01 - Pengantar Kriptografi

ENC%????Ü3E«Q)_lp?²D¹J„

ö´ÖôGx)€_Ûëoej8*5gkp23

@¶<æ¨Äó~„³^TGRflkdpoý~eÿw—uah)Éf80

Selamat datang

di kelas Kriptografi

Prodi Teknik Informatika - ITB

Kriptografi

- Merupakan kakas (*tool*) yang sangat penting di dalam keamanan informasi

- Kata *cryptography* berasal dari bahasa Yunani:

  cryptós (*secret*)

  gráphein (*writing*)

  Artinya "*secret writing*"

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

- **Kriptografi**: ilmu dan seni untuk menjaga keamanan pesan. (Schneier, 1996):

“Aman” artinya:

1. Terjaga kerahasiaannya (*confidentiality*)

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)

Ztäxzp/epëp/qtüyp{p}<yp{p}/sx/□p}
âpx;pêp/|t}t|äzp}/qp}êpz/étzp{x/z
t□xâx}v□□êp}v/|tüp}vzpz/|t}äyä/{p
ää=/\tützp□□psp{pw/p}pz<p}pz/zt□x
åx}v/êp}v/qpüä□□|t}tâpé/spüx/sp{p
|/□péxü=/]p{äüx□□|ttüzp/|t}vpâpzp
}/qpwâp/{pää/psp{pw□□ât|□pä/ztwxs
ä□p}/|tützp=

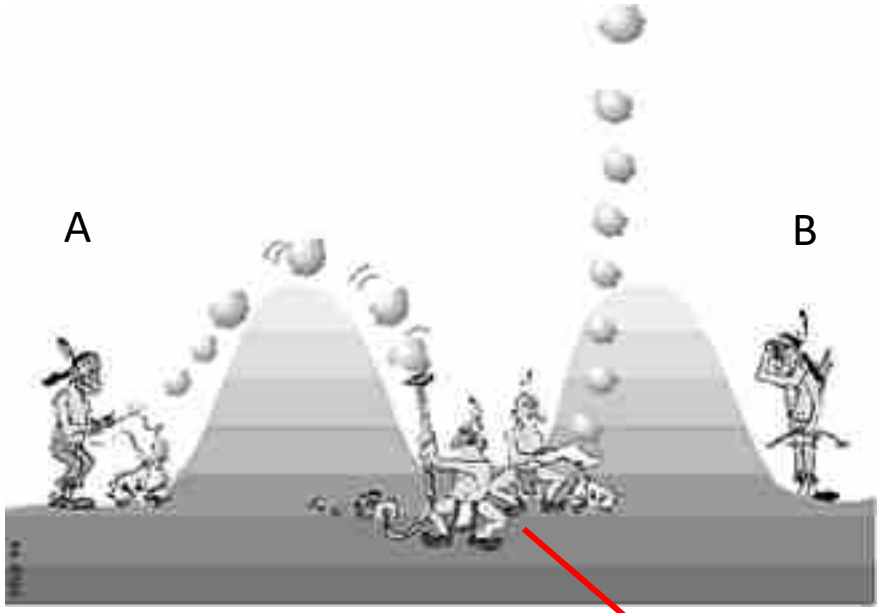
(b) Cipherteks dari (a)

2. Terjaga keasliannya (*data integrity*)

Pesan asli

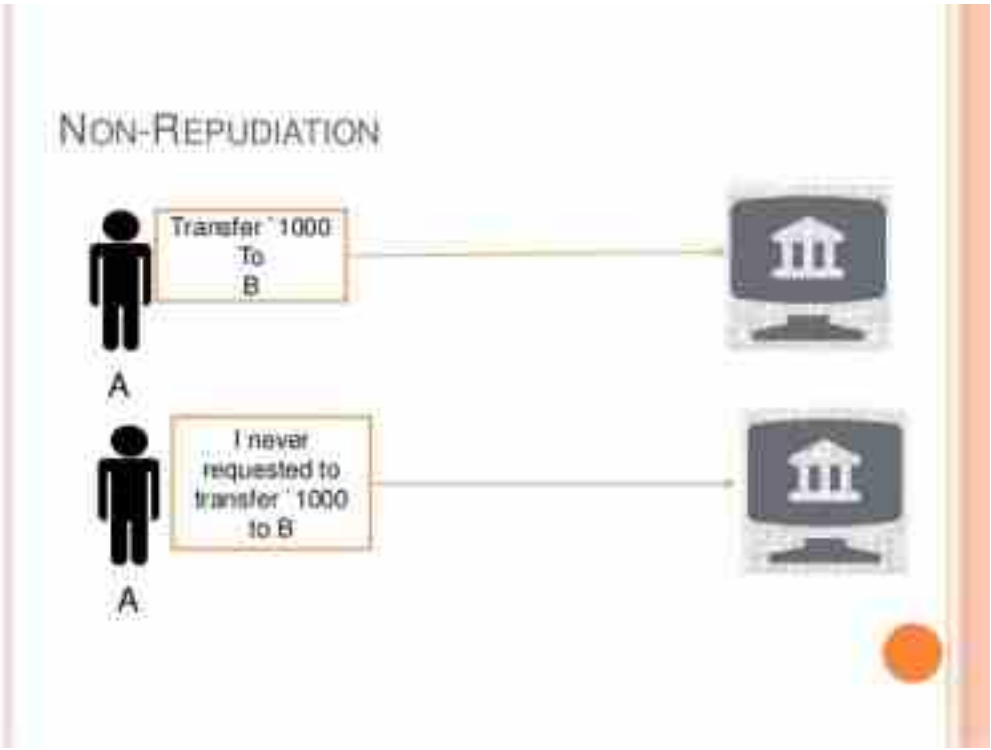
Pesan sudah diubah

3. Yakin pengirim pesan adalah asli (*authentication*), bukan pihak ketiga yang menyamar.



Dia mengklaim bahwa dia adalah *A*

4. Pengirim pesan tidak dapat menyangkal (*non repudiation*) telah mengirim pesan.



Layanan Kriptografi

1. Kerahasiaan pesan (*Confidentiality/privacy/secrecy*)

2. Keaslian pesan (*Data integrity*)

3. Keaslian pengirim dan penerima pesan (*Authentication*)

4. Anti penyangkalan (*Non-repudiation*)

Terminologi di dalam Kriptografi

1. **Pesan**: informasi yang dapat dibaca dan dimengerti maknanya (baik dipersepsi secara visual maupun audial)

   Nama lain: **plainteks** (*plaintext*), *plain-image*, *plain-video*, *plain-video*

   Rupa pesan: teks, gambar, musik, video, tabel, daftar belanja, gambar 3D,

(a) Teks “Kita semua bersaudara” “Hello, world!” “Namaku Alice”	(b) Gambar 
(c) Audio  Sumber: http://cloudinary.com	(d) Video  Sumber: http://www.engineersgarage.com

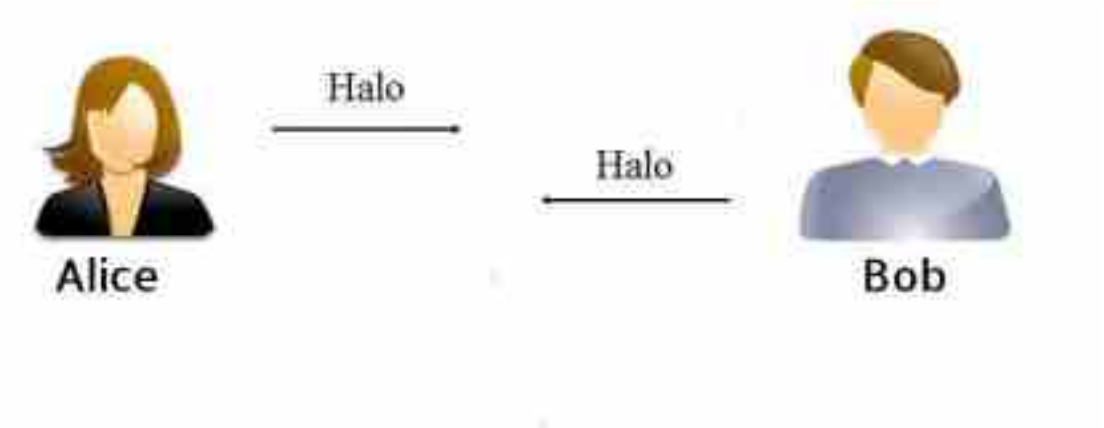
2. **Pengirim** (*sender*): pihak yang mengirim pesan
3. **Penerima** (*receiver*): pihak yang menerima pesan

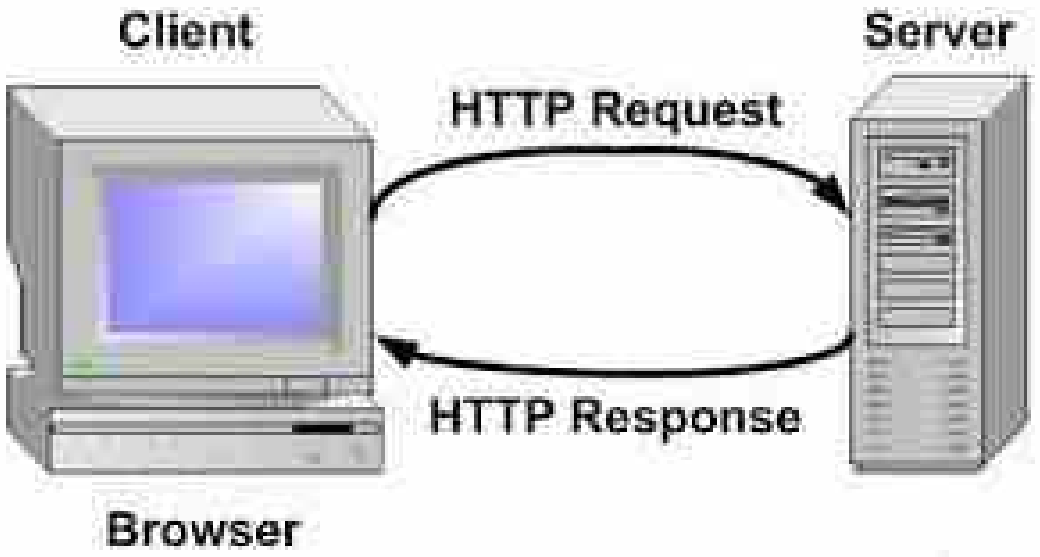
- Pengirim/penerima bisa berupa orang, komputer, mesin, dll
- Contoh:

  pengirim = Alice, penerima = Bob;

