

# Pengantar Kriptografi

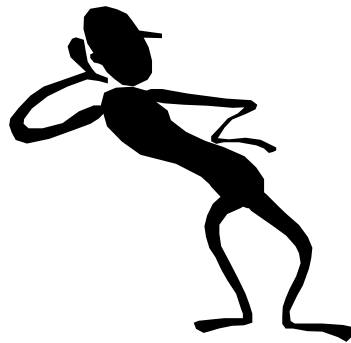


Bahan Kuliah *IF4020 Kriptografi*

Oleh: Rinaldi Munir

ENC □ %???? □ Ü3E«Q)\_l □ p?²D¹J,,ö´Ö ô  
Gx)€\_ Ûë¶<æ“Äó~,,□³ý~eÿw—  
Ô □ ÖÉf80 □

????????????????

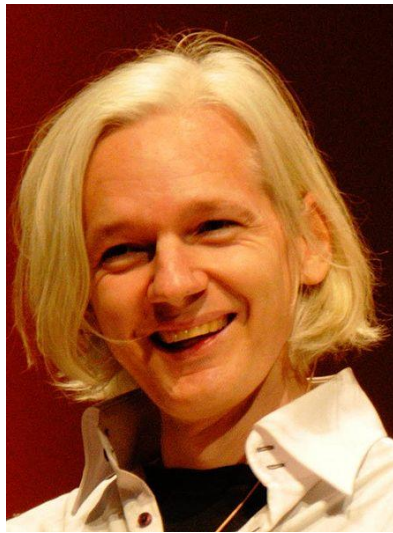




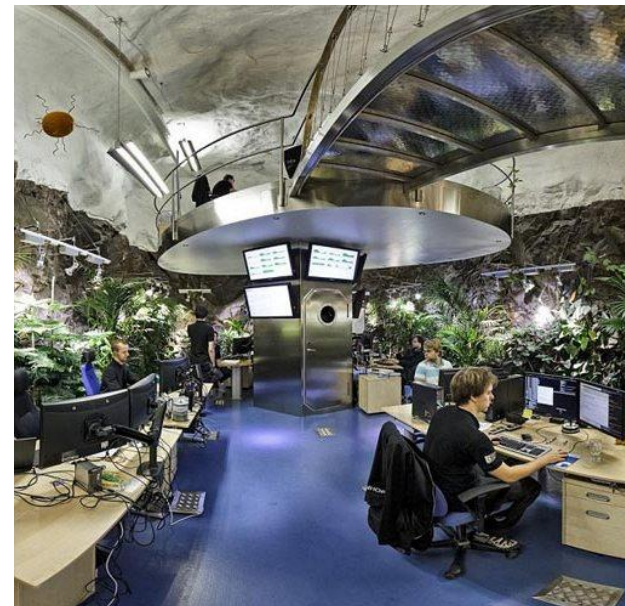
# Selamat datang di kelas Kriptografi

# Masih ingat dengan kasus2 berikut?

1. **Wikileaks**: mengungkapkan dokumen-dokumen rahasia negara dan perusahaan kepada publik melalui situs web.



Julian Assange, salah satu pendiri situs WikiLeaks.



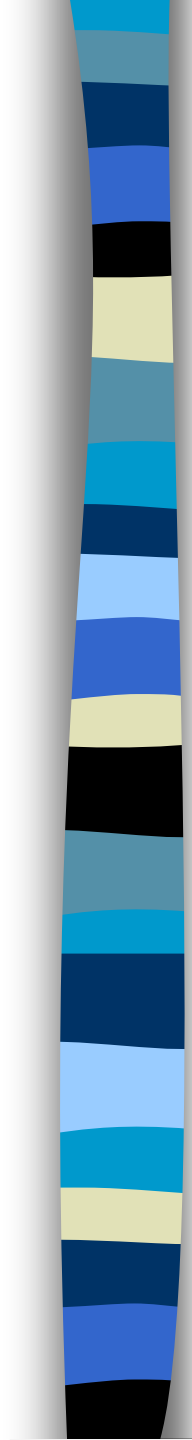
Kantor dan tempat penyimpanan data WikiLeaks.



## Dokumen yang dibocorkan:

1. Data Nasabah Bank Julius Baer
2. Surel Sarah Palin
3. Video Helikopter Apache
4. Perang Afganistan
5. Berkas Guantanamo
5. Dokumen Perang Irak
6. Kawat diplomatik Amerika Serikat

**(Sumber: Wikipedia)**



2. Kasus penyadapan percakapan ponsel antara Artalyta Suryani (Ayin) dan Kemas Yahya Rahman yang melibatkan Jaksa Urip Tri Gunawan tentang “dugaan” suap Rp 6 Milyar lebih.

Transkrip percakapan:

A: Halo..

K: Halo.

A: Ya, siap.

K: Sudah dengar pernyataan saya (Soal penghentian penyelidikan kasus BLBI)? He...he...he

A: Good, very good.

K: Jadi tugas saya sudah selesai.

A: Siap, tinggal...

K: Sudah jelas itu, gamblang. Tidak ada permasalahan lagi



A: Bagus itu

K: Tapi saya dicaci maki. Sudah baca Rakyat Merdeka (surat kabar Rakyat Merdeka yang terbit di Jakarta)?

A: Aaah Rakyat Merdeka, mah nggak usah dibaca

K: Bukan, katanya saya mau dicopot ha..ha...ha. Jadi gitu ya...

A: Sama ini Bang, saya mau informasikan

K: Yang mana?

A: Masalah si Joker.

K: Ooooo nanti, nanti, nanti.

A: Nggak, itu kan saya perlu jelasin, Bang

K: Nanti, nanti, tenang saja.

A: Selasa saya ke situ ya...

K: Nggak usah, gampang itu, nanti, nanti. Saya sudah bicarakan dan sudah ada pesan dari sana. Kita...

A: Iya sudah

K: Sudah sampai itu

A: Tapi begini Bang...

K: Jadi begini, ini sudah telanjur kita umumkan. Ada alasan lain, nanti dalam perencanaan



# Menyingkap Dunia Penyadapan (1)

## Pejabat Gerah Gunakan Ponsel

Sjamsir Siregar - [inilah.com/Abdul Rauf](http://inilah.com/Abdul%20Rauf)

INILAH.COM, Jakarta Penyadapan seperti jadi dunia terang benderang di Pengadilan Tipikor. Apa saja yang dikatakan Artalyta Suryani, tersangka kasus penyuaapan jaksa, diumbar. Seperti apa sebenarnya penyadapan? Bagaimana aturannya?

Suara Sjamsir Siregar terdengar keras dari balik teleponnya. "Aku sedang sibuk bekerja. Kalau mau bertemu, silahkan. Tapi nantilah dicarikan waktu. Kalau bicara di telepon, jangan! Banyak penyadapan sekarang. Sudah ya, aku mau sholat Jumat dulu," kata Kepala Badan Intelijen Negara (BIN) itu.





## **Moral of the story:**

Kasus-kasus kebocoran informasi dan penyadapan tersebut menunjukkan bahwa **KRIPTOGRAFI** itu sangat penting.



