Prinsip Kerja Kriptografi dalam Mengamankan Informasi

Dian Wirdasari

Abstrak

Kriptografi adalah ilmu sekaligus seni untuk menjaga keamanan pesan (*message*) dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Proses menyandikan plainteks menjadi cipherteks disebut enkripsi (*encryption*) atau *enciphering* sedangkan proses mengembalikan cipherteks menjadi plainteksnya disebut dekripsi (decryption) atau *deciphering*. Aplikasi enkripsi dan dekripsi adalah: (1) Pengiriman data melalui saluran komunikasi (*data encryption on motion*), (2) Penyimpanan data di dalam *disk storage*. (*data encryption at rest*). 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 cipherteks menjadi plainteks.

Kata Kunci: Kriptografi, Enkripsi, Dekripsi

A. PENDAHULUAN

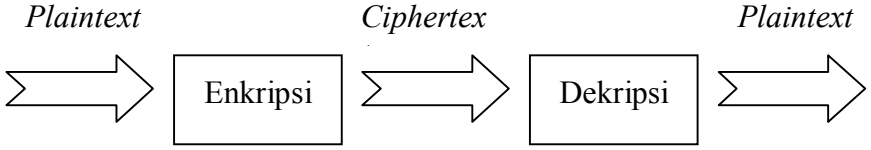
Seorang pengirim pesan (*sender*) adalah orang yang ingin mengirim pesan kepada seorang penerima (*receiver*). Pengirim menginginkan pesan dapat dikirim secara aman, yaitu ia yakin bahwa tidak ada pihak lain yang dapat membaca isi pesan. Pesan adalah data atau informasi yang dapat dibaca dan dimengerti 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@

a. 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. Proses Enkripsi dan Dekripsi

b. Kriptografi

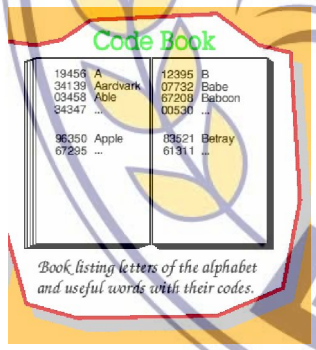
Definisi lama: **kriptografi** adalah ilmu sekaligus seni untuk menjaga keamanan pesan (*message*) dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. **Kriptografi** adalah ilmu sekaligus seni untuk menjaga keamanan pesan (*message*) [Schneier, 1996]. Kata cryptography berasal dari kata Yunani yaitu ”kryptos” yang artinya tersembunyi dan ”graphein” yang berarti menulis.

Algoritma kriptografi adalah:

- aturan untuk *enciphering* dan *deciphering*
- fungsi matematika yang digunakan untuk enkripsi dan dekripsi.

c. Encoding dan Decoding

Encoding adalah Transformasi dari plainteks menjadi kode sedangkan ***decoding*** adalah proses transformasi kebalikan dari kode menjadi plainteks. Buku kode (*codebook*) merupakan dokumen yang digunakan untuk mengimplementasikan suatu kode. Buku kode terdiri dari tabel *lookup* (*lookup table*) untuk *encoding* dan *decoding*.



Cipher tidak sama dengan kode (*code*). Kode mempunyai sejarah tersendiri di dalam kriptografi. *Codebreaker* adalah orang yang memecahkan kode untuk menemukan plainteks.

Contoh kode:

Pesan: kapal api datang
Kode: hutan bakau hancur

Pesan: kapal api datang
Kode: xyztvq bkugbf hjqpot

d. Kunci Kriptografi

Enkripsi dan Dekripsi pada umumnya membutuhkan penggunaan sejumlah informasi rahasia, disebut sebagai kunci. **Kunci** adalah parameter yang digunakan untuk transformasi *enciphering* dan *deciphering*. 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*)