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

  pengirim = Alice, penerima = mesin penjawab





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

4. **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*)

- Contoh:

  Plainteks: `culik anak itu jam 11 siang`

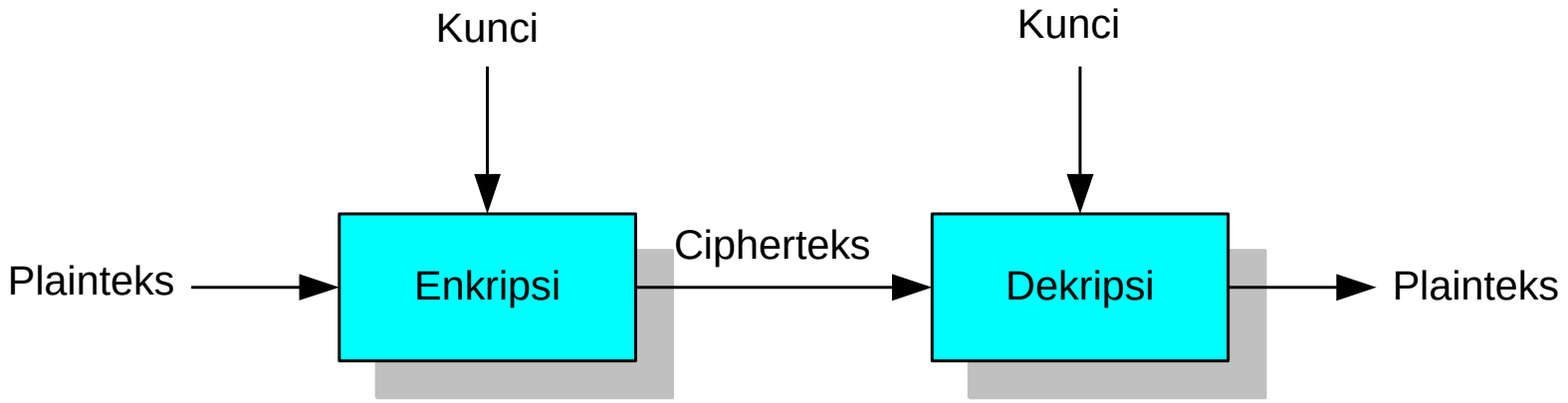
  Cipherteks: `t^$gfUi89rewoFpfdWqL:p[uTcxZ`

5. **Enkripsi** (*encryption*): proses menyandikan plainteks menjadi cipherteks.

   Nama lain: *enciphering*

6. **Dekripsi** (*decryption*): Proses mengembalikan cipherteks menjadi plainteks semula.

   Nama lain: *deciphering*



Misalkan:

C = chiperteks

P = plainteks

Fungsi enkripsi E memetakan P ke C,

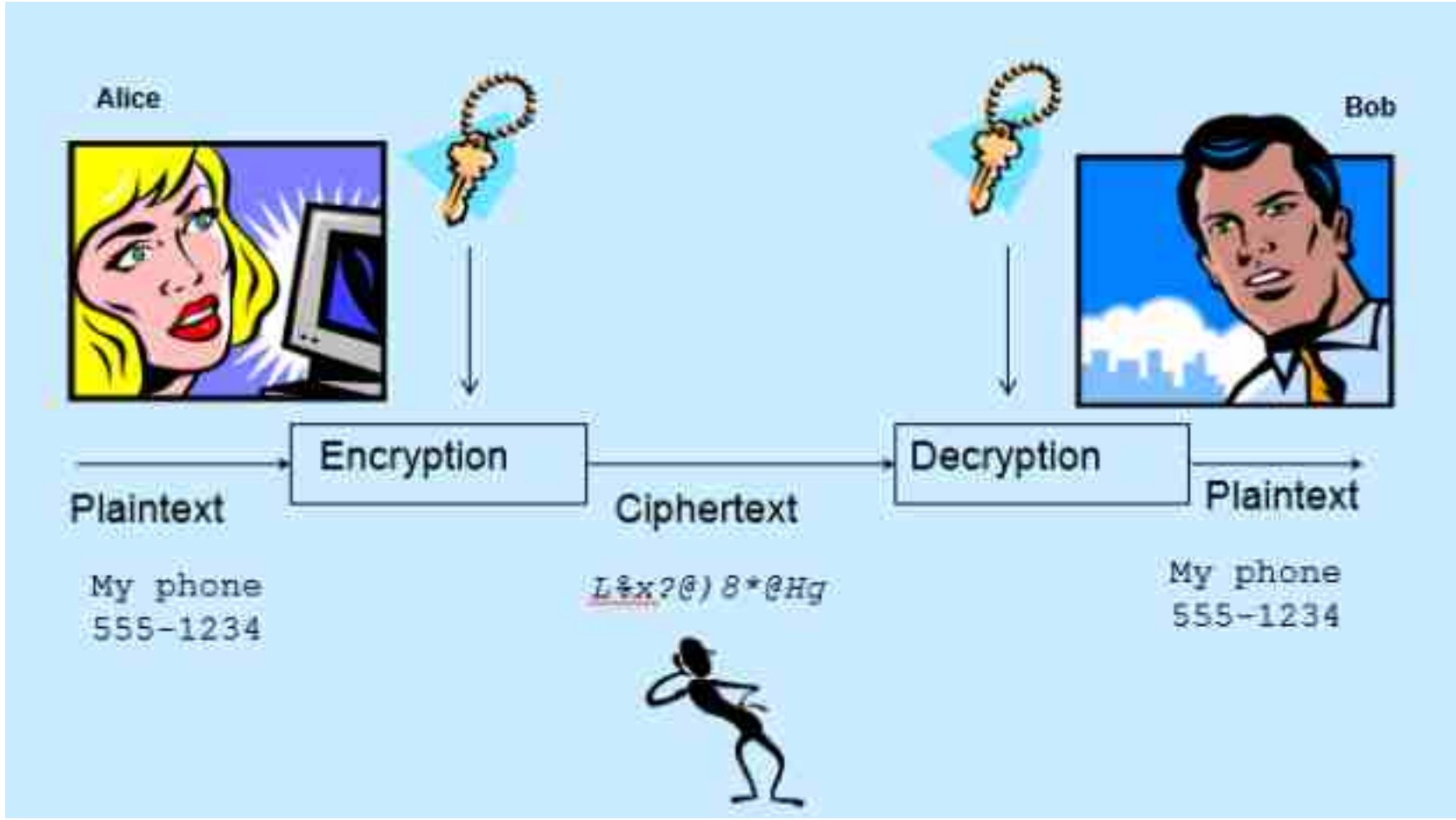
$$E(P) = C$$

Fungsi dekripsi D memetakan C ke P,

$$D(C) = P$$

Fungsi enkripsi dan dekripsi harus memenuhi sifat:

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


Alice
Bob
Encryption
Decryption
Plaintext
Ciphertext
Plaintext
My phone
555-1234
L&x?@)8*@Hg
My phone
555-1234

Dua Aplikasi Utama Enkripsi

- Enkripsi dokumen di dalam storage (*encryption at rest*)

- Enkripsi pesan yang dikirim (*encryption on motion*)

Sumber: https://gadgetren.com/2016/04/06/fitur-enkripsi-end-to-end-di-whatsapp-bikin-percakapan-semakin-aman/

Data Encryption on Motion

- Enkripsi PIN kartu ATM yang ditransmisikan dari mesin ATM ke komputer *server* bank.
- Enkripsi *password* yang diberikan oleh pengguna ke computer *host/server*
- Enkripsi nomor kartu kredit pada transaksi *e-commerce* di internet.
- Enkripsi siaran televisi berbayar (*Pay TV*)
- Enkripsi pesan (teks, audio, video) melalui *Whatsapp*
- Enkripsi percakapan melalui ponsel (di negara-negara tertentu)

Data Encryption at Rest

Enkripsi dokumen (*file*) di dalam *hard disk*, *flashdisk*, CD, DVD, *smartcard*, *cloud storage*.