# Terminologi

- **Pesan:** data atau informasi yang dapat dibaca dan dimengerti maknanya.  
Nama lain: **plainteks** (*plaintext*)  
**teks-jelas** (*cleartext*)
- Rupa pesan: teks, gambar, musik mp3, video, tabel, daftar belanja, dll
- Pesan ada yang:
  - dikirim (via pos, kurir, saluran telekom., dll),
  - disimpan di dalam storage (*disk*, kaset, *CD*)

# Pesan

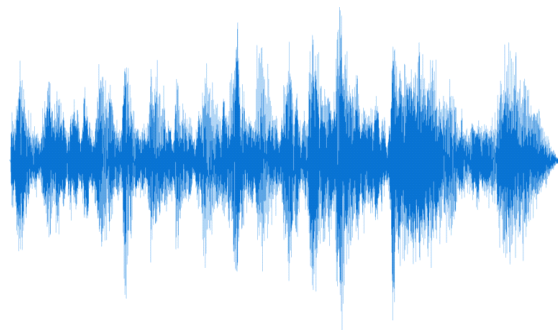
(a) Teks

“Kita semua bersaudara”  
“Hello, world!”  
“Namaku Alice”

(b) Gambar



(c) Audio



Sumber: <http://cloudinary.com>

(d) Video

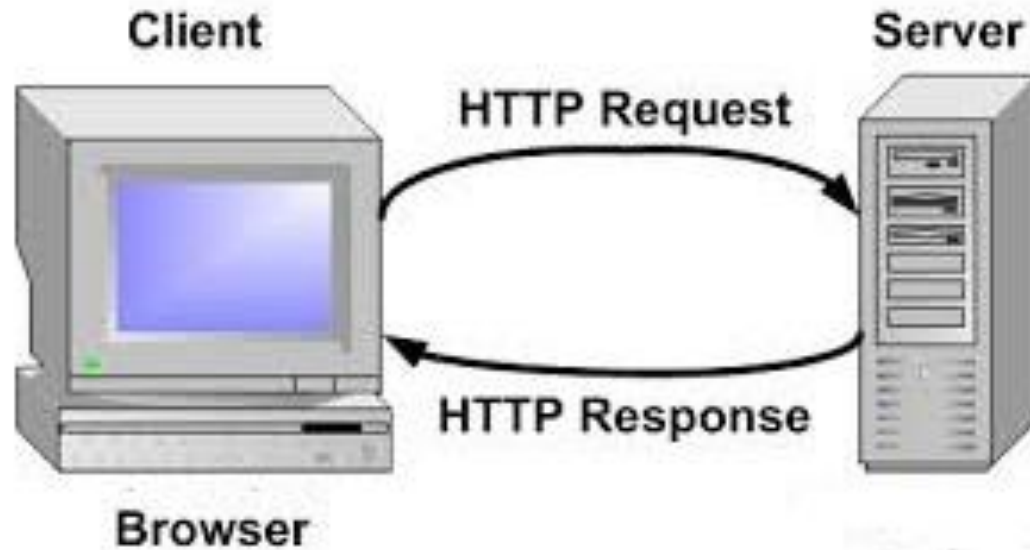


Sumber: <http://www.engineersgarage.com>



# Terminologi

- **Pengirim** (*sender*): pihak yang mengirim pesan
- **Penerima** (*receiver*): pihak yang menerima pesan
- Pengirim/penerima bisa berupa orang, komputer, mesin, dll
- Contoh:
  - pengirim = Alice, penerima = Bob;
  - pengirim = komputer *client*, penerima = komp. *server*;
  - pengirim = Alice, penerima = mesin penjawab
- Pengirim ingin pesan dapat dikirim secara aman, yaitu pihak lain tidak dapat membaca/memanipulasi pesan.



Contoh pengirim = komputer *client*,  
penerima = komp. *server*



# Terminologi

- **Cipherteks** (*ciphertext*): pesan yang telah disandikan sehingga tidak bermakna lagi.  
Tujuan: agar pesan tidak dapat dibaca oleh pihak yang tidak berhak.  
Nama lain: **kriptogram** (*cryptogram*)
- Cipherteks harus dapat dikembalikan menjadi plainteks semula



# Terminologi

Contoh:

Plainteks:

culik anak itu jam 11 siang

Cipherteks:

t^\$gfUi89rewoFpfdWqL:p[uTcxZ

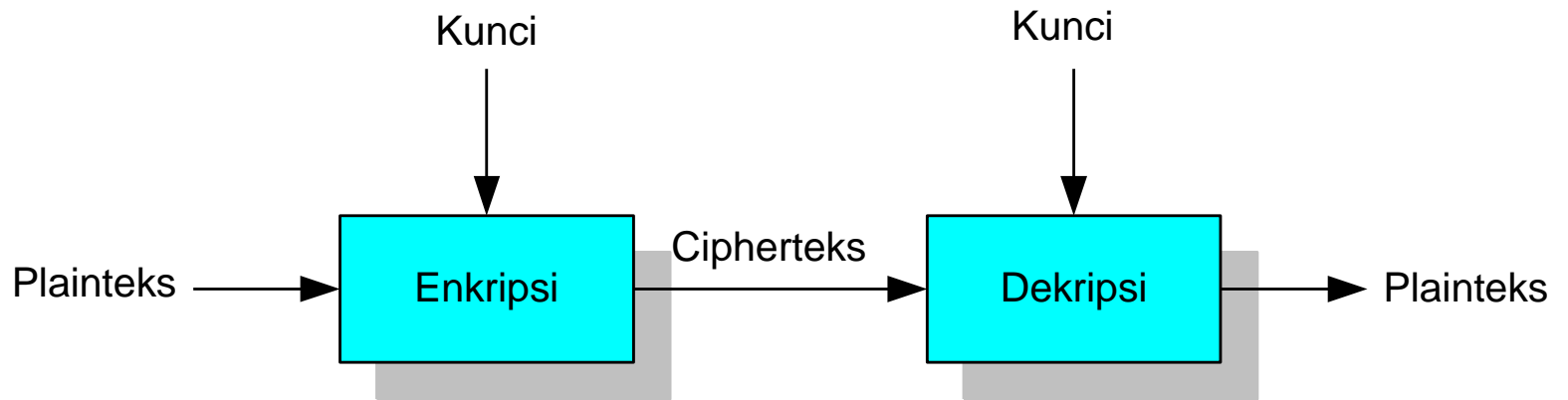


# Terminologi

- **Enkripsi** (*encryption*): proses menyandikan plainteks menjadi cipherteks.  
Nama lain: *enciphering*
- **Dekripsi** (*decryption*): Proses mengembalikan cipherteks menjadi plainteks semula.  
Nama lain: *deciphering*



# Terminologi





# Notasi Matematis

Misalkan:

$C$  = chiperteks

$P$  = plainteks

Fungsi enkripsi  $E$  memetakan  $P$  ke  $C$ ,

$$E(P) = C$$

Fungsi dekripsi  $D$  memetakan  $C$  ke  $P$ ,

$$D(C) = P$$



Fungsi enkripsi dan dekripsi harus memenuhi sifat:

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



# Aplikasi Enkripsi – Dekripsi

1. Pengiriman data melalui saluran komunikasi (*data encryption on motion*).
2. Penyimpanan data di dalam *disk storage* (*data encryption at rest*)



# *Data Encryption on Motion*

- 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.
- Siaran televisi berbayar (Pay TV)
- Pesan melalui *BlackBerry Messenger* (BBM)



# *Data Encryption at Rest*

## 1. Dokumen teks

Plainteks (`plain.txt`):

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

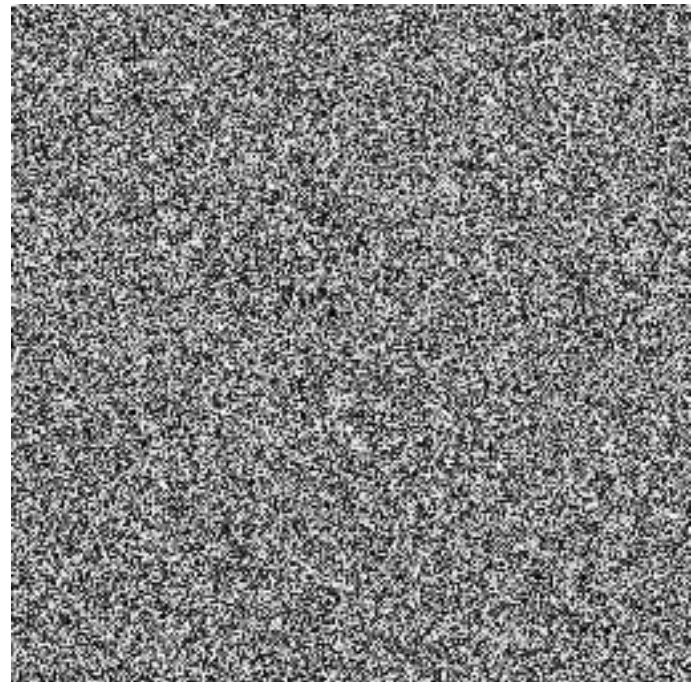
Cipherteks (`cipher.txt`):

```
Ztâxzp/épêp/qtüyp{p}<yp{p}/sx/□p}âpx;  
□□épêp/|t}t|äzp}/qp}êpz/étzp{x/zt□xâx  
}v□□êp}v/|tüp}vzpz/|t}äyâ/{pââ=/\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}/qpwâp/{pââ  
/psp{pw□□â|□pâ/ztwxsâ□p}/|tützp=
```