e. Sistem Kriptografi

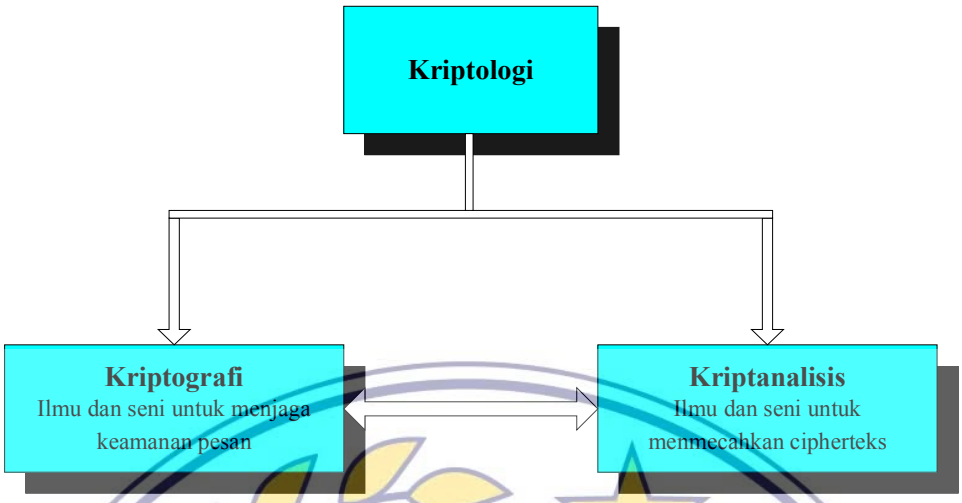
Sistem kriptografi (atau ***cryptosystem***) adalah algoritma kriptografi, plainteks, cipherteks, dan kunci. *Cryptographic system* atau *cryptosystem* adalah suatu fasilitas untuk mengkonversikan plaintext ke ciphertext dan sebaliknya. Dalam sistem ini, seperangkat parameter yang menentukan transformasi pencipheran tertentu disebut suatu set kunci. Proses enkripsi dan dekripsi diatur oleh satu atau beberapa kunci kriptografi.

f. Penyadap

Penyadap (*eavesdropper*) adalah orang yang mencoba menangkap pesan selama ditransmisikan. Nama lain: *enemy*, *adversary*, *intruder*, *interceptor*, *bad guy*

g. Kriptanalisis dan kriptologi

Kriptanalisis (*cryptanalysis*) adalah ilmu dan seni untuk memecahkan cipherteks menjadi plainteks tanpa mengetahui *kunci* yang diberikan. Pelakunya disebut **kriptanalis**. **Kriptanalisis** merupakan lawan dari **kriptografi**. **Kriptologi** (*cryptology*) adalah studi mengenai kriptografi dan kriptanalisis.



Gambar 2. Pembagian Ilmu Kriptografi

Perancang algoritma kriptografi disebut **kriptografer**. Persamaan kriptografer dan kriptanalis adalah keduanya sama-sama menerjemahkan cipherteks menjadi plainteks. Perbedaan kriptografer dan kriptanalis adalah:

- Kriptografer bekerja atas legitimasi pengirim atau penerima pesan
- Kriptanalis bekerja atas nama penyadap yang tidak berhak.

B. SEJARAH KRIPTOGRAFI

Kriptografi memiliki sejarah yang panjang dan mengagumkan. Penulisan rahasia ini dapat dilacak kembali ke 3000 tahun SM saat digunakan oleh bangsa Mesir. Mereka menggunakan hieroglyphcs untuk menyembunyikan tulisan dari mereka yang tidak diharapkan. Hieroglyphcs diturunkan dari bahasa Yunani hieroglyphica yang berarti ukiran rahasia. Hieroglyphs berevolusi menjadi hieratic, yaitu stylized script yang lebih mudah untuk digunakan.

Sekitar awal tahun 400 SM, kriptografi militer digunakan oleh bangsa Spartan di Yunani. Mereka menggunakan alat yang disebut *scytale*. *Scytale* merupakan 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 3. Kriptografi dengan *Scytale*

Sejarah lengkap kriptografi dapat ditemukan di dalam buku David Kahn, "*The Codebreakers*" . Empat kelompok orang yang menggunakan dan berkontribusi pada kriptografi:

1. Militer (termasuk intelijen dan mata-mata)
2. Korp diplomatik
3. *Diarist*
4. *Lovers*

Kriptografi juga digunakan untuk alasan keagamaan, untuk menjaga tulisan relijius dari gangguan otoritas politik atau budaya yang dominan saat itu. Contoh: "666" atau "Angka si Buruk Rupa (*Number of the Beast*) di dalam Kitab Perjanjian Baru.