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}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/{päâ
/psp{pw  ât|□pâ/ztwxsä□p}/|tützp=
```

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/sp	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

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

foreman.avi

Foreman-encrypt.avi

7. *Cipher*

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

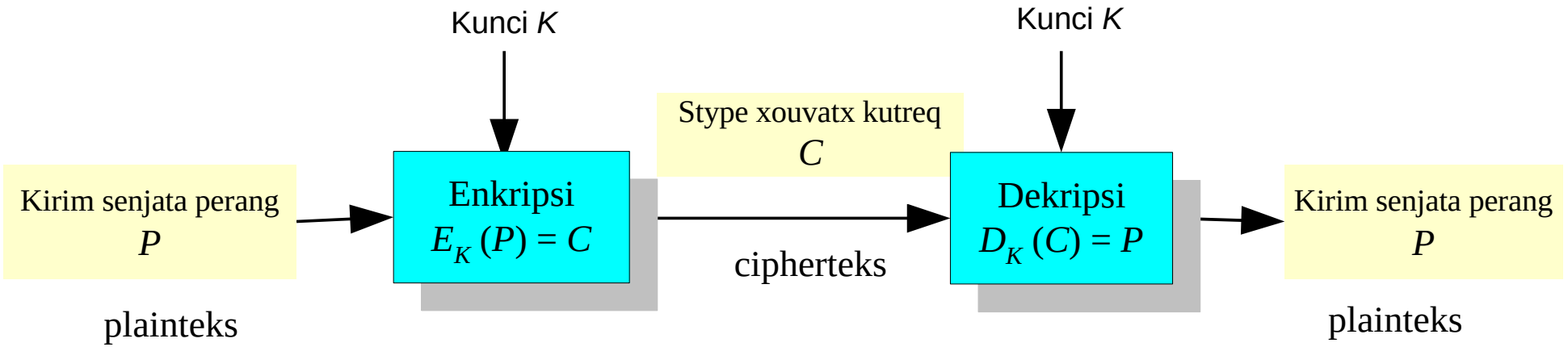
Contoh: Enkripsi: Geser tiga huruf ke kanan
Dekripsi: Geser tiga huruf ke kiri

$E(p) = (p + k) \bmod 26$
$D(c) = (c – k) \bmod 26$

8. **Kunci**: parameter yang digunakan di dalam enkripsi dan dekripsi

- Prinsip Kherkoff: semua algoritma kriptografi harus publik (tidak rahasia), sedangkan kunci harus rahasia.

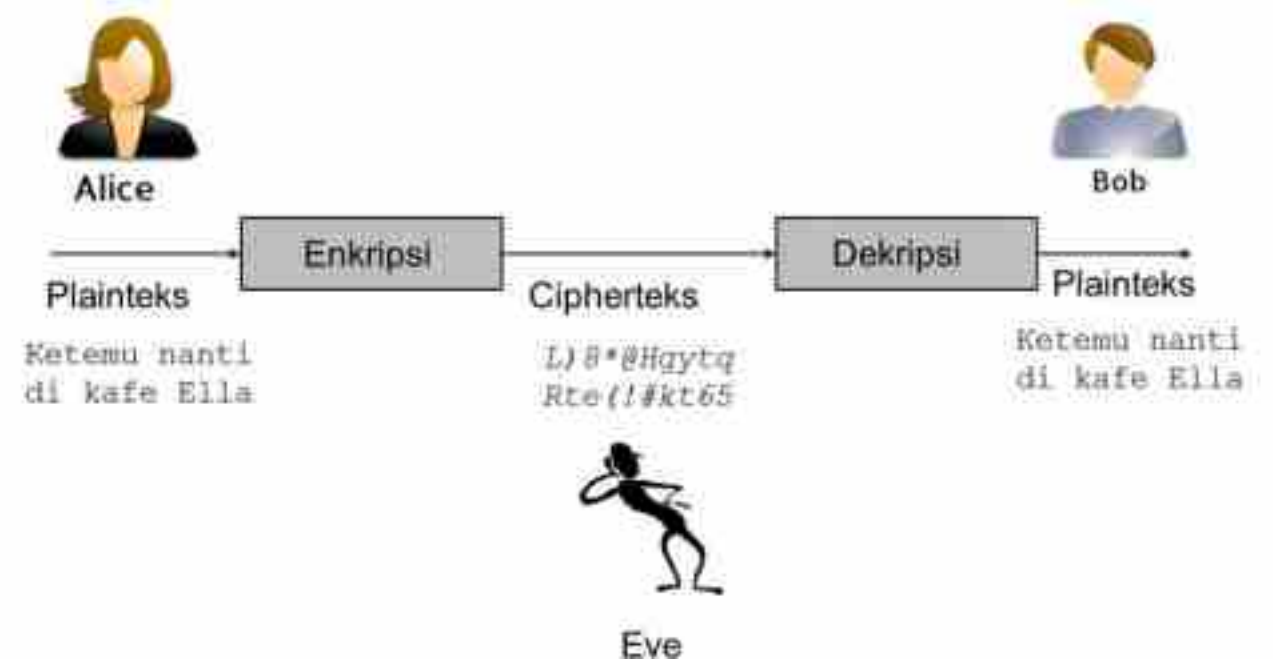
- Enkripsi: $E_K(P) = C$; Dekripsi: $D_K(C) = P$



9. **Penyadap** (*eavesdropper*): orang/mesin 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*"



10. Kriptanalisis (*cryptanalysis*): ilmu dan seni untuk memecahkan chiperteks menjadi plainteks tanpa mengetahui *kunci* yang digunakan.

- Pelakunya disebut **kriptanalis**
- Kriptanalisis merupakan “lawan” kriptografi
- Teknik kriptanalisis sudah ada sejak abad ke-9.

Kriptanalisis 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**.

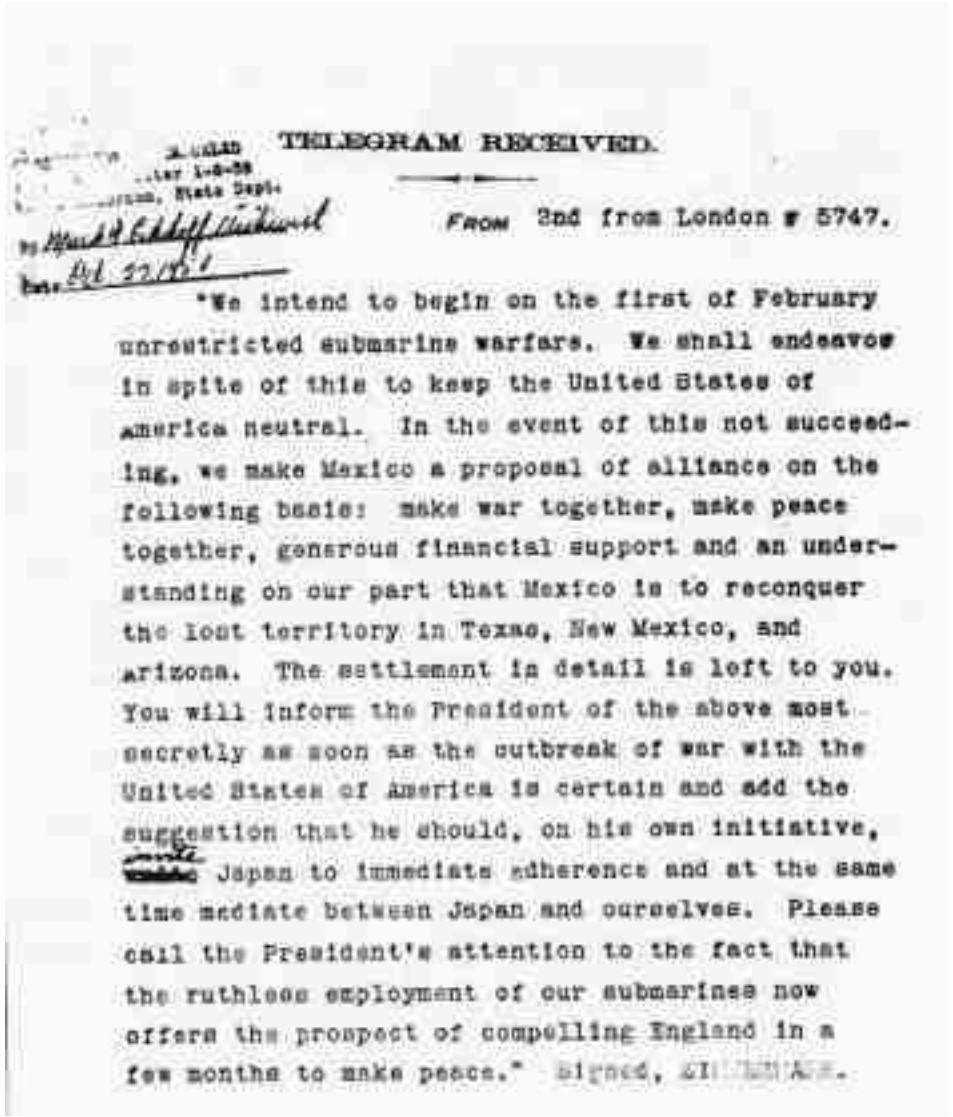
- Al-Kindi menulis buku tentang seni memecahkan kode, buku yang berjudul *'Risalah fi Istikhraj al-Mu'amma* (*Manuscript for the Deciphering Cryptographic Messages*)

