Cryptography

YAYASAN SASMITA JAYA

Program Studi Teknik Informatika, Universitas Pamulang

Cryptography

Ilmu sekaligus seni untuk menjaga keamanan pesan

Cryptography

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).

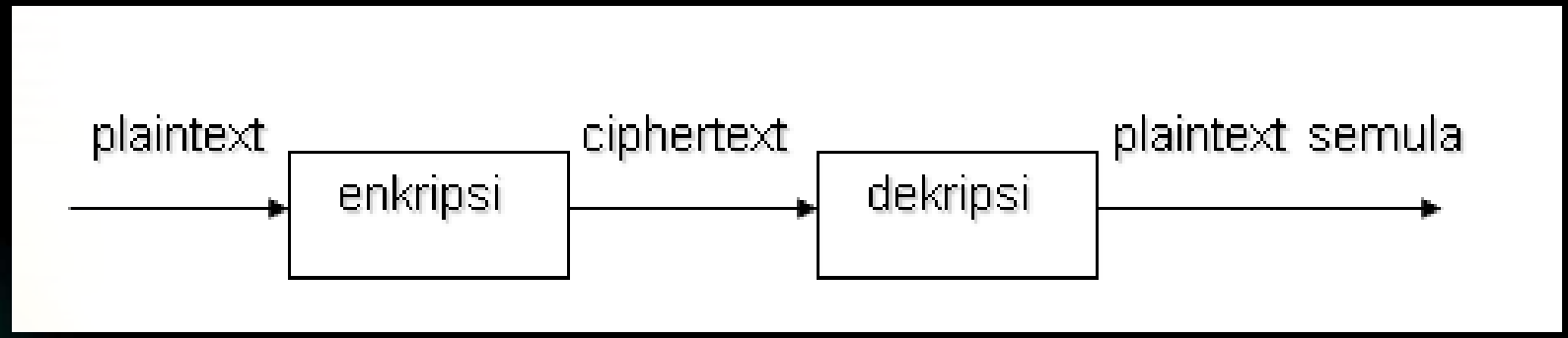
Cryptography

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*.

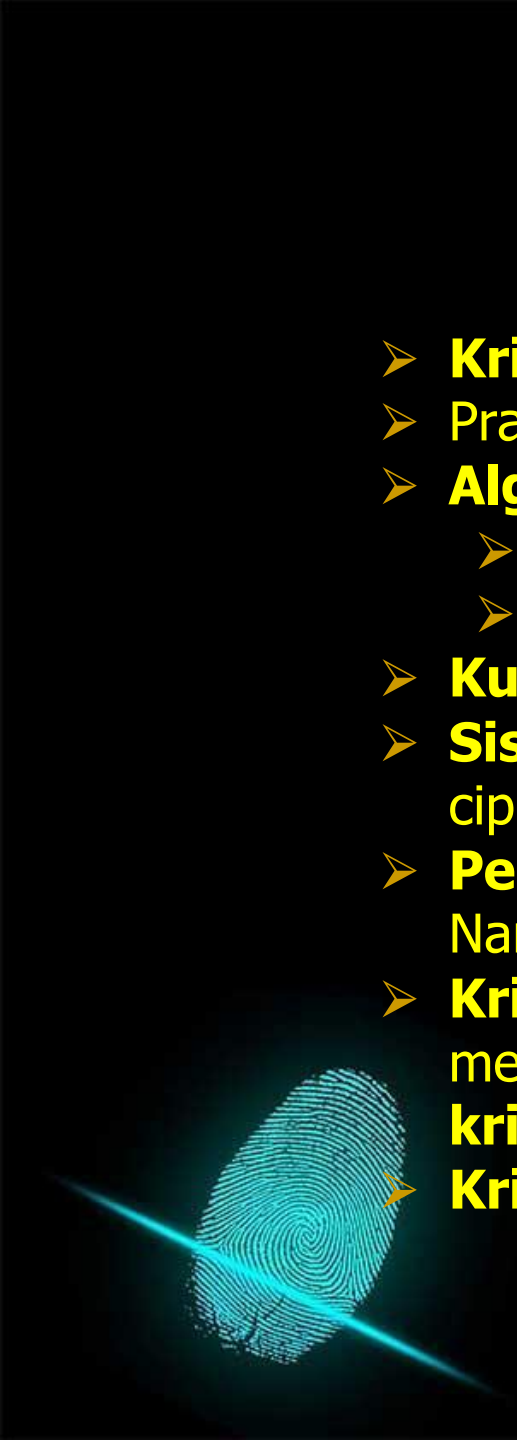
Cryptography

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



Cryptography

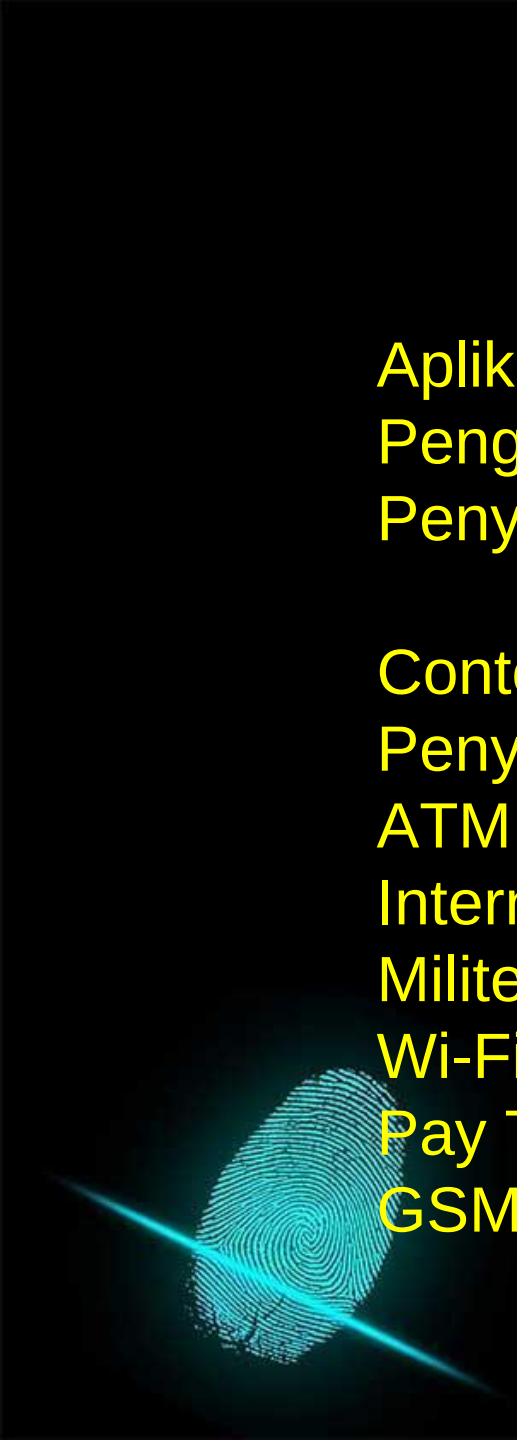
- **Kriptografi** adalah ilmu sekaligus seni untuk menjaga keamanan pesan
- Praktisi (pengguna kriptografi) disebut **kriptografer** (*cryptographer*).
- **Algoritma kriptografi** adalah:
  - aturan/metode untuk enkripsi dan dekripsi
  - fungsi matematika yang digunakan untuk enkripsi dan dekripsi.
- **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.



Cryptography

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

Contoh-contoh pada pengiriman data melalui saluran komunikasi
Penyimpanan data di dalam *disk storage*.
ATM tempat mengambil uang
Internet
Militer
Wi-Fi
Pay TV
GSM



Cryptography

Aplikasi kriptografi:

- Pengiriman data melalui saluran komunikasi
- Penyimpanan data di dalam *disk storage*.

Contoh-contoh pada pengiriman data melalui saluran komunikasi

- Penyimpanan data di dalam *disk storage*.
- ATM tempat mengambil uang
- Internet
- Militer
- Wi-Fi
- Pay TV
- GSM

Cryptography

Contoh-contoh pada data tersimpan:
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):

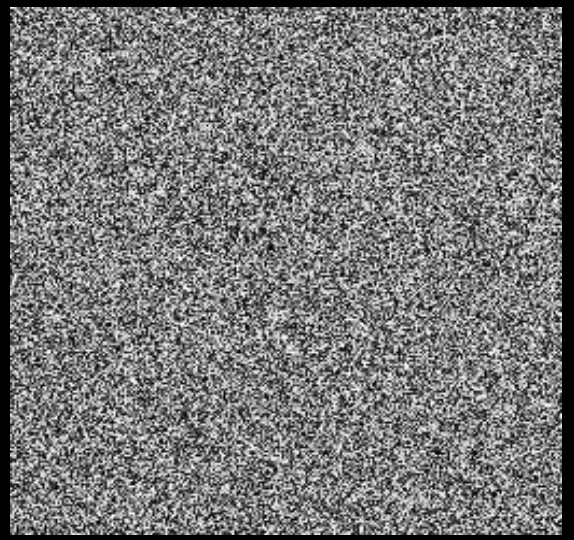
> Ztâxzp/épêp/qtüyp{p}<yp{p}/sx/• p}âpx;épêp/|t}t|äzp}/qp}êpz/ét zp{x/zt• xâx}vêp}v/|tüp}vzpz/|t}äyä/{päâ=/\tützppsp{pw/p}pz<p} pz/zt• xâx}v/êp}v/qpüä|t}tâpé/spüx/sp{p|/• péxü=/]p{äüx|ttüzp/|t} vpâpzp}/qpwåp/{päâ/psp{pwât|• pâ/ztwxsä• p}/|tützp=

Cryptography

Dokumen gambar

plainteks (lena.bmp):

Cipherteks (lena2.bmp):



Cryptography

Dokumen basisdata

Plainteks (siswa.dbf):

NIM	Nama	Tinggi	Berat
000001	Soleha	160	46
000002	Cahaya	156	41
000003	Aisyah	165	55
000004	Kasih	170	62

Cipherteks (siswa2.dbf):

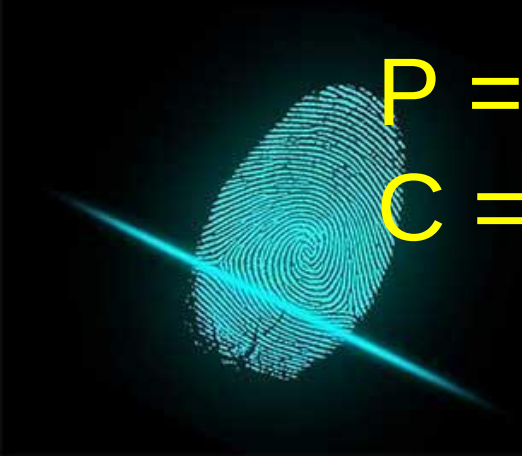
NIM	Nama	Tinggi	Berat
000001	tüp}vzpz/| {ää	|äzp}	épêp
000002	tâpé/spüx/sp	péxü=	ztwx
000003	pâ/ztwxsä□p	}/|tü	spüx
000004	|äzp}/qp	qp}ê	wxsä

Cryptography

Fungsi Enkripsi dan Dekripsi

E(P) = C
D(C) = P
D(E(P)) = P

P = Plainteks
C = Cipherteks



Cryptography

Contoh algoritma yang menggunakan model tersebut:

Metode Substitusi Sederhana
Metode Cipher Tranposisi

Cryptography

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	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

- Plaintext: Let us talk one to one.
- Ciphertext: F5n om n1fe ih5 ni ih5.

Cryptography

Kekuatan Algoritma Enkripsi dan Dekripsi

Algoritma kriptografi dikatakan aman bila memenuhi tiga kriteria berikut:

Persamaan matematis yang menggambarkan operasi algoritma kriptografi sangat kompleks sehingga algoritma tidak mungkin dipecahkan secara analitik.

Biaya untuk memecahkan cipherteks melampaui nilai informasi yang terkandung di dalam cipherteks tersebut.

Waktu yang diperlukan untuk memecahkan cipherteks melampaui lamanya waktu informasi tersebut harus dijaga kerahasiaannya.

Cryptography

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.

Cryptography

Algoritma Enkripsi dan Dekripsi

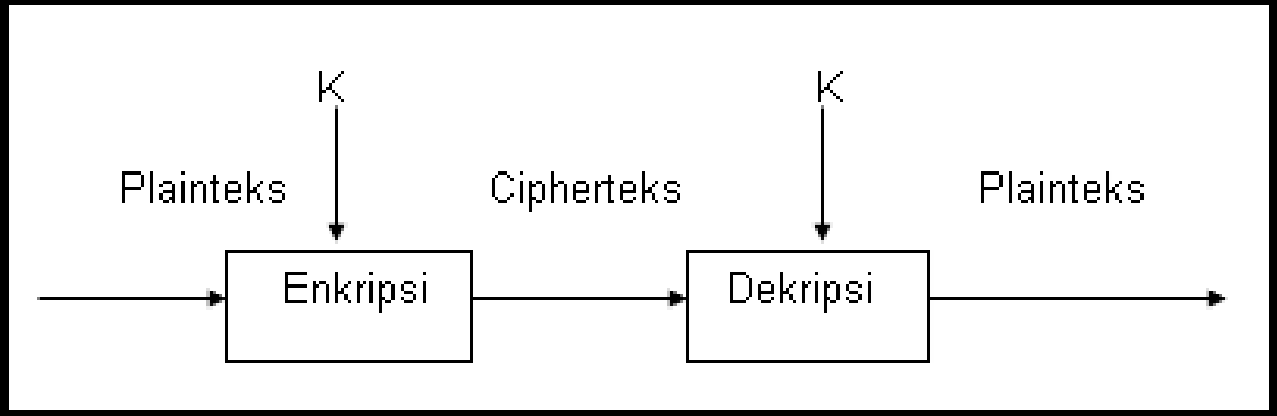
Dengan menggunakan kunci *K*, maka fungsi enkripsi dan dekripsi menjadi

E(P,K) = C

D(C,K) = P

dan kedua fungsi ini memenuhi

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



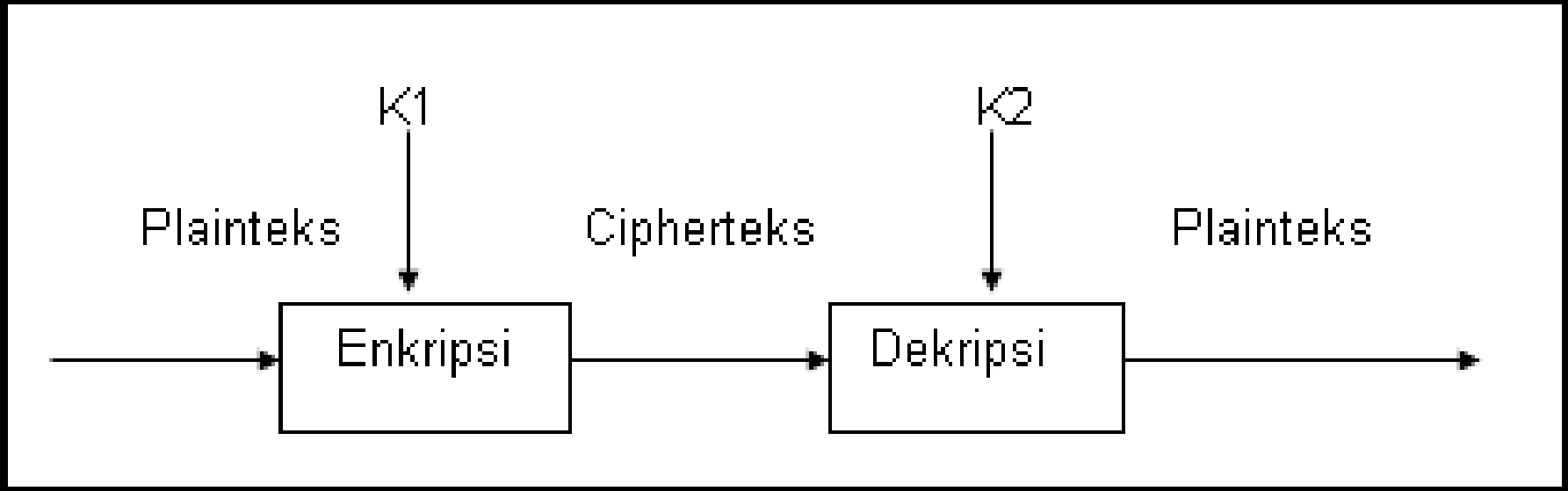
Cryptography

Algoritma Enkripsi dan Dekripsi

Jika kunci enkripsi sama dengan kunci dekripsi, maka sistem kriptografinya disebut **sistem simetris** atau **sistem konvensional**. Algoritma kriptografinya disebut algoritma simetri atau algoritma konvensional atau algoritma kunci private/rahasia.

Beberapa sistem kriptografi menggunakan kunci yang berbeda untuk enkripsi dan dekripsi. Misalkan kunci enkripsi adalah K1 dan kunci dekripsi yang adalah K2, yang dalam hal ini K1 ≠ K2. Sistem kriptograsi semacam ini dinamakan sistem **sistem nirsimetris** atau **sistem kunci-publik**. Algoritma kriptografinya disebut algoritma nirsimetri atau algoritma kunci-publik.

Cryptography



Cryptography

Kriptografi Dengan Kunci Simetris/Private

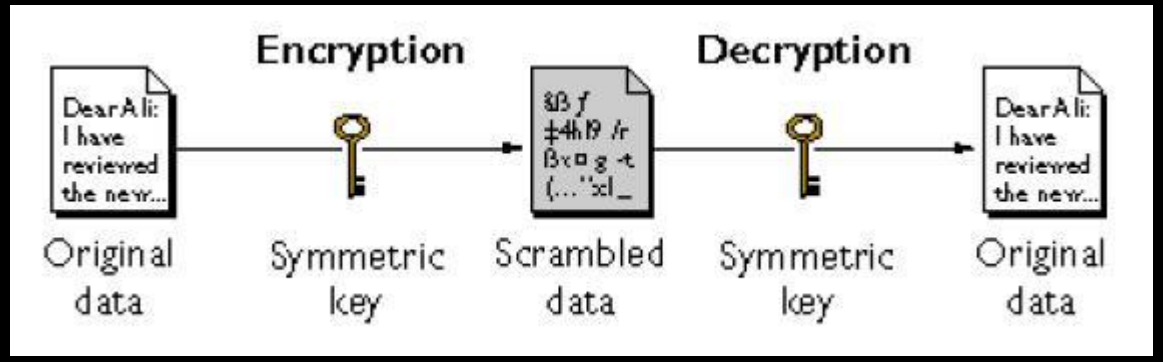
Bentuk kriptografi tradisional

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



Cryptography

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 Vernam Cipher

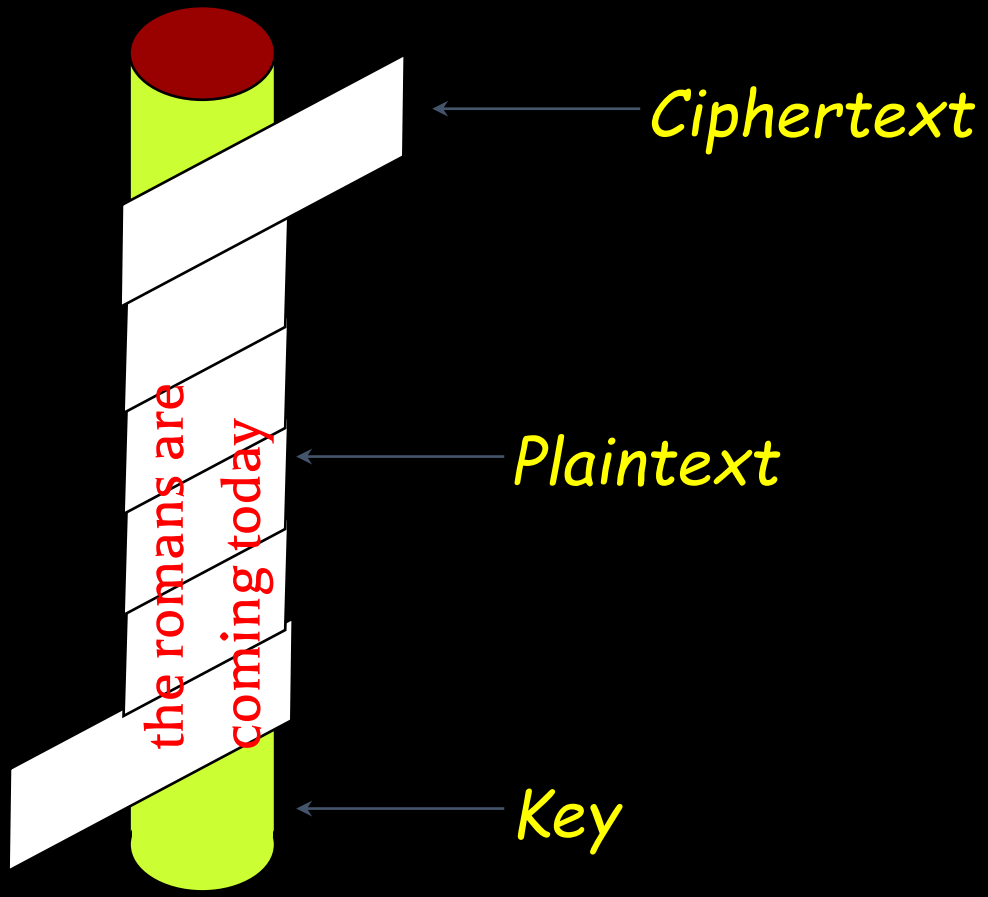
- Huruf A-Z diberi nilai 0-25
- Kunci terdiri dari sekumpulan random karakter
- Karakter pesan dijumlah dengan kunci lalu di modulo 26

Metode Book Key Cipher

- Menggunakan teks dari sebuah sumber (misalnya buku) untuk mengenkrip plainteks
- Karakter pesan dijumlah dengan kunci lalu di modulo 26

Cryptography

Contoh Metode Kriptografi Dengan Kunci Simetris/Private
Simple Cipher



Cryptography

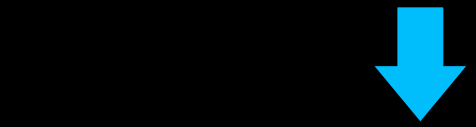
Contoh Metode Kriptografi Dengan Kunci Simetris/Private
Caesar Cipher

Subsitusi setiap huruf plain text dengan huruf yang telah dirotasi selama dalam bentuk huruf

Cryptography

13 steps rotation

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



N O P Q R S T U V W X Y Z A B C D E F G H I J K L M

SAYA LAGI — *Plaintext*

MAKAN — *13* — *Key*

FNLN YNTV ZNXNA — *Ciphertext*

Cryptography

Contoh Metode Kriptografi Dengan Kunci Simetris/Private

Running Key Cipher

- Karakter ciphertext ditentukan pada pertemuan antara baris dan kolom
- Baris untuk karakter yang akan dienkrip, kolom untuk karakter dari keyword
- Dikenal juga sebagai vigenere cipher

Cryptography

ABCDEFGHIJKLMNOPQRSTUVWXYZ
BCDEFGHIJKLMNOPQRSTUVWXYZA
CDEFGHIJKLMNOPQRSTUVWXYZAB
DEFGHIJKLMNOPQRSTUVWXYZABC
EFGHIJKLMNOPQRSTUVWXYZABCD
FGHIJKLMNOPQRSTUVWXYZABCDE
GHIJKLMNOPQRSTUVWXYZABCDEF
HIJKLMNOPQRSTUVWXYZABCD...

SOUND THE RETREAT *plaintext*

DEADFED *key*

VSUQI XKH VEWWIDW *ciphertext*

Cryptography

CAESAR

1. ONYV ONTHF (key : 13) PT?
2. **TERIMAKASIH AKU AKAN INGAT SELALU (key 6)**

VIGENERE

3. **THE ART OF WRITING SECRET (Key : DEADHEAD) CT?**
4. **QIVHY KIYH YP (Key : DEADHEAD**) PT?
5. **ZEZA VPRUA NUTBM (KEY: HEBAT)PT ?**

Cryptography

CAESAR

C = (P-K) + 26 MOD 26

P = C+K MOD 26

VIGENERE

C = P + K MOD 26

P = (C-K) + 26 MOD 26

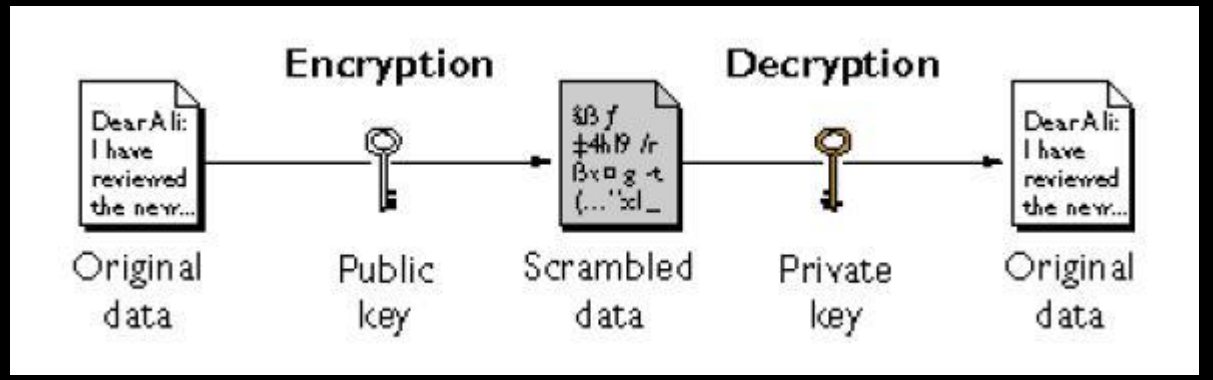
Cryptography

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

Cryptography

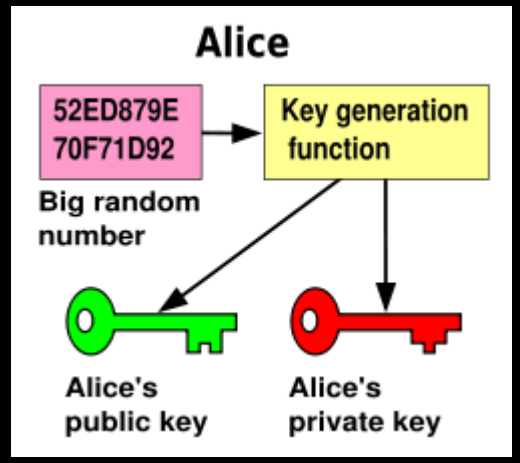
Kunci Nirsimetris/Publik
Setiap orang memiliki sepasang kunci, kunci publik dan kunci private.
Kunci publik dipublikasikan
Kunci private disimpan rahasia dan tidak boleh ditransmisikan atau dipakai bersama

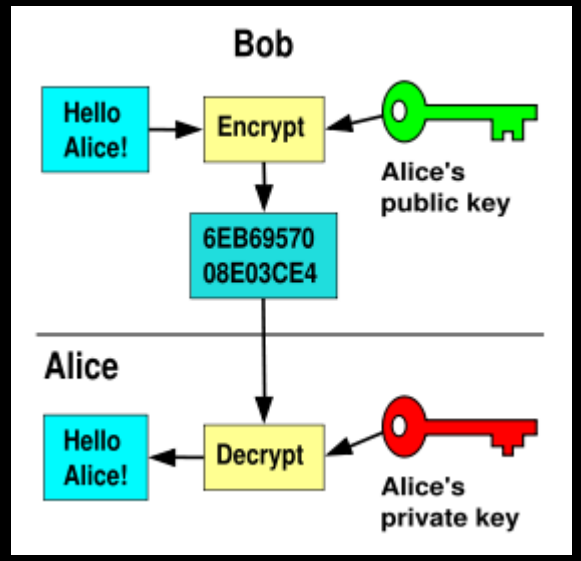


Cryptography

Proses pengiriman pesan dari Bob ke Alice dengan Kunci Publik

1. Alice membuat Kunci Publik dan Kunci private
2. Bob mengenkrip pesan dengan kunci publik Alice
3. Alice mengdekrip pesan dengan menggunakankan kunci private alice





Cryptography

Contoh Metode Kriptografi Dengan Kunci NirSimetris/Publik

Metode RSA (Ronald Rivest, Adi Shamir, Leonard Adleman)
Metode Diffie Hellman Key Exchange
Metode El Gamal

Cryptography

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

Contoh:

- MD5 (Message Diggest)
  - Hasilnya 128-bit
- SHA (Secure Hash Function)
  - Hasilnya 160-bit

Cryptography

One-Way Function / Fungsi Hash

Fungsi Hash diperoleh melalui persamaan

$$h = H(M)$$

Fungsi Hash dapat diterapkan pada blok data berukuran berapa saja
Fungsi H menghasilkan nilai (h) dengan panjang yang tetap
Untuk setiap h yang dihasilkan, tidak mungkin dikembalikan nilai x sedemikian sehingga H(x) = h, maka itu disebut satu arah
Untuk setiap x yang diberikan, tidak mungkin mencari $x \neq y$, sedemikian sehingga H(x) = H(y)
Tidak mungkin mencari pasangan x dan y sedemikian sehingga

$$H(x) = H(y)$$

Cryptography

Otentikasi dan Tanda Tangan Digital

Kriptografi juga menangani masalah keamanan berikut

Keabsahan pengirim

Apakah pesan yang diterima benar-benar dari pengirim yang sesungguhnya?

Keaslian pesan

Apakah pesan yang diterima tidak mengalami perubahan(modifikasi)?

Anti penyanggahan

Pengirim tidak dapat menyanggah tentang isi pesan atau ia yang mengirim pesan

Ketiga masalah ini dapat diselesaikan dengan teknik otentikasi

Teknik otentikasi adalah prosedur yang digunakan untuk membuktikan keaslian pesan atau identitas pemakai

Cryptography

Tanda Tangan Digital

Tanda tangan digunakan untuk membuktikan otentikasi dokumen kertas

Fungsi tanda tangan dapat diterapkan untuk otentikasi pada data digital

Pada data digital, tanda tangan ini disebut tanda tangan digital (*digital signature*).

Bukan berupa tanda tangan yang di-scan, tetapi nilai kriptografi dari pesan dan pengirim pesan

Beda dengan tanda tangan pada dokumen:

- Tanda tangan pada dokumen sama semua
- Tanda tangan digital berbeda

Integritas data dapat dijamin dan dapat juga membuktikan asal pesan(keabsahan pengirim dan anti penyanggahan)

Cryptography

Tanda Tangan Digital dengan Algoritma Kunci Publik
Algoritma kunci publik dapat digunakan untuk membuat tanda tangan digital
Misalkan M adalah pesan yang akan dikirim. Tanda tangan digital S untuk pesan M diperoleh dengan mengenkripsi M dengan menggunakan kunci rahasia/*private key* (SK)

S = E(M, SK)

E adalah algoritma enkripsi

S dikirim melalui saluran komunikasi. Oleh penerima, pesan dibuktikan kebenaran tanda tangan digital dengan menggunakan kunci publik(PK)

M = D(S, PK)

D adalah algoritma dekripsi

Tanda tangan digital dianggap absah apabila pesan M yang dihasilkan merupakan pesan yang mempunyai makna Algoritma yang sering digunakan adalah RSA dan El Gamal

Cryptography

Tanda Tangan Digital dengan Fungsi Hash

Dari pesan yang hendak dikirim, dibuatkan message digest(MD) dengan fungsi Hash

MD = H(M)

MD dienkrip dengan algoritma kunci publik dengan kunci rahasia (SK) pengirim menjadi tanda tangan digital (S)

S = E(MD, SK)

Pesan M digabung dengan tanda tangan digital (S), lalu dikirim melalui saluran komunikasi (seolah-olah M sudah ditandatangani oleh pengirim)

Cryptography

Tanda Tangan Digital dengan Fungsi Hash

Di tempat penerima, pesan diverifikasi

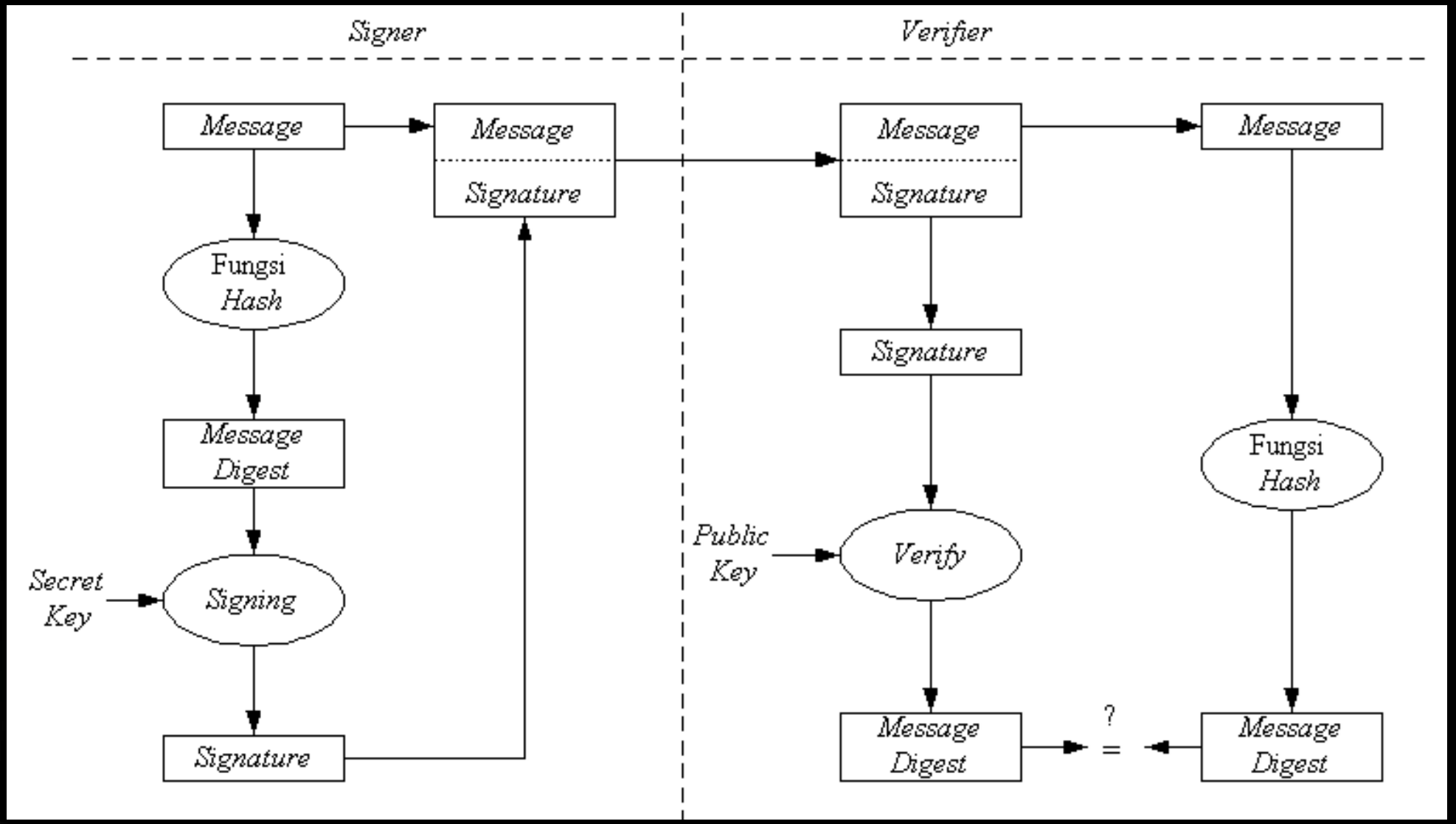
Tanda tangan digital S didekripsi dengan kunci publik (PK) pengirim pesan, sehingga menghasilkan message digest semula (MD)

MD = D(S, PK)

Pengirim membuat Message Digest (MD1) dari pesan M dengan menggunakan fungsi hash yang sama dengan fungsi hash yang digunakan pengirim

Jika MD1 = MD, berarti pesan yang diterima otentik dan berasal dari pengirim yang benar

Cryptography



Cryptography

Serangan Terhadap Kriptografi

Penyadap berusaha mendapatkan data yang digunakan untuk kegiatan kriptanalisis

Kriptanalis berusaha mengungkapkan plainteks atau kunci dari data yang disadap

Kriptanalis dapat juga menemukan kelemahan dari sistem kriptografi yang pada akhirnya mengarah untuk menemukan kunci dan mengungkapkan plainteks

Penyadapan dapat dilakukan melalui saluran kabel komunikasi dan saluran wireless

Cryptography

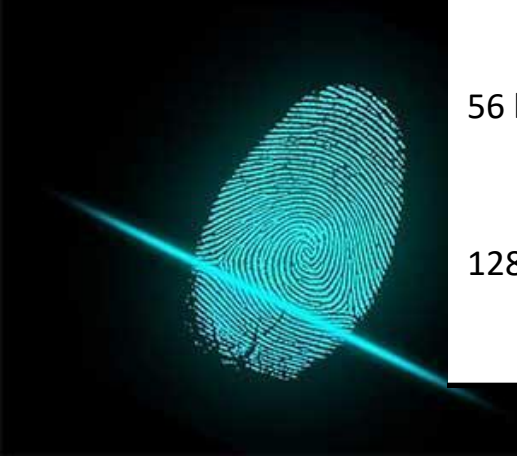
Jenis-jenis serangan:

1. Exhaustive attach atau brute force attack
    - Percobaan yang dibuat untuk mengungkapkan plainteks atau kunci dengan mencoba semua kemungkinan kunci (trial and error)
    - Diasumsikan kriptanalis:
        - Memiliki sebagian plainteks dan cipherteks yang bersesuaian
    - Caranya:
        - Plainteks yang diketahui dienkripsi dengan setiap kemungkinan kunci, lalu hasilnya dibandingkan dengan cipherteks yang bersesuaian
        - Jika hanya cipherteks yang tersedia, cipherteks tersebut didekripsi dengan setiap kemungkinan kunci dan plainteks hasilnya diperiksa apakah mengandung makna atau tidak
    - Serangan ini membutuhkan waktu yang sangat lama
    - Untuk menghindari serangan ini, gunakan kunci yang panjang dan tidak mudah ditebak

Cryptography

Waktu yang diperlukan untuk *exhaustive key search*
(Sumber: William Stallings, *Data and Computer Communication Fourth Edition*)

Ukuran Kunci	Jumlah Kemungkinan Kunci	Lama waktu untuk 10^6 percobaan per detik	Lama waktu untuk 10^{12} percobaan per detik
16 bit	$2^{16} = 65536$	32.7 milidetik	0.0327 mikrodetik
32 bit	$2^{12} = 4.3 \times 10^9$	35.8 menit	2.15 milidetik
56 bit	$2^{56} = 7.2 \times 10^{16}$	1142 tahun	10.01 jam
128 bit	$2^{128} = 4.3 \times 10^1$	5.4×10^{24} tahun	5.4×10^{18} tahun



Cryptography

Jenis-jenis serangan:

2. Analytical attach

   Kriptanalis tidak mencoba semua kemungkinan kunci, tetapi menganalisa kelemahan algoritma kriptografi untuk mengurangi kemungkinan kunci yang tidak ada.

   Analisa yang dilakukan dengan memecahkan persamaan-persamaan matematika yang diperoleh dari definisi suatu algoritma kriptografi

   Diasumsikan kriptanalis mengetahui algoritma kriptografi

   Metode *analytical attack* biasanya lebih cepat menemukan kunci dibandingkan dengan *exhaustive attack*.

   Untuk menghindari serangan ini, kriptografer harus membuat algoritma yang kompleks.

Cryptography

Memastikan keamanan dari algoritma kriptografi

Algoritma harus dievaluasi oleh pakar

Algoritma yang tertutup (tidak dibuka kepada publik) dianggap tidak aman

Membuat algoritma yang aman tidak mudah

Code maker VS code breaker akan terus berlangsung

THANK YOU

Computer Security