## 2. Dokumen gambar



Plain image



Cipher image

### 3. 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}äyâ/{ää	äzp}	épêp
000002	□□ t}tâpé/spüx/sp	péxü=	ztxsä□
000003	□□ât □pâ/ztxsä□p}/	}/ tü	spüx/
000004	épêp/ t}t äzp}/qpêpz	qp}êpz	wxsä
000005	étzp{x/ztxâx}v□□êp}	pää/psp	étzp{
000006	spüx/sp{p /□péxü=/>]	xâx}v	ttüzp/
000007	Ztâxzp/épêp/qtüypp}<	äzp}	}äyâ/{
000008	qpwâp/{pää/psp{pw□	Ztxs	xâx}v□□
000009	}t äzp}/qp}êpz/ép{	qp}êp	äzp}/qp

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

## 4. Video



Sebuah *frame* plain-video



*Cipher-video* (Chung, 2015)



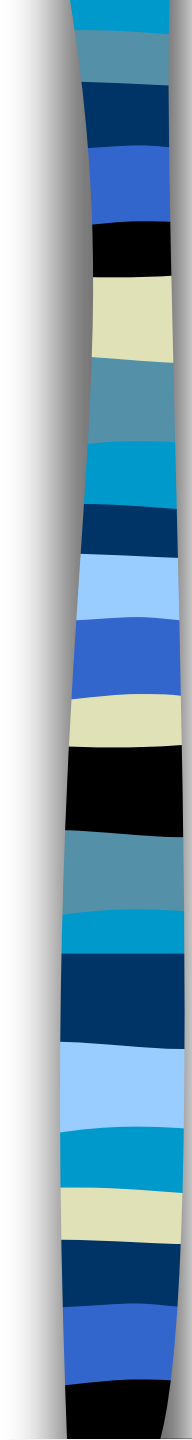
# Terminologi

- **Kriptografi (*cryptography*)**
- Kata *cryptography* berasal dari bahasa Yunani: κρυπτο (*hidden* atau *secret*) dan γραφή (*writing*)  
Artinya “*secret writing*”
- Definisi lama:  
**Kriptografi** adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya.



# Terminologi

- Kriptografi berkembang sedemikian rupa sehingga tidak lagi sebatas mengenkripsi pesan, tetapi juga memberikan aspek keamanan yang lain (akan dibahas nanti).
- Definisi baru: **Kriptografi** adalah ilmu dan seni untuk menjaga keamanan pesan (*message*) [Schneier, 1996].  
*“art and science to keep message secure”*

- 
- Definisi pembandingan (Menez, 1996):
  - **Kriptografi** adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi



# Terminologi

- **Algoritma kriptografi (*cipher*)**
  - aturan untuk *enchipering* dan *dechipering*, atau
  - fungsi matematika yang digunakan untuk enkripsi dan dekripsi pesan.



# Terminologi

- *Cipher* tidak sama dengan kode (*code*)
- Kode mempunyai sejarah tersendiri di dalam kriptografi
- Contoh kode:

Pesan: kapal api datang

Kode: hutan bakau hancur

Pesan: kapal api datang

Kode: xzytvq bkugbf hjqpot

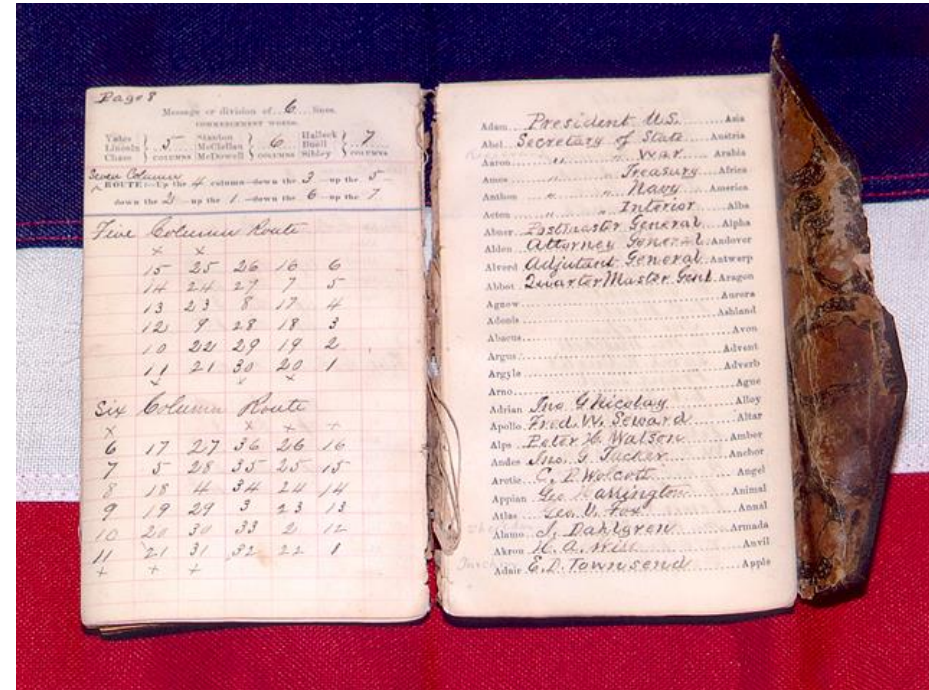
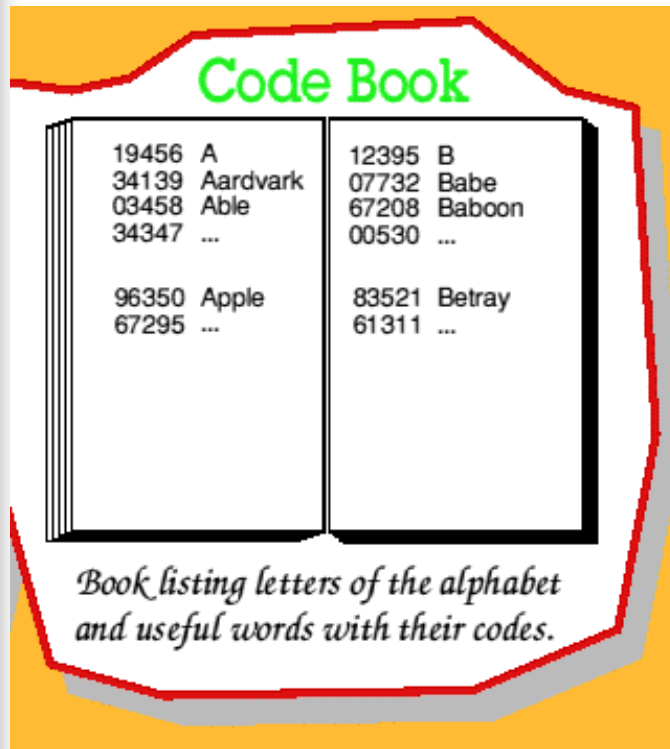