- 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

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.



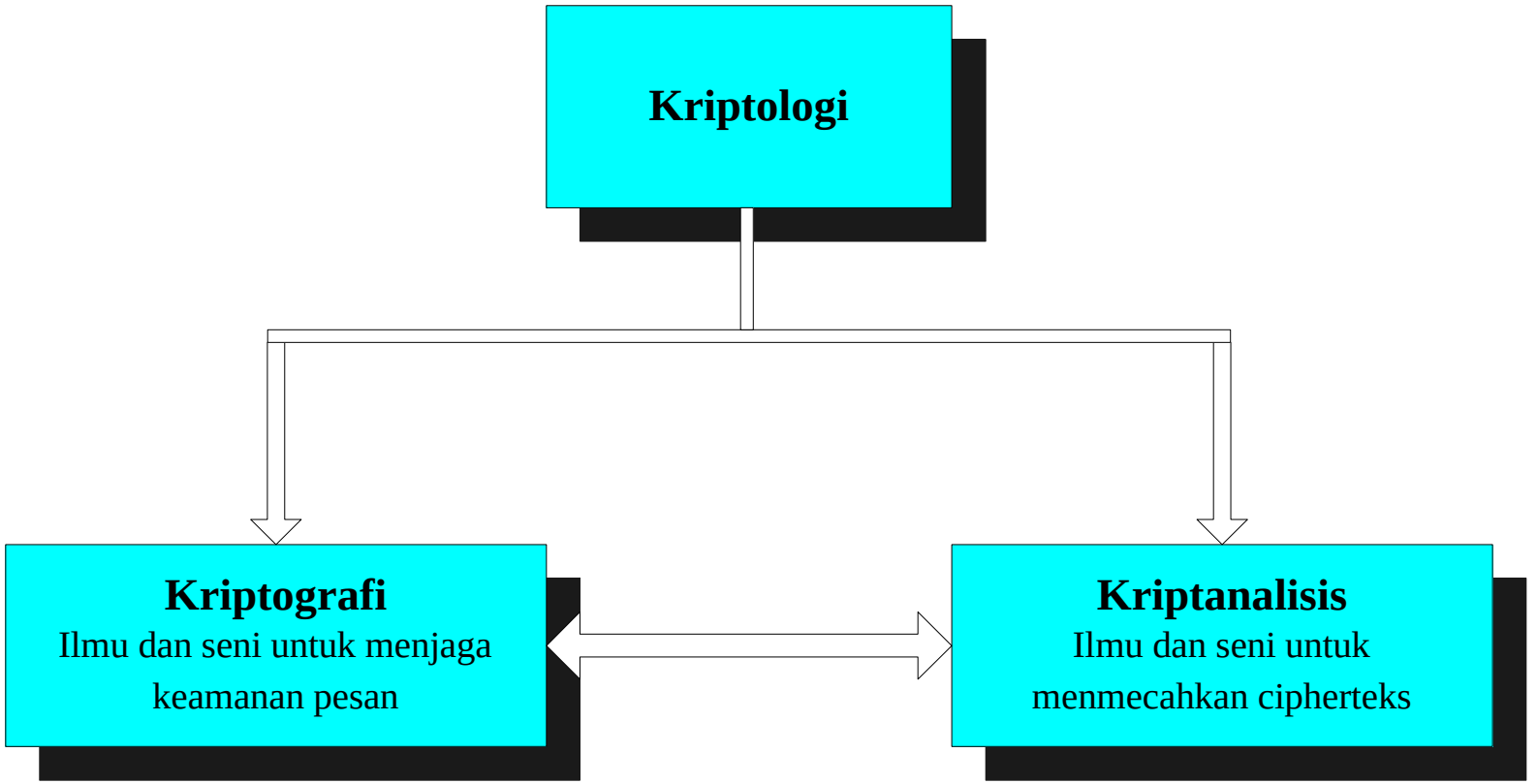
TELEGRAM RECEIVED.

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 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, ZI[illegible].

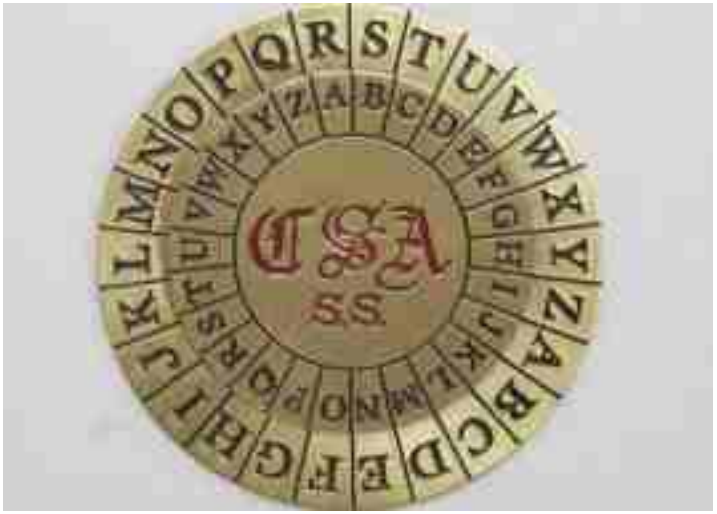
Telegram Zimmerman yang sudah berhasil didekripsi (Sumber: Wikipedia.org)

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



Old Cryptography

- *Ancient cryptography*
- Kriptografi zaman dulu (sebelum Masehi - sebelum komputer digital)
- Hanya mengenkripsi huruf dan angka, menggunakan kertas dan pena



- Caesar cipher
- Vigenere cipher
- Playfair cipher
- Hill cipher
- Enigma cipher
- dll

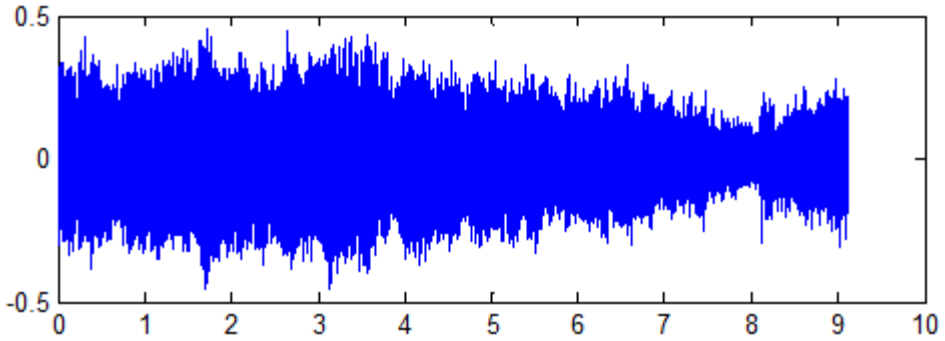
Modern Cryptography

- Enkripsi dan dekripsi pesan dalam bentuk digital

1. Teks

A Quick Brown Fox Jumps Over The Lazy Dog 0123456789
A Quick Brown Fox Jumps Over The Lazy Dog 0123456789
A Quick Brown Fox Jumps Over The Lazy Dog 0123456789
A Quick Brown Fox Jumps Over The Lazy Dog 0123456789
A Quick Brown Fox Jumps Over The Lazy Dog 0123456789
A Quick Brown Fox Jumps Over The Lazy Dog 0123456789
A Quick Brown Fox Jumps Over The Lazy Dog 0123456789
A Quick Brown Fox Jumps Over The Lazy Dog 0123456789
A Quick Brown Fox Jumps Over The Lazy Dog 0123456789
A Quick Brown Fox Jumps Over The Lazy Dog 0123456789
A Quick Brown Fox Jumps Over The Lazy Dog 0123456789

2. Audio



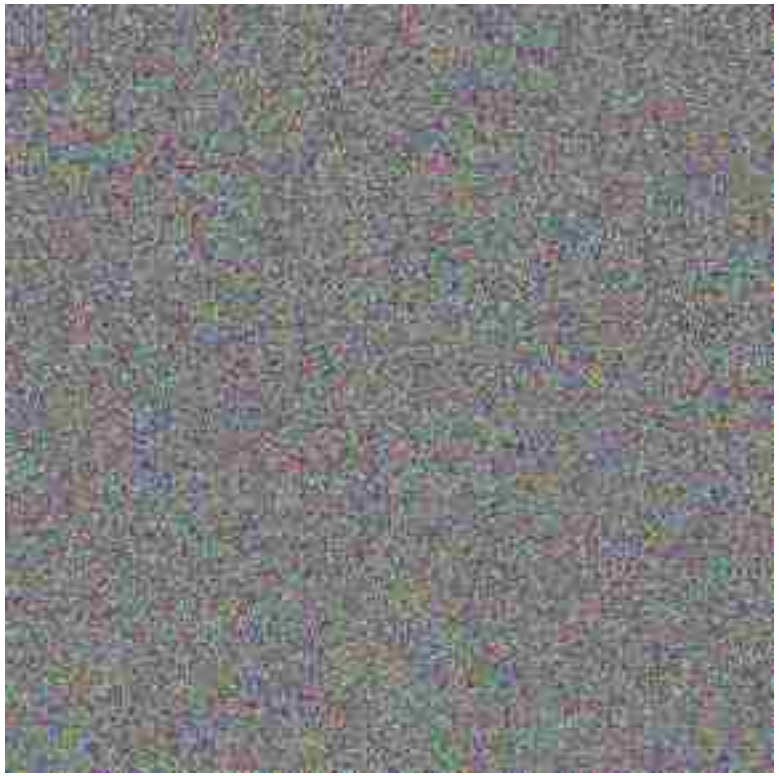
3. Gambar (*image*)

4. Video

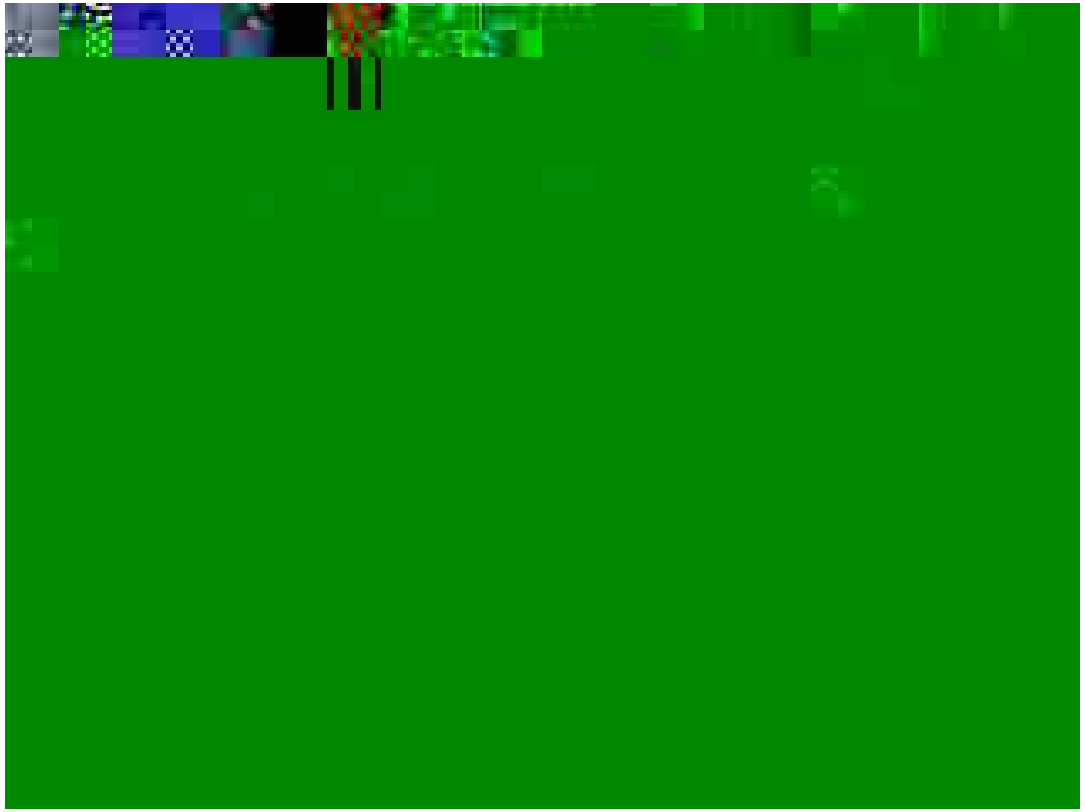