Sekitar 50 SM, Julius Caesar, kaisar Roma, menggunakan cipher substitusi untuk mengirim pesan ke Marcus Tullius Cicero. Pada cipher ini, huruf-huruf alfabet disubstitusi dengan huruf-huruf yang lain pada alfabet yang sama. Karena hanya satu alfabet yang digunakan, cipher ini merupakan substitusi monoalfabetik. Cipher semacam ini mencakup penggeseran alfabet dengan 3 huruf dan mensubstitusikan huruf tersebut. Substitusi ini kadang dikenal dengan C3 (untuk Caesar menggeser 3 tempat). Secara umum sistem cipher Caesar dapat ditulis sebagai berikut:

$$Zi = Cn(Pi)$$

Dimana Zi adalah karakter-karekter ciphertext, Cn adalah transformasi substitusi alfabetik, n adalah jumlah huruf yang digeser, dan Pi adalah karakter-karakter plaintext.

Disk mempunyai peranan penting dalam kriptografi sekitar 500 tahun yang lalu. Di Italia sekitar tahun 1460, Leon Battista Alberti mengembangkan disk cipher untuk enkripsi. Sistemnya terdiri dari dua disk konsentris. Setiap disk memiliki alfabet di sekelilingnya, dan dengan memutar satu disk berhubungan dengan yang lainnya, huruf pada satu alfabet dapat ditransformasi ke huruf pada alfabet yang lain.

Tidak ditemukan catatan kriptografi di Cina dan Jepang hingga abad 15. 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 pernah mencatat korban di Inggris. Queen Mary of Scotland, dipancung setelah pesan rahasianya dari balik penjara (pesan terenkripsi yang isinya rencana membunuh Ratu Elizabeth I) pada Abad Pertengahan berhasil dipecahkan oleh Thomas Phelippes, seorang pemecah kode.

Bangsa Arab menemukan cryptanalysis karena kemahirannya dalam bidang matematika, statistik, dan linguistik. Karena setiap orang muslim harus menambah pengetahuannya, mereka mempelajari peradaban terdahulu dan mendekodekan tulisan-tulisannya ke huruf-huruf Arab. Pada tahun 815, Caliph al-Mamun mendirikan House of Wisdom di Baghdad yang merupakan titik pusat dari usaha-usaha translasi. Pada abad ke-9, filsuf Arab al-Kindi menulis risalat (ditemukan kembali tahun 1987) yang diberi judul "A Manuscript on Deciphering Cryptographic Messages".

Pada 1790, Thomas Jefferson mengembangkan alat enkripsi dengan menggunakan tumpukan yang terdiri dari 26 disk yang dapat diputar secara individual. Pesan dirakit dengan memutar setiap disk ke huruf yang tepat di bawah batang berjajar yang menjalankan panjang tumpukan disk. Kemudian, batang berjajar diputar dengan sudut tertentu, A, dan huruf-huruf di bawah batang adalah pesan yang terenkripsi. Penerima akan menjajarkan karakter-karakter cipher di bawah batang berjajar, memutar batang kembali dengan sudut A dan membaca pesan plaintext. Sistem disk digunakan secara luas selama perang sipil US. Federal Signal Officer mendapatkan hak paten pada sistem disk mirip dengan yang ditemukan oleh Leon Battista Alberti di Italia, dan dia menggunakannya untuk mengkode dan mendekodekan sinyal-sinyal bendera diantara unit-unit.

Pada 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.

Gambar 4. Enigma

Sistem Unix menggunakan cipher substitusi yang disebut ROT 13 yang menggeser alfabet sebanyak 13 tempat. Penggeseran 13 tempat yang lain membawa alfabet kembali ke posisi semula, dengan demikian mendekodekan pesan.

Mesin kriptografi mekanik yang disebut Hagelin Machine dibuat pada tahun 1920 oleh Boris Hagelin di Scockholm, Swedia. Di US, mesin Hagelin dikenal sebagai M-209.