# Terminologi

- *Encoding*: Transformasi dari plainteks menjadi kode
- *Decoding*: transformasi kebalikan dari kode menjadi plainteks.
- **Buku kode** (*codebook*): dokumen yang digunakan untuk mengimplementasikan suatu kode
- Buku kode terdiri dari tabel *lookup* (*lookup table*) untuk *encoding* dan *decoding*



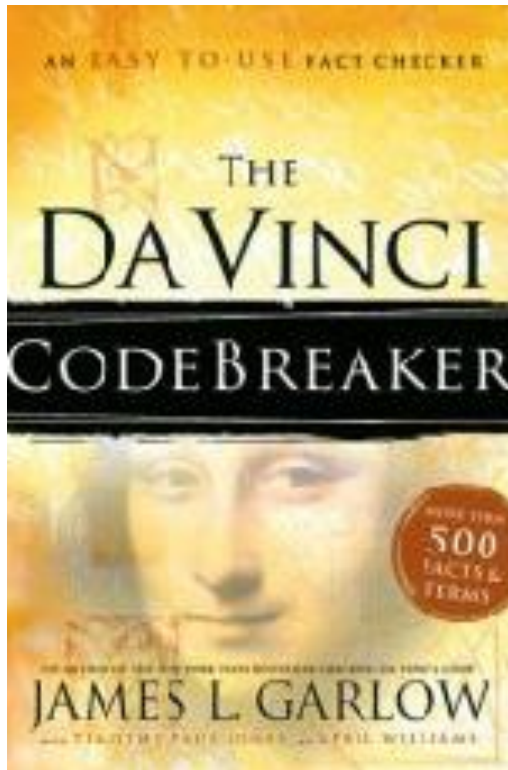
# Terminologi



Kiri: Buku kode, Kanan: Sebuah buku kode yang digunakan untuk korespondensi telegraf (Sumber gambar:

# Terminologi

- *Codebreaker*: Orang yang memecahkan kode (untuk menemukan plainteks)





# Terminologi

- Kunci: parameter yang digunakan untuk transformasi *enciphering* dan *dechipering*
- 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*)

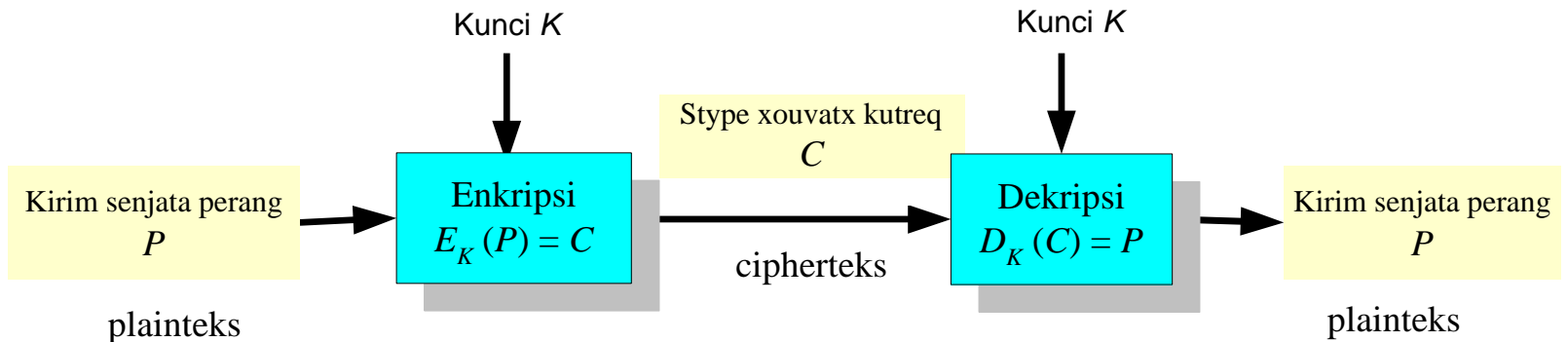
# Terminologi

- Enkripsi dan dekripsi dengan kunci:

Enkripsi:  $E_K(P) = C$

Dekripsi:  $D_K(C) = P$

Harus dipenuhi:  $D_K(E_K(P)) = P$





# Terminologi

## ■ **Sistem kriptografi** (*cryptosystem*)

Terdiri dari:

- algoritma kriptografi,
- plainteks,
- cipherteks,
- dan kunci.



# Terminologi

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

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

- Ron Rivest (pakar kriptografi): “*cryptography is about communication in the presence of adversaries*”

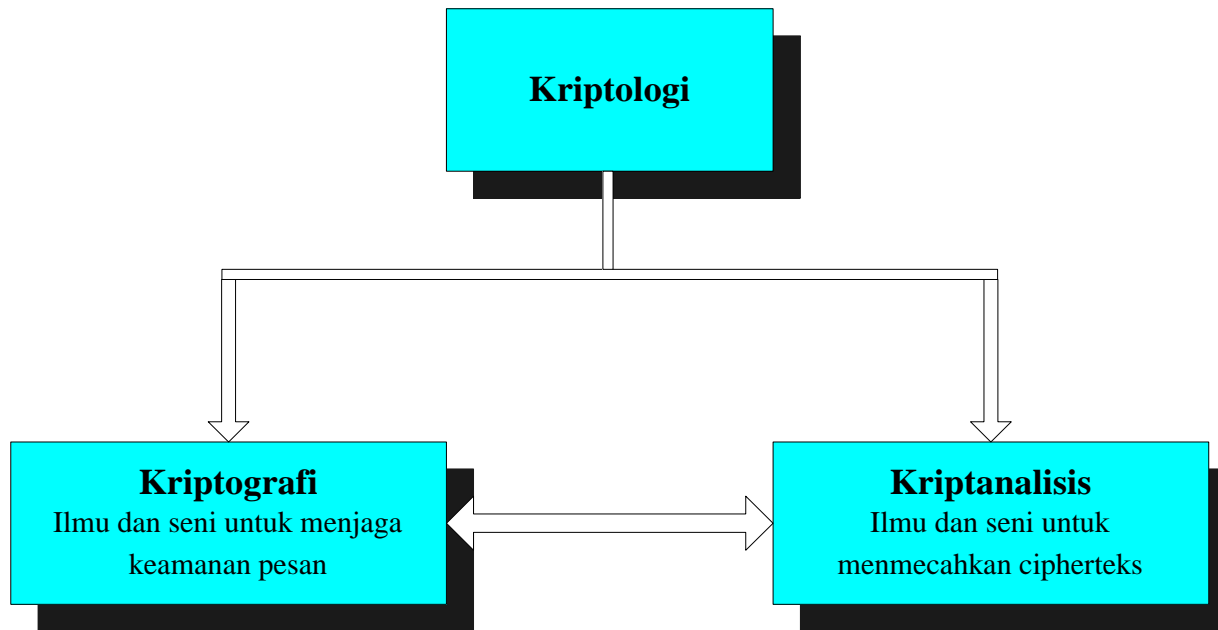


# Terminologi

- **Kriptanalisis** (*cryptanalysis*): ilmu dan seni untuk memecahkan ciperteks menjadi plainteks tanpa mengetahui *kunci* yang digunakan.
- Pelakunya disebut **kriptanalisis**
- (Perancang algoritma kriptografi: **kriptografer**)
- Kriptanalisis merupakan “lawan” kriptografi

# Terminologi

- **Kriptologi** (*cryptology*): studi mengenai kriptografi dan kriptanalisis.