1. Text Encryption

wisuda.txt	cipher.txt
Pada wisuda sarjana baru, ternyata ada seorang wisudawan yang paling muda. Umurnya baru 21 tahun. Ini berarti dia masuk ITB pada umur 17 tahun. Zaman sekarang banyak sarjana masih berusia muda belia. Mungkin masuk sekolah pada usia dini dan mengikuti kelas akselerasi pada tingkatan SD, SMP, dan SMA.	7 □S□□□□S□ □□H□□□□IS□□□□□□□ A□□□E □ □S□□□ □□ □G□□ □H□□ □H□□□KSek2□□□□ G□□□□HSVA□□□□□IA' □H□□□□□□A□□□E- □□N,'*A□ □S□□□NTDH□□ □]H1m;□□□□A□□□□□ □ A□□□ A□□□□ N□□□□□A □□□ N□□ G□ □ OG,□ □□□ A□□ □ jk□ □□ □ N□□ G□□□H□□□E□ □G □□ □□□E□ □□N□□□□ □□□ □A□ □S□□ □□□ □G2*I~b2*1BE□ □G2#$]—

2. Image encryption



3. Video encryption



Sejarah Kriptografi

Kriptografi pada zaman Mesir Kuno

- Bangsa Mesir 4000 tahun yang lalu menggunakan *hieroglyph* yang tidak standard untuk menulis pesan di dinding piramid.

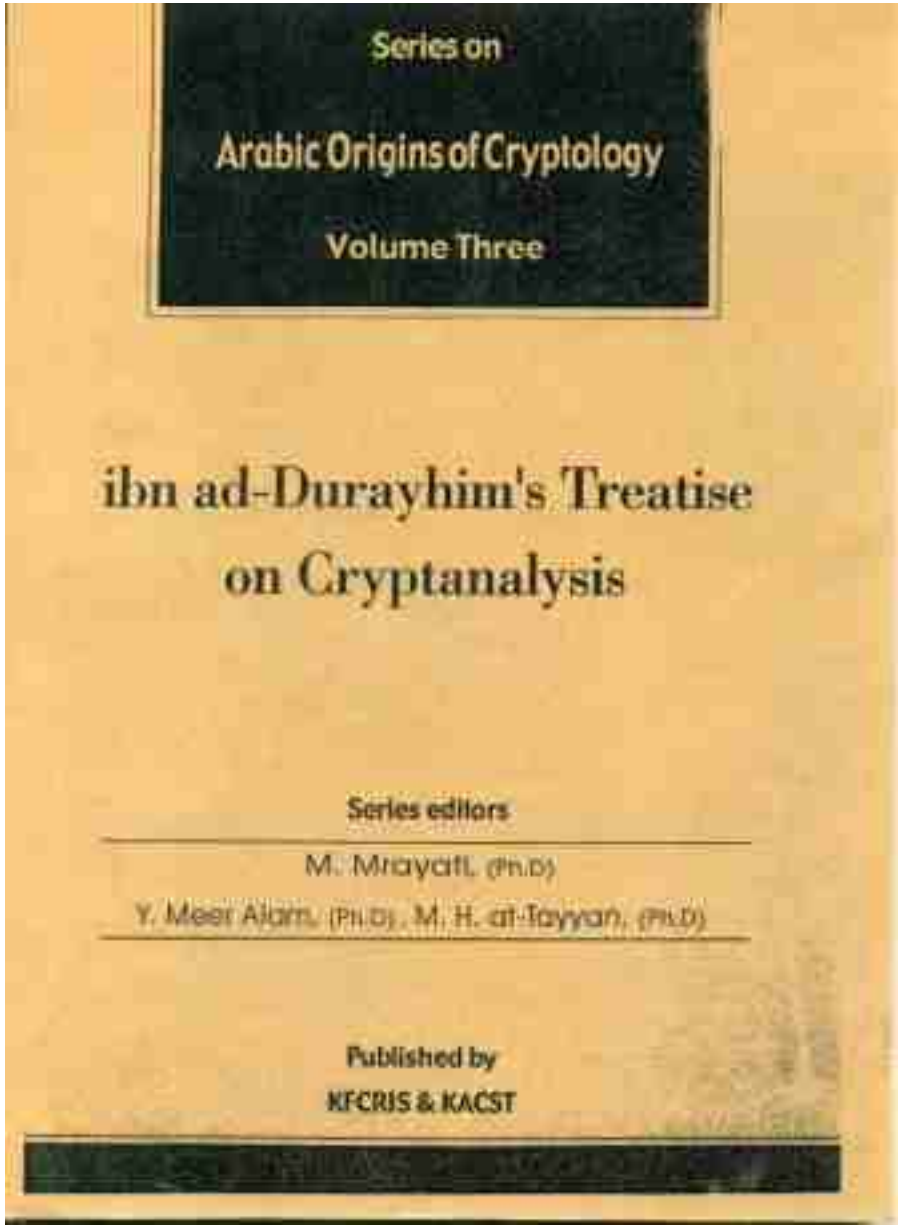
Kriptografi pada Zaman Yunani dan Romawi Kuno

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

Plainteks: KILLKINGTOMORROWMIDNIGHT
Ciphrteks: KIMWIINOMGLGRIHLTRDTKOON

Kriptografi pada Bangsa Arab

Sejarah kriptologi 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.



Ibn ad-Durayhim bernama lengkap Ali ibn Muhammad ibn Abd al Aziz, Tag ad-Din. Dia lahir di Mosul, Irak, pada bulan Sya'ban tahun 712 H atau 1312 M. Dia sering berdagang antara Kairo dan Damaskus dan ditunjuk sebagai guru di Masjid Umayah Damaskus. Dia pindah ke Mesir tahun 760 H/1359 M dan dikirim oleh Sultan sebagai duta kepada raja Abyssinia (sekarang Etiopia).

