II4031 Kriptografi dan Koding

01 - Pengantar Kriptografi

Oleh: Rinaldi Munir

Program Studi Sistem dan Teknologi Informasi

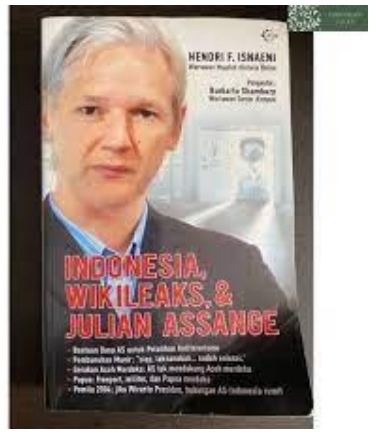
Sekolah Teknik Elektro dan Informatika ITB

2023

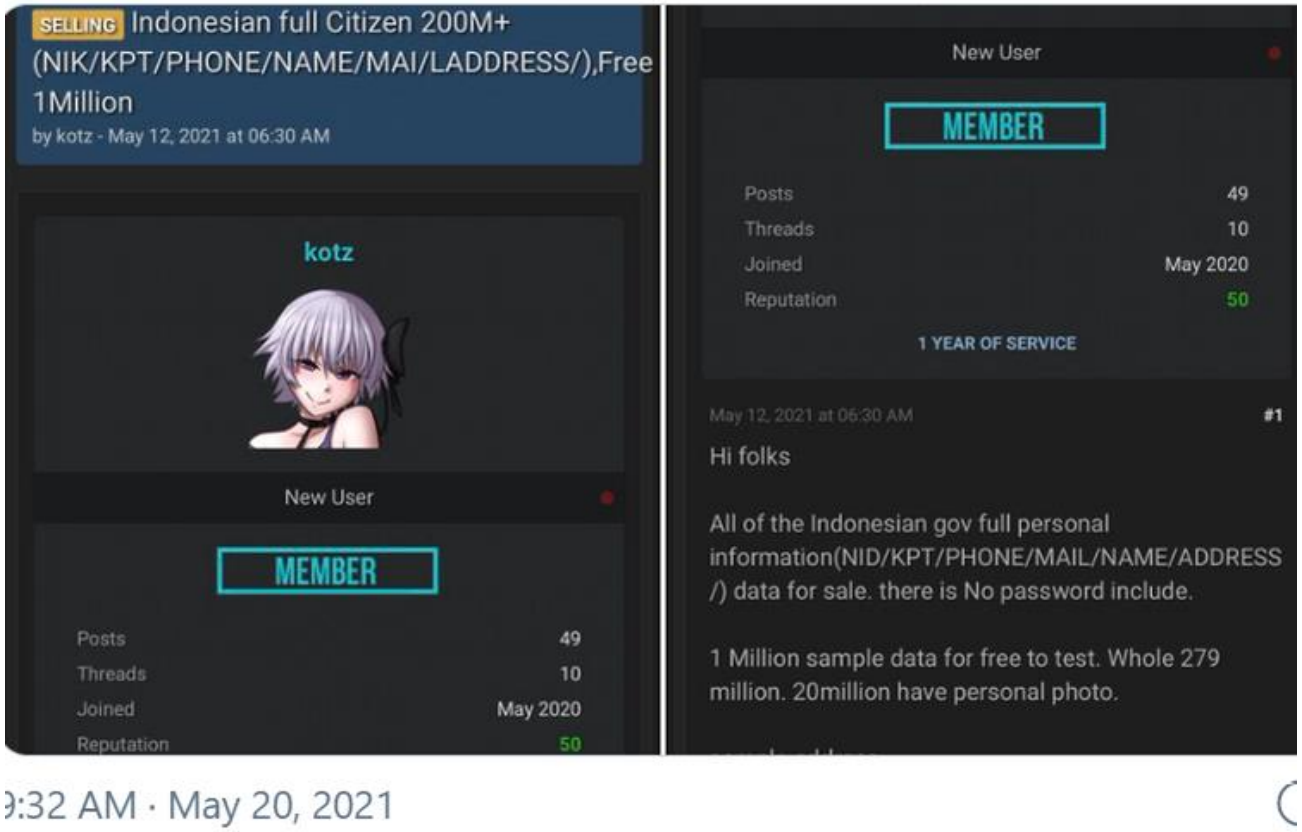
Masih ingat dengan kasus-kasus ini?