# Terminologi

Persamaan kriptografer dan kriptanalis:

- → Keduanya sama-sama menerjemahkan cipherteks menjadi plainteks

Perbedaan kriptografer dan kriptanalis:

- → Kriptografer bekerja atas legitimasi pengirim atau penerima pesan
- → Kriptanalis bekerja tanpa legitimasi pengirim atau penerima pesan

# Sejarah Kriptografi

- Kriptografi mempunyai sejarah yang panjang.
- Tercatat Bangsa Mesir 4000 tahun yang lalu menggunakan *hieroglyph* yang tidak standard untuk menulis pesan



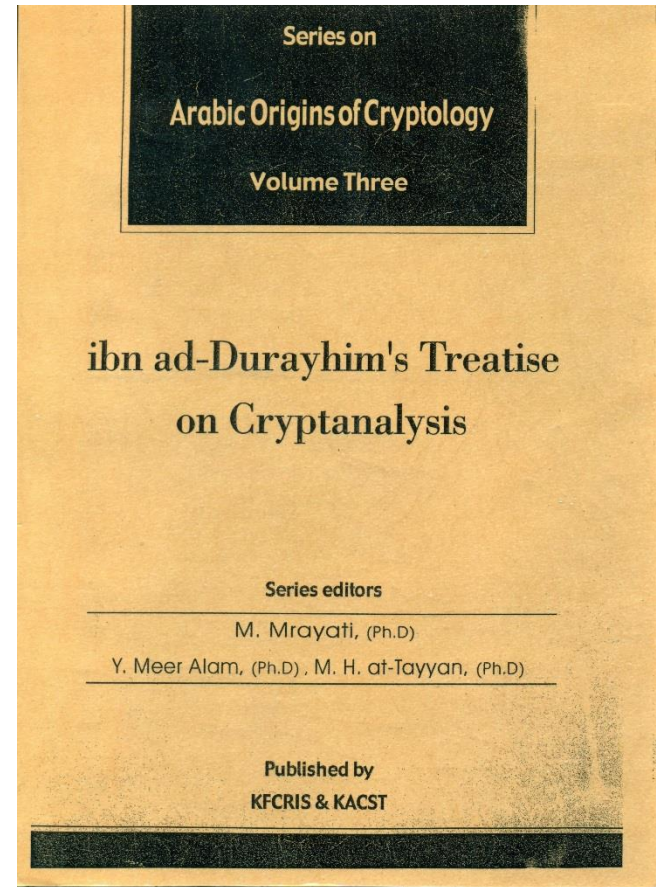
# Sejarah Kriptografi

- Di Yunani, kriptografi sudah digunakan 400 BC
- Alat yang digunakan: *scytale*



Sejarah kriptografi pada bangsa Arab dapat dibaca pada seri buku *Arabic Origins of Cryptology* yang diterbitkan oleh *King Faisal Center for Research and Islamic Studies*, Arab Saudi

Seri pertama menyajikan manuskrip kuno tentang kriptanalisis yang ditulis oleh al-Kindi. Seri kedua tentang risalah Ibn Adlan yang berisi manual kriptanalisis yang ditulis pada abad 13. Seri ketiga adalah risalah ibn ad-Durayhim.





# Sejarah Kriptografi

- 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*



# Sejarah Kriptografi

- 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*



# Sejarah Kriptografi

- Tidak ditemukan catatan kriptografi di Cina dan Jepang hingga abad 15.
- 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.



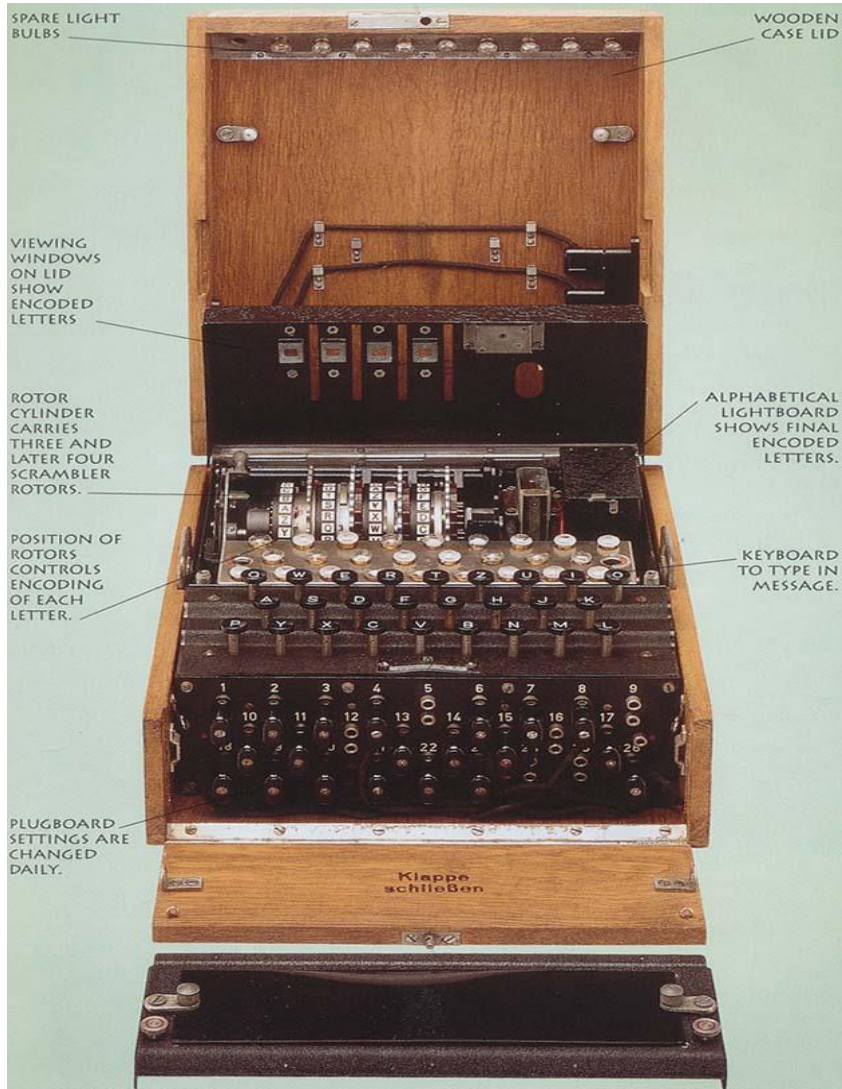
Queen Mary



# Sejarah Kriptografi

- 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





# Enigma

# 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**.





# Kriptanalisis

- 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

# Kriptanalisis

ثم سمى الذهب ساء والذهب نصفه فان الكلام بالفتحين اخرجت من ذلك القول وهو لا يحتمل ما اخرج له  
من ما فيقال ان به اخرج نصيبه ويجعل في مستطاب طبر ونياس من طبا بيا محل الشعر ويصنع فلا يسط  
ما في حاشيتا انا الطير ويا حشران والاول من ائير لفتح من الما عنسجة وبها لونه وسفله في  
ولاحتر نصيبه سمى بعلم السيد الصمد في السبل في اسباعه والوزن يسجل للبحر والاسراع  
من الا حشا المرباه في الشاه از المرح ذكره وانكس وركب في حيا السر من الساه السواد في الهم  
من سمى من الامانة وياط اهل نور والرحمة والتبع وحسن والعمارة من الحصار وياط الخوخ و  
انصهر والسفاه المبر ما بالخمر والمربا ويجعل القطر بالصورة الظاهر الفستق م

من القول - والحمد لله رب العالمين صلوات الله عليهم اجمعين

سنة الله الاحمر الرحمة وحسن الله وجهه م  
رسالة الاله في عصور من احوال الدروع استعراج المعمر م  
لكن في حاشيتا هذا وقد علمنا ان من سمي وكانت اوجدت الجملة التي استعملت ما في م  
الكلمة الحكما وانصهر ذلك وجر من الغنول فالجمله الامر من ساه الاكبر الناجم الفصول  
عن قول الاله اسل الابرار ومع هذا على ان الله يحسن النور وهو يسرور الغنى والجمع  
الناهار وسعد م واد الرنا وسعد الساه وقدره انما انطقه واصل ما الابرار المعمر

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

Sejarah kriptanalisis mencatat hasil gemilang seperti pemecahan Telegram Zimmermann yang membawa Amerika Serikat ke kancah Perang Dunia I.