Menurut ad-Durayhim, jenis-jenis *cipher* dapat dikelompokkan ke dalam delapan tipe:
(1) transposisi,
(2) substitusi,
(3) penambahan atau reduksi jumlah huruf,
(4) penggunaan piranti sandi,
(5) penggantian huruf dengan angka yang diboboti secara desimal,
(6) penyandian huruf dengan menggunakan kata-kata,
(7) penggantian huruf dengan nama generik,
(8) menggunakan simbol atau tanda untuk menyatakan huruf.

Cryptology was born among Arabs. They were the first to discover and write down the methods of cryptanalysys.
(David Kahn – Penulis buku: The Code Breaker)

Kriptografi pada zaman India Kuno

- 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*.

- Di dalam buku tersebut, Vātsyāyana, penulis Kama Sutra, merekomendasikan kepada para wanita untuk mempelajari seni memahami tulisan menggunakan *cipher*. Ada dua macam *cipher*, yang pertama bernama *Kautiliyam* and kedua *Mulavediy.*

Kriptografi pada Zaman Renaisans di Eropa

- Zaman renaisans → abad pertengahan (abad 15-16)
- *Cipher* terkenal pada abad pertengahan:

  1. *Vigenere Cipher*

     Dipublikasikan oleh diplomat Perancis bernama Blaise de Vigenere pada tahun 1586.

  2. *Playfair Cipher*

     Dipromosikan oleh diplomat Inggris, Lord Playfair, meskipun penemu aslinya adalah Charles Wheastone pada tahun 1854.

- 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

Kriptografi pada Perang Dunia II

- Perang Dunia ke II, Pemerintah Nazi Jerman membuat mesin enkripsi yang dinamakan *Enigma*.

- *Enigma cipher* berhasil dipecahkan oleh pihak Sekutu.

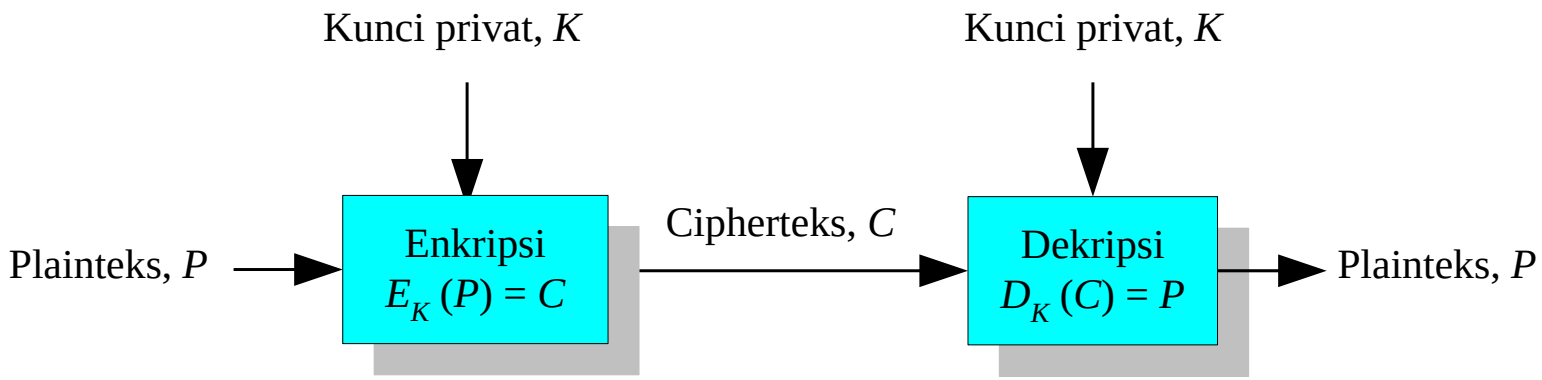