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

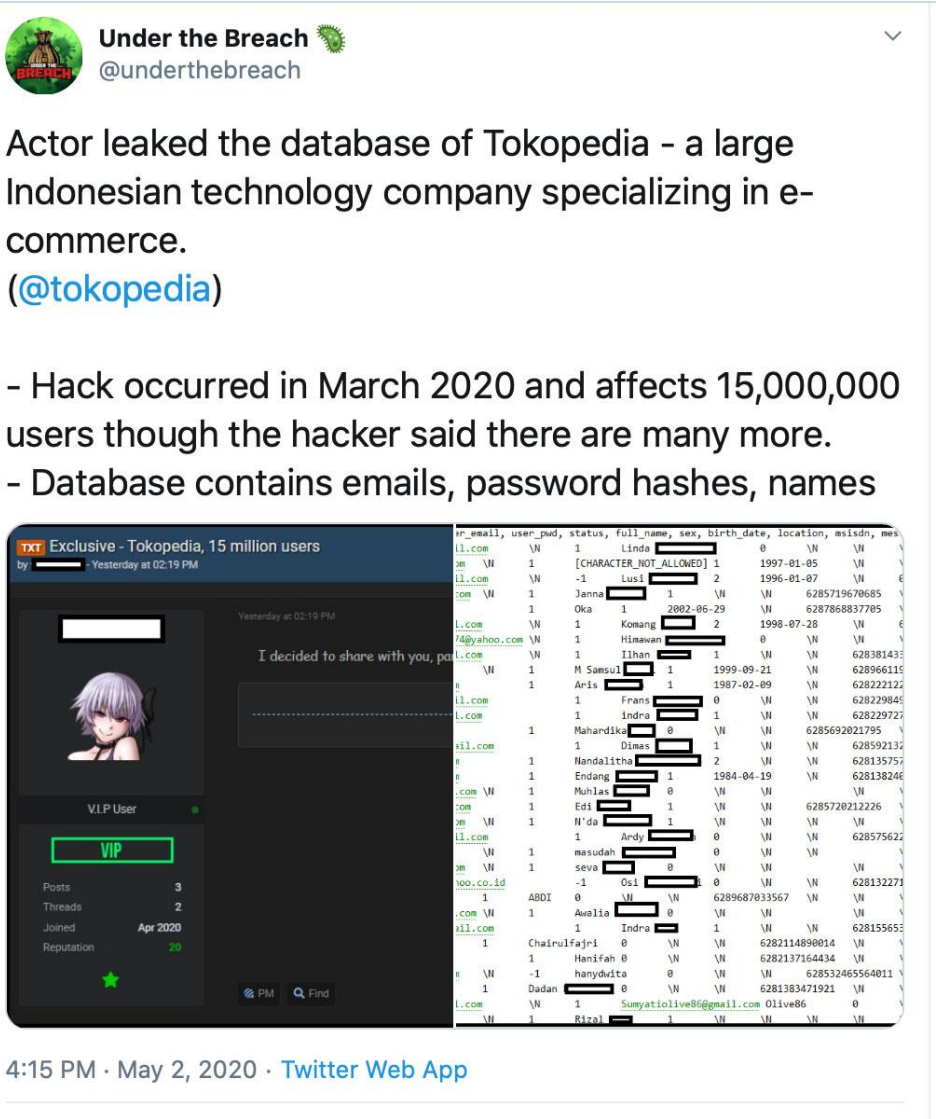
Julian Assange, salah satu pendiri situs WikiLeaks.

