor pusat melalui saluran komunikasi mungkin saja data yang dikirim disadap oleh pihak ketiga, namun pihak ketiga ini tidak dapat mengembalikan cipherteks ke plainteksnya karena ia tidak mengetahui kunci untuk dekripsi.

Meski berusia relatif muda (sejak 1976), kriptografi kunci-publik mempunyai kontribusi yang luar biasa dibandingkan dengan sistem kriptografi simetri. Kontribusi yang paling penting adalah tanda-tangan digital pada pesan untuk memberikan aspek keamanan otentikasi, integritas data, dan nirpenyangkalan. Tanda-tangan digital adalah nilai kriptografis yang bergantung pada isi pesan dan kunci yang digunakan. Pengirim pesan mengenkripsi pesan (yang sudah diringkas) dengan kunci privatnya, hasil enkripsi inilah yang dinamakan tanda-tangan digital. Tanda-tangan digital dilekatkan (*embed*) pada pesan asli. Penerima pesan memverifikasi tanda-tangan digital dengan menggunaklan kunci publik. Gambar 1.11 memperlihatkan sebuah surat elektronik yang di bagia bawah sudah dibubuhi tanda-tangan digital (di antara BEGIN dan END SIGNATURE).

Kepada Yth.
Bapak Dekan FTI
Di Tempat

Dengan hormat.
Bersama surat ini saya ingin mengabarkan bahwa nilai skripsi mahasiswa yang bernama Faisal Saleh dengan NIM 13902021 adalah 86,5 atau dalam nilai indeks A. Sidang skripsi sudah dilakukan pada Hari Rabu Tanggal 21 Januari 20 Juli 2005.

Atas perhatian Bapak saya ucapkan terima kasih.

Bandung, 25 Juli 2005

Dosen Pembimbing Skripsi

Ir. Ahmad Agus

-----BEGIN PGP SIGNATURE-----

iQA/AwUAQnibsbPbxejK4Bb3EQJXvQCg8zN6UL0xnwBTPR5
FfWNt4uxh3AEAn2NC/G2VTUrLpcSyo2l/S/D/+rUl=pZeh

-----END PGP SIGNATURE-----

Gambar 1.11 Sebuah surat yang dibubuhi tanda-tangan digital

Pembahasan lebih lanjut mengenai keseluruhan materi buku ini akan diberikan di dalam bab-bab sesudah ini.