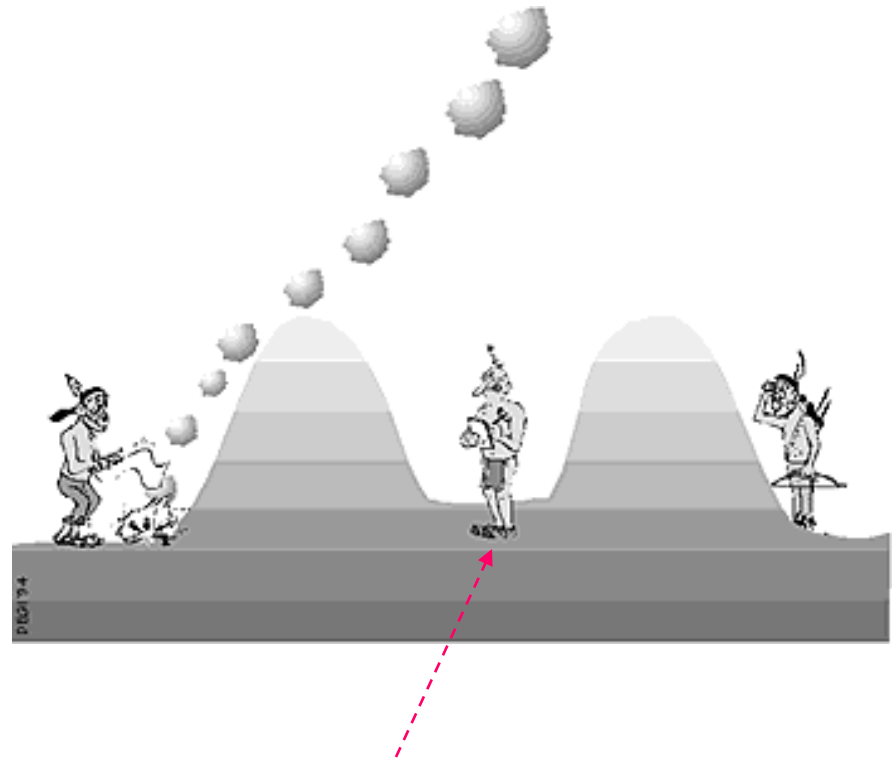
MAILED TELEGRAM RECEIVED.  
October 1-8-18  
Director, State Dept.  
By *Wm. A. Eckhoff*  
Date *Oct. 27, 1918* FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, ~~invite~~ *invite* Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

Telegram Zimmerman yang sudah berhasil didekripsi (Sumber: Wikipedia.org)

# Layanan yang Disediakan Kriptografi

1. Kerahasiaan  
(*confidentiality*)  
Layanan yang digunakan untuk menjaga isi pesan dari siapapun yang tidak berhak untuk membacanya.



Dia bisa ikut menerima pesan tapi tidak mengerti

*Sumber: Tutun Juhana (EL)*

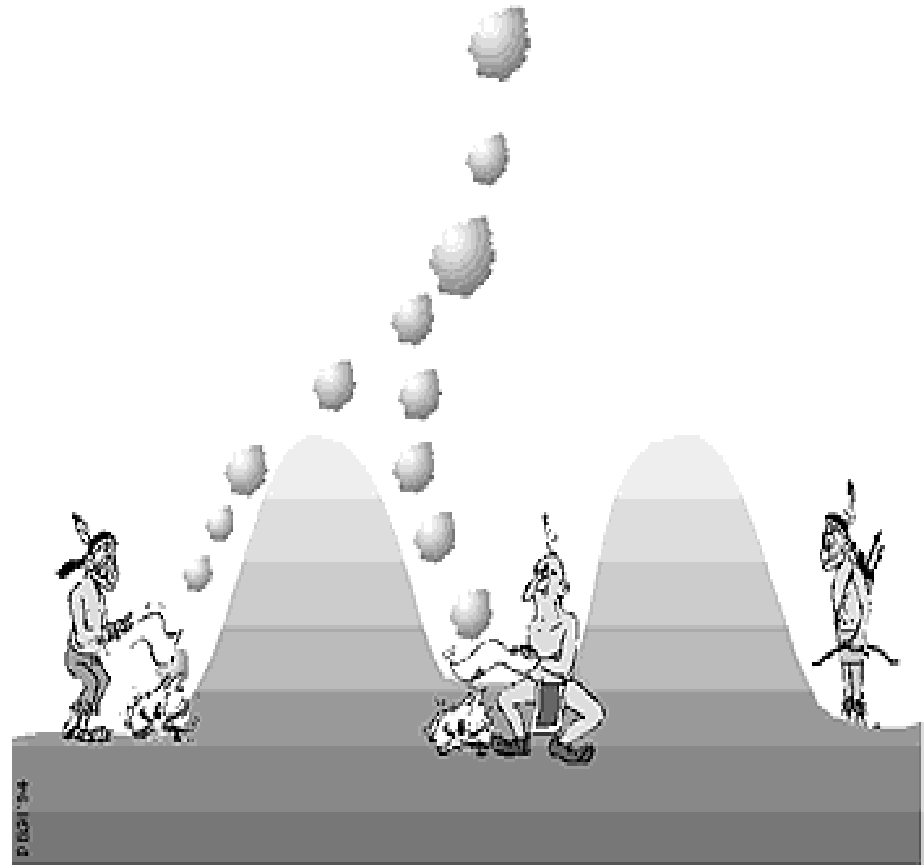


# Layanan yang Disediakan Kriptografi

## 2. **Integritas data** (*data integrity*)

Layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman.

“Apakah pesan yang diterima masih asli atau tidak mengalami perubahan (modifikasi)?”.



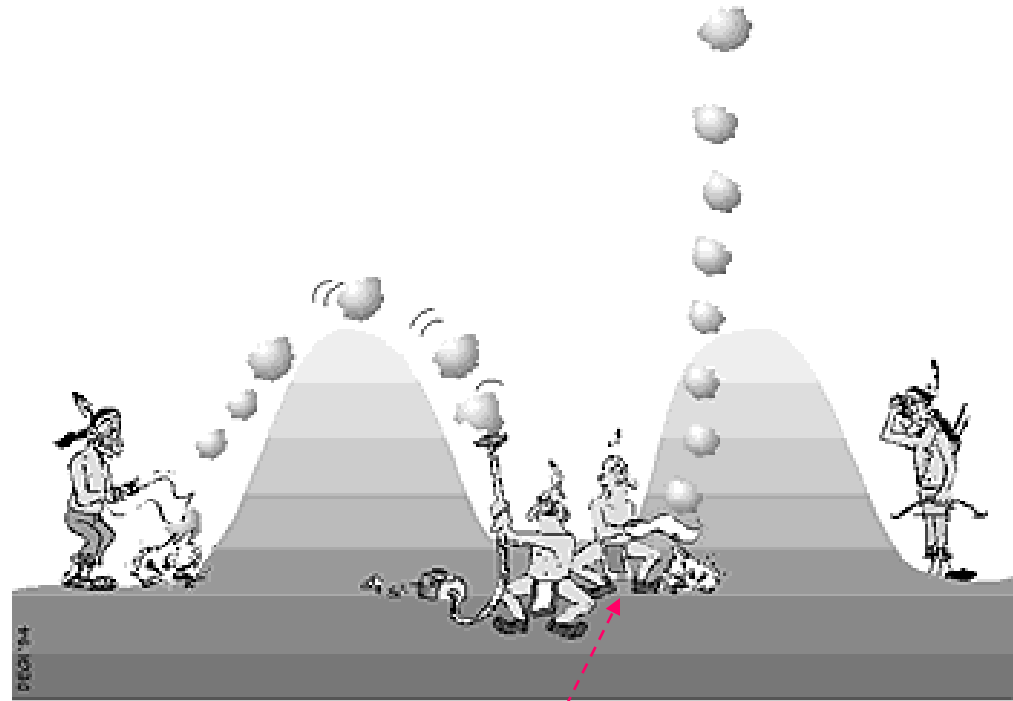
# Layanan yang Disediakan Kriptografi

## 3. Otentikasi

(*authentication*)

Layanan yang untuk mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication*) dan untuk mengidentifikasi kebenaran sumber pesan (*data origin authentication*).