- Keberhasilan memecahkan *Enigma* sering dikatakan sebagai faktor yang memperpendek perang dunia ke-2

Enigma

Algoritma Kriptografi

1. Algoritma kriptografi simetri (*symmetric-key cryptography*)

- Kunci enkripsi = kunci dekripsi



- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)
- Serpent
- Blowfish
- Loki

- MARS
- RC6
- Twofish
- 3-DES
- IDEA

- FEAL
- RC4
- SEAL
- Panama
- dll

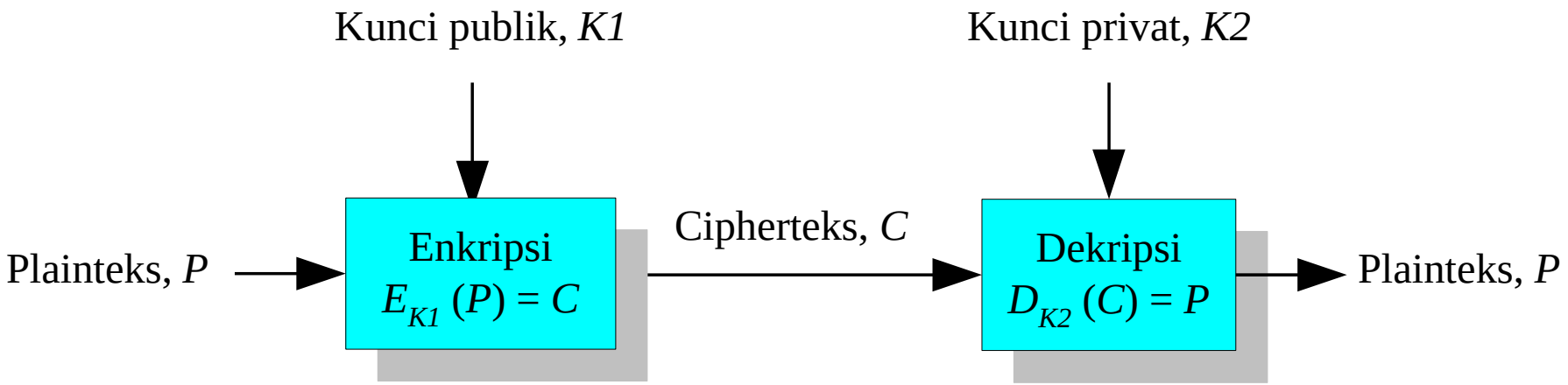
2. Algoritma kriptografi nir-simetri (*asymmetric-key cryptography*)

- Kunci enkripsi ≠ kunci dekripsi

  Kunci enkripsi → tidak rahasia (*public key*)

  Kunci dekripsi → rahasia (*private key*)

Nama lain: **Kriptografi kunci –publik** (*public-key cryptography*)

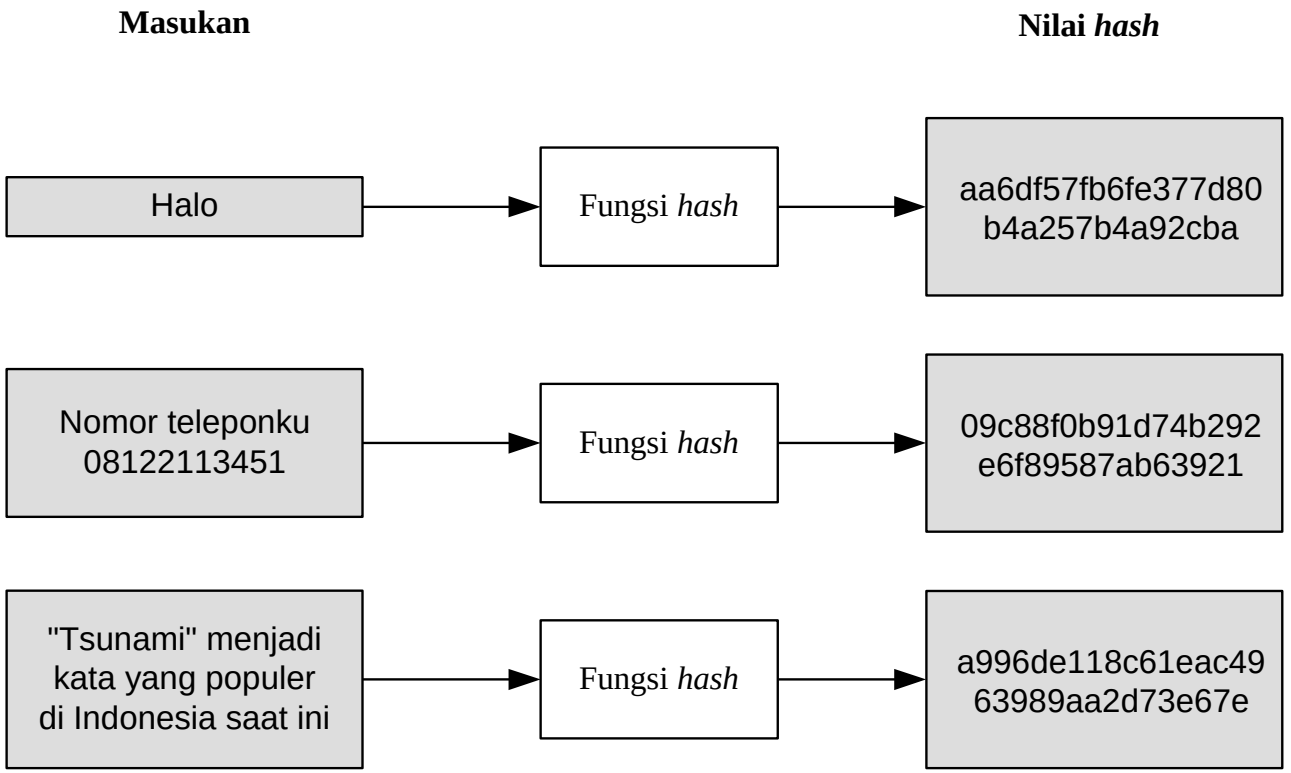


- RSA (Rivest-Shamir-Adleman)
- ElGamal
- DSA
- Diffie-Hellman
- Mercke Knapsack Algorithm

- Rabin
- EPOC
- Mc Eliece
- XTR
- ECC (*Elliptic Curve Cryptography*)

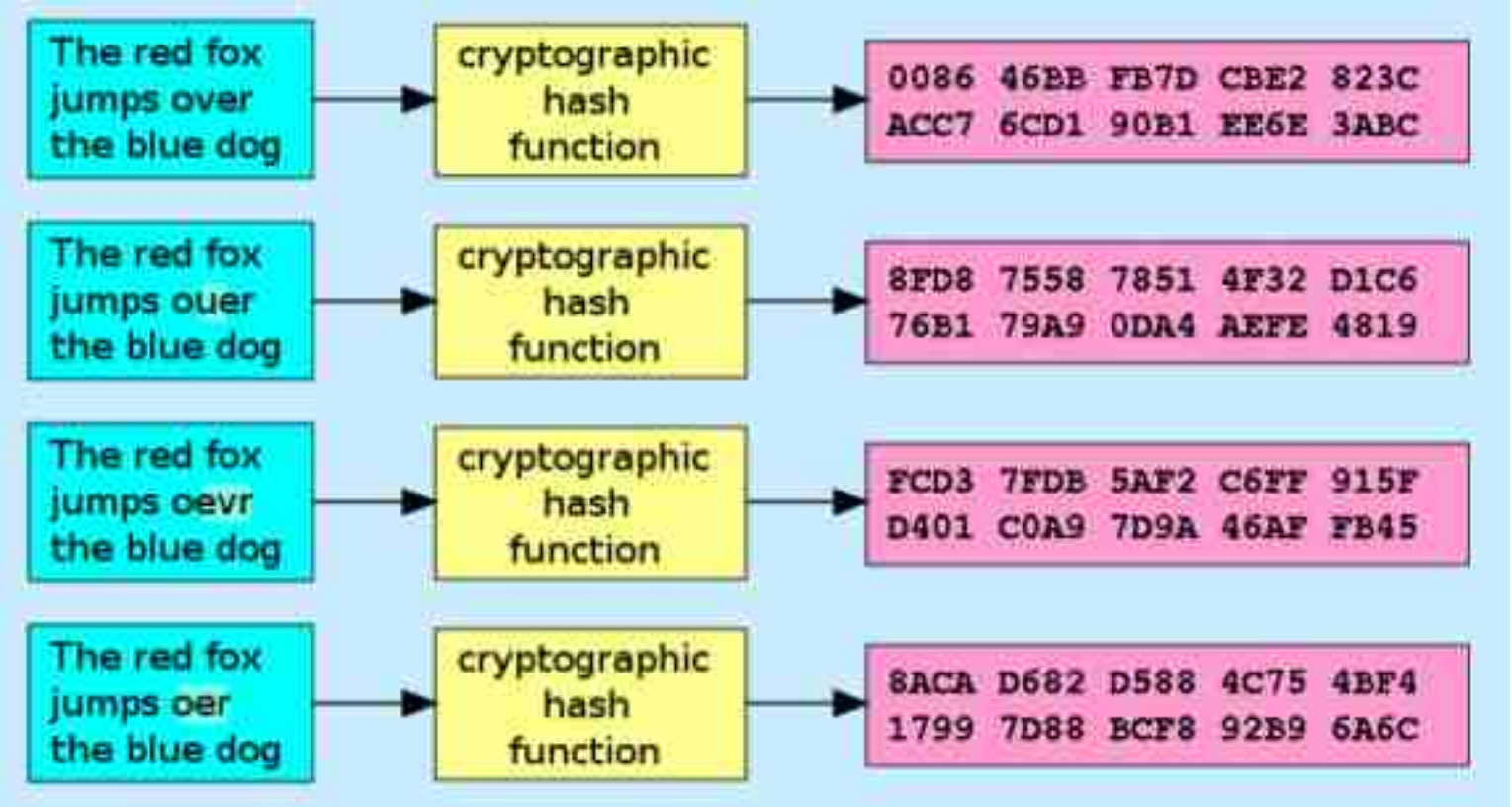
3. Fungsi Hash

- Mengkompresi pesan ukuran sembarang menjadi *message-digest* berukuran *fixed*.
- *Irreversible* (tidak bisa dikembalikan menjadi pesan semula)



- MD5
- SHA-1
- SHA-2
- Keccak (SHA-3)
- RIPEMD
- WHIRLPOOL

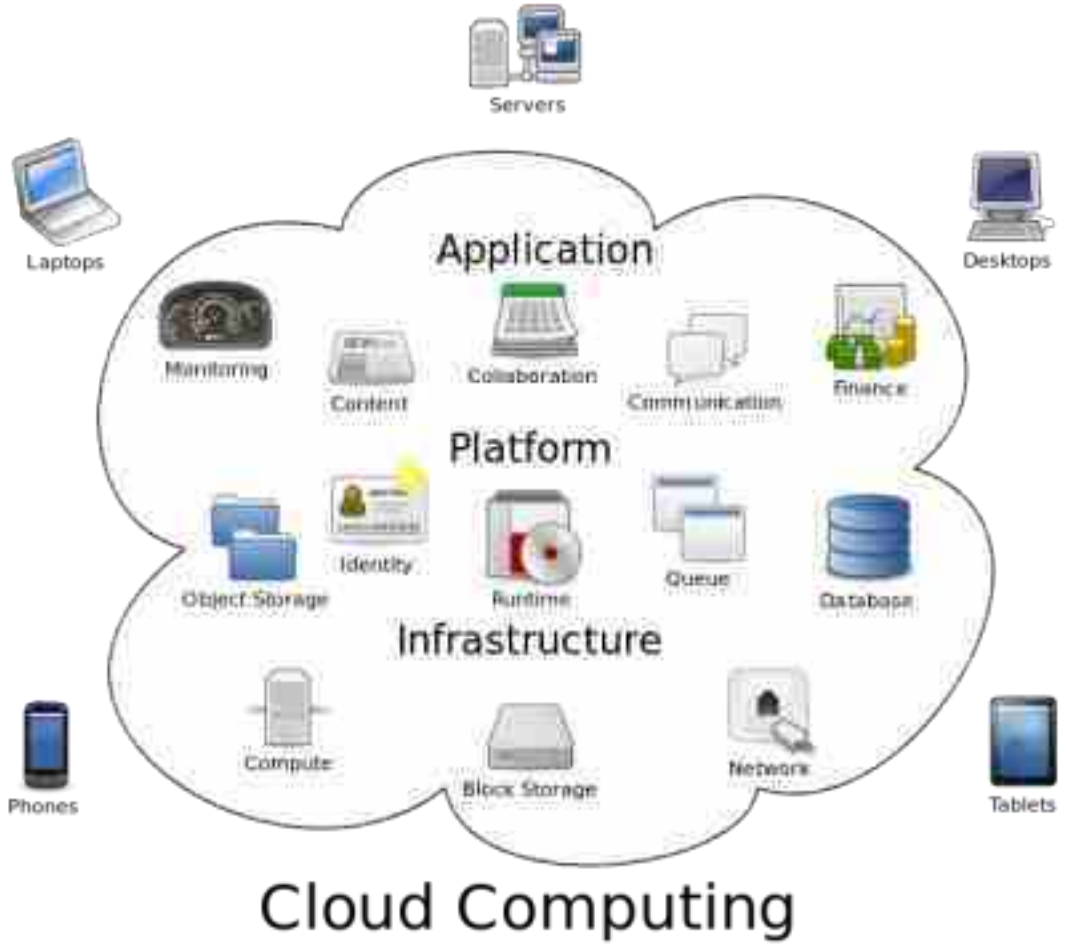
Kegunaan: memeriksa integritas pesan



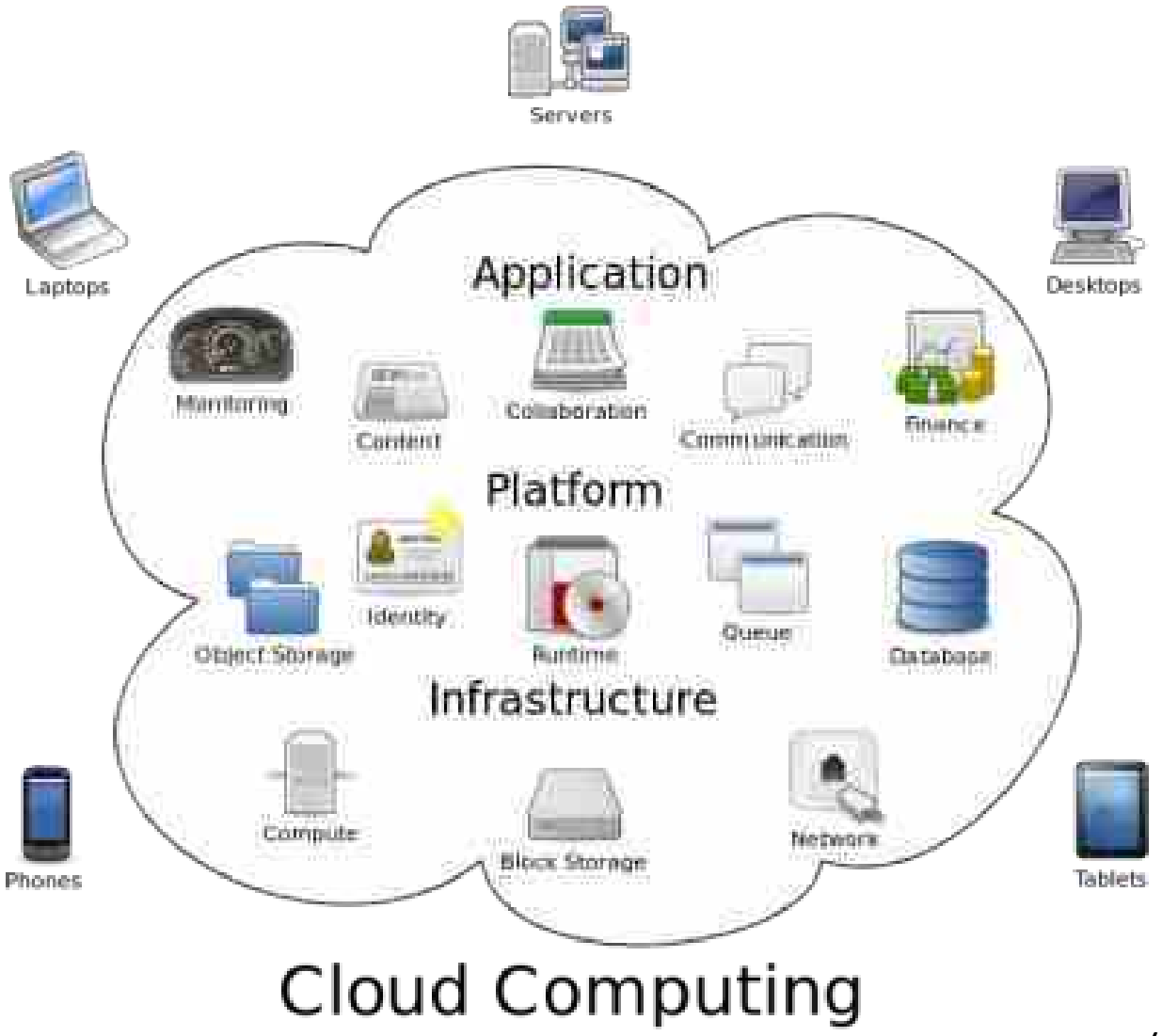
(Sumber gambar: Wikipedia)

Cloud Cryptography

- *Cloud computing* (komputasi awan): gabungan pemanfaatan teknologi komputer ('komputasi') dan pengembangan berbasis Internet ('awan').



(Sumber gambar: Wikipedia)



(Sumber gambar: Wikipedia)