Pada tahun 20-an, Herbert O. Yardley bertugas pada organisasi rahasia US MI-8 yang dikenal sebagai "Black Chamber". MI-8 menjebol kode-kode sejumlah negara. Selama konferensi Angkatan Laut Washington tahun 1921-1922, US membatasi negosiasi dengan Jepang karena MI-8 telah memberikan rencana negosiasi Jepang yang telah disadap kepada sekretaris negara US. Departemen negara menutup MI-8 pada tahun 1929 sehingga Yardley merasa kecewa. Sebagai wujud kekecewaanya, Yardley menerbitkan buku The American Black Chamber, yang menggambarkan kepada dunia rahasia dari MI-8. Sebagai konsekuensinya, pihak Jepang menginstal kode-kode baru. Karena kepeloporannya dalam bidang ini, Yardley dikenal sebagai "Bapak Kriptografi Amerika".

C. KRIPTANALISIS

Sejarah kriptografi paralel dengan sejarah kriptanalisis (*cryptanalysis*), yaitu bidang ilmu dan seni untuk memecahkan cipherteks. Teknik kriptanalisis sudah ada sejak abad ke-9. Dikemukakan pertama kali oleh 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**.

Al-Kindi menulis buku tentang seni memecahkan kode, buku yang berjudul '*Risalah fi Istikhraj al-Mu'amma* (*Manuscript for the Deciphering Cryptographic Messages*). Al-Kindi menemukan frekuensi perulangan huruf di dalam Al-Quran. Teknik yang digunakan Al-Kindi kelak dinamakan **analisis frekuensi**. Yaitu teknik untuk memecahkan cipherteks berdasarkan frekuensi kemunculan karakter di dalam pesan.

Gambar 5. Halaman pertama buku Al-Kindi, *Manuscript for the Deciphering Cryptographic*

D. APLIKASI KRIPTOGRAFI

Aplikasi enkripsi dan dekripsi adalah: (1) Pengiriman data melalui saluran komunikasi (*data encryption on motion*), (2) Penyimpanan data di dalam *disk storage*. (*data encryption at rest*). 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 cipherteks menjadi plainteks.

Contoh-contoh enkripsi dan dekripsi data pada saluran komunikasi:

- Sinyal yang ditransmisikan dalam percakapan dengan *handphone*.
- Nomor PIN kartu ATM yang ditransmisikan dari mesin ATM ke komputer bank.
- Nomor PIN kartu kredit pada transaksi *e-commerce* di internet.

Contoh-contoh enkripsi dan dekripsi pada data tersimpan:

1. Dokumen teks

Plainteks (plain.txt):

```
Kriptografi mempunyai 2 (dua)
bagian yang penting, yaitu
enkripsi dan dekripsi. Enkripsi
adalah proses dari penyandian
pesan asli menjadi pesan yang
tidak dapat diartikan seperti
aslinya. Dekripsi sendiri
berarti merubah pesan yang sudah
disandikan menjadi pesan
aslinya.
```

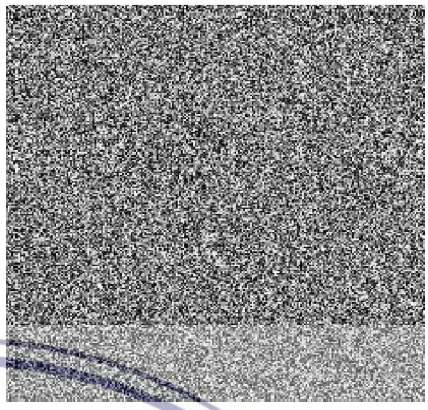
Cipherteks (cipher.txt):

```
Ztâxzp/épêp/qtüyp{p}<yp{p}/sx/•p
}âpx; t|äzp}/qp}êpz
/étzp{x/zt•_épêp/|t}t|äzp}/qp}êp
z/étzp{x/zt•x êp}tâpé /}v_êp
}v/|tüp}vzpz/|t}yä/{pää=/\tütz|t
}äyä/{p p_psp{p
w/p}|t}äyä/{ppz<p}pz/zt•xâx}v/ds
püx/sp{ v/qpüä_|t}t
âpé/spüx/sp{p|/•péxü=/]
p{äüx_|ttüzp/|t}vpâpzp} /qpwåp
päâztwxsä•p}/|tützp=
```