“Apakah pesan yang diterima benar-benar berasal dari pengirim yang benar?”



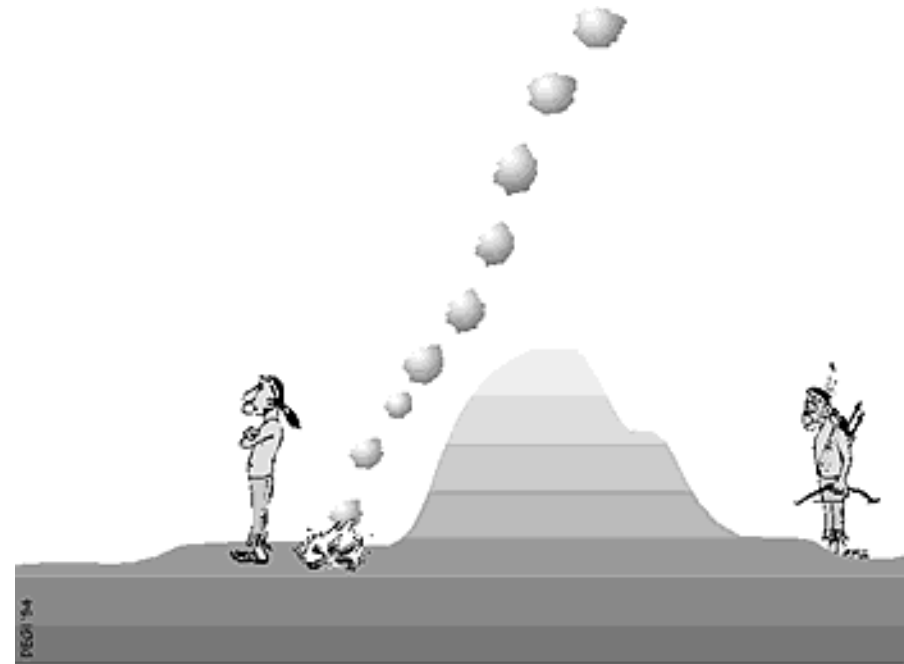
He can claim that he is A



# Layanan yang Disediakan Kriptografi

## 4. Nirpenyangkalan (*non-repudiation*)

Layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.





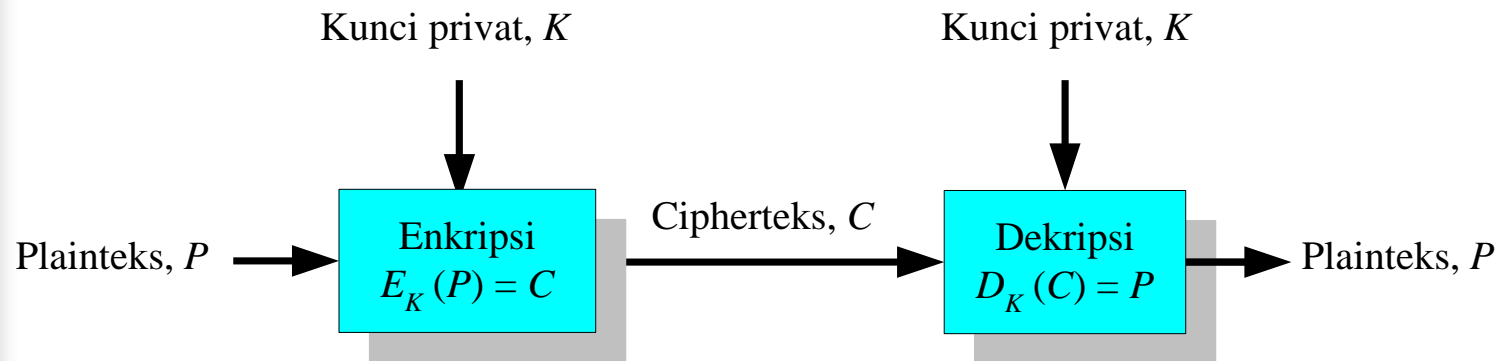
# Saat ini....

Kehidupan kita 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

# Kriptografi kunci-simetri

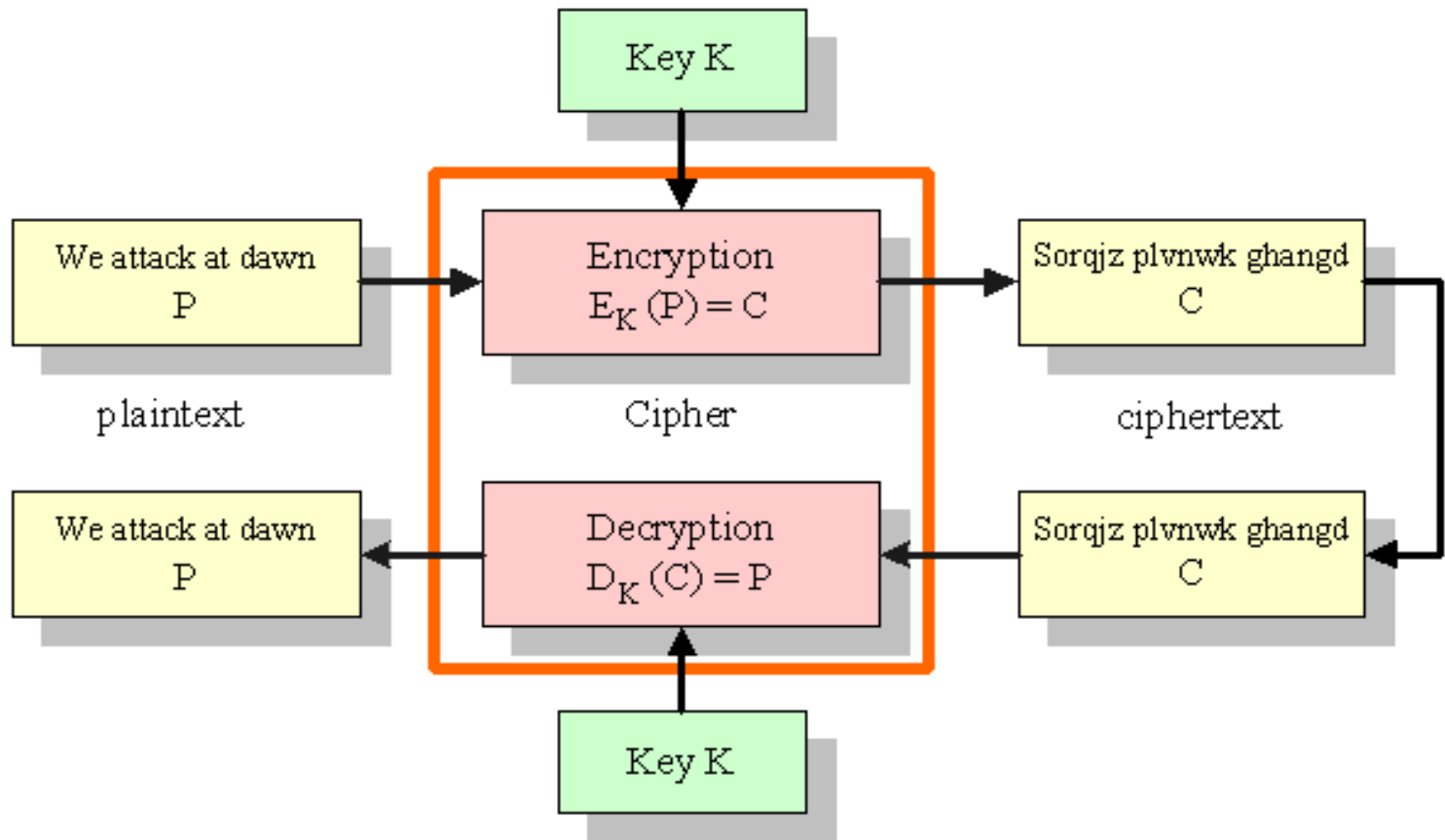
- *Symmetric-key cryptography*
- Kunci enkripsi = kunci dekripsi
- Istilah lainnya: kunci simetri, kunci privat, kunci rahasia (secret key)
- Algoritma kriptografinya disebut algoritma simetri
- Istilah lainnya: algoritma konvensional





# Kriptografi kunci-simetri

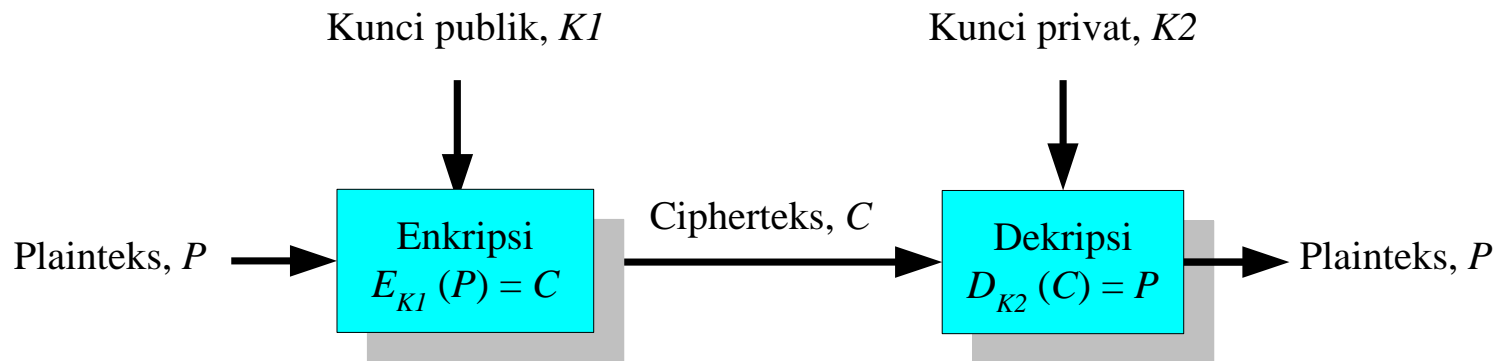
- Contoh algoritma simetri:
  - AES (*Advanced Encryption Standard*)
  - DES (*Data Encryption Standard*)
  - Blowfish
  - IDEA
  - GOST
  - Serpent
  - dll



## Skema algoritma simetri

# Kriptografi kunci-nirsimetri

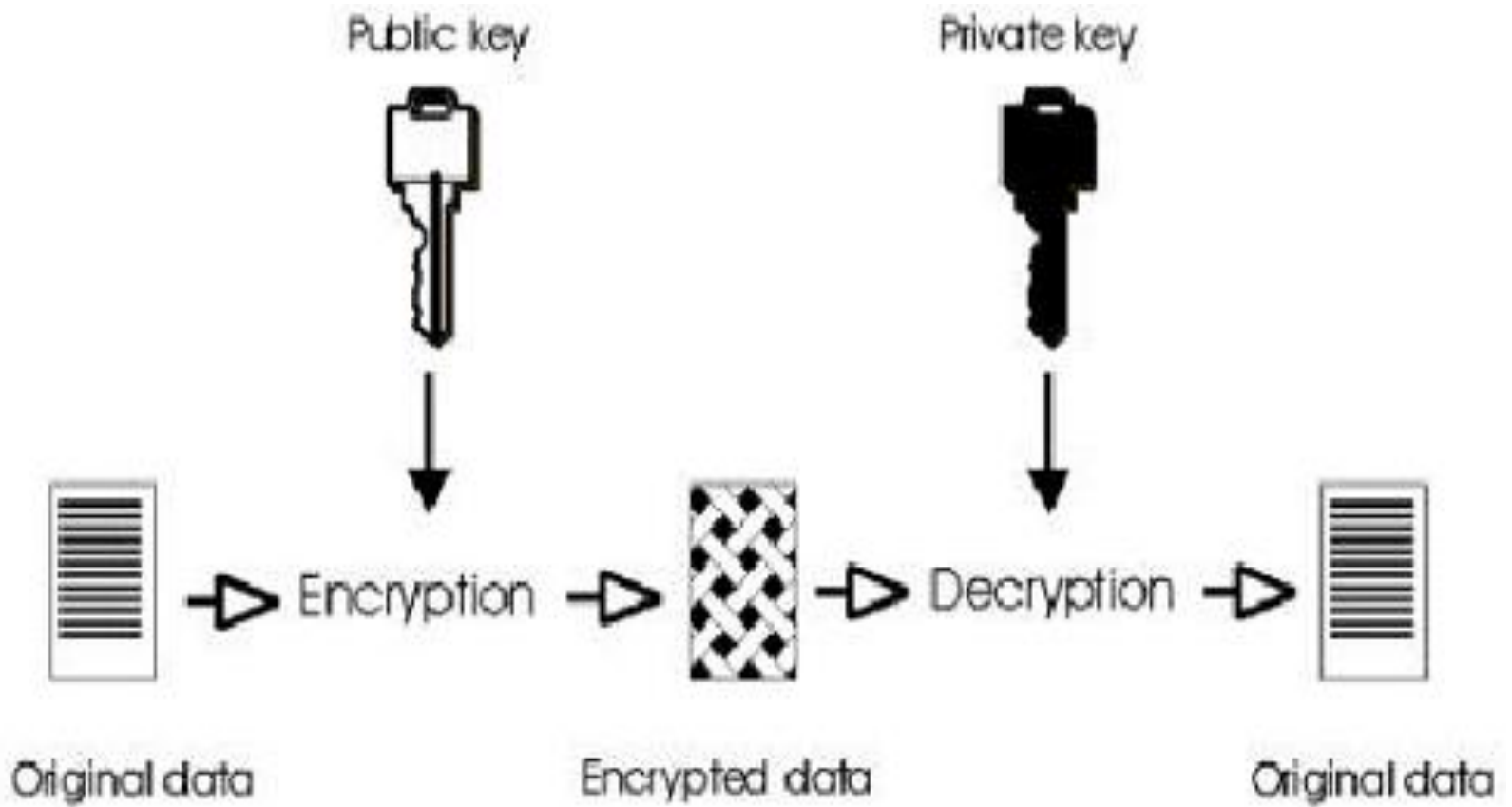
- *Asymmetric-key cryptography*
- Kunci enkripsi  $\neq$  kunci dekripsi
- Nama lain: **kriptografi kunci-publik**
- karena kunci enkripsi bersifat publik (*public key*) sedangkan kunci dekripsi bersifat rahasia (*secret key* atau *private key*).





# Kriptografi kunci-nirsimetri

- Kriptografi kunci-publik dapat dianalogikan seperti kotak surat yang terkunci dan memiliki lubang untuk memasukkan surat.
- Kotak surat digembok dengan kunci. Kunci hanya dimiliki oleh pemilik kotak 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.







# Kriptografi kunci-nirsimetri

- 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.



# Kriptografi kunci-nirsimetri

- Contoh algoritma nirsimetri:
  - ECC (*Ellyptic Curve Cryptography*)
  - RSA
  - ElGamal
  - Rabin
  - Diffie-Hellman Key Exchange
  - DSA
  - dll



# Lembaga Terkait Kriptografi

- Di Indonesia:

1. Lembaga Sandi Negara (Lemsaneg)

(*National Crypto Agency*), <http://www.lemсанeg.go.id/>

2. Sekolah Tinggi Sandi Negara (STSN)

<http://stsn-nci.ac.id/>

- Di Amerika

1. National Security Agency (NSA)



Museum Sandi di Yogyakarta (Sumber: <http://museum.lemsaneg.go.id/>)