

01 - Pengantar Kriptografi



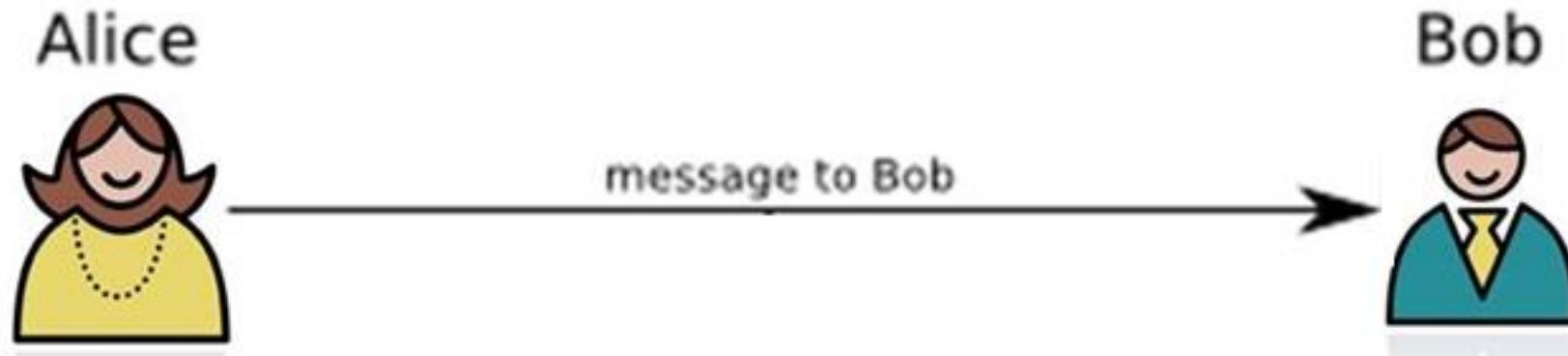
Oleh: Rinaldi Munir

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika ITB
2025



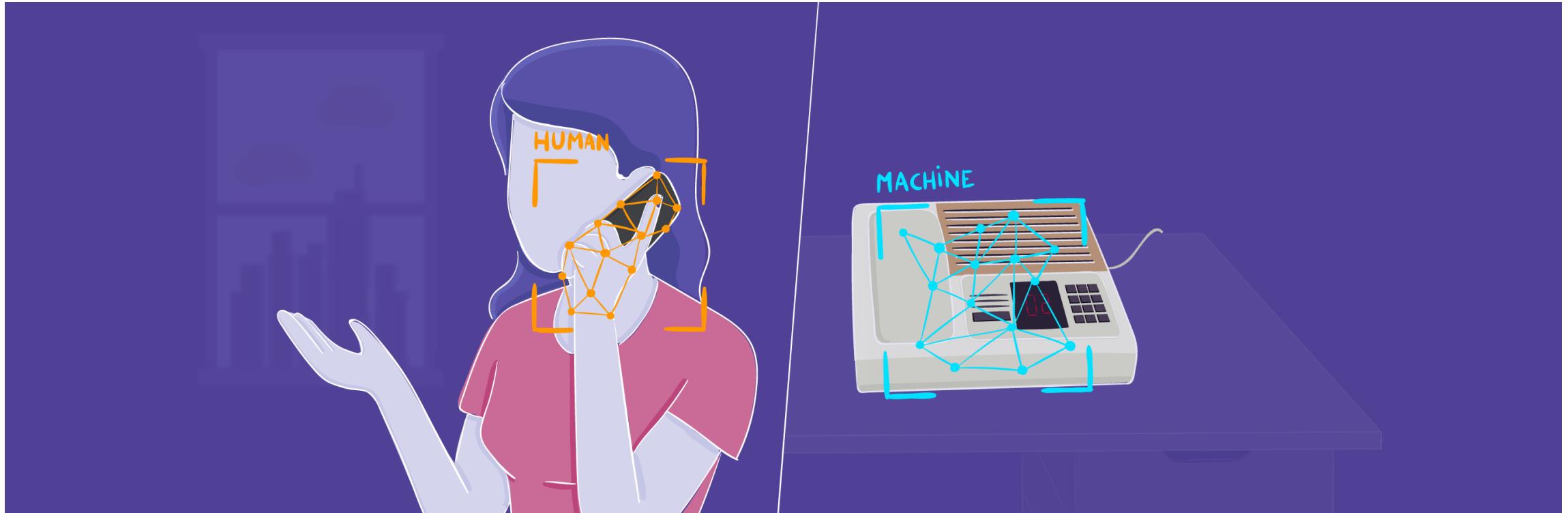
- Misalkan Alice dan Bob saling berkomunikasi dengan berkirim pesan:
 - via surat menyurat,
 - via telepon
 - via email
 - via SMS
 - dll

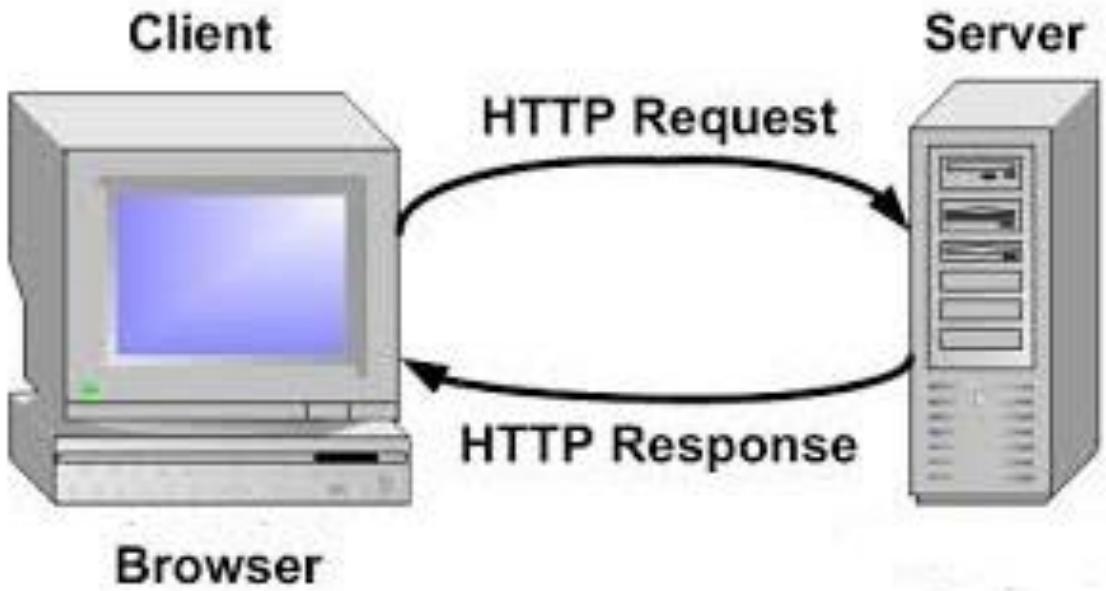
menggunakan saluran komunikasi publik (pos, telepon, jaringan seluler, internet)



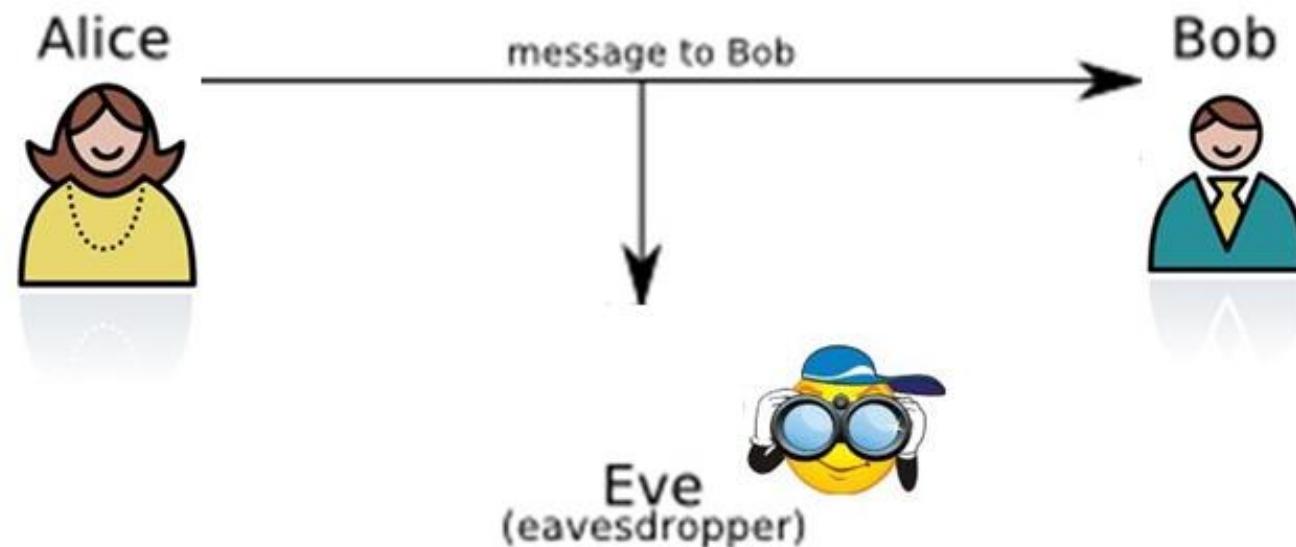
- FYI, Alice dan Bob di dalam dunia nyata bisa berupa
 - Alice dan Bob adalah manusia dalam arti sesungguhnya
 - manusia dengan mesin (misalnya mesin penjawab telepon)
 - mesin dengan mesin (misalnya komputer *client* dengan komputer *server*)
 - web browser dengan sistem server di dalam jaringan komputer
 - online banking client/server
 - DNS server, router, mesin penjawab telepon, dsb





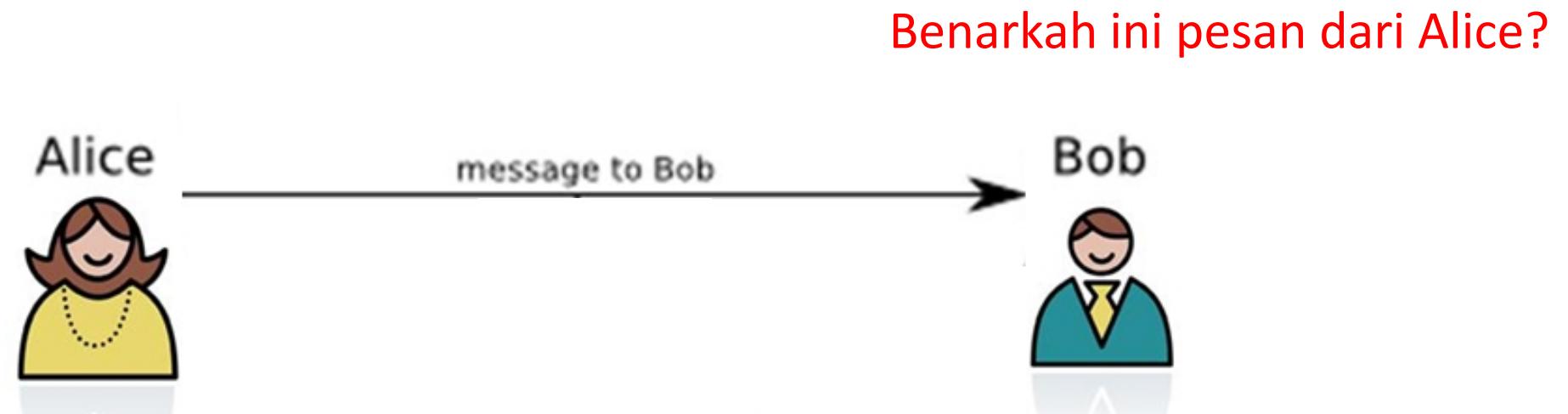


- **Case 1:** Bagaimana Alice memastikan pesan-pesannya tidak dapat dibaca oleh penyadap (*eavesdropper*) yang menguping komunikasinya dengan Bob?