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	□□ät|•pâ/ztwxsä•p}	}/|tü	spüx/
000004	épêp/|t}t|äzp}/qpêpz	qp}êp z	wxsä
000005	étzp{x/zt•xâx}v□êp}	pää/p sp	étzp{
000006	spüx/sp{p|/•péxü=/]	xâx}v	ttüzp/|
000007	Ztâxzp/épêp/qtüypp}<	äzp}	}äyä/{
000008	qpwåp/{pää/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

E. NOTASI MATEMATIS

Misalkan:

C = cipherteks
P = plainteks

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 cipherteks 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.

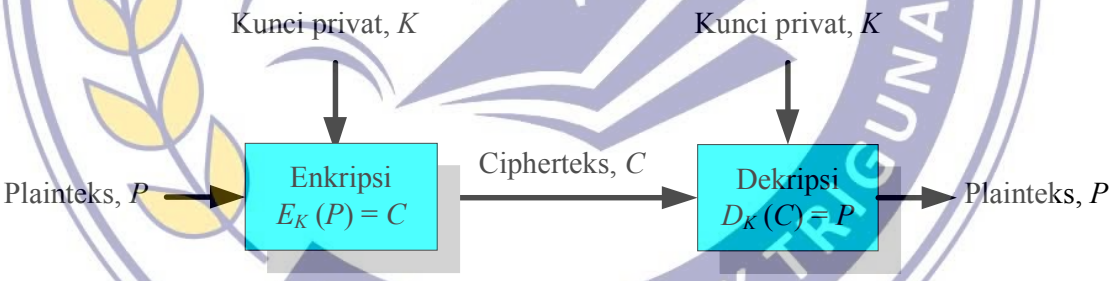
Pada sistem kriptografi modern, kekuatan kriptografinya terletak pada kunci, yang berupa deretan karakter atau bilangan bulat, dijaga kerahasiaannya. Dengan menggunakan kunci K, maka fungsi enkripsi dan dekripsi menjadi:

$$E_K(P) = C$$

$$D_K(C) = P$$

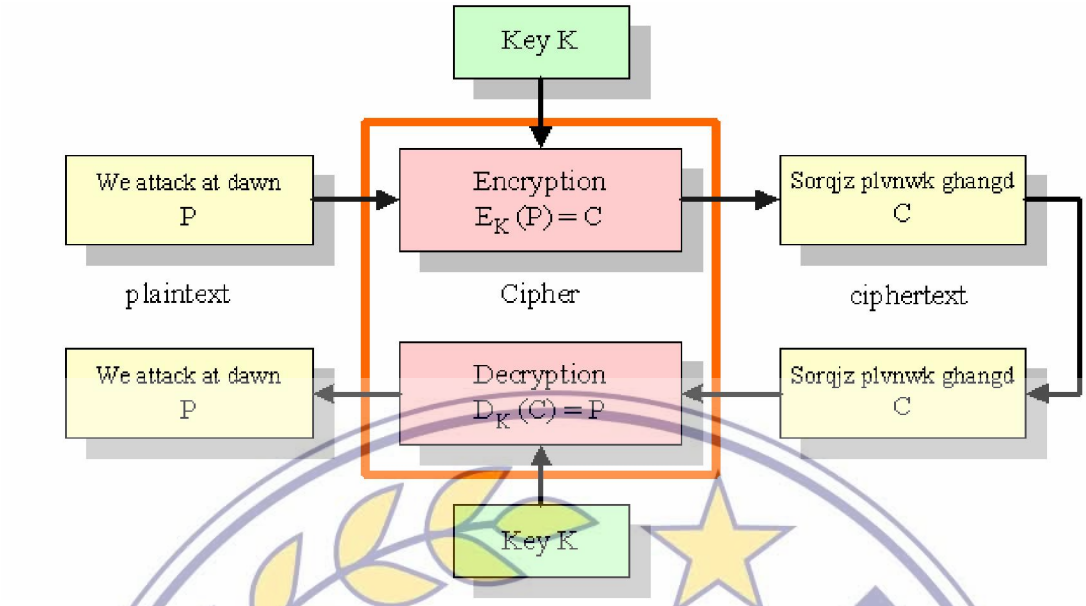
dan kedua fungsi ini memenuhi:

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



Gambar 6. Enkripsi dan Dekripsi dengan Kunci yang sama

Untuk beberapa mekanisme enkripsi, kunci yang sama digunakan baik untuk enkripsi dan dekripsi; untuk mekanisme yang lain, kunci yang digunakan untuk enkripsi dan dekripsi berbeda. Dua tipe dasar dari teknologi kriptografi adalah, pertama *symmetric key* (*secret/private key*) *cryptography*, algoritma kriptografinya disebut algoritma simetri atau algoritma konvensional, dan yang kedua *asymmetric key* (*public key*) *cryptography*, algoritma kriptografinya disebut algoritma asimetri atau algoritma kunci-publik.



Gambar 7. Skema Algoritma Simetri

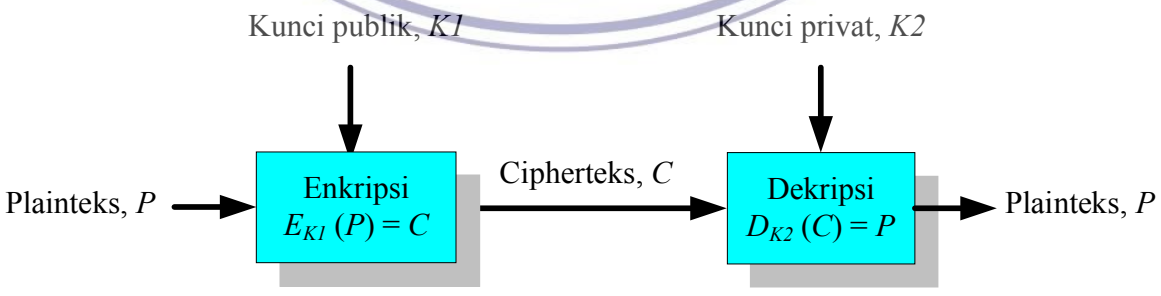
Pada *symmetric key* cryptography, baik pengirim maupun penerima memiliki kunci rahasia yang umum. Kunci-kunci ini harus dirahasiakan. Oleh karena itulah sistem ini sering disebut sebagai *secret-key ciphersystem*. Jumlah kunci yang dibutuhkan umumnya adalah :

$$ {}_nC_2 = \frac{n(n-1)}{2} $$

Dengan *n* menyatakan banyaknya pengguna.

Contoh algoritma simetri antara lain: *DES* (*Data Encyption Standard*), Blowfish, IDEA.

Pada *asymmetric key* cryptography, digunakan dua buah kunci. Satu kunci yang disebut kunci publik (*public* key) dapat dipublikasikan, sedang kunci yang lain disebut kunci privat (*private key*) harus dirahasiakan. Pengirim dan penerima masing-masing berbagi kunci publik dan privat, misalkan kunci enkripsi adalah *K*1 dan kunci dekripsi yang adalah *K*2, yang dalam hal ini *K1* □□*K2*. Proses menggunakan sistem ini dapat diterangkan secara sederhana sebagai berikut : bila A ingin mengirimkan pesan kepada B, A dapat menyandikan pesannya dengan menggunakan kunci publik B, dan bila B ingin membaca surat tersebut, ia perlu mendekripsikan surat itu dengan kunci privatnya. Dengan demikian kedua belah pihak dapat menjamin asal surat serta keaslian surat tersebut, karena adanya mekanisme ini. Contoh algoritma asimetri antara lain: *RSA* (Rivest-Shamir-Adleman) dan Merkle-Hellman Scheme.