Cloud Computing versus *Cryptography:*

- *cloud computing* menghadirkan tantangan keamanan sebab provider *cloud* tidak bisa sepenuhnya dipercaya (dapat memanipulasi data *client*).
- Riset-riset dalam *cloud cryptography* fokus pada primitif2 dan protokol kriptografi yang mencoba menyeimbangkan antara kemanan, efisiensi, dan fungsionalitas.
- Contoh judul riset*: cryptography cloud storage*

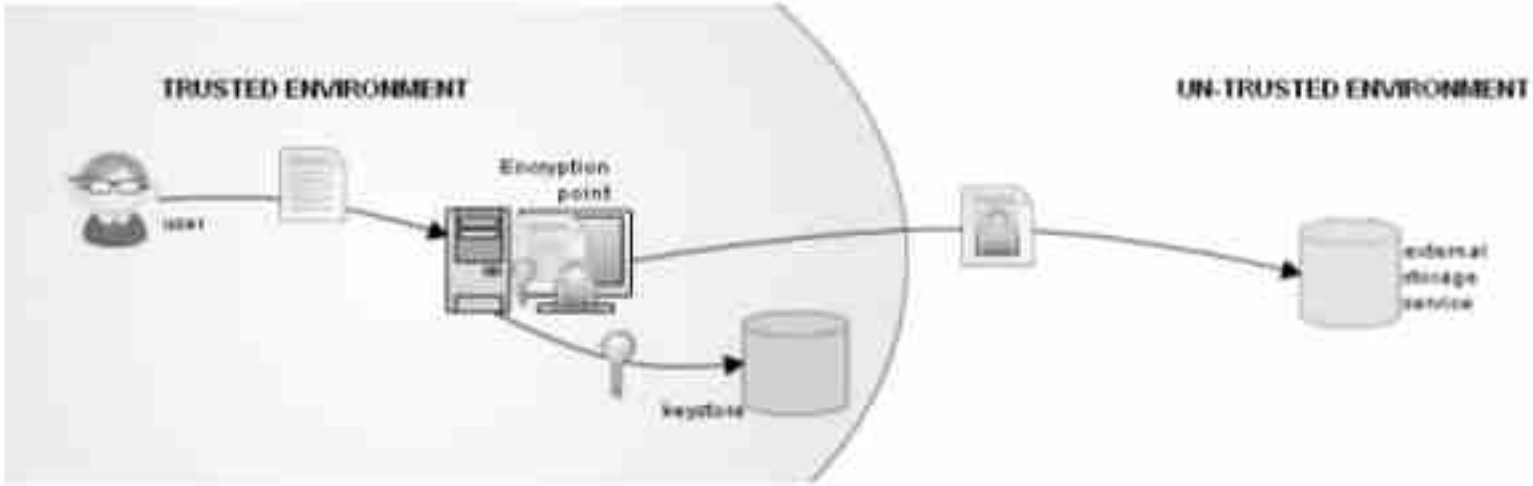
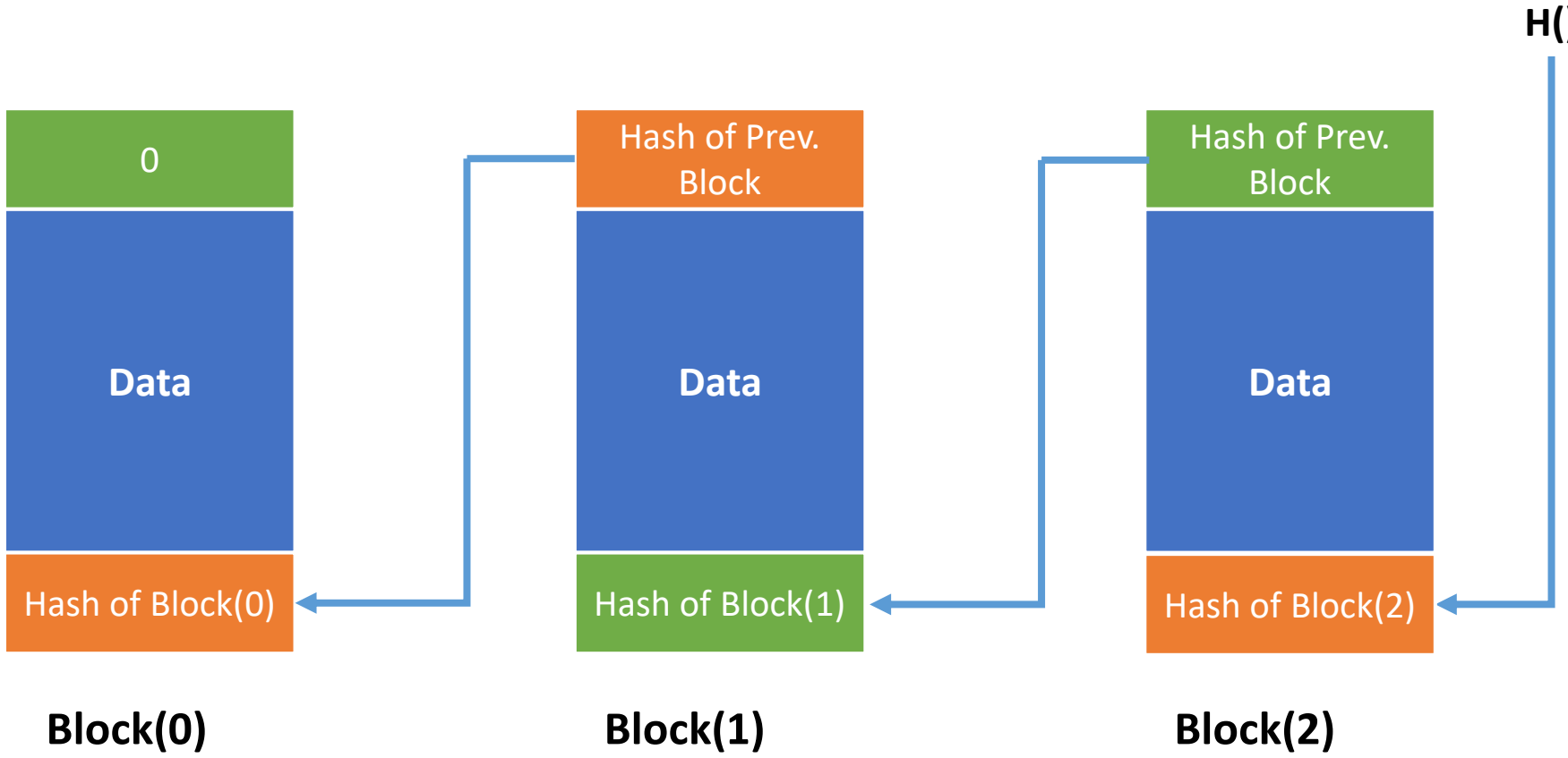


Fig. 1. Basic architecture of a secure storage system

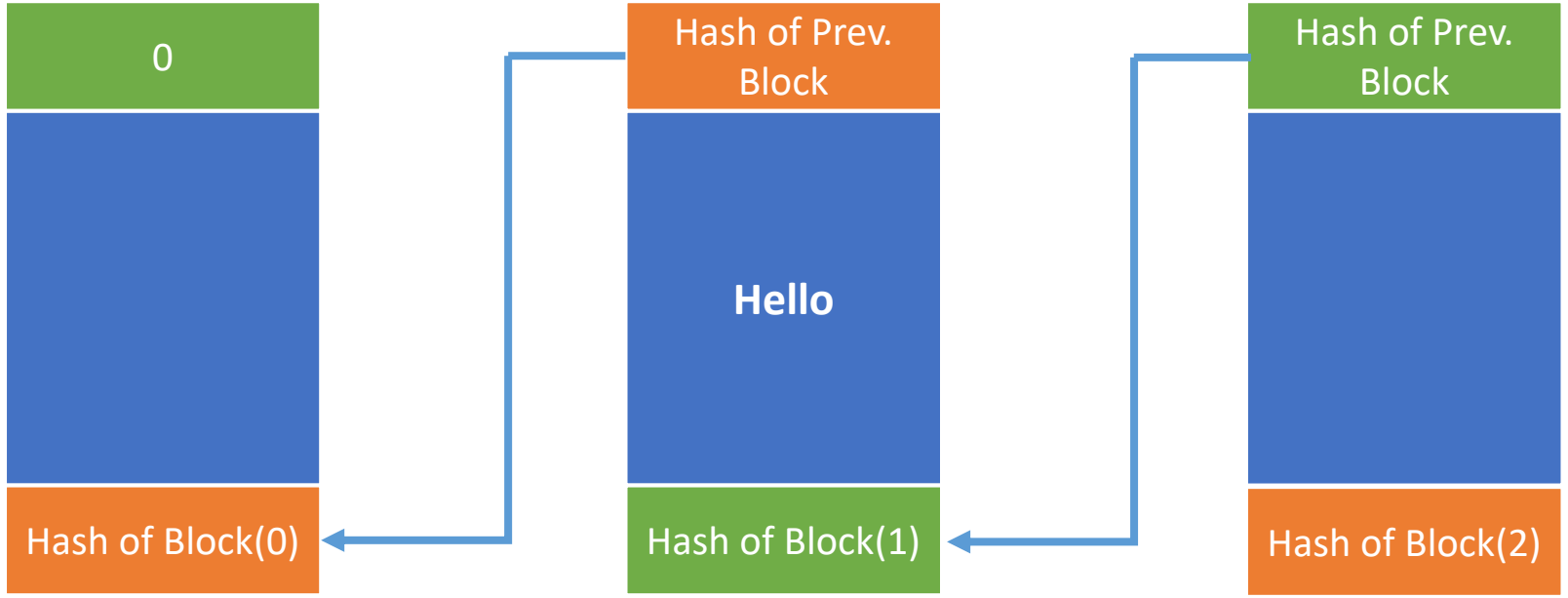
Blockchain *)

- Mengaitkan blok-blok data menggunakan *hash pointer*

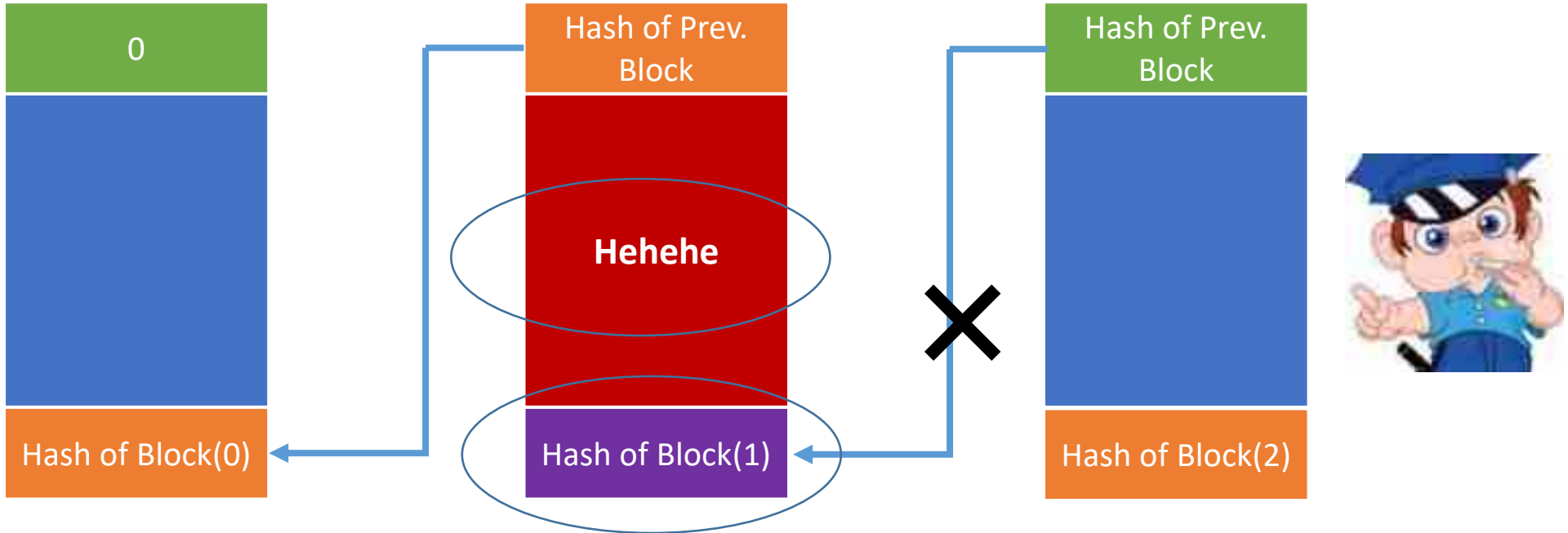


Sumber: I Gusti Bagus Baskara Nugraha, *Blockchain at Glance*, STEI ITB, 2018

Sumber: I Gusti Bagus Baskara Nugraha, *Blockchain at Glance*, STEI ITB, 2018



Someone **tampered** data in Block(1)



Lembaga Terkait Kriptografi di Indonesia

1. Badan Siber dan Sandi Negara (BSSN)

   http://bssn.go.id

   Merupakan penggabungan Lembaga Sandi Negara (Lemsaneg) dan Direktorat Jenderal Aplikasi Informatika (Aptika), Kementerian Komunikasi dan Informatika

2. Sekolah Tinggi Sandi Negara (STSN)

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

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

Alamat Jl. Faridan Muridan Noto No. 21, Kota Baru, Yogyakarta. Ini museum san satu-satunya di Indonesia, bahkan di dunia. Di dalamnya terdapat berbagai koleksi alat sandi yang pernah digunakan di Indonesia

Mesin sandi di Museum Sandi Yogyakarta