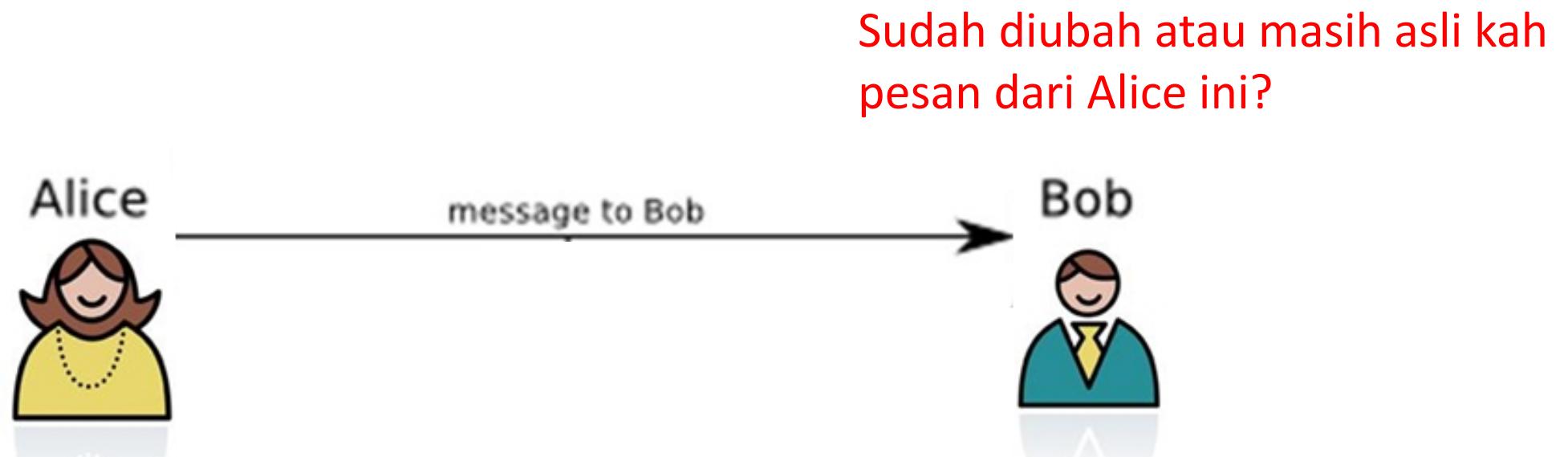
→ masalah kerahasiaan pesan (*confidentiality*)

- **Case 2:** Bagaimana cara Bob memastikan bahwa pesan tersebut dari Alice dan bukan dari Carol (yang menyamar menjadi Alice)?



→ masalah otentikasi (*authentication*) pengirim atau penerima pesan

- **Case 3:** Bagaimana cara Bob memastikan bahwa pesan dari Alice masih utuh, asli, tidak diubah, atau dimanipulasi selama komunikasi,



→ masalah keutuhan (*integrity*) pesan?

- **Case 4:** Bagaimana Bob melakukan anti-sangkalan apabila Alice menyangkal telah mengirim pesan kepada Bob?

*Swer, saya nggak pernah
kirim pesan ini kepadamu,
Bob!*

Hmmmm....



→ masalah nir-penyangkalan (*non-repudiation*)

- Keempat masalah tersebut:

- *confidentiality*,
 - *authentication*,
 - *data integrity*,
 - *non-repudiation*

solusinya adalah menggunakan KRIPTOGRAFI

Kriptografi

- Kata *cryptography* berasal dari bahasa Yunani:

cryptós (*secret or hidden*)

gráphein (*writing*)

Artinya “*secret writing* or “*hidden writing*”

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



Definisi lainnya:

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

Ztaxzp/épép/qtüyp{p}<yp{p}/sx/Øp)
âpx;pêp/|t}t|äzp}/qp}êpz/étzp{x/z
tØxâx}vØØép}v/|tüp}vzpz/|t}äyä/{p
ää=/\tützpØØpsp{pw/p}pz<p}pz/ztØx
âx}v/êp}v/qpuäØØ|t}tâpé/spüx/sp{p
|/Øpéxü=/]p{äüxØØ|ttüzp/|t}vpâpzp
}/qpwäp/{pää/psp{pwØØåt|Øpå/ztwxs
äØp)/|tützp=

(b) Cipherteks dari (a)

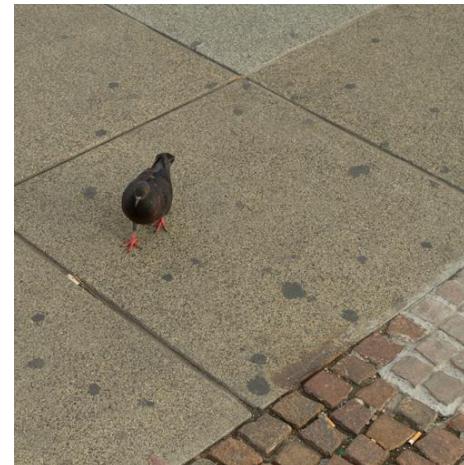
2. Terjaga keasliannya (*data integrity*)

Suhu di luar 33
derajat celcius

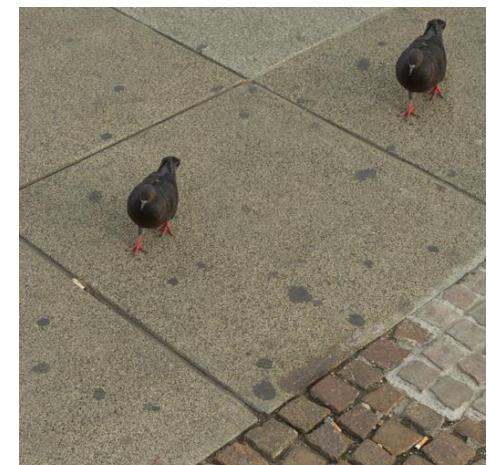
Pesan asli

Suhu di luar 32
derajat celcius

Pesan sudah diubah

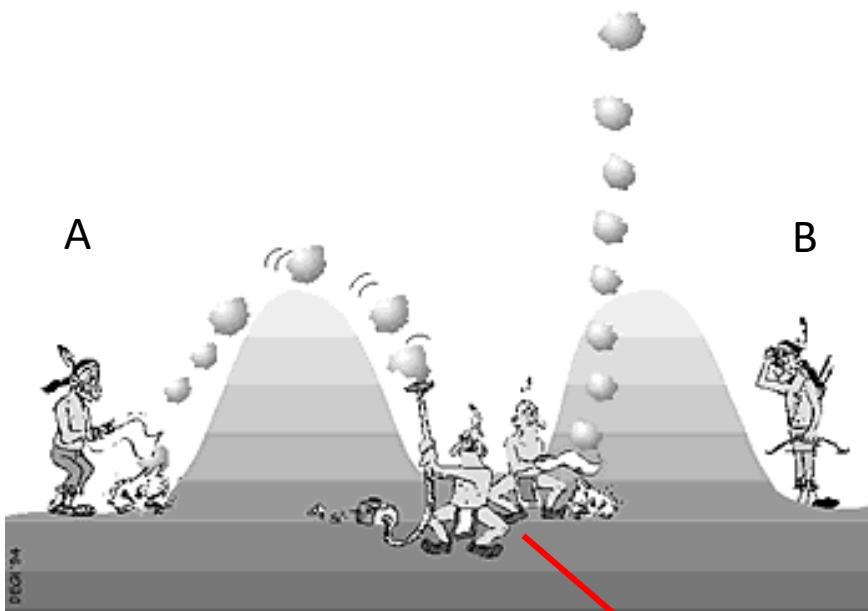


Pesan asli



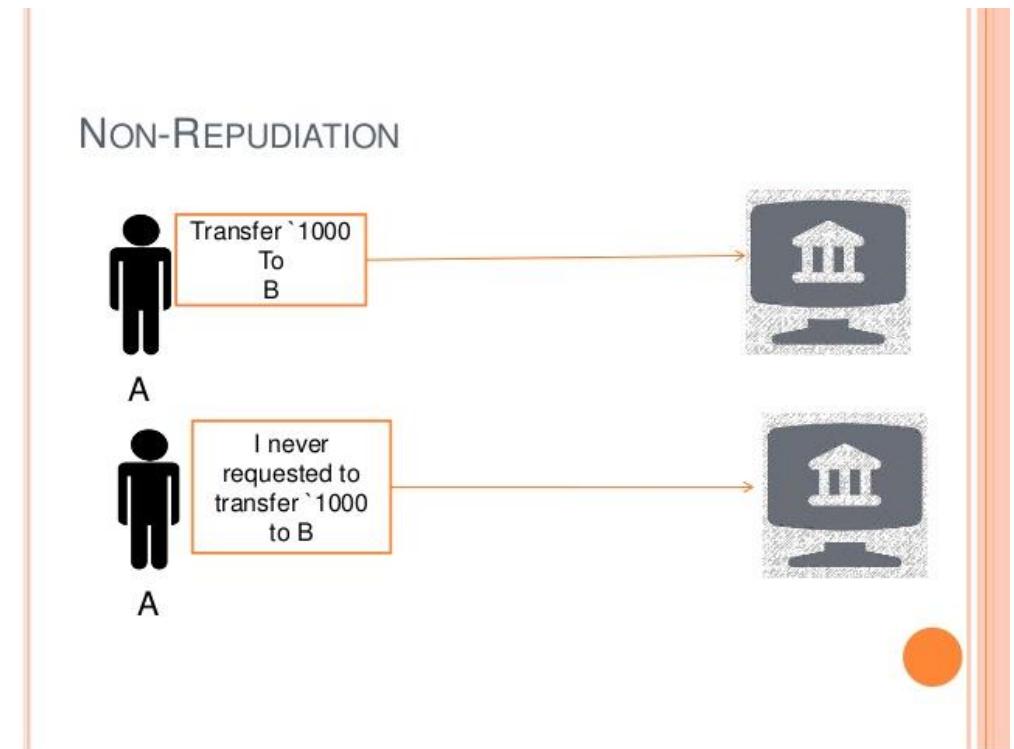
Pesan sudah diubah

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



Dia mengklaim bahwa dia adalah *A*

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



Empat 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*)

“Cryptography lies at the heart of all cybersecurity technologies, and understanding the role it plays is vital to understanding how to secure cyberspace” (Keith M. Martin)

Kriptografer masih menjadi sosok yang langka di Indonesia.
Namun, bidang ini sangat penting untuk segera ditumbuhkan

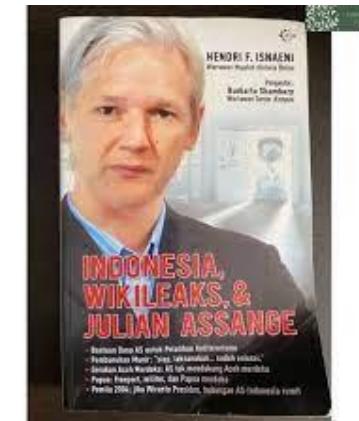
Masih ingat dengan kasus-kasus ini?

- **Wikileaks**

- pembocoran dokumen Perang Afghanistan (Juli, 2010)
- Pembocoran 400.000 dokumen Perang Irak (Oktober 2010)
- Pembocoran kawat diplomatik Amerika Serikat (November 2010)
- dll



Julian Assange, salah satu pendiri situs WikiLeaks.



- Penyadapan di Kedubes RI di luar negeri

detiknews Home Berita Jabodetabek Internasional Hukum detikX Kolom Blak Blaka

detikNews > Berita

Menlu: Penyadapan KBRI di Myanmar Langgar Konvensi Wina

- detikNews

Rabu, 14 Jul 2004 14:47 WIB

Banten - Menteri Luar Negeri Hasan Wirajuda menyesalkan terjadinya indikasi penyadapan kantor Kedutaan Besar RI di Yangon. Penyadapan dinilai melanggar konvensi Wina. Kedubes Myanmar hingga kini masih berkelit."Ada indikasi kuat mengarah kesana. Itu berdasarkan temuan tim dan hasil pemeriksaan. Atas peristiwa ini, kita sampaikan keprihatinan yang mendalam dan keras bahwa ini terjadi antar sesama anggota ASEAN dan jelas melanggar konvensi Wina. Dalam konvensi itu dilarang mengganggu fasilitas kedutaan karena itu menyangkut masalah kerahasiaan". Hal ini disampaikan Menteri Luar Negeri Hasan Wirajuda usai mendampingi Presiden Megawati Soekarnoputri pada peringatan Dasawarsa Komprensi Internasional Kependudukan dan Pembangunan di Kabupaten Pandeglang, Provinsi Banten, Rabu (14/7/2004). Menurut



- Penyadapan telepon Presiden SBY oleh Pemerintah Australia



Jakarta, Setkab -Pemerintah Indonesia akan memanggil Duta Besar RI dari Australia menyusul dugaan penyadapan telepon Presiden Yudhoyono oleh pemerintah Australia. Menteri Luar Negeri Marty Natalegawa menyampaikan hal ini dalam jumpa pers mendadak di kantor Kementerian Luar Negeri pada Senin (18/11).