Gambar 8. Enkripsi dan Dekripsi dengan Kunci yang Berbeda

Kriptografi saat ini lebih dari enkripsi dan dekripsi saja. Otentikasi menjadi bagian dari kehidupan kita sama seperti privasi. Kita menggunakan otentikasi dalam kehidupan sehari-hari, sebagai contoh saat kita menandatangani sejumlah dokumen dan saat kita berpindah ke dunia dimana keputusan dan persetujuan kita dikomunikasikan secara elektronis, kita membutuhkan teknik-teknik untuk otentikasi. Kriptografi menyediakan mekanisme untuk prosedur semacam itu. *Digital signature* (tanda tangan digital) mengikat dokumen dengan kepemilikan kunci tertentu, sedangkan *digital timestamp* mengikat dokumen dengan pembuatnya pada saat tertentu.
Keuntungan sistem ini:

1. Tidak ada kebutuhan untuk mendistribusikan kunci privat sebagaimana pada sistem kriptografi simetri.
2. Kunci publik dapat dikirim ke penerima melalui saluran yang sama dengan saluran yang digunakan untuk mengirim pesan. Saluran untuk mengirim pesan umumnya tidak aman
3. Kedua, jumlah kunci dapat ditekan.

F. LAYANAN KRIPTOGRAFI YANG DISEDIAKAN

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.

Karakteristik cryptosytem yang baik sebagai berikut :

1. Keamanan sistem terletak pada kerahasiaan kunci dan bukan pada kerahasiaan algoritma yang digunakan.
2. Cryptosystem yang baik memiliki ruang kunci (keyspace) yang besar.
3. Cryptosystem yang baik akan menghasilkan ciphertext yang terlihat acak dalam seluruh tes statistik yang dilakukan terhadapnya.
4. Cryptosystem yang baik mampu menahan seluruh serangan yang telah dikenal sebelumnya

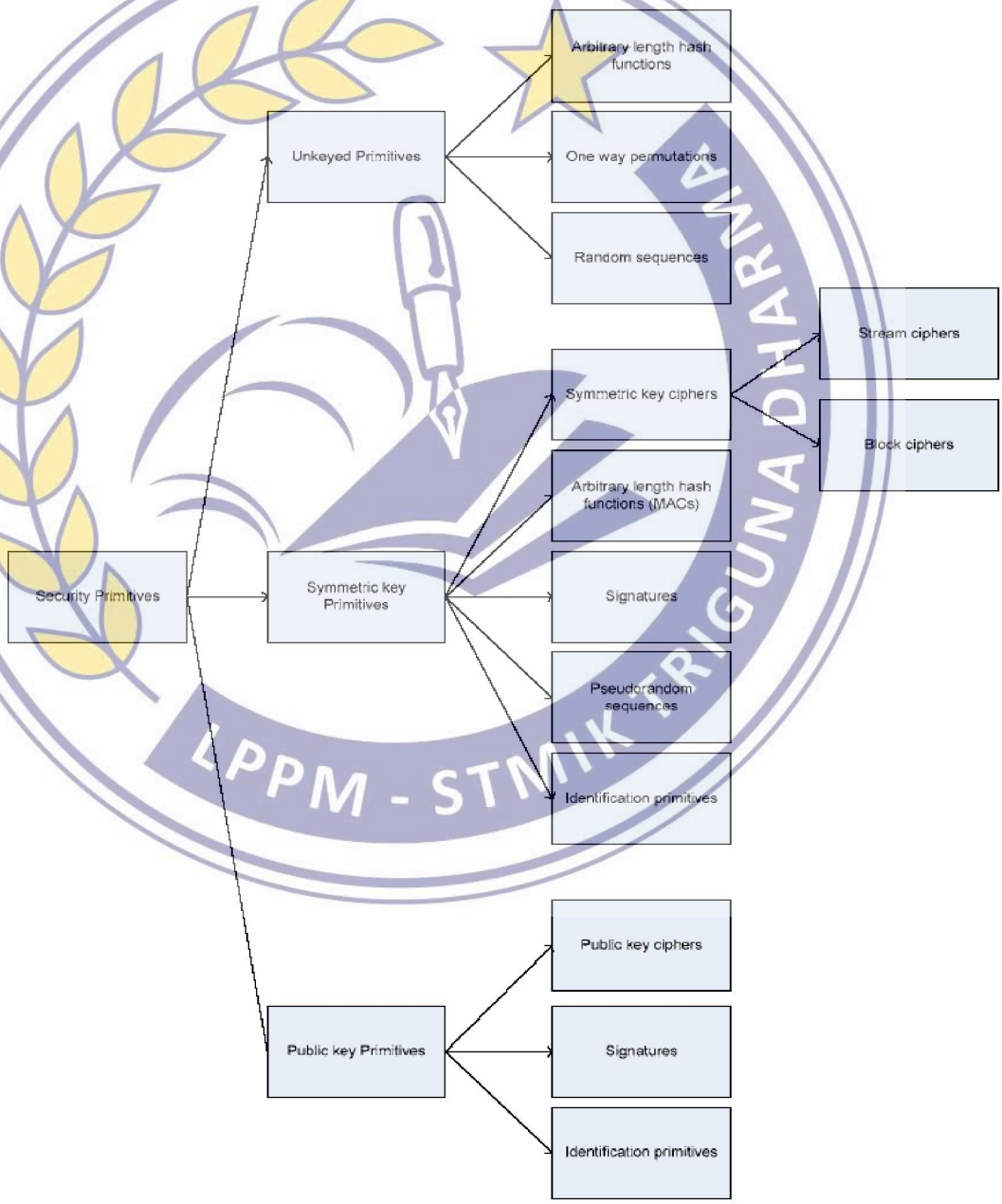
G. TAKSONOMI PRIMITIF-PRIMITIF KRIPTOGRAFI

Ada beberapa dasar tool kriptografi (primitif) yang digunakan untuk mendukung keamanan informasi. Contoh dari primitif termasuk skema enkripsi, fungsi hash, dan skema tanda tangan digital. Gambar 2.8 menunjukkan daftar primitif yang dimaksud dan bagaimana hubungan mereka. Primitif-primitif ini harus dapat dievaluasi berdasarkan beberapa kriteria seperti:

- Level keamanan. Hal ini biasanya sulit untuk dihitung. Sering diwakili dengan jumlah operasi yang dibutuhkan (menggunakan metode terbaik yang diketahui) untuk melawan tujuan yang diharapkan. Level keamanan biasanya didefinisikan work factor.
- Fungsionalitas. Primitif-primitif dibutuhkan untuk memenuhi tujuan keamanan informasi yang bermacam-macam. Primitif mana yang paling efektif untuk tujuan yang diberikan akan ditentukan dengan properti dasar dari primitif.

- Metode operasi. Primitif, saat diterapkan dengan bermacam cara dan dengan bermacam input, biasanya akan menunjukkan karakteristik yang berbeda, sehingga satu primitif dapat menyediakan fungsionalitas yang sangat berbeda pada mode operasi atau penggunaannya.
- Unjuk kerja. Merupakan efisiensi sebuah primitif pada mode tertentu. (sebagai contoh algoritma enkripsi dapat dihitung dengan jumlah bit per detik yang dapat dienkripsinya)
- Kemudahan implementasi. Merupakan kesulitan dalam merealisasikan primitif pada prakteknya. Dapat meliputi kompleksitas pengimplementasian primitif dalam lingkungan software maupun hardware.

Kepentingan relatif dari bermacam kriteria ini sangat tergantung pada aplikasi dan sumber daya yang tersedia.



Gambar 9. Taksonomi Primitif Kriptografi

H. DAFTAR PUSTAKA

Agus Kurniawan, 2008, **Konsep dan Implementasi Cryptography dengan .Net**, Jakarta: Dian Rakyat.

Eryanto Sitorus, 2003, **Hacker dan Keamanan**, Yogyakarta: Andi Offset.

Simarmata, Janner., 2006, **Pengamanan Sistem Komputer**, Edisi I, Yogyakarta: ANDI.

Thomas, Tom., 2005, ***Network Security First Step***, Diterjemahkan oleh: Tim Penerjemah ANDI, Edisi I, Yogyakarta: ANDI.

Wahana Komputer, 2003, **Memahami Model Enkripsi dan Security Data**, Yogyakarta: ANDI.