**Kriptografi – Keamanan Sistem Komputer Pertemuan 6**

**Kriptografi**, secara umum adalah [ilmu](http://id.wikipedia.org/wiki/Ilmu" \o "Ilmu) dan [seni](http://id.wikipedia.org/wiki/Seni" \o "Seni) untuk menjaga kerahasiaan [berita](http://id.wikipedia.org/wiki/Berita" \o "Berita) [bruce Schneier - *Applied Cryptography*]. Selain pengertian tersebut terdapat pula pengertian ilmu yang mempelajari teknik-teknik [matematika](http://id.wikipedia.org/wiki/Matematika" \o "Matematika) yang berhubungan dengan [aspek keamanan informasi](http://id.wikipedia.org/wiki/Aspek_keamanan_informasi" \o "Aspek keamanan informasi) seperti [kerahasiaan data](http://id.wikipedia.org/w/index.php?title=Kerahasiaan_data&action=edit&redlink=1), [keabsahan data](http://id.wikipedia.org/w/index.php?title=Keabsahan_data&action=edit&redlink=1), [integritas data](http://id.wikipedia.org/w/index.php?title=Integritas_data&action=edit&redlink=1), serta [autentikasi data](http://id.wikipedia.org/w/index.php?title=Autentikasi_data&action=edit&redlink=1" \o "Autentikasi data (halaman belum tersedia)) [A. Menezes, P. van Oorschot and S. Vanstone - Handbook of Applied Cryptography]. Tidak semua aspek keamanan [informasi](http://id.wikipedia.org/wiki/Informasi" \o "Informasi) ditangani oleh kriptografi.

Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu :

* [Kerahasiaan](http://id.wikipedia.org/wiki/Kerahasiaan), adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau [kunci rahasia](http://id.wikipedia.org/wiki/Kunci_%28kriptografi%29" \o "Kunci (kriptografi)) untuk membuka/mengupas informasi yang telah [disandi](http://id.wikipedia.org/wiki/Enkripsi" \o "Enkripsi).
* [Integritas](http://id.wikipedia.org/w/index.php?title=Integritas&action=edit&redlink=1) data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.
* [Autentikasi](http://id.wikipedia.org/w/index.php?title=Autentikasi&action=edit&redlink=1), adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
* [Non-repudiasi.](http://id.wikipedia.org/w/index.php?title=Non-repudiasi.&action=edit&redlink=1), atau nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat.

**Terminologi**

Sampai zaman modern kriptografi disebut hampir secara eksklusif untuk enkripsi, yang merupakan proses konversi informasi biasa (disebut plaintext) menjadi teks yang tidak dimengerti (disebut ciphertext). Dekripsi sebaliknya, dengan kata lain, bergerak dari tidak dimengerti ciphertext kembali ke plaintext. Sebuah cipher (atau nol) adalah sepasang algoritma yang membuat enkripsi dan dekripsi membalikkan. Operasi rinci cipher dikendalikan baik oleh algoritma dan dalam setiap contoh oleh "kunci". Ini adalah rahasia (idealnya hanya diketahui oleh komunikan), biasanya string pendek karakter, yang diperlukan untuk mendekripsi ciphertext. A "cryptosystem" adalah daftar memerintahkan unsur kemungkinan plainteks terbatas, mungkin cyphertexts terbatas, mungkin kunci terbatas, dan enkripsi dan dekripsi algoritma yang sesuai dengan setiap tombol. Kunci yang penting, karena tanpa cipher kunci variabel dapat sepele rusak hanya dengan pengetahuan tentang cipher digunakan dan karena itu tidak berguna (atau bahkan kontra-produktif) untuk sebagian besar tujuan. Secara historis, cipher sering digunakan secara langsung untuk enkripsi atau dekripsi tanpa prosedur tambahan seperti otentikasi atau pemeriksaan integritas.

|  |
| --- |
| http://upload.wikimedia.org/wikipedia/commons/thumb/f/f8/Crypto.png/300px-Crypto.png |
| Kriptografi Symmetric-kunci, dimana kunci yang sama digunakan baik untuk enkripsi dan dekripsi |

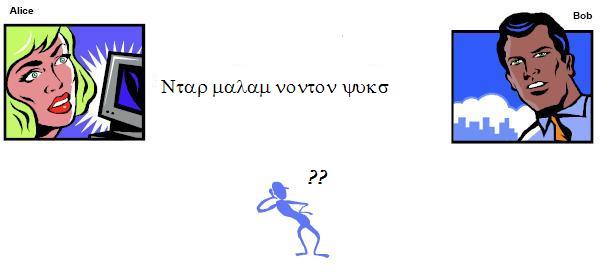
Dalam penggunaan sehari-hari, istilah "kode" sering digunakan untuk berarti setiap metode enkripsi atau penyembunyian makna. Namun, dalam kriptografi, kode memiliki arti yang lebih khusus. Ini berarti penggantian unit plaintext (yaitu, sebuah kata atau frase yang bermakna) dengan kata kode (misalnya, walabi menggantikan serangan pada waktu fajar). Kode tidak lagi digunakan dalam kriptografi serius-kecuali kebetulan untuk hal-hal seperti unit sebutan (misalnya, Bronco Flight atau Operasi Overlord)-karena cipher yang dipilih benar keduanya lebih praktis dan lebih aman daripada kode terbaik dan juga lebih baik disesuaikan dengan komputer .  
  
Cryptanalysis adalah istilah yang digunakan untuk studi tentang metode untuk memperoleh arti dari informasi yang dienkripsi tanpa akses ke kunci yang biasanya diperlukan untuk melakukannya, yaitu, itu adalah studi tentang bagaimana untuk memecahkan algoritma enkripsi atau implementasi mereka.  
  
Beberapa menggunakan istilah kriptografi dan kriptologi bergantian dalam bahasa Inggris, sementara yang lain (termasuk latihan militer AS umumnya) menggunakan kriptografi untuk merujuk secara khusus untuk penggunaan dan praktek teknik kriptografi dan kriptologi untuk merujuk pada studi gabungan kriptografi dan kriptanalisis. Inggris lebih fleksibel daripada beberapa bahasa lain di mana kriptologi (dilakukan oleh ahli kriptologi) selalu digunakan dalam arti kedua di atas. Di Wikipedia bahasa Inggris istilah umum yang digunakan untuk seluruh bidang adalah kriptografi (dilakukan oleh kriptografer).  
  
Studi tentang karakteristik bahasa yang memiliki beberapa aplikasi dalam kriptografi (atau kriptologi), yaitu frekuensi data, kombinasi huruf, pola yang universal, dll, disebut cryptolinguistics.

**Contoh Kriptografi Pengirim dan Penerima pesan**



Pesan 🡺 *Plaintext* atau *Cleartext*

Pesan dapat berupa data atau informasi yang dikirim (melalui kurir, saluran komunikasi data, dsb) Pesan dapat 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 *ciphertext* atau *cryptogram*. Tidak bergantung dengan suatu program.



*Ciphertext* harus dapat ditransformasi kembali menjadi *plaintext*.

**Jadi dapat disimpulkan bahwa :**

Kriptografi adalah ilmu sekaligus seni untuk menjaga keamanan pesan

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

Algoritma kriptografi adalah: aturan/metode untuk enkripsi dan dekripsi dan fungsi matematika yang digunakan untuk enkripsi dan dekripsi.

Kunci adalah parameter yang digunakan untuk transformasi enkripsi dan dekripsi*.*

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

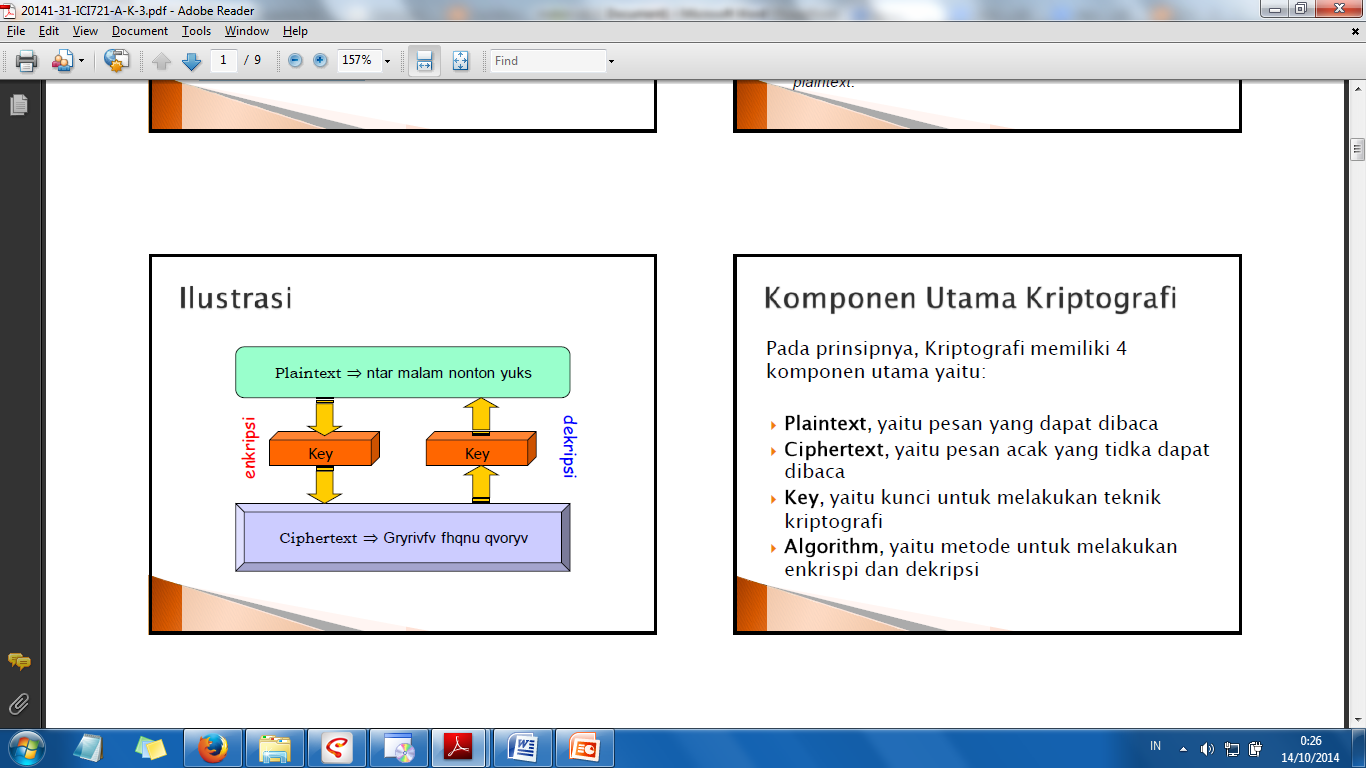
Penyadap adalah orang yang mencoba menangkap pesan selama ditransmisikan. Nama lain: *enemy*, *adversary*, *intruder*, *interceptor*, *bad guy*

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

Kriptologi (*cryptology*) adalah studi mengenai kriptografi dan kriptanalisis.

Proses menyandikan *plaintext* menjadi *ciphertext* disebut enkripsi (*encryption*) atau *enciphering* Sedangkan Proses mengembalikan *ciphertext* menjadi *plaintext*nya disebut dekripsi (decryption) atau *deciphering*

**Ilustrasi**



**Komponen utama kriptografi**

Pada prinsipnya, Kriptografi memiliki 4 komponen utama yaitu:

Plaintext, yaitu pesan yang dapat dibaca

Ciphertext, yaitu pesan acak yang tidka dapat dibaca

Key, yaitu kunci untuk melakukan teknik kriptografi

Algorithm, yaitu metode untuk melakukan enkrispi dan dekripsi

**Tujuan Kriptografi**

Menjaga kerahasiaan (*confidentiality*) pesan.

Keabsahan pengirim (*user authentication*).

Keaslian pesan (*message authentication*).

Anti-penyangkalan (*non-repudiation*).

**Definsi Enkripsi**

Enkripsi (Encryption) adalah sebuah proses menjadikan pesan yang dapat dibaca (plaintext) menjadi pesan acak yang tidak dapat dibaca (ciphertext). Berikut adalah contoh enkripsi yang digunakan oleh Julius Caesar, yaitu dengan mengganti masing-masing huruf dengan 3 huruf selanjutnya (disebut juga Additive/Substitution Cipher)

Contoh Enkripsi :

Plain Text: TEST ONLY

Cipher Text: &^\*#^@%&\*

**Definisi Deskripsi**

Dekripsi merupakan proses kebalikan dari enkripsi dimana proses ini akan mengubah ciphertext menjadi plaintext dengan menggunakan algortima „pembalik‟ dan key yang sama.

Sehingga Kata yang telah di Enkripsi akan dapat dimengerti oleh pembaca.

Contoh Deskripsi:

Cipher Text: &^\*#^@%&\*

Plain Text: TEST ONLY

**Aplikasi kriptografi:**

Pengiriman data melalui saluran komunikasi

Penyimpanan data di dalam *disk storage*.

Contoh-contoh pada pengiriman data melalui saluran komunikasi ATM tempat mengambil uang , Internet, Militer , Wi-Fi, Pay TV, GSM

**Contoh-contoh pada data tersimpan:**

**a. Dokumen teks**

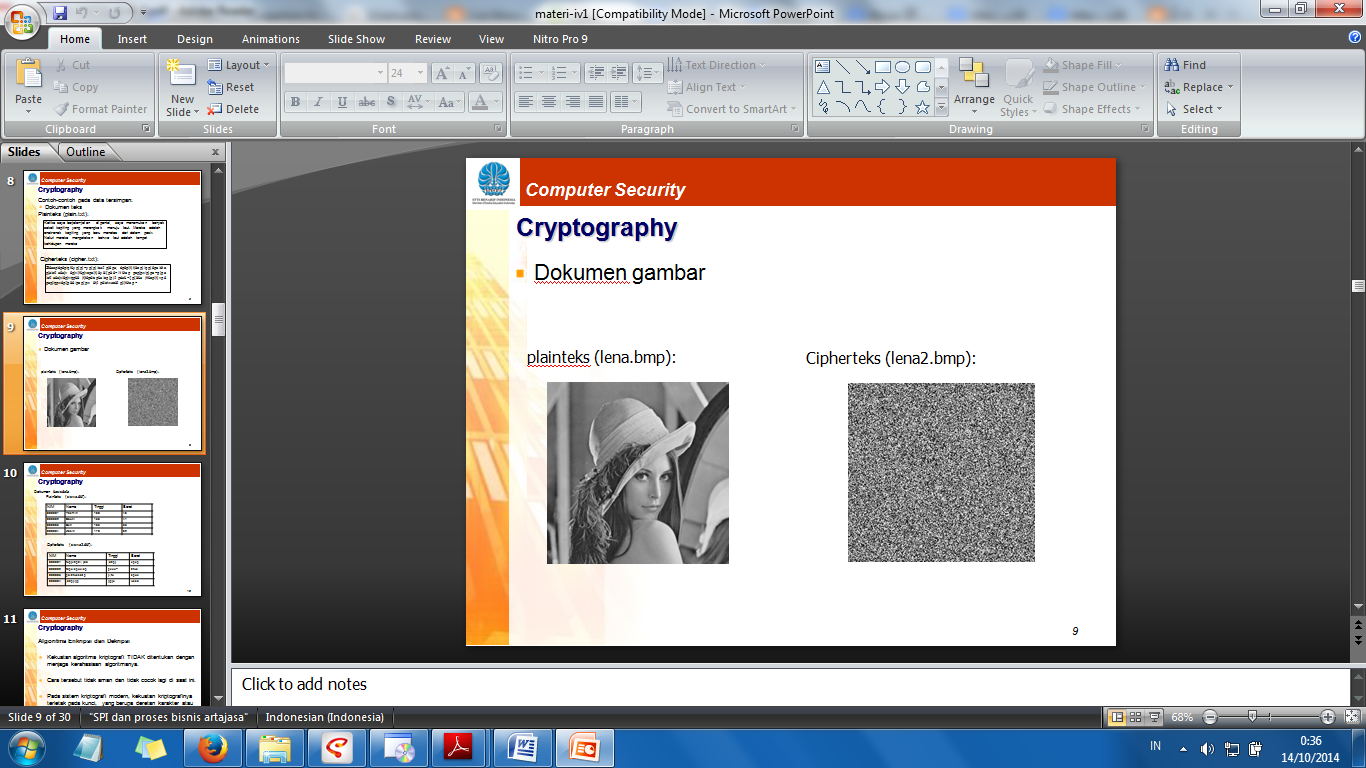
Plainteks (plain.txt):

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

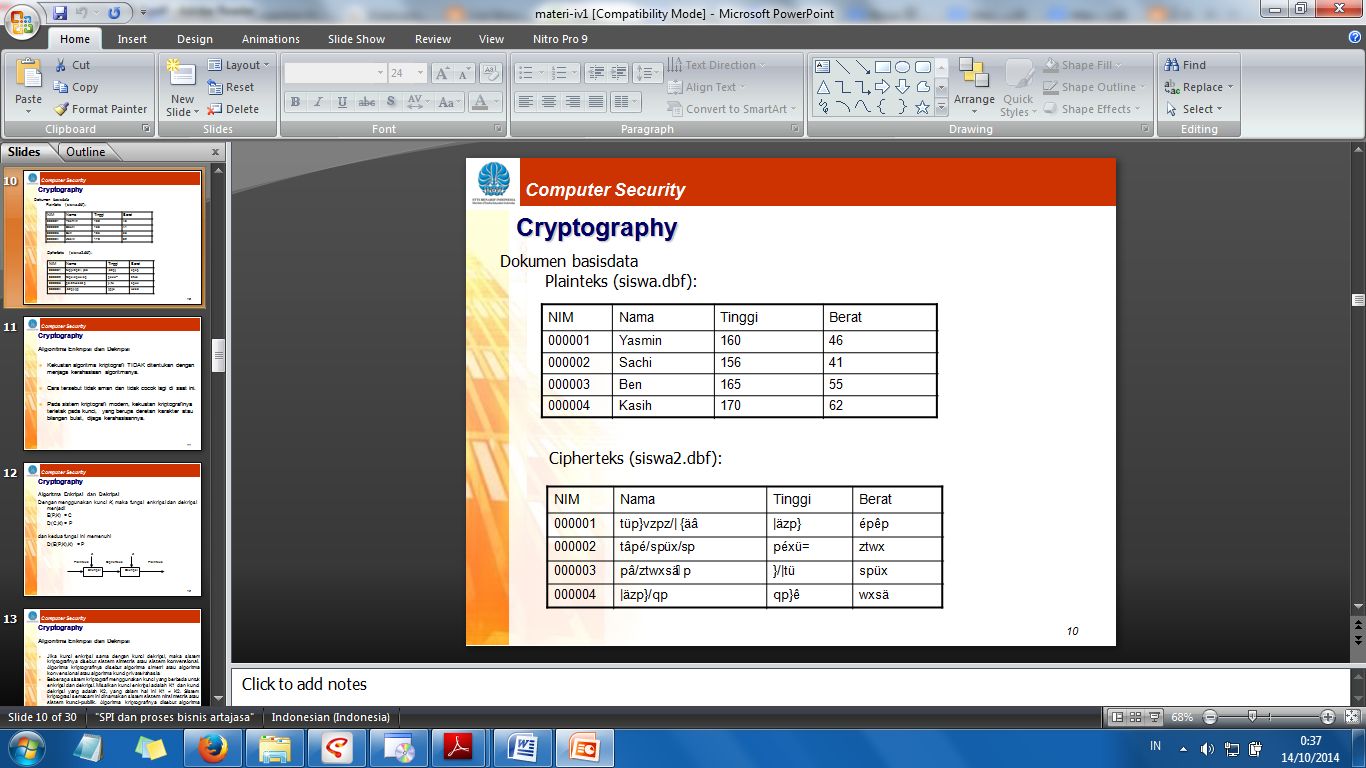
Cipherteks

Ztâxzp/épêp/qtüyp{p}<yp{p}/sx/p}âpx;épêp/|t}t|äzp}/qp}êpz/étzp{x/ztxâx}vêp}v/|tüp}vzpz/|t}äyä/{päâ=/\tützppsp{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{pwât|pâ/ztwxsäp}/|tützp=

b. Dokumen Gambar

****

c. Dokumen Basis Data

****

**Algoritma Enkripsi dan Dekripsi**

Kekuatan algoritma kriptografi TIDAK ditentukan dengan menjaga kerahasiaan algoritmanya.

Cara tersebut tidak aman dan tidak cocok lagi di saat ini.

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

**Algoritma Enkripsi dan Dekripsi**

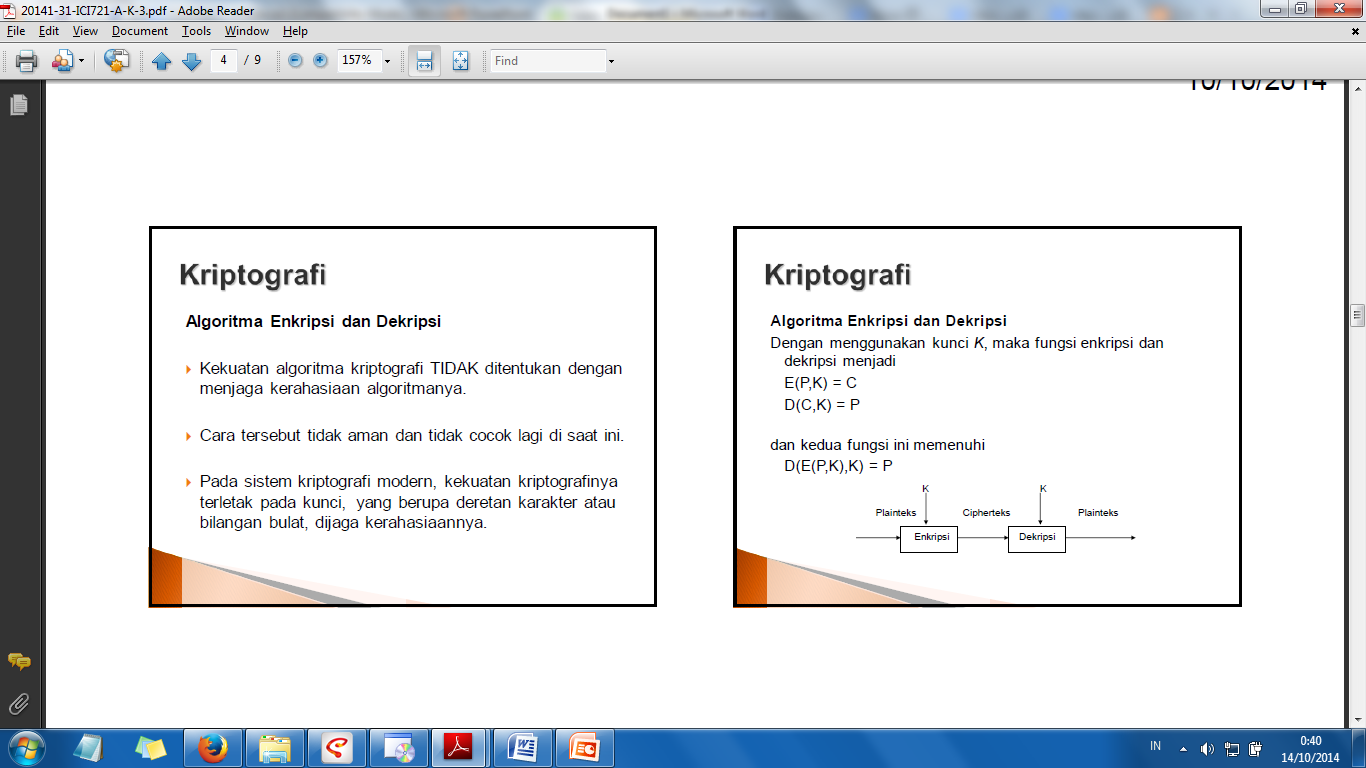
Dengan menggunakan kunci *K*, maka fungsi enkripsi dan dekripsi menjadi

E(P,K) = C

D(C,K) = P

dan kedua fungsi ini memenuhi

D(E(P,K),K) = P



Teknik Dasar Kriptografi Diantaranya :Substitusi, Blocking , Permutasi , Ekspansi dan Pemampatan

**Subtitusi**

Langkah pertama adalah membuat suatu tabel substitusi. Tabel substitusi dapat dibuat sesuka hati, dengan catatan bahwa penerima pesan memiliki tabel yang sama untuk keperluan dekripsi. Bila tabel substitusi dibuat secara acak, akan semakin sulit pemecahan ciphertext oleh orang yang tidak berhak.

Contoh :

Tabel subsitusi

Caesar Chipher

ROT 13

**Tabel Subtitusi**

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-1-2-3-4-5-6-7-8-9-0-.-,

B-F-1-K-Q-G-A-T-P-J-6-H-Y-D-2-X-5-M-V-7-C-8-4-I-9-N-R-E-U-3-L-S-W-,-.-O-Z-0

Contoh :

SISTEM

7P7CQY (TABEL SUBSITUSI)

VLVWHP (CAESAR CHIPHER)

FVFGRZ (ROT13)

**Caesar Cipher**

Algoritma enkripsi sederhana pada masa raja Julius Caesar. Tiap huruf alfabet digeser 3 huruf ke kanan secara wrapping

Plainteks : AWASI ASTERIX DAN TEMANNYA OBELIX

Cipherteks : DZDVL DVWHULA GDQ WHPDQQBA REHOLA

Model Perhitungan

Misalkan setiap huruf dikodekan dengan angka:

A = 0, B = 1, C = 2, …, Z = 25

Maka secara matematis enkripsi dan dekripsi pada Caesar cipher dirumuskan sebagai berikut:

Enkripsi: ci = E(pi) = (pi + 3) mod 26

Dekripsi: pi = D(ci) = (ci – 3) mod 26

Jika pergeseran huruf sejauh k, maka :

Enkripsi: ci = E(pi) = (pi + k) mod 26

Dekripsi: pi = D(ci) = (ci – k) mod 26

k = kunci rahasia

Pada Caesar Cipher, k = 3

Untuk alfabet ASCII 256 karakter :

Enkripsi: ci = E(pi) = (pi + k) mod 256

Dekripsi: pi = D(ci) = (ci – k) mod 256

**Contoh Soal**

Plainteks : MATH

Cipherteks: RFYM

k = 5

p1 = „M‟ = 12 🡺 c1 = E(12) = (12 + 5) mod 26 = 17 = „R‟

p2 = „A‟ = 0 🡺c2 = E(0) = (0 + 5) mod 26 = 5 = „F‟

p3 = „T‟ = 19 🡺 c3 = E(19) = (19 + 5) mod 26 = 24 = „Y‟

p4 = „H‟ = 7 🡺c4 = E(7) = (7 + 5) mod 26 = 12 = „M‟

**ROT13**

Pada sistem ini sebuah huruf digantikan dengan huruf yang letaknya 13 posisi darinya.

Sebagai contoh, huruf “A” digantikan dengan huruf “N”, huruf “B” digantikan dengan huruf “O”, dan seterusnya.

Secara matematis, hal ini dapat dituliskan sebagai: C ROT13 = (M) Untuk mengembalikan kembali ke bentuk semulanya dilakukan proses enkripsi ROT13 dua kali.

M = ROT13(ROT13(M))

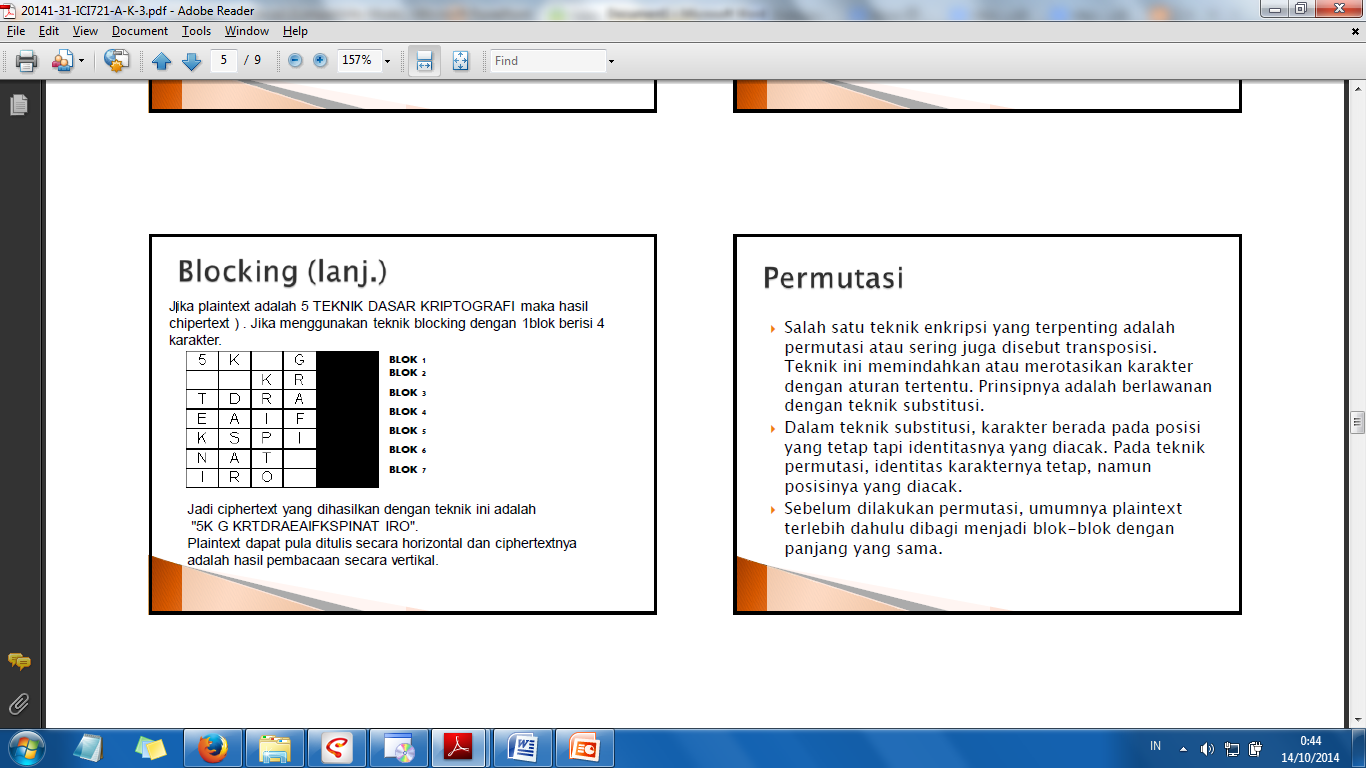
**Blocking**

Sistem enkripsi terkadang membagi plaintext menjadi blok-blok yang terdiri dari beberapa karakter yang kemudian dienkripsikan secara independen.

Dengan menggunakan enkripsi blocking dipilih jumlah lajur dan kolom untuk penulisan pesan. Jumlah lajur atau kolom menjadi kunci bagi kriptografi dengan teknik ini.

Plaintext dituliskan secara vertikal ke bawah berurutan pada lajur, dan dilanjutkan pada kolom berikutnya sampai seluruhnya tertulis. Ciphertext-nya adalah hasil pembacaan plaintext secara horizontal berurutan sesuai dengan blok-nya.

Jika plaintext adalah 5 TEKNIK DASAR KRIPTOGRAFI maka hasil chipertext ) . Jika menggunakan teknik blocking dengan 1blok berisi 4 karakter.



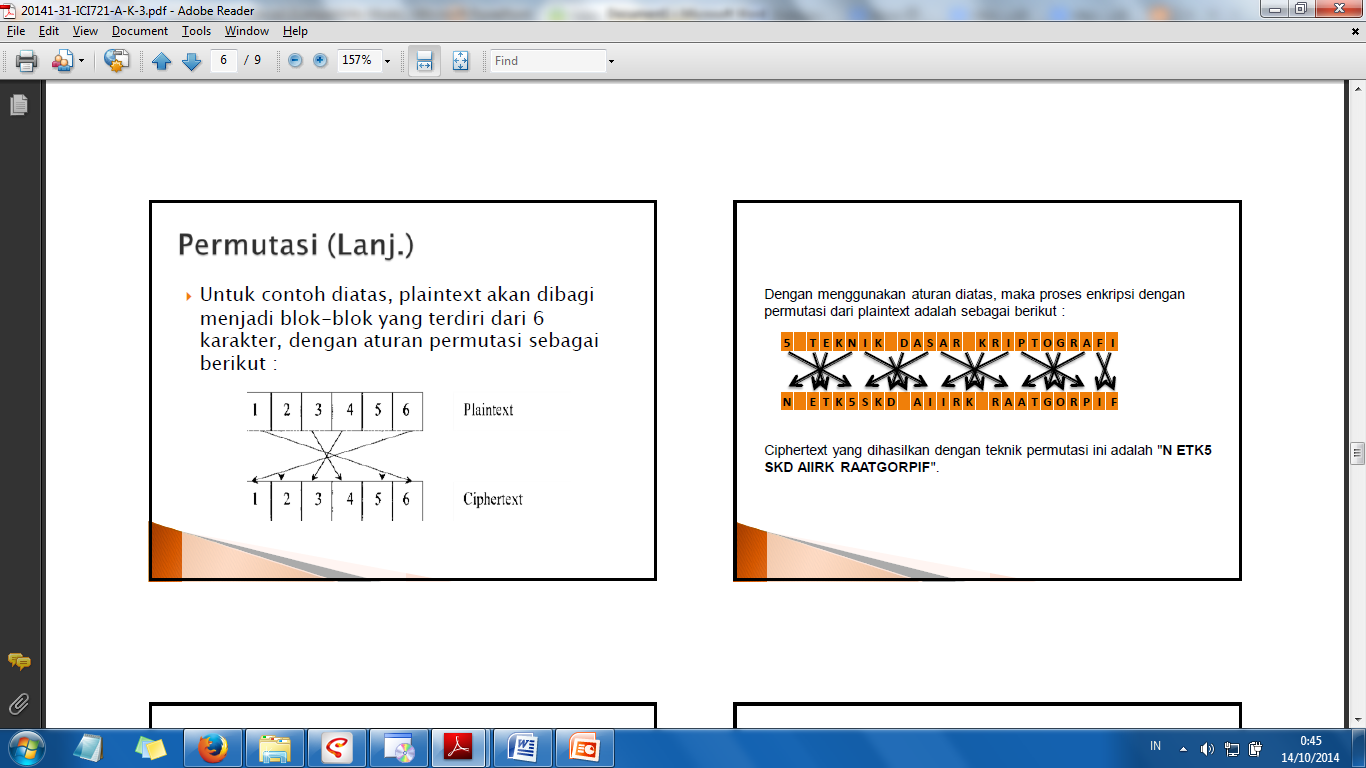
Jadi ciphertext yang dihasilkan dengan teknik ini adalah "5K G KRTDRAEAIFKSPINAT IRO". Plaintext dapat pula ditulis secara horizontal dan ciphertextnya adalah hasil pembacaan secara vertikal.

**Permutasi**

Salah satu teknik enkripsi yang terpenting adalah permutasi atau sering juga disebut transposisi. Teknik ini memindahkan atau merotasikan karakter dengan aturan tertentu. Prinsipnya adalah berlawanan dengan teknik substitusi.

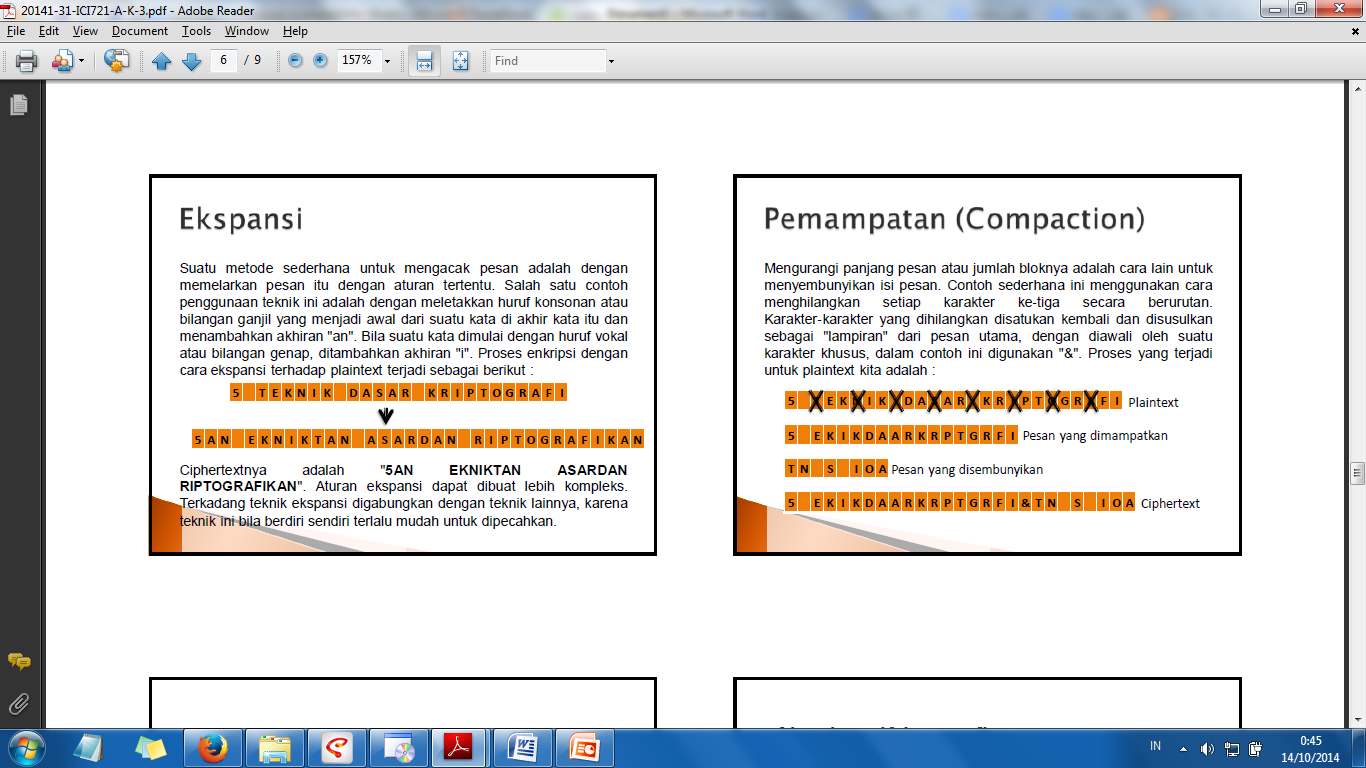
Dalam teknik substitusi, karakter berada pada posisi yang tetap tapi identitasnya yang diacak. Pada teknik permutasi, identitas karakternya tetap, namun posisinya yang diacak. Sebelum dilakukan permutasi, umumnya plaintext terlebih dahulu dibagi menjadi blok-blok dengan panjang yang sama.

Untuk contoh diatas, plaintext akan dibagi menjadi blok-blok yang terdiri dari 6 karakter, dengan aturan permutasi sebagai berikut :



**Ekspansi**

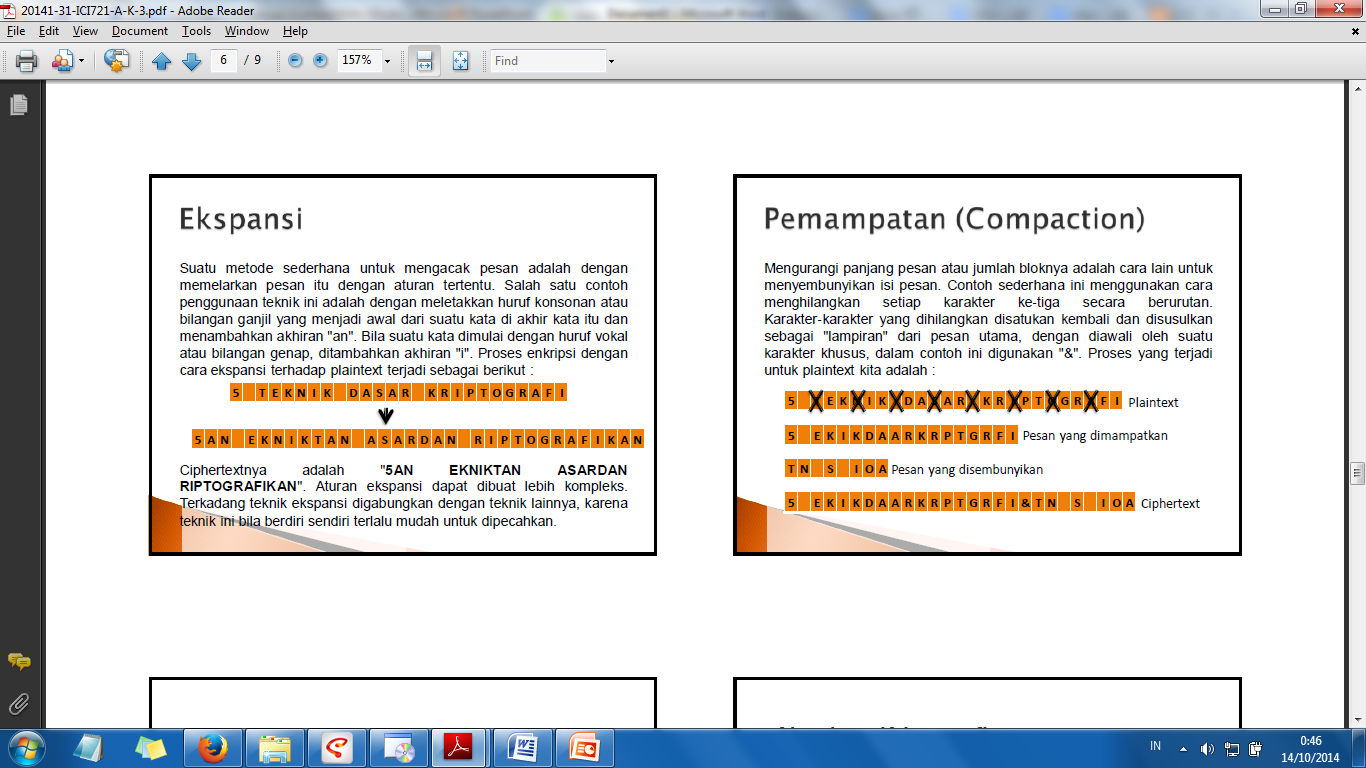
Suatu metode sederhana untuk mengacak pesan adalah dengan memelarkan pesan itu dengan aturan tertentu. Salah satu contoh penggunaan teknik ini adalah dengan meletakkan huruf konsonan atau bilangan ganjil yang menjadi awal dari suatu kata di akhir kata itu dan menambahkan akhiran "an". Bila suatu kata dimulai dengan huruf vokal atau bilangan genap, ditambahkan akhiran "i". Proses enkripsi dengan cara ekspansi terhadap plaintext terjadi sebagai berikut :



Ciphertextnya adalah "**5AN EKNIKTAN ASARDAN RIPTOGRAFIKAN**". Aturan ekspansi dapat dibuat lebih kompleks. Terkadang teknik ekspansi digabungkan dengan teknik lainnya, karena teknik ini bila berdiri sendiri terlalu mudah untuk dipecahkan.

**Pemampatan**

Mengurangi panjang pesan atau jumlah bloknya adalah cara lain untuk menyembunyikan isi pesan. Contoh sederhana ini menggunakan cara menghilangkan setiap karakter ke‐tiga secara berurutan. Karakter‐karakter yang dihilangkan disatukan kembali dan disusulkan sebagai "lampiran" dari pesan utama, dengan diawali oleh suatu karakter khusus, dalam contoh ini digunakan "&". Proses yang terjadi untuk plaintext kita adalah :



Aturan penghilangan karakter dan karakter khusus yang berfungsi sebagai pemisah menjadi dasar untuk proses dekripsi ciphertext menjadi plaintext kembali.

Dengan menggunakan kelima teknik dasar kriptografi diatas, dapat diciptakan kombinasi teknik kriptografi yang amat banyak, dengan faktor yang membatasi semata‐mata hanyalah kreativitas dan imajinasi kita. Walaupun sekilas terlihat sederhana, kombinasi teknik dasar kriptografi dapat menghasilkan teknik kriptografi turunan yang cukup kompleks, dan beberapa teknik dasar kriptografi masih digunakan dalam teknik kriptografi modern.

**Algoritma Kriptografi :**

Berdasarkan jenis kunci yang digunakan : Algoritma Simetris , Algoritma Asimetris

Berdasarkan besar data yang diolah : Algoritma Block Cipher , Algoritma Stream Cipher

Berdasarkan Kunci Yang digunakan : Algoritma Simetris , Algoritma simetris (symmetric algorithm) adalah suatu algoritma dimana kunci enkripsi yang digunakan sama dengan kunci dekripsi sehingga algoritma ini disebut juga sebagai single-key algorithm.

Kelebihan algoritma simetris :

Kecepatan operasi lebih tinggi bila dibandingkan dengan algoritma asimetrik.

Karena kecepatannya yang cukup tinggi, maka dapat digunakan pada sistem real-time

Kelemahan algoritma simetris :

Untuk tiap pengiriman pesan dengan pengguna yang berbeda dibutuhkan kunci yang berbeda juga, sehingga akan terjadi kesulitan dalam manajemen kunci tersebut.

Permasalahan dalam pengiriman kunci itu sendiri yang disebut “key distribution problem”

Algoritma Asimetris

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

Kelebihan algoritma asimetris :

Masalah keamanan pada distribusi kunci dapat lebih baik

Masalah manajemen kunci yang lebih baik karena jumlah kunci yang lebih sedikit

Kelemahan algoritma asimetris :

Kecepatan yang lebih rendah bila dibandingkan dengan algoritma simetris

Untuk tingkat keamanan sama, kunci yang digunakan lebih panjang dibandingkan dengan

algoritma simetris.

**Berdasarkan data yang diolah**

**Block Cipher**

Informasi/data yang hendak dikirim dalam bentuk blok-blok besar (misal 64-bit) dimana blok-blok ini dioperasikan dengan fungsi enkripsi yang sama dan akan menghasilkan informasi rahasia dalam blok-blok yang berukuran sama juga. Contoh: RC4, Seal, A5, Oryx.

**Stream Cipher**

Informasi/data yang hendak dikirim dioperasikan dalam bentuk blok-blok yang lebih kecil (*byte* atau *bit*), biasanya satu karakter per-satuan waktu proses, menggunakan tranformasi enkripsi yang berubah setiap waktu. Contohnya: Blowfish, DES, Gost, Idea, RC5, Safer, Square, Twofish, RC6, Loki97.

**Kriptografi Dengan Kunci Simetris/Private**

Bentuk kriptografi tradisional

Kunci Simetris digunakan untuk mengenkrip dan mendekrip pesan

Kunci Simetris juga berkaitan dengan otentikasi

Masalah utama:

Pengirim dan penerima menyetujui kunci simetris tanpa ada orang lain yang mengetahui.

Butuh metode dimana kedua pihak dapat berkomunikasi tanpa takut disadap

**Contoh Metode Kriptografi Dengan Kunci Simetris/Private**

Metode Caesar Cipher

- Huruf A-Z diberi nilai 0-25

- Karakter pesan dijumlah dengan kunci lalu di modulo 26

Metode Vigenere Cipher

- Huruf A-Z diberi nilai 0-25

- Kunci terdiri dari sekumpulan random karakter

- Karakter pesan dijumlah dengan kunci lalu di modulo 26

Metode Book Key Cipher

- Menggunakan teks dari sebuah sumber (misalnya buku) untuk mengenkrip plainteks

- Karakter pesan dijumlah dengan kunci lalu di modulo 26

**Contoh Metode Kriptografi Dengan Kunci Simetris/Private** - Metode DES (Data Encryption Standard) - Metode Triple DES Melakukan 3 kali pengenkripan - Metode AES (Advanced Encryption Standard) Menggantikan DES (karena dapat dibobol) - Metode Rijndael Block Cipher - Metode IDEA (Internatinal Data Encryption Algorithm) - Metode RC5 dan RC6

**Kunci Nirsimetris/Publik**

Setiap orang memiliki sepasang kunci, kunci publik dan kunci private.

Kunci publik dipublikasikan

Kunci private disimpan rahasia dan tidak boleh ditransmisikan atau dipakai bersama

**Contoh Metode Kriptografi Dengan Kunci NirSimetris/Publik -** Metode RSA (Ronald Rivest, Adi Shamir, Leonard Adleman) - Metode Diffie Hellman Key Exchange - Metode El Gamal

**One-Way Function / Fungsi Hash**

Merupakan fungsi satu arah yang dapat menghasilkan ciri (signature) dari data (berkas) Fungsi yang memproduksi output dengan panjang tetap dari input yang berukuran variabel Perubahan satu bit saja akan mengubah keluaran hash secara drastis Digunakan untuk menjamin integritas dan digital signature . Plaintext yang di hash, tidak dapat dikembalikan ke bentuk asalnya. Oleh karena itu Hash sering disebut sebagai one-way Hash, proses mengubah plaintext menjadi bentuk unik dari plaintext. Hasil dari hash algorithm disebut hash atau digest

Contoh:

MD5 (Message Diggest) Hasilnya 128-bit

SHA (Secure Hash Function) Hasilnya 160-bit

**Hash Algoritm**

Contoh penggunaan Hash Function adalah pada mesin ATM. Pengguna memiliki nomer PIN Nomer PIN tersebut di hash dan tersimpan dalam pita magnet yang ada dalam ATM.

**Stenografi dan Kriptografi**

Steganography Membuat seolah-olah pesan tidak ada Film: “Mercury rising”, “Beautiful mind”

Cryptography Transposition (letters arranged), Substitution (letters substituted with other letters)

**Soal Latihan**

Julius Caesar, seorang kaisar terkenal Romawi yang menaklukkan banyak bangsa di Eropa dan Timur Tengah juga menggunakan suatu teknik kriptografi yang sekarang disebut Caesar cipher untuk berkorespondensi sekitar tahun 60 S.M. Teknik yang digunakan oleh Sang Caesar adalah mensubstitusikan alfabet secara beraturan, yaitu oleh alfabet ketiga yang mengikutinya, misalnya, alfabet ‘’A" digantikan oleh "D", "B" oleh "E", dan seterusnya.

Dengan menggunakan tabel substitusi di atas, rubah sandi berikut menjadi sebuah kalimat yang benar :

**DNXDQDNFHUGDVEUR**

Dari ciphertext menjadi plaintext ‐nya ?

Sumber:

<http://muhammad-ikhsan74.blogspot.com/2012/05/pengertian-kriptografi.html>

<http://id.wikipedia.org/wiki/Kriptografi>

<http://asalkena.blogspot.com/2012/11/pengertian-dan-contoh.html>

<http://nemmalasari.blogspot.com/2012/11/keamanan-komputer-dan-jaringan21.html>