"Indonesia akan memanggil pulang Dubes di Canberra untuk konsultasi. Ini tidak bisa dianggap ringan. Ini menunjukkan sikap tegas dan terukur," kata Menlu Marty.

Marty menambahkan mengatakan tindakan itu melukai hubungan kedua negara. "Australia telah melanggar privasi individual, hak asasi manusia dan melukai hubungan Australia-Indonesia," katanya.

• Kebocoran data BPJS

SELLING Indonesian full Citizen 200M+
(NIK/KPT/PHONE/NAME/MAI/LADDRESS/),Free
1Million
by kotz - May 12, 2021 at 06:30 AM

kotz
New User
MEMBER

Posts: 49
Threads: 10
Joined: May 2020
Reputation: 50

New User
MEMBER

Posts: 49
Threads: 10
Joined: May 2020
Reputation: 50

May 12, 2021 at 06:30 AM #1
Hi folks

All of the Indonesian gov full personal information(NID/KPT/PHONE/MAIL/NAME/ADDRESS /) data for sale. there is No password include.

1 Million sample data for free to test. Whole 279 million. 20million have personal photo.

9:32 AM · May 20, 2021

KEBOCORAN DATA PRIBADI YANG TERUS BERULANG

DATA BPJS KESEHATAN BOCOR

- 279 juta data pengguna diperjualbelikan (Mei 2021)

- NIK, nama, alamat, telepon, e-mail, foto
- Harga jual 0,15 BTC (Rp 70-80 juta)
- Dijual di Raid Forums

Data penduduk Indonesia rawan disalahgunakan, tapi hingga kini belum ada regulasi perlindungan data pribadi.

SUMBER: ENGELBERTUS WENDRATAMA (2021), KEMENKOMINFO, KATADATA NASKAH: ANDREA LIWINA DESAIN: PRETTY | FOTO: 123RF



KEBOCORAN DATA PERNAH TERJADI

• Kasus 2020

- 91 juta data pengguna & 7 juta data merchant (Tokopedia)
- 2,3 juta data pemilih Pemilu 2014 (KPU)
- 230 ribu data pasien Covid-19

• Pentingnya regulasi

- Masyarakat berhak:
 - Tahu tujuan penggunaan data
 - Hapus data ke pengelola
- Pengelola wajib mitigasi kebocoran
- Sanksi/denda, jika bocor

• Kebocoran data pengguna Tokopedia

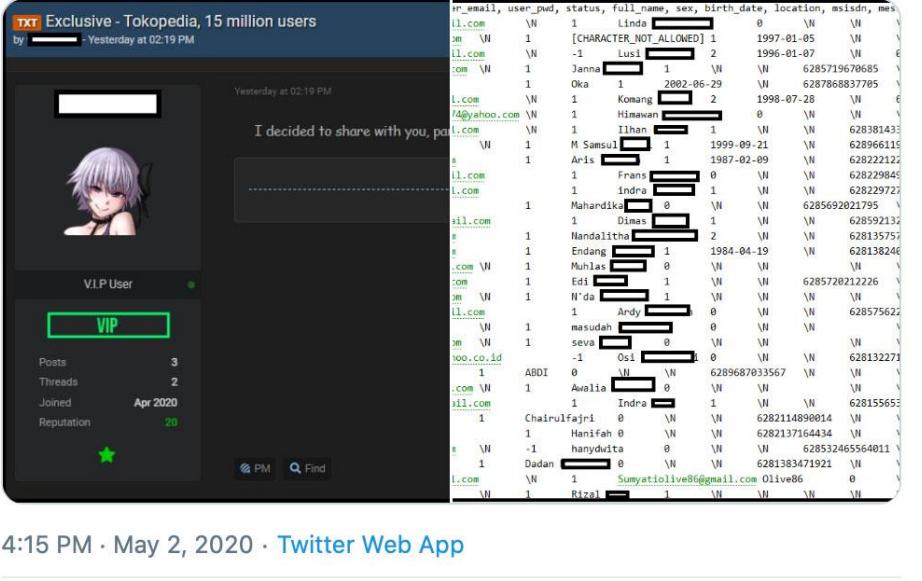
 Under the Breach 
@underthebreach

Actor leaked the database of Tokopedia - a large Indonesian technology company specializing in e-commerce.

(@tokopedia)

- Hack occurred in March 2020 and affects 15,000,000 users though the hacker said there are many more.

- Database contains emails, password hashes, names



4:15 PM · May 2, 2020 · Twitter Web App



- Dugaan kebocoran data pemilih Pemilu 2014, kebocoran sertifikat vaksin Jokowi

KOMPAS.com
JERNIH MELIHAT DUNIA

f t WhatsApp LINE

Sertifikat Vaksin Jokowi Bocor, Satgas: PeduliLindungi Kini Gunakan 5 Parameter Keamanan

Selasa, 7 September 2021 | 19:59 WIB

f t WhatsApp LINE

Lihat

Periksa Sertifikat Vaksinasi COVID-19

Nama Lengkap NIK / No Paspor Tempat Lahir

Tanggal Vaksin Masukan NIK / No Paspor

NIP/BBM/HP

Jenis Vaksin

WNI/Non WNI

PDF Jquery validate

Jika sertifikat Anda tidak terdeteksi, segera menghubungi CALL CENTER 119 dengan extensio...

Dkatadata.co.id

Ad

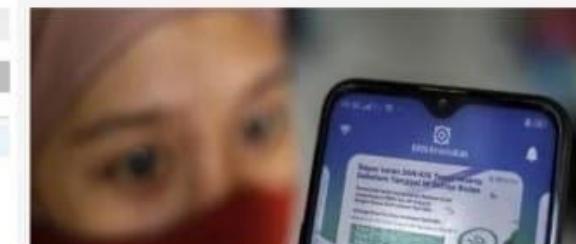
■ TEKNOLOGI

Kebocoran Data BPJS Kesehatan Disebut Bikin Rugi Negara Rp 600 Triliun

CISRT menyebutkan, kebocoran 279 juta data peserta BPJS Kesehatan merugikan negara Rp 600 triliun. Ini karena data KTP ikut bocor, sehingga bisa mengganggu program pemerintah.

Jum'at, 25 Juni 2021 | 14:58 WIB

Fahmi Ahmad Burhan



KOMPAS.com
JERNIH MELIHAT DUNIA

f t WhatsApp LINE

Baca artikel lebih nyaman tanpa terganggu banyak iklan di aplikasi Kompas.com.

UNDUH

Home > News > Nasional

Data Pemilih Diduga Bocor, KPU Pastikan Tak Ada Peretasan DPT Pemilu 2014

Minggu, 24 Mei 2020 | 13:46 WIB

f t WhatsApp LINE

Lihat Foto



- Kebocoran data di Kemenhan dan Bank BSI

KEJAHATAN SIBER

Situs Kementerian Pertahanan Diduga Diretas, Dokumen Rahasia Berpotensi Bocor

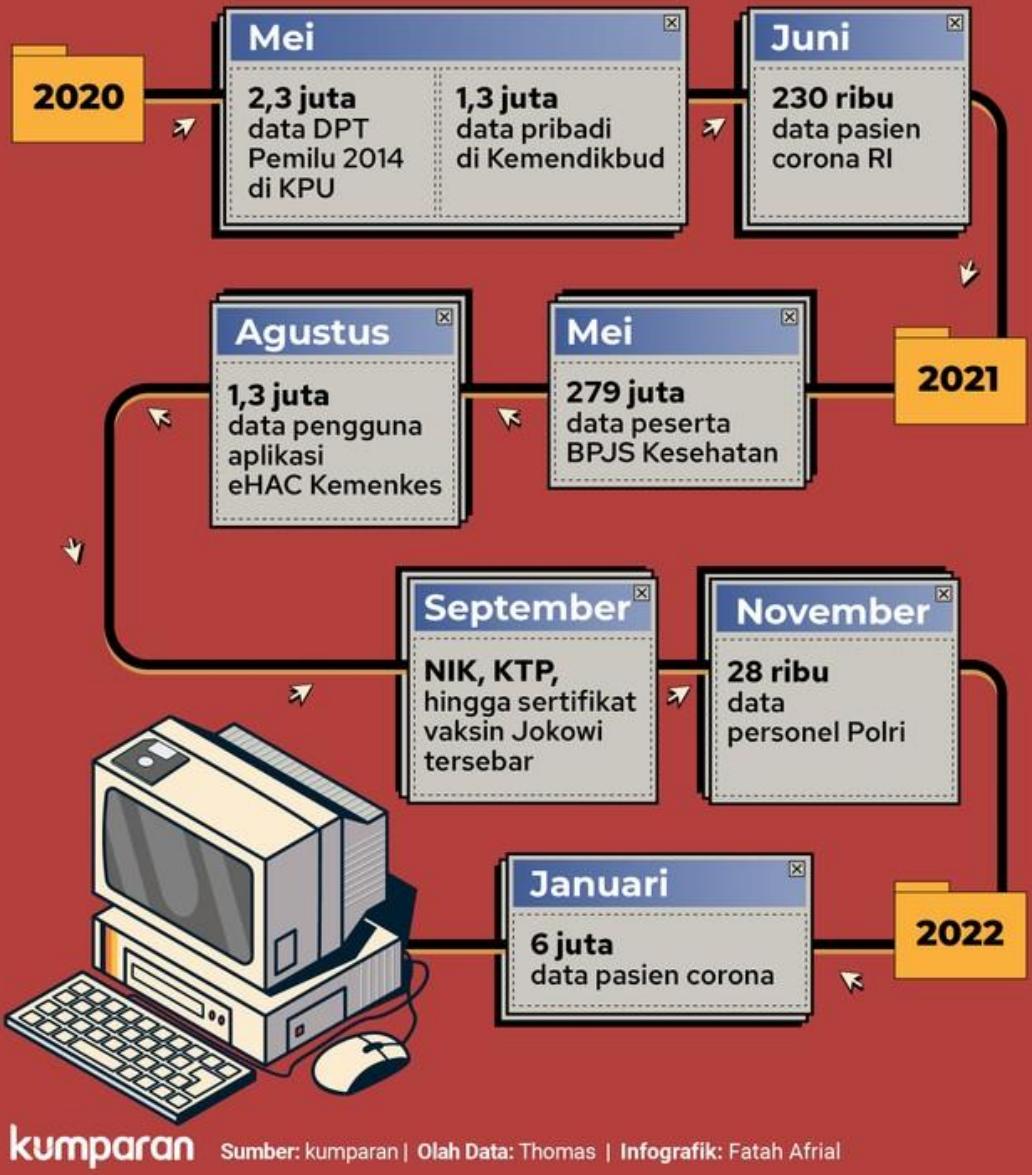
Data Kementerian Pertahanan sebesar 1,64 terabita berpotensi bocor setelah situs resmi kementerian itu dibobol peretas.

1,5 TB Data Nasabah BSI Dibobol Hacker LockBit 3.0

 Taufan Bara Mukti  Sabtu, 13 Mei 2023 | 12:03 WIB



Deretan Kasus Dugaan Kebocoran Data di RI



- Kasus-kasus seperti:
 - kebocoran data,
 - pencurian data,
 - pengaksesan data secara ilegal, dll

menunjukkan pentingnya **kriptografi** menjaga keamanan data dan informasi.

Terminologi di dalam Kriptografi

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

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

Di dalam kriptografi, data dan informasi disebut pesan (*message*)

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

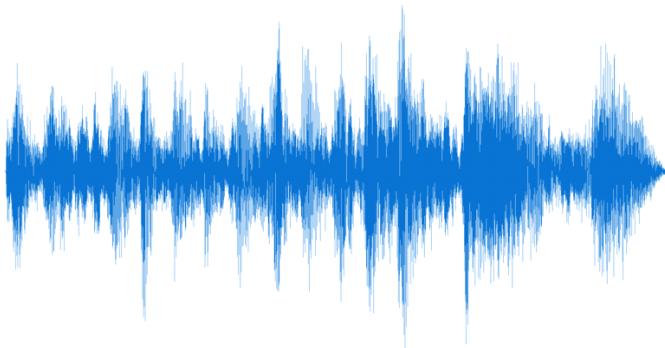
(a) Teks

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

(b) Gambar

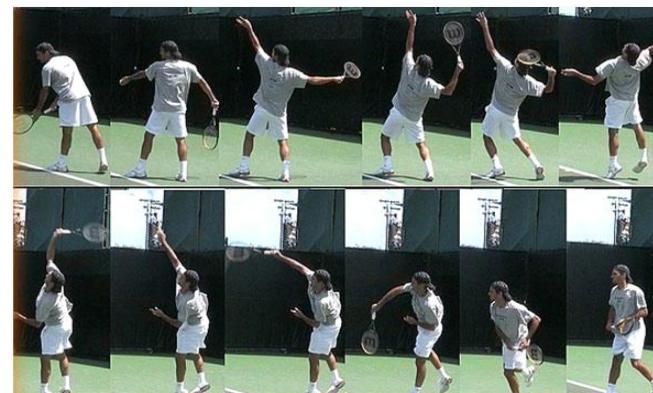


(c) Audio



Sumber: <http://cloudinary.com>

(d) Video



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

TABEL PENJUALAN

No	Nama sales	Jan	Feb	Item	Total
1	edi	95	65	Monitor	160
2	edo	65	52	Speaker	117
3	danu	98	57	PDA	155
4	didi	57	36	Printer	93
5	barra	84	98	Printer	182
6	hery	51	29	PDA	80
7	rio	19	97	Speaker	116
8	juni	66	47	Monitor	113
9	lala	16	36	PDA	52
10	endang	47	100	Printer	147
11	andi	99	69	Monitor	168
12	yudi	31	54	Speaker	85
13	widi	52	20	Speaker	72
14	eko	34	52	PDA	86
15	santi	74	43	Monitor	117

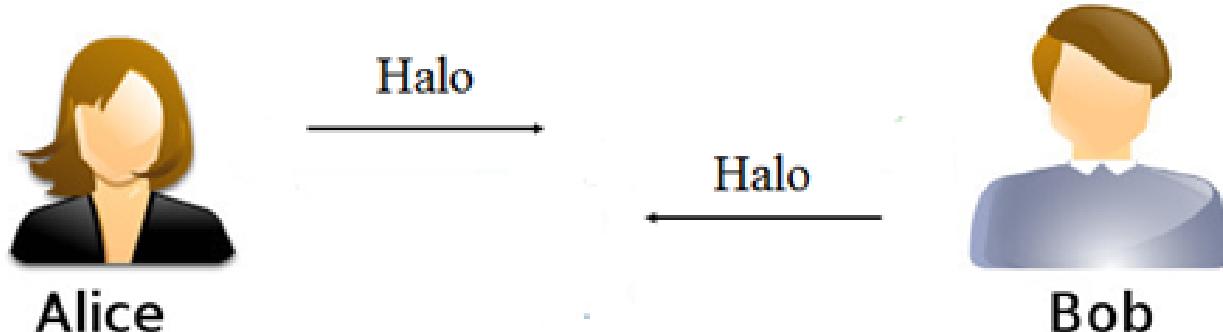


2. Pengirim (*sender*) dan penerima (*receiver*)

Pengirim: pihak yang mengirim pesan

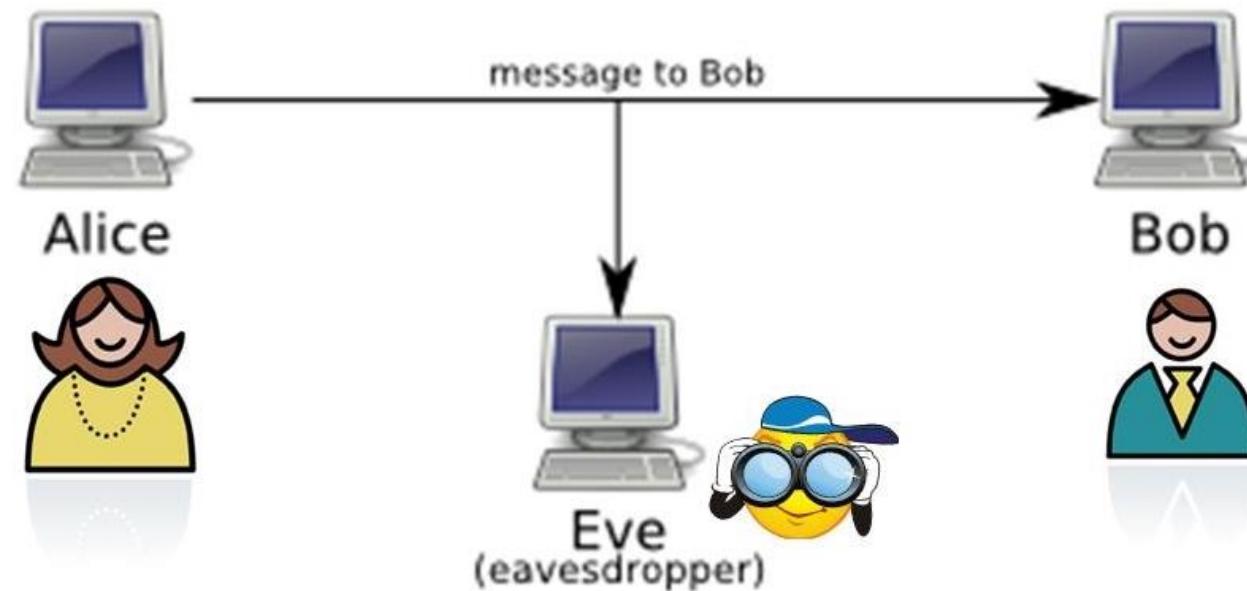
Penerima (*receiver*): pihak yang menerima pesan

- Di dalam kriptografi, pengirim pesan ditokohkan sebagai Alice dan penerima pesan ditokohkan sebagai Bob (agar terkesan lebih manusiawi ketimbang menggunakan simbol A, B, C, dan sebagainya).



3. Penyusup (*intruder*)

- Pihak ketiga yang menyadap, mengintersepsi, menghapus, menambah, atau mengubah pesan
- Sebutan lain: *eavesdropper*, *enemy*, *adversary*, *interceptor*, *bad guy*, dsb
- Nama tokohnya: Eve, Carol, Trudy, Mallory, dsb



Ronald Rivest: “*cryptography is about communication in the presence of adversaries*”

Q: What can a “bad guy” do?

A: a lot!

- *eavesdrop*: intercept messages
- actively *insert* messages into connection
- *impersonation*: can fake (spoof) source address in packet (or any field in packet)
- *hijacking*: “take over” ongoing connection by removing sender or receiver, inserting himself in place
- *denial of service*: prevent service from being used by others (e.g., by overloading resources)

Sumber: Chapter 8, Network Security

4. Cipherteks (ciphertext): pesan yang telah disandikan sehingga tidak bermakna lagi.

Tujuan: agar pesan tidak dapat dibaca oleh pihak yang tidak berhak.

Nama lain: **kiptogram (cryptogram)**

- Contoh:

Plainteks: culik anak itu jam 11 siang

Cipherteks: t^\$gfUi89rewoFpfWqLMp [uTcxZ

Kriptogram: t^\$gfU i89rewo FpfWqLM p [uTcxZ

Plainteks:

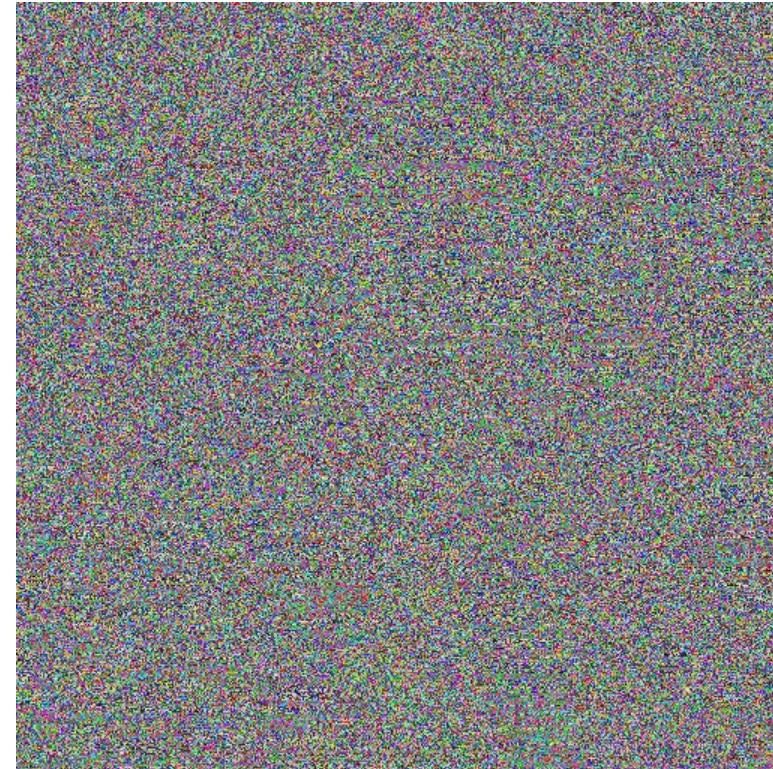
Dinas Pendidikan Kota Ternate meminta kepada pihak sekolah dan orang tua siswa untuk jenjang pendidikan SD dan SMP se-Kota Ternate untuk melarang para siswa membawa permainan lato-lato yang sedang tren itu ke sekolah, karena akan mengganggu kegiatan belajar mengajar yang dinilai berbahaya sehingga mengantisipasi kecelakaan bagi anak di daerah itu.

Cipherteks:

HAWFHZDOHAHANGOMKLGFCVWFLBOCPRKFGNHOFNIN
SPGNLHMPFVBEFWMVFWTBWRHSFZRWFQMVHPAFWIK
DOHAHANGPFEWNFPFNKLHMPFGLBAMGFCXKFQMOCFV
AVKANIAVHSFZRN CODGAFOHYUVGWFOFGFXEGFMLFWIT
HEFWTBVCPAYQOBLHMPFVBPVADOVWGNFWOCKARVKA
RQOBRGFFWCHFVGVYUDORVGVYCFWABAPVSVGCHGCI
DRFIFHBAPVQRVOCKAFWSGHNSIHSOBDHFVNGFWDGRGF
WGNHANFCVIDGSWZ



Plain-image

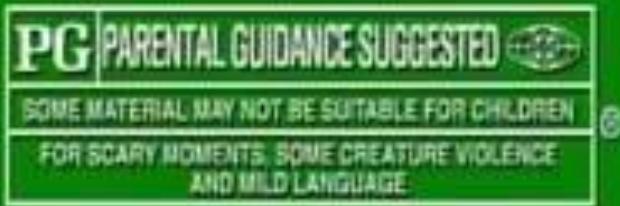


Cipher-image

Total Video Converter
<http://effectmatrix.com>

THE FOLLOWING **PREVIEW** HAS BEEN APPROVED FOR
ALL AUDIENCES
BY THE MOTION PICTURE ASSOCIATION OF AMERICA

THE FILM ADVERTISED HAS BEEN RATED



Plain-video



Cipher-video

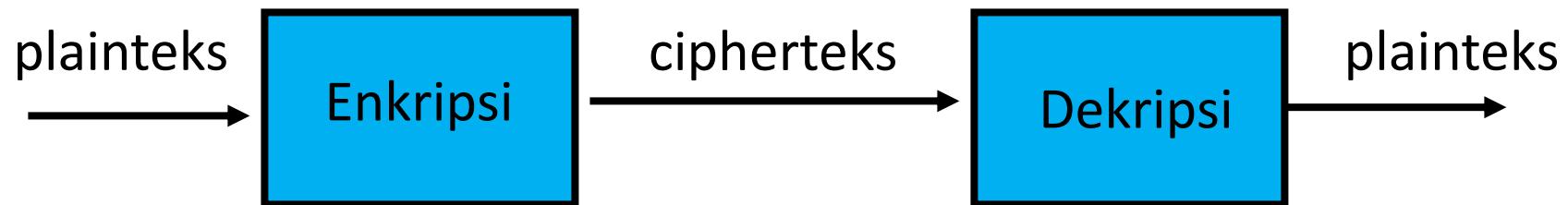
5. Enkripsi (*encryption*) dan dekripsi (*decryption*)

- Enkripsi: proses menyandikan plainteks menjadi cipherteks.

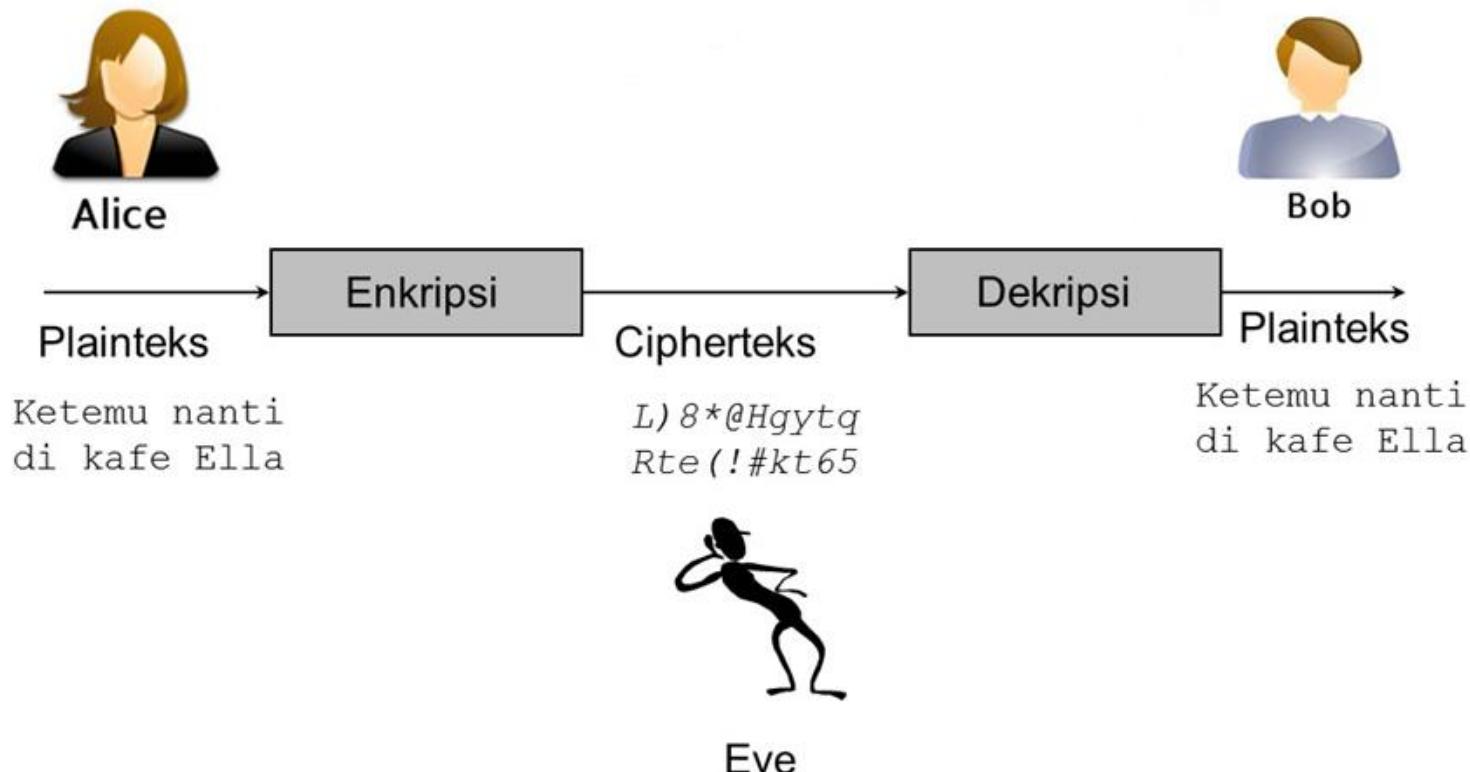
Nama lain: *enciphering*

- Dekripsi: proses mengembalikan cipherteks menjadi plainteks semula.

Nama lain: *deciphering*



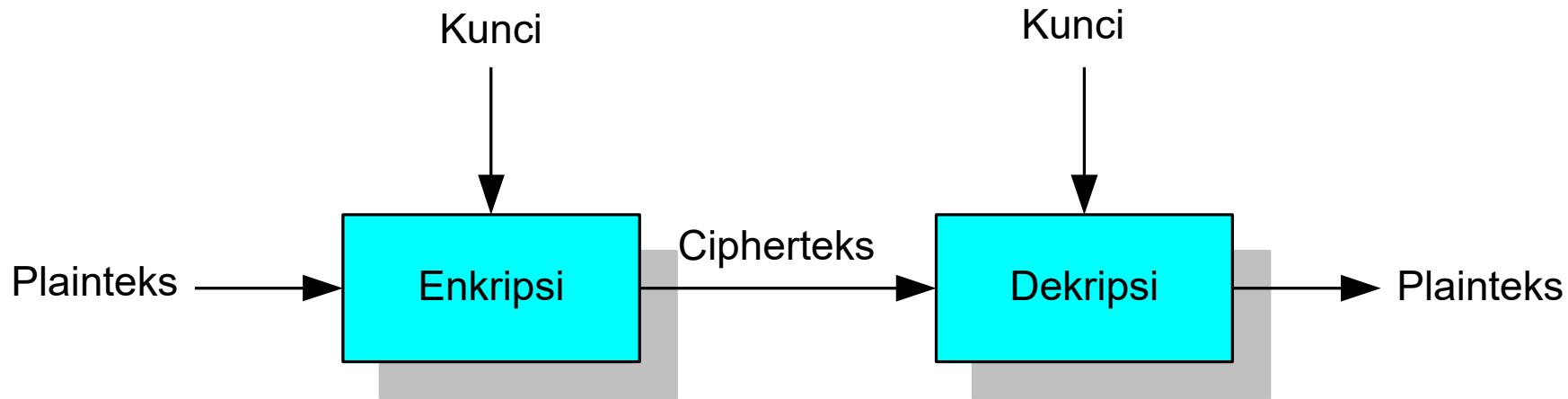
- Meskipun Eve dapat menyadap komunikasi antara Alice dan Bob, namun karena pesan sudah dienkripsi menjadi cipherteks, Eve tidak dapat memahami pesan yang disadapnya



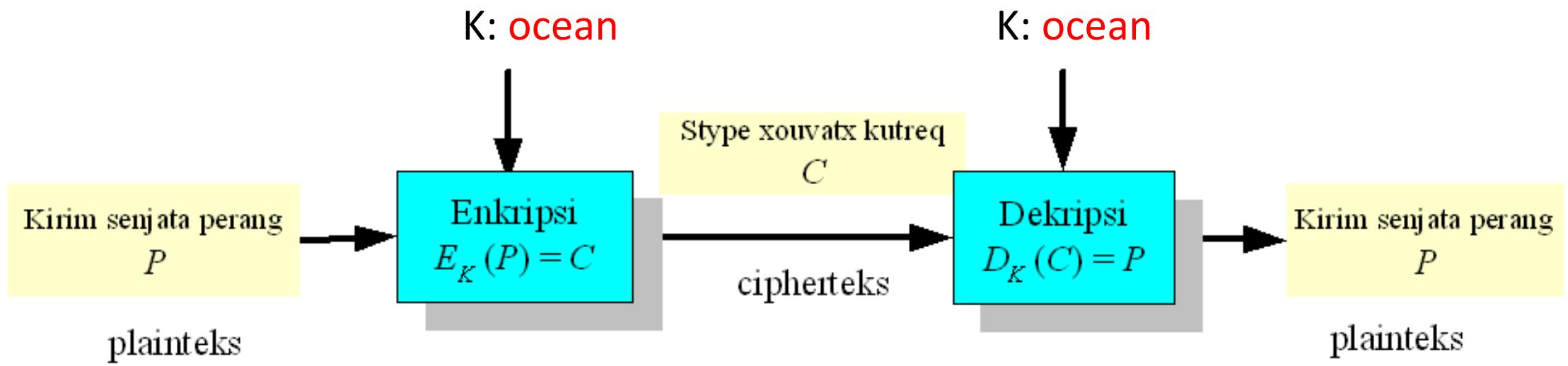
6. Kunci

- Agar enkripsi dan dekripsi hanya dapat dilakukan oleh dua pihak yang berkomunikasi, maka diperlukan **kunci** rahasia.
- Kunci adalah parameter yang digunakan di dalam enkripsi dan dekripsi
Simbol: K (K dapat berupa integer, string, alphanumeric, dsb)

$$\text{Enkripsi: } E_K(P) = C \quad ; \quad \text{Dekripsi: } D_K(C) = P$$



Prinsip Kherkoff: semua algoritma kriptografi harus publik (tidak rahasia), hanya kunci yang harus rahasia.



7. *Cipher*

- Algoritma untuk enkripsi dan dekripsi pesan
- Aturan (*rule*) untuk *enchipering* dan *dechiper*ing, atau berupa fungsi matematika yang digunakan untuk enkripsi dan dekripsi pesan.

Contoh: Enkripsi: Geser tiga huruf ke kanan (rule)

Dekripsi: Geser tiga huruf ke kiri (rule)

$E(p) = (p + k) \text{ mod } 26$ (fungsi matematika)

$D(c) = (c - k) \text{ mod } 26$ (fungsi matematika)

- *Classical cipher*: Caesar cipher, Vigenere cipher, Playfair Cipher, Enigma cipher, dll
- *Modern cipher*: DES, AES, Blowfish, Serpent, RSA, ElGamal, RC4, RC5, A5, dll

8. Sistem kriptografi (*cryptosystem*)

Sistem kriptografi adalah *quintuple* $(\mathcal{E}, \mathcal{D}, \mathcal{M}, \mathcal{K}, C)$

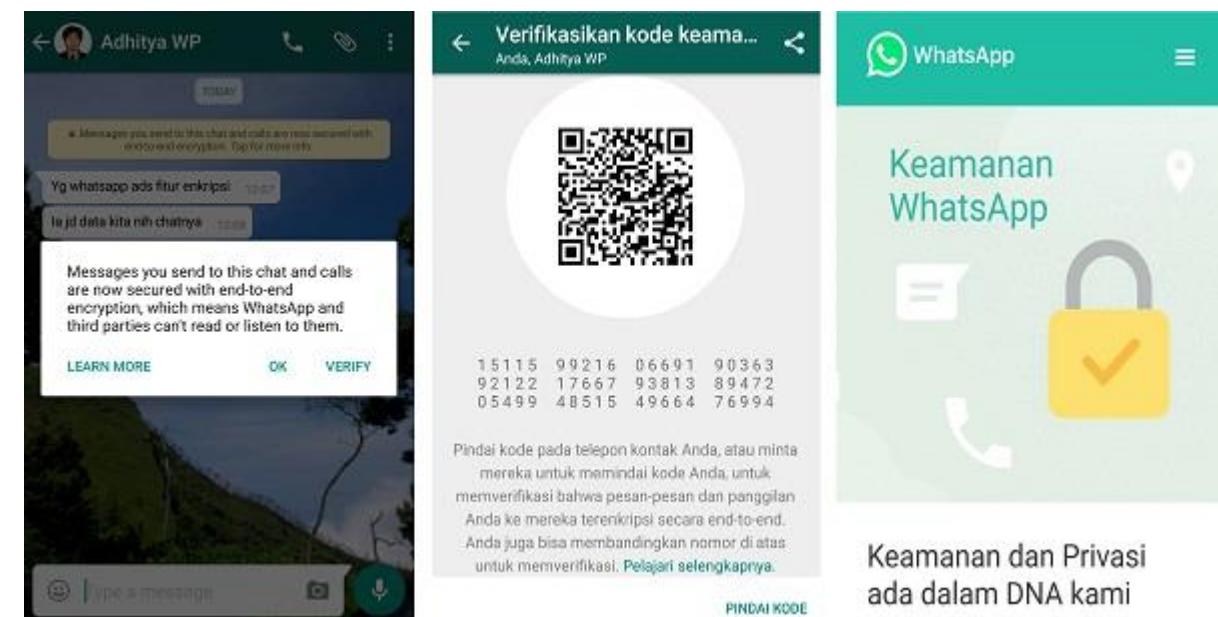
- \mathcal{M} adalah himpunan plainteks
- \mathcal{K} adalah himpunan kunci
- C adalah himpunan cipherteks
- \mathcal{E} adalah himpunan fungsi enkripsi $E: \mathcal{M} \times \mathcal{K} \rightarrow C$
- \mathcal{D} adalah himpunan fungsi dekripsi $D: C \times \mathcal{K} \rightarrow \mathcal{M}$

Contoh: Caesar cipher (ingat kembali materi di dalam kuliah Matdis ☺)

- $\mathcal{M} = \{ \text{huruf-huruf alfabet} \}$
- $\mathcal{K} = \{ k \mid k \text{ adalah bilangan bulat dan } 0 \leq k \leq 25 \}$
- $\mathcal{E} = \{ E_k \mid k \in \mathcal{K} \text{ dan untuk semua plainteks } m,$
$$E_k(m) = (m + k) \bmod 26 \}$$
- $\mathcal{D} = \{ D_k \mid k \in \mathcal{K} \text{ dan untuk semua cipherteks } c,$
$$D_k(c) = (c - k) \bmod 26 \}$$
- $\mathcal{C} = \mathcal{M}$

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 di mesin ATM yang kemudian ditransmisikan ke komputer *server* bank.
- Enkripsi *password* yang diberikan oleh pengguna ke komputer *host/server*
- Enkripsi nomor kartu kredit pada transaksi *e-commerce* di internet.
- Enkripsi siaran televisi berbayar (*Pay TV*)
- Enkripsi pesan (teks, audio, video, dsb) melalui *Whatsapp*, *Email*, dll
- 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*.



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 OS0000SO 00H00001S0000000 A000E
□ OS000 □□ OG00
□H000
□H000KSeK20000 G000HSVA00000IA'
□H000000A000E- □DN, '*A0
□S000NTD000 □]Hlm;□000A00000 □
A000 A0000 N0000A □□ N00 GO
□ OG,□
□□ A00 □
jk□ □□ □ N00 G000H000ED OG
□□ 000E□
□N0000 □□□ OAO
□S00 □□□
OG2*I~b2*IBE0 OG2#§]-

wisuda.txt

cipher.txt

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/ztxâx}v êp}	pää/psp	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.



foreman.avi



Foreman-encrypt.avi

Kriptanalisis

- **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

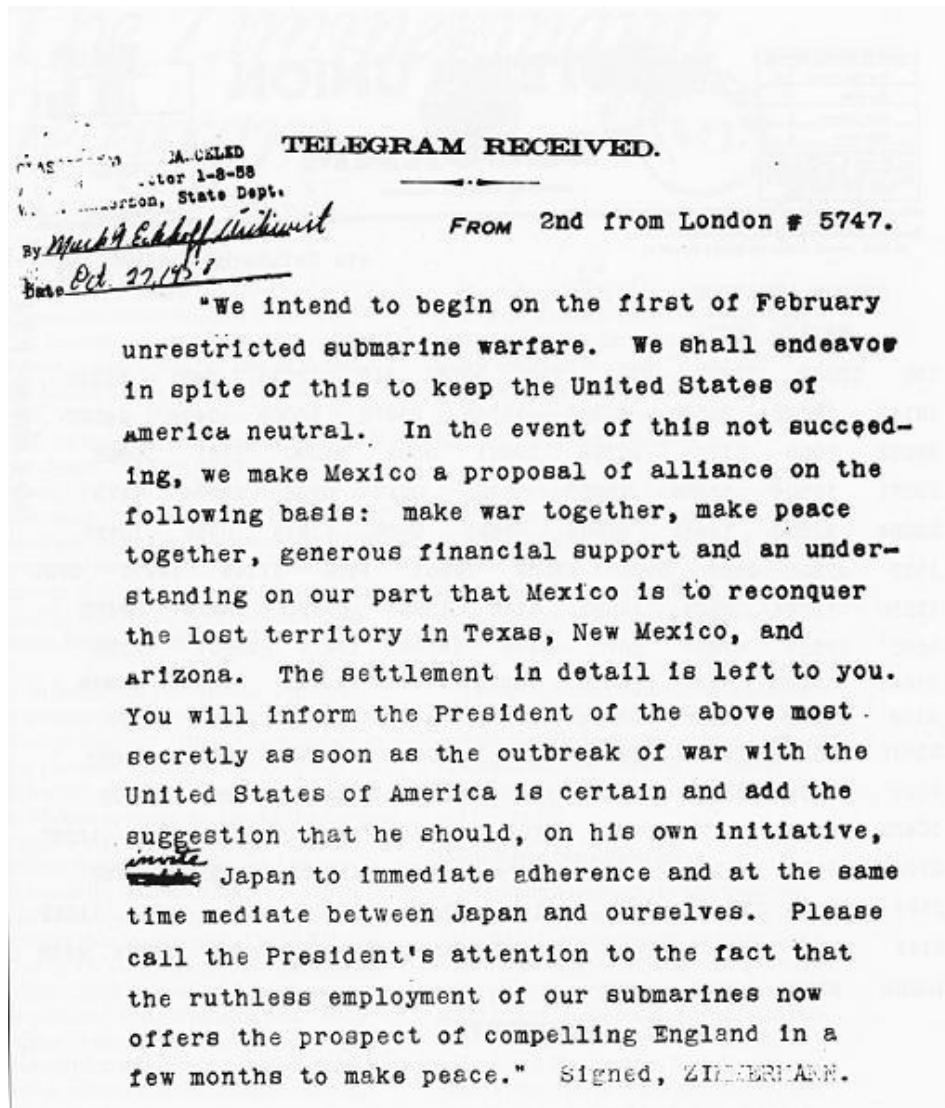
٢١- اسم الوجه ٢٢- والد وهو يصف ملوكها الصنوات اعنة سرطان الثور وبرهانهم على هزله
٢٣- باسمه الـ زعيم اصحابه يحيى في منظمه طلاقه وشاعرهم بـ حامل الفجر وفتحه للابطال
٢٤- ماء العسل واسمها واسمها واسمها واسمها واسمها واسمها واسمها واسمها
٢٥- لاجرميسيه ٢٦- على مثال المتصوفة المطلقة مياو مياو والدر سلطان الحمراء اسطورة
٢٧- من الاعمال الـ فدا وفداء ارجح دكتور واسك وارتكب طلاقها السرطان طلاقاً السراطون طلاقاً
٢٨- سرطان الـ اسماه ويلات القملة وليلة طلاقه وفتحه للعلم من تصاريق كل الجمجمة ٢٩-
٣٠- اسم والسماء البر ما يطلقه البرايا وجعله الفخر بالصوت والنظر الفضي

مَرَاةَ اللَّهِ وَالْعَالِيَّ وَصَلَّى اللَّهُ عَلَى مُحَمَّدٍ وَسَلَّمَ

لسم الله الرحمن الرحيم
رساله اسرار فطور رسمو الدارع اسرار العمر والراصان
لهم صل الله عز وجل واقر عالمي امانتك رس، وثبات مأمورتك الحبل الاصغر ملائكة
الكل العجماء واتصل بالقمر وحرر المخلوق، فلكم الله الامر سهل سلاطك النافع
عن كل لذة اسلامي ونور العرش وعذاب عذاب النجس الدموي وسرور الفتن والضراء
الاسفار، وسعدكم دار الارض وسبعينها، ولهم، اهل الاعلام، اصحاب لما يحيى العمر

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

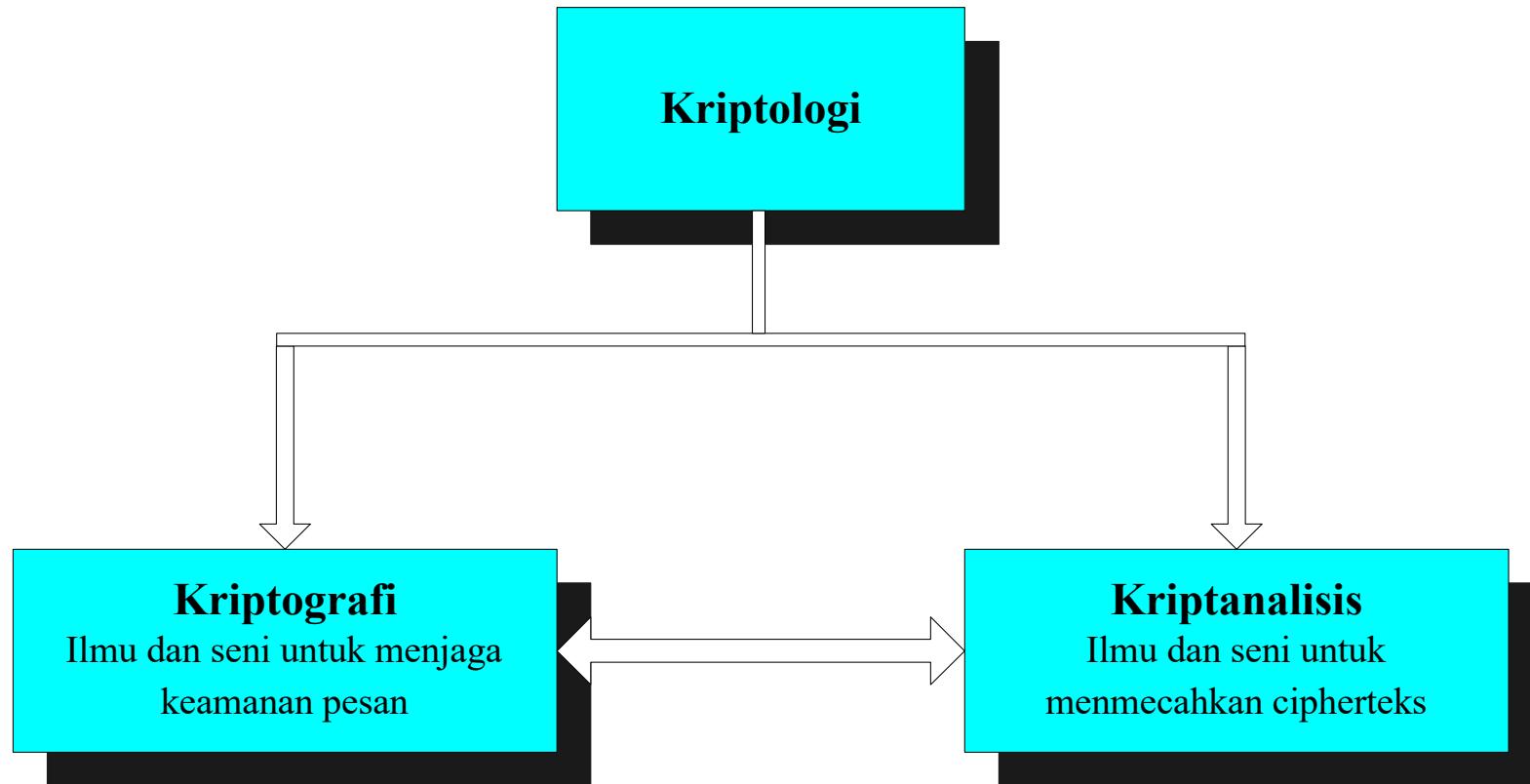
Sejarah kriptanalisis
mencatat hasil
gemilang seperti
pemecahan Telegram
Zimmermann yang
membawa Amerika
Serikat ke kancalah
Perang Dunia I.



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

Kriptologi

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



Sejarah Kriptografi

- Kriptografi sudah berusia sangat tua, sudah ada sejak peradaban manusia di bumi
- Secara historis, kriptografi diasosiasikan dengan kegiatan mata-mata, pemerintahan, dan militer, dan telah digunakan di dalam perang selama ribuan tahun.
- Tiga pihak yang memiliki kontribusi penting di dalam perkembangan kriptografi zaman dahulu: kalangan militer, diplomat, dan *diarist*.
- Sejak lebih dari 50 tahun yang lalu, kriptografi mendapatkan landasan matematika, dan telah bergeser dari aplikasi militer ke aplikasi komersil.
- Secara garis besar, kriptografi dibagi menjadi dua era: **kriptografi klasik** dan **kriptografi modern**.

Old Cryptography



- *Ancient cryptography* atau *classical cryptography*
- Kriptografi zaman dulu (sebelum Masehi s/d sebelum ada komputer digital)
- Hanya mengenkripsi huruf dan angka, menggunakan kertas dan pena saja
- Semua *cipher* nya sudah kadaluarsa (sudah tidak aman, karena sudah berhasil dikriptanalisis)
 - Caesar cipher
 - Vigenere cipher
 - Playfair cipher
 - Hill cipher
 - Beauford cipher
 - Enigma cipher
 - dll



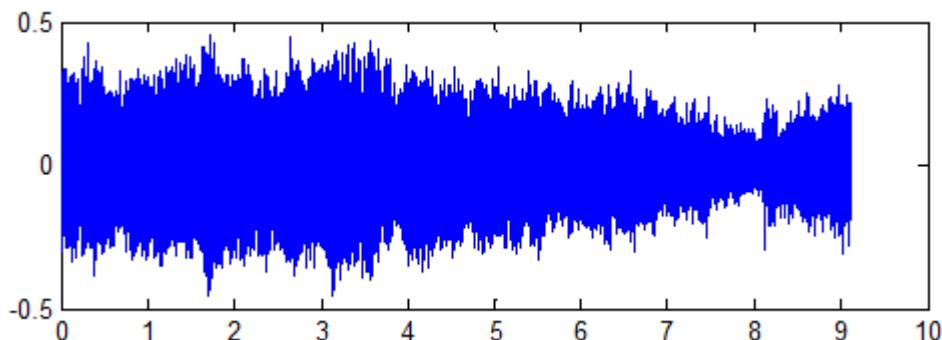
Modern Cryptography

- Enkripsi dan dekripsi pesan dalam bentuk digital dengan komputer digital

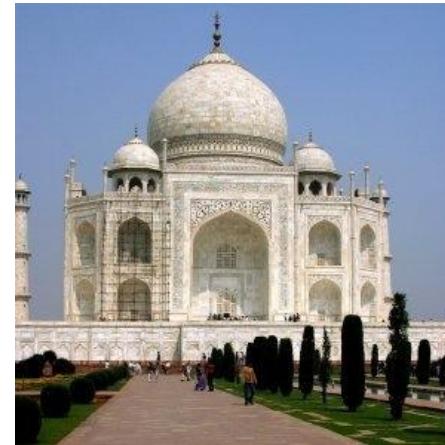
1. Teks

```
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  
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*)



- DES, 3DES
- AES, Serpent
- RSA, ElGamal, ECC
- Diffie-Hellman
- MD5, SHA-3
- DSA
- TLS
- dll

4. Video



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*



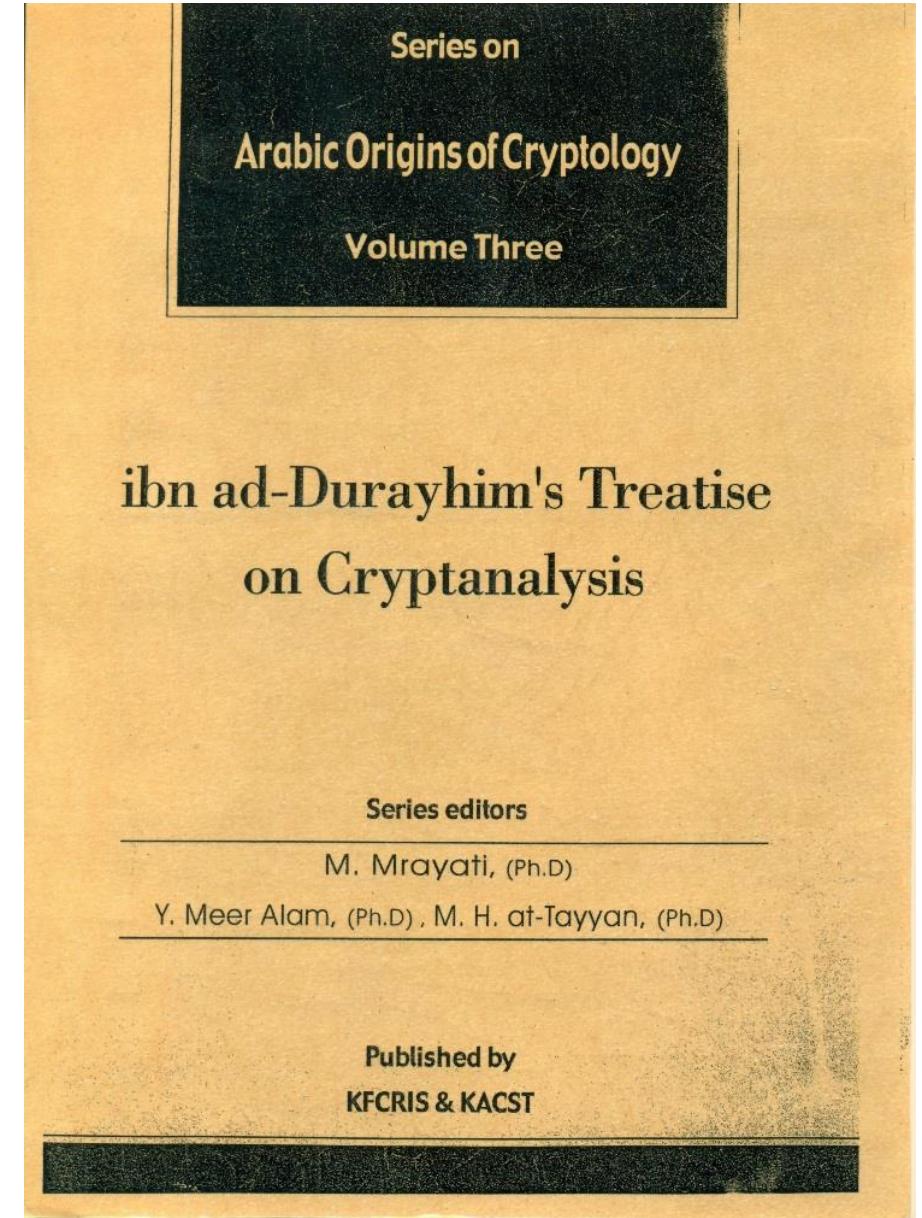
Plainteks: KILLKINGTOMORROWMIDNIGHT

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 Umayyah 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 cryptanalysis.
(David Kahn – Penulis buku: The Code Breaker)*

Kriptografi di Eropa dari Zaman Renaisans sampai Abad 19

- Zaman renaisans → abad pertengahan (abad 15-16)
- *Cipher* terkenal pada abad pertengahan hingga abad 19:
 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 Wheatstone 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 (sebuah cipherteks yang isinya rencana membunuh Ratu Elizabeth I) pada Abad Pertengahan berhasil dipecahkan oleh Thomas Phelippes, seorang pemecah kode (*codebreaker*).



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

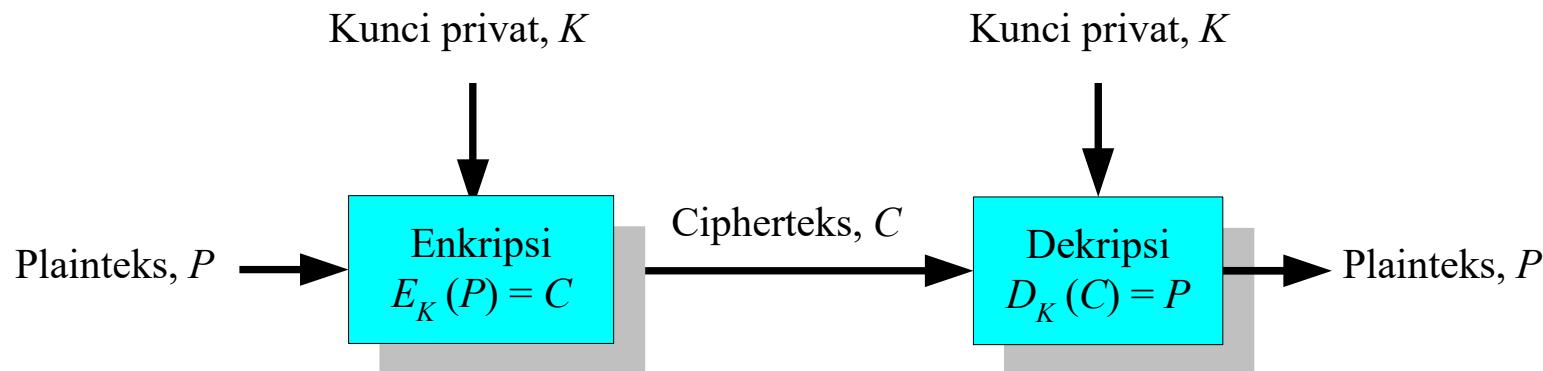


Enigma

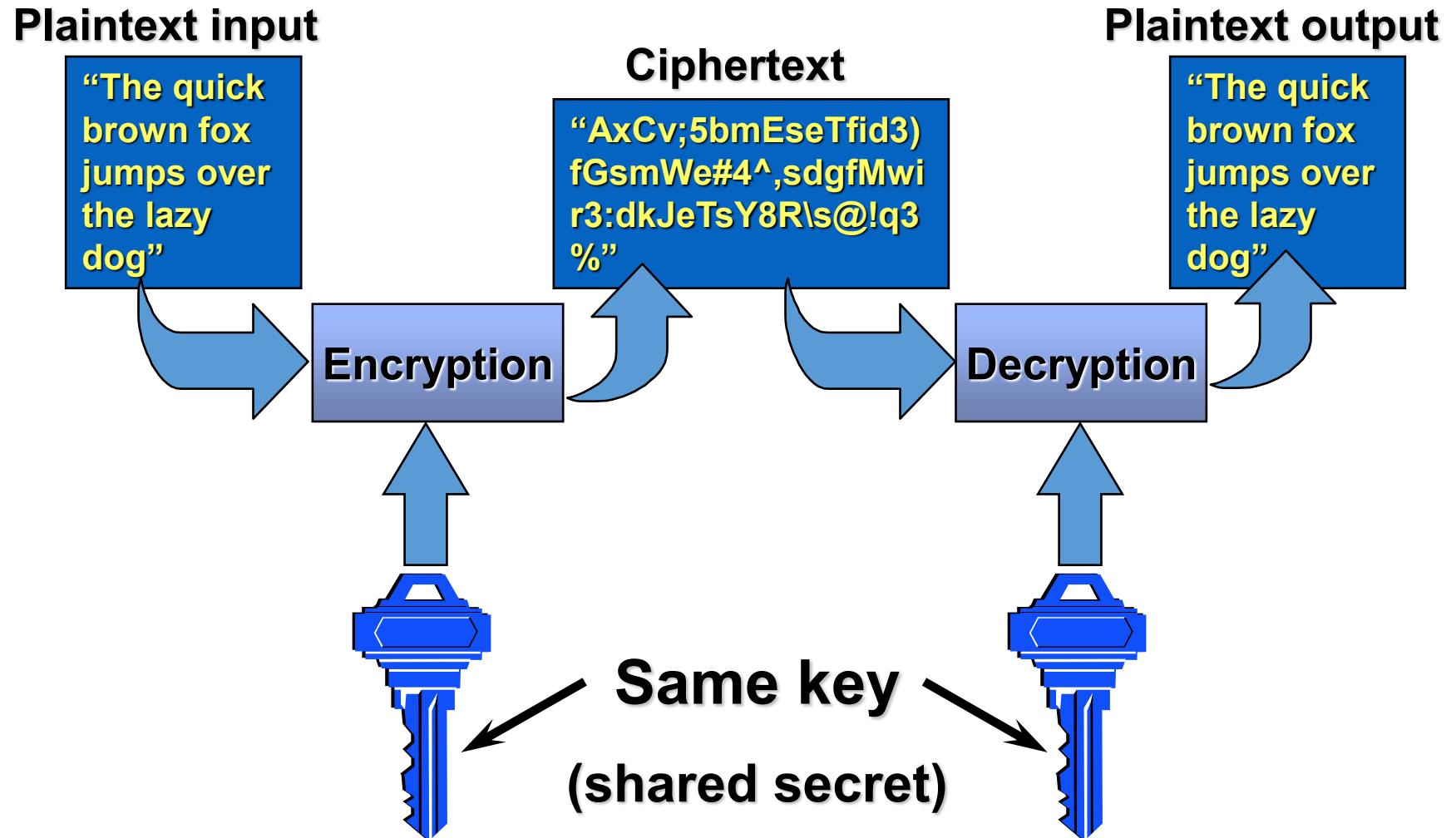
Tiga (3) Jenis Algoritma Kriptografi

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

- Kunci enkripsi = kunci dekripsi, harus dijaga privat (rahasia) atau *secret*
- Sudah ada sejak ribuan tahun yang hingga tahun 1976



- 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*)

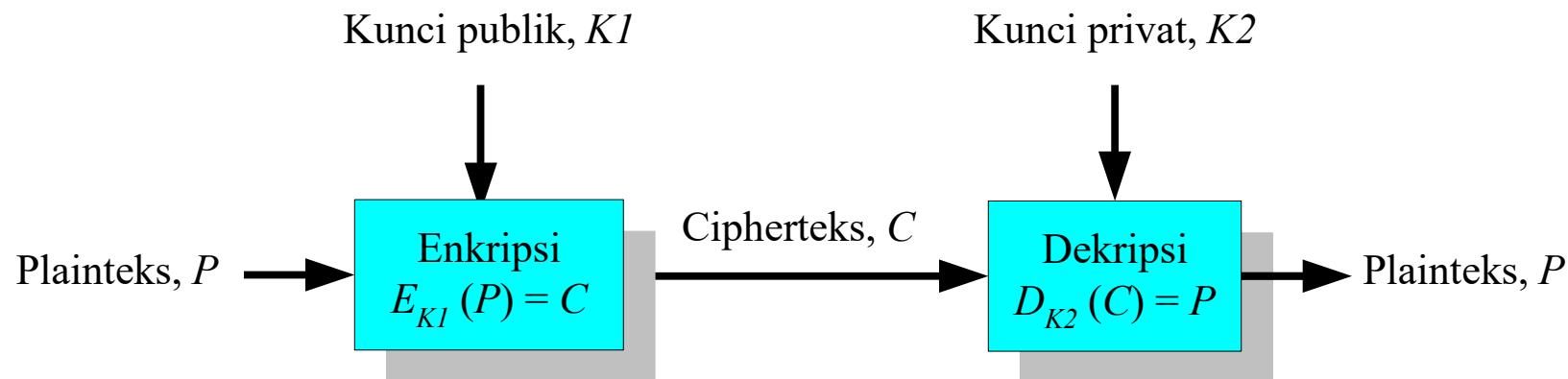
- Kunci enkripsi \neq kunci dekripsi ($K1 \neq K2$)

Kunci enkripsi \rightarrow tidak rahasia (*public key*)

Kunci dekripsi \rightarrow rahasia (*private key*)

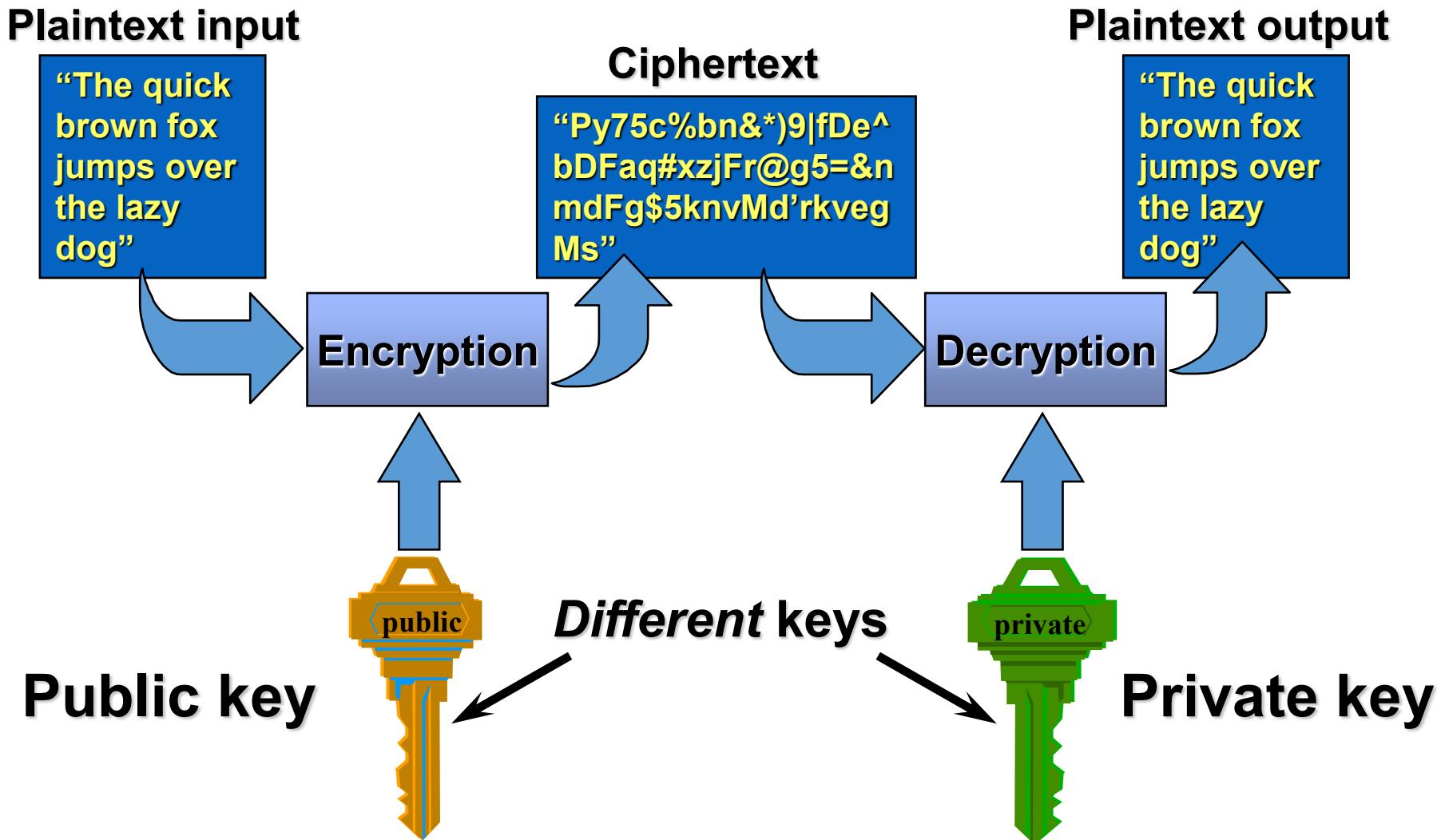
- Mulai ditemukan sejak tahun 1976

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



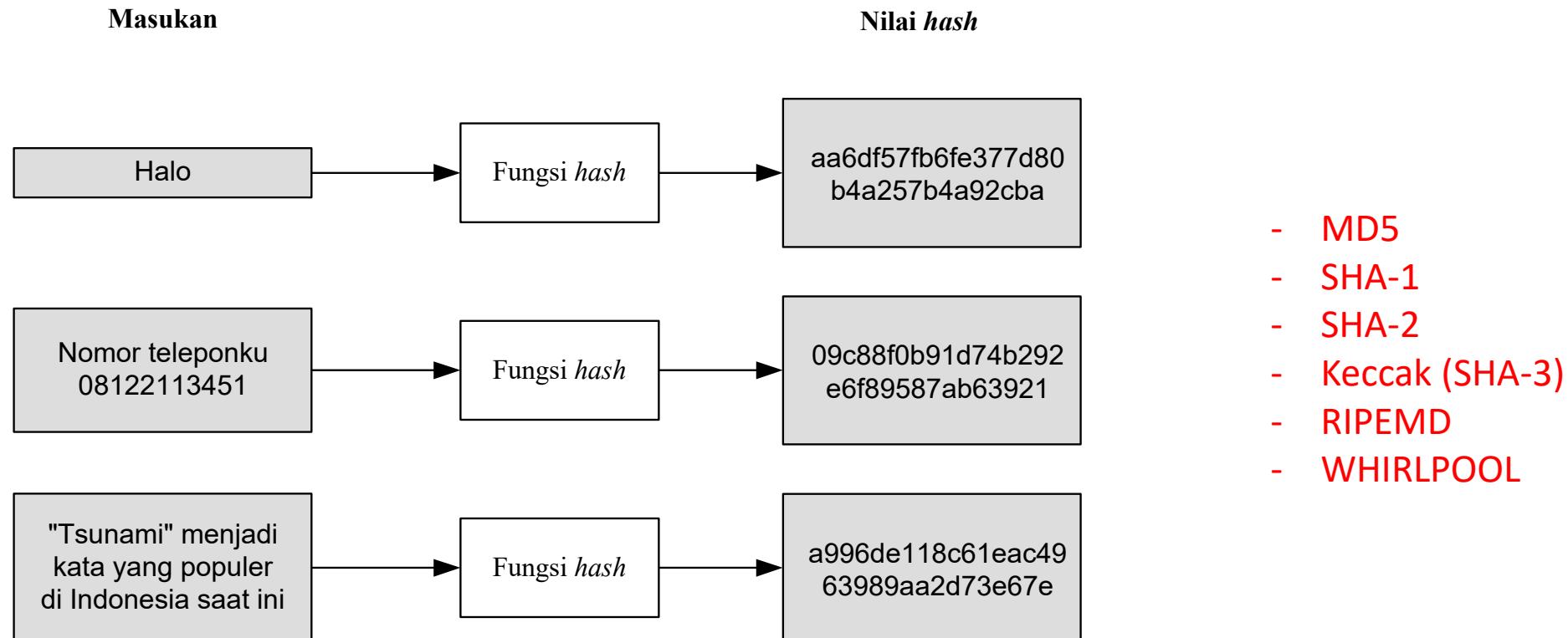
- RSA (Rivest-Shamir-Adleman)
- ElGamal
- DSA
- Diffie-Hellman
- Merkle Knapsack Algorithm

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

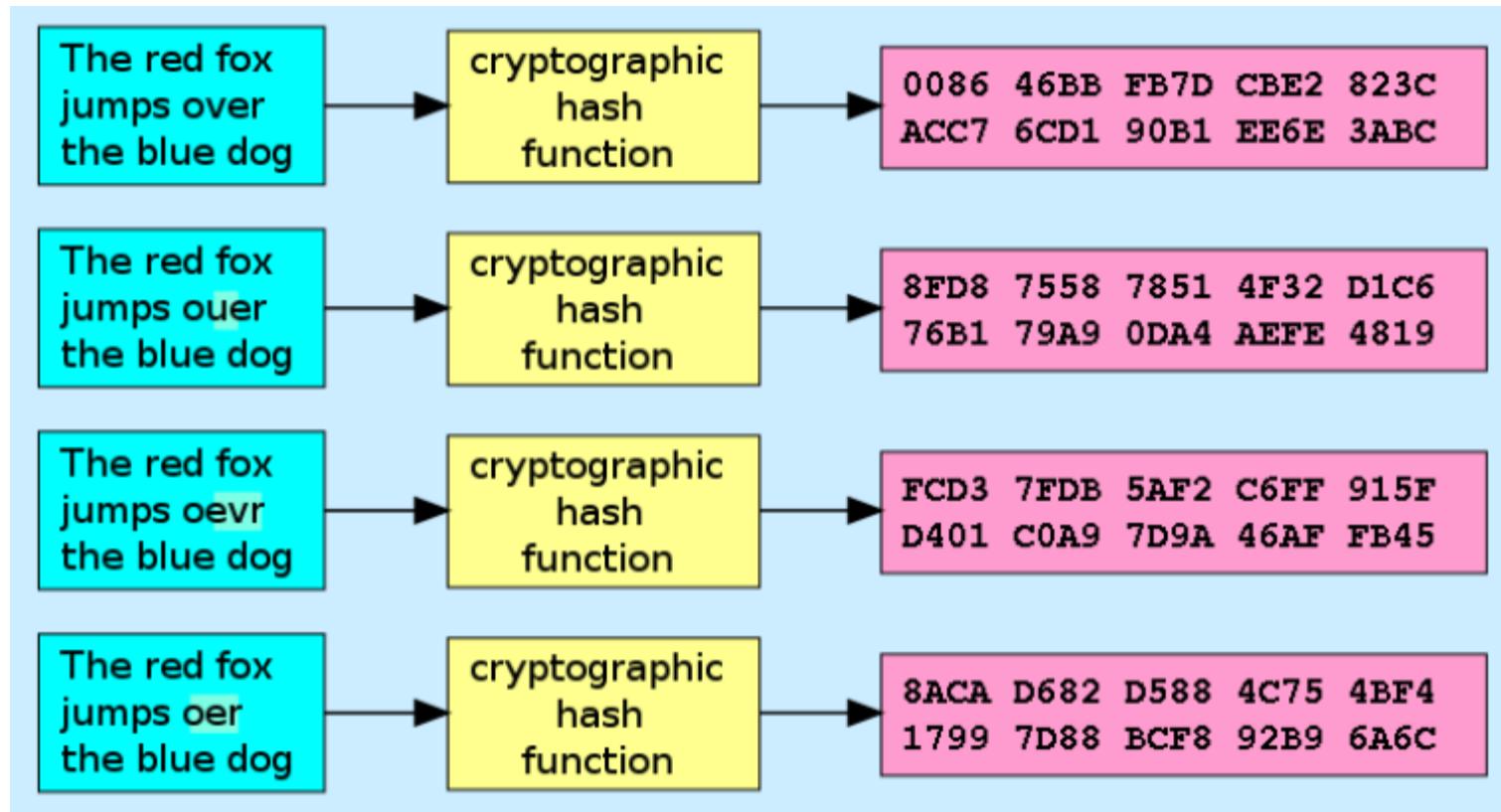


3. Fungsi Hash

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



Kegunaan: memeriksa integritas pesan



(Sumber gambar: Wikipedia)

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. Politeknik Siber dan Sandi Negara (PSSN)

<https://poltekssn.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