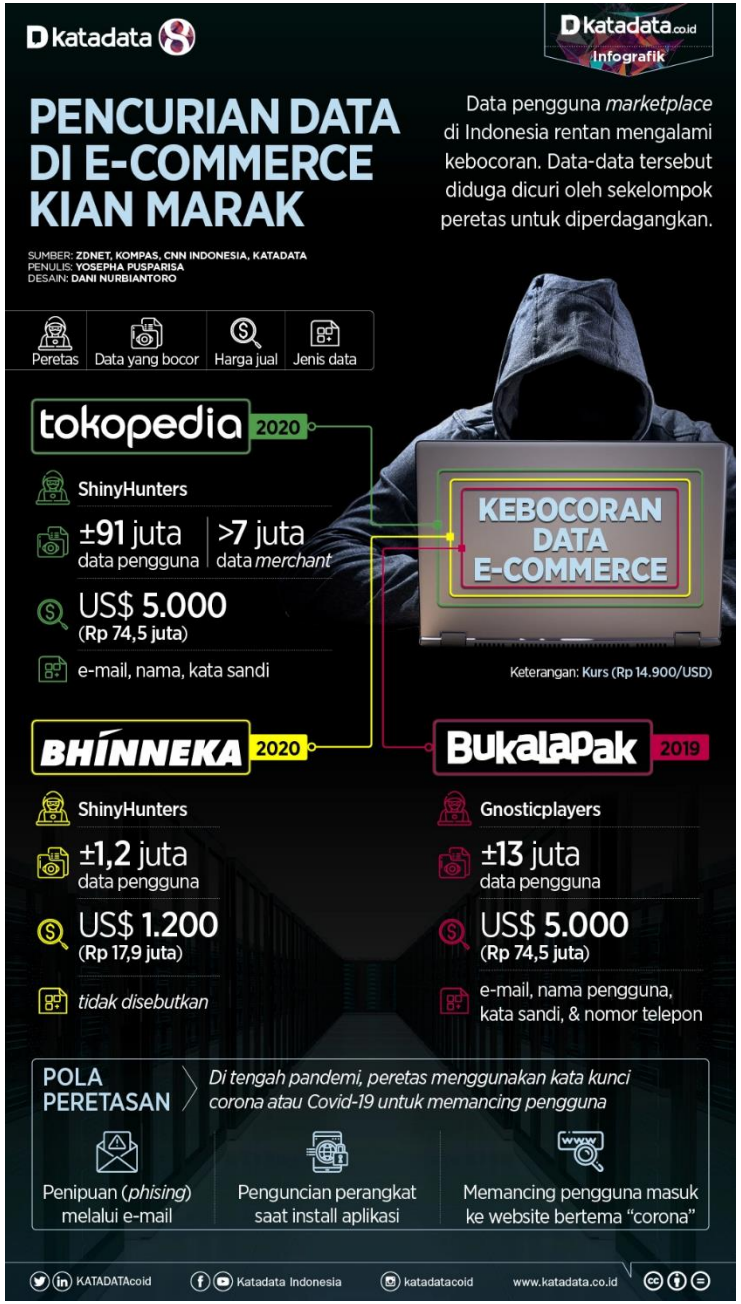


- **Kebocoran data BPJS**

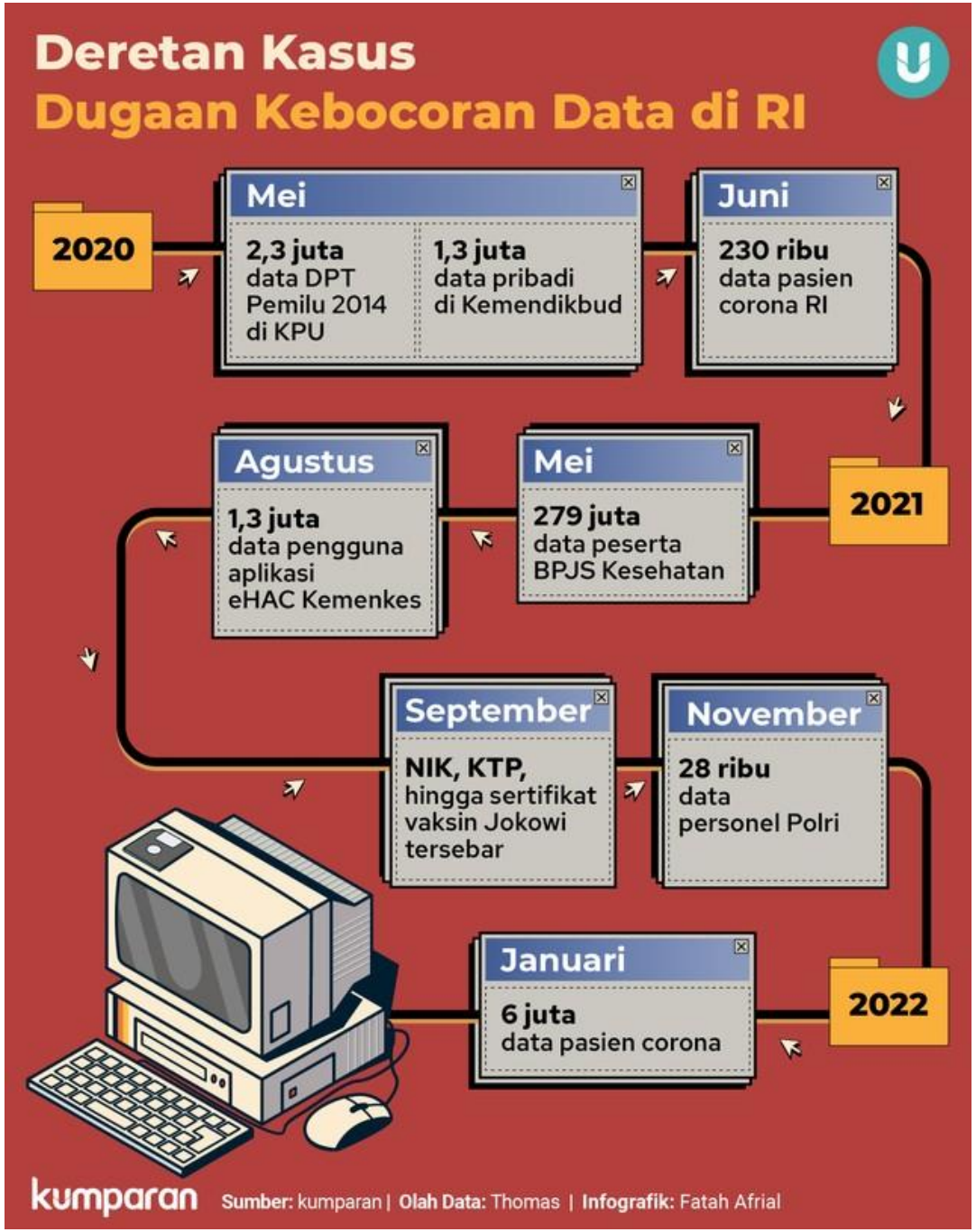


- **Kebocoran data penguna Tokopedia**





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



…dan masih banyak lagi

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

  menunjukkan pentingnya menjaga keamanan data dan informasi.

- Data dan informasi yang bersifat rahasia harus dijaga dari pembacaan dan pengubahan dari pihak-pihak yang tidak berhak (tidak memiliki otoritas).

- Solusinya adalah menggunakan **KRIPTOGRAFI**

Kriptografi

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

- 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*)

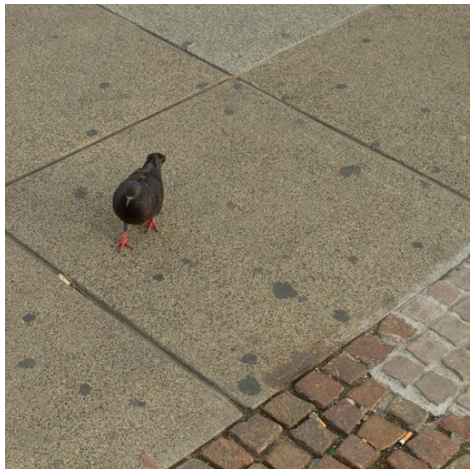
Ketika saya berjalan-jalan di pantai, saya menemukan banyak sekali kepiting yang merangkak menuju laut. Mereka adalah anak-anak kepiting yang baru menetas dari dalam pasir. Naluri mereka mengatakan bahwa laut adalah tempat kehidupan mereka.

(a) Plainteks (teks)

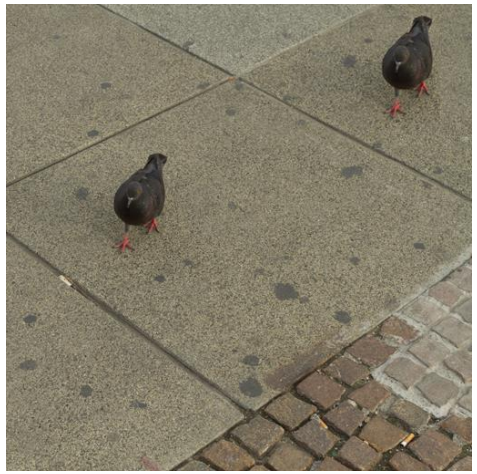
Ztãxzp/épëp/qtüyp{p}<yp{p}/sx/□p}
âpx;pêp/|t}t|äzp}/qp}êpz/étzp{x/z
t□xâx}v□□êp}v/|tüp}vzpz/|t}äyä/{p
ääâ=/\tützp□□psp{pw/p}pz<p}pz/zt□x
âx}v/êp}v/qpüä□□|t}tâpé/spüx/sp{p
|/□péxü=/]p{äüx□□|ttüzp/|t}vpâpzp
}/qpwăp/{päâ/psp{pw□□ât|□pâ/ztwxs
ä□p}/|tützp=

(b) Cipherteks dari (a)

2. Terjaga keasliannya (*data integrity*)

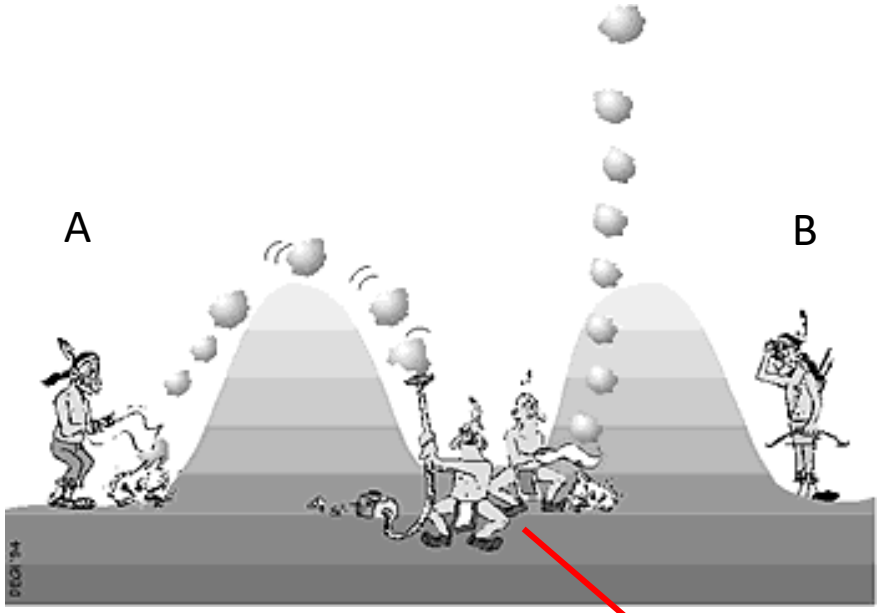


Pesan asli



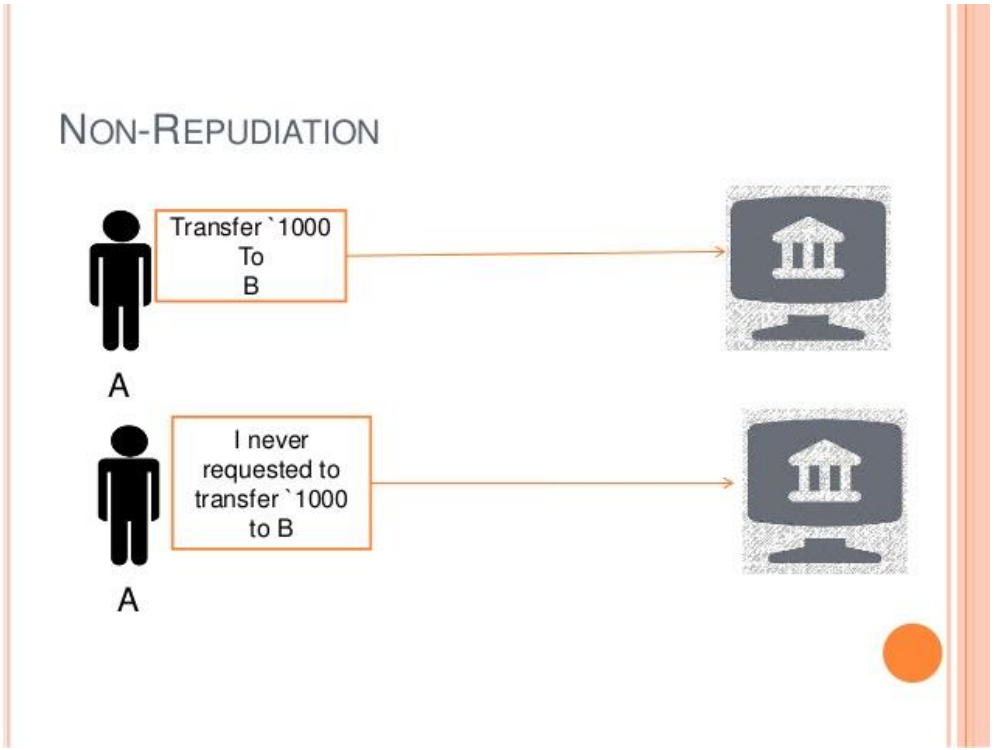
Pesan sudah diubah

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



Dia mengklaim bahwa dia adalah *A*

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

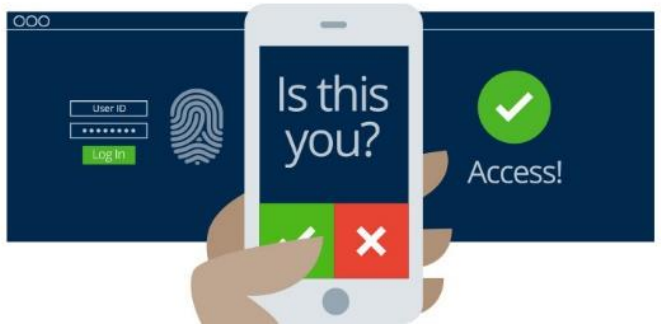


Empat Layanan Kriptografi

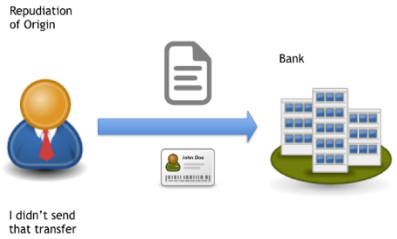
1. Kerahasiaan pesan (*Confidentiality/privacy/secrecy*)

2. Keaslian pesan (*Data integrity*)

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



4. Anti penyangkalan (*Non-repudiation*)



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*)

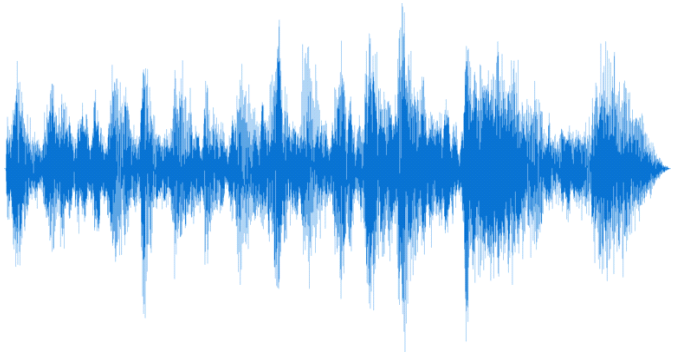
   Rupa pesan: teks, gambar, musik, video, tabel, daftar belanja, gambar 3D, sinyal control, dll

(a) Teks

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

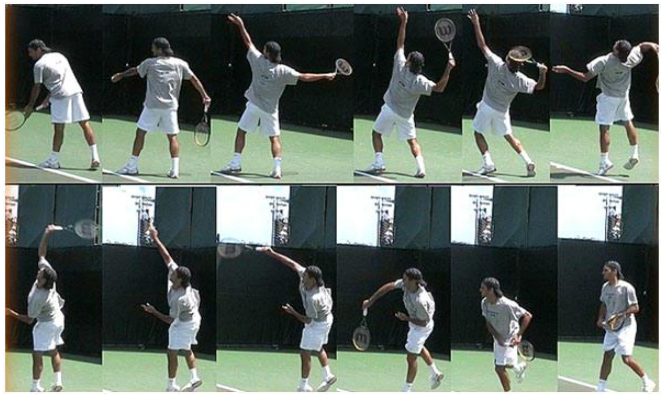
(b) Gambar

(c) Audio



Sumber: http://cloudinary.com

(d) Video



Sumber: http://www.engineersgarage.com

TABEL PENJUALAN

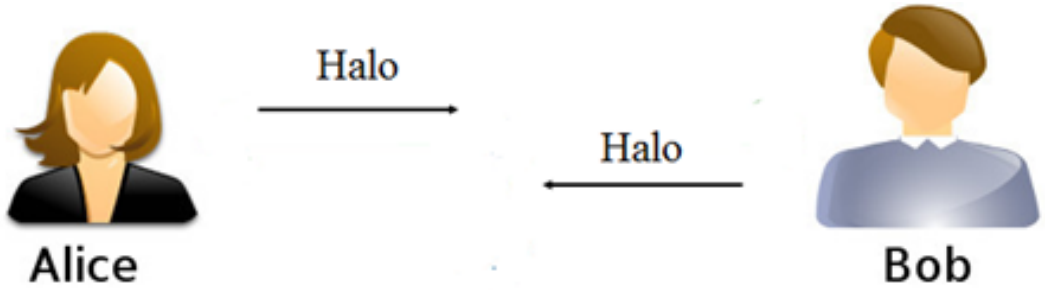
No	Nama sales	Jan	Feb	Item	Total
1	edi	95	65	Monitor	160
2	edo	65	52	Speaker	117
3	danu	98	57	PDA	155
4	didi	57	36	Printer	93
5	barra	84	98	Printer	182
6	hery	51	29	PDA	80
7	rio	19	97	Speaker	116
8	juni	66	47	Monitor	113
9	lala	16	36	PDA	52
10	endang	47	100	Printer	147
11	andi	99	69	Monitor	168
12	yudi	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*)

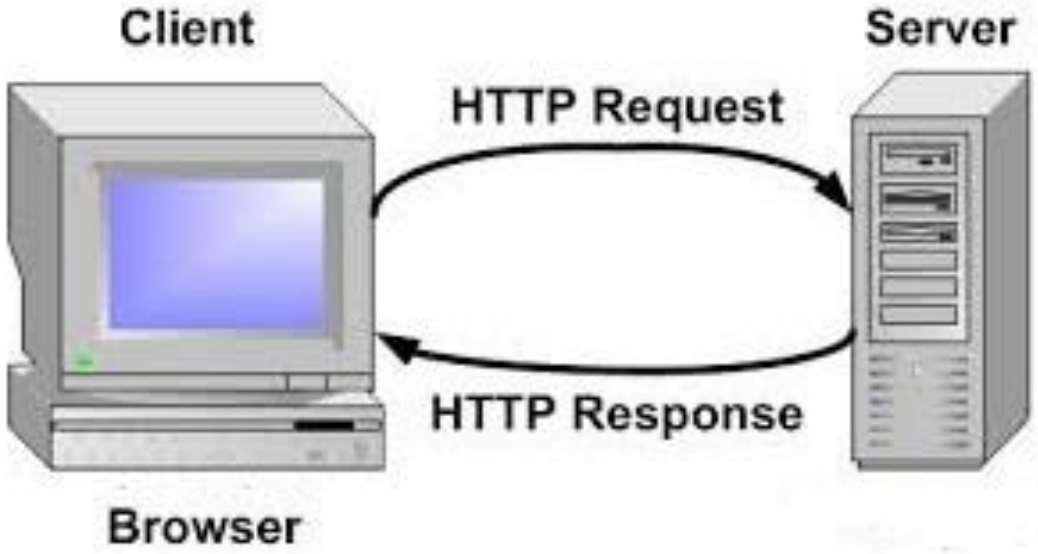
Pengirim: pihak yang mengirim pesan

Penerima (*receiver*): pihak yang menerima pesan

- Di dalam kriptografi, pengirim pesan ditokohkan sebagai Alice dan penerima pesan ditokohkan sebagai Bob.



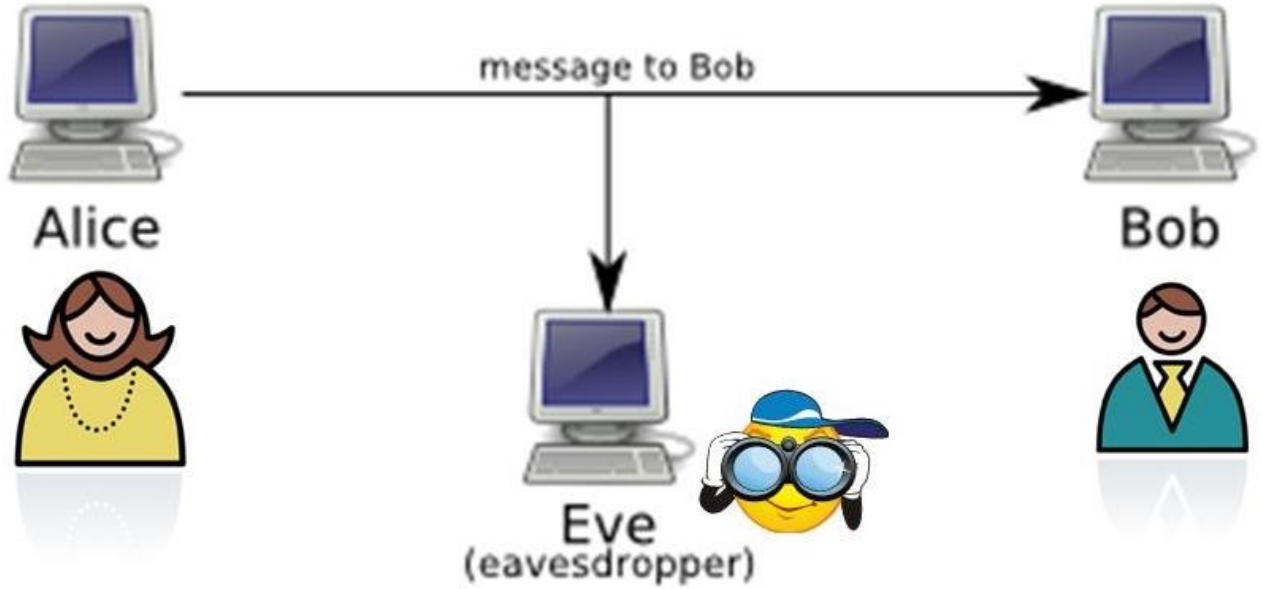
- Alice dan Bob di dalam dunia nyata bisa berupa
  - Alice dan Bob riil manusia sebenarnya
  - web browser/server di dalam transaksi elektronik
  - online banking client/server
  - DNS server, router, mesin penjawab telepon, dsb



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

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: **kriptogram** (*cryptogram*)

- Contoh:

  Plainteks: `culik anak itu jam 11 siang`

  Cipherteks: `t^$gfUi89rewoFpfdWqLMp[uTcxZ`

  Kriptogram: `t^$gfU, i89rewo, FpfdWqLM, p[uTcxZ`

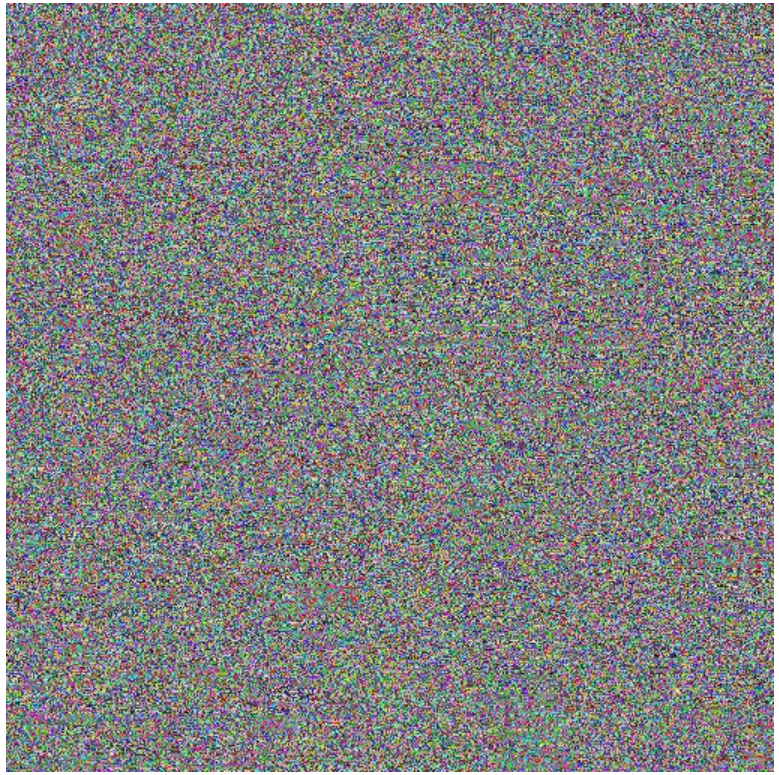
Plainteks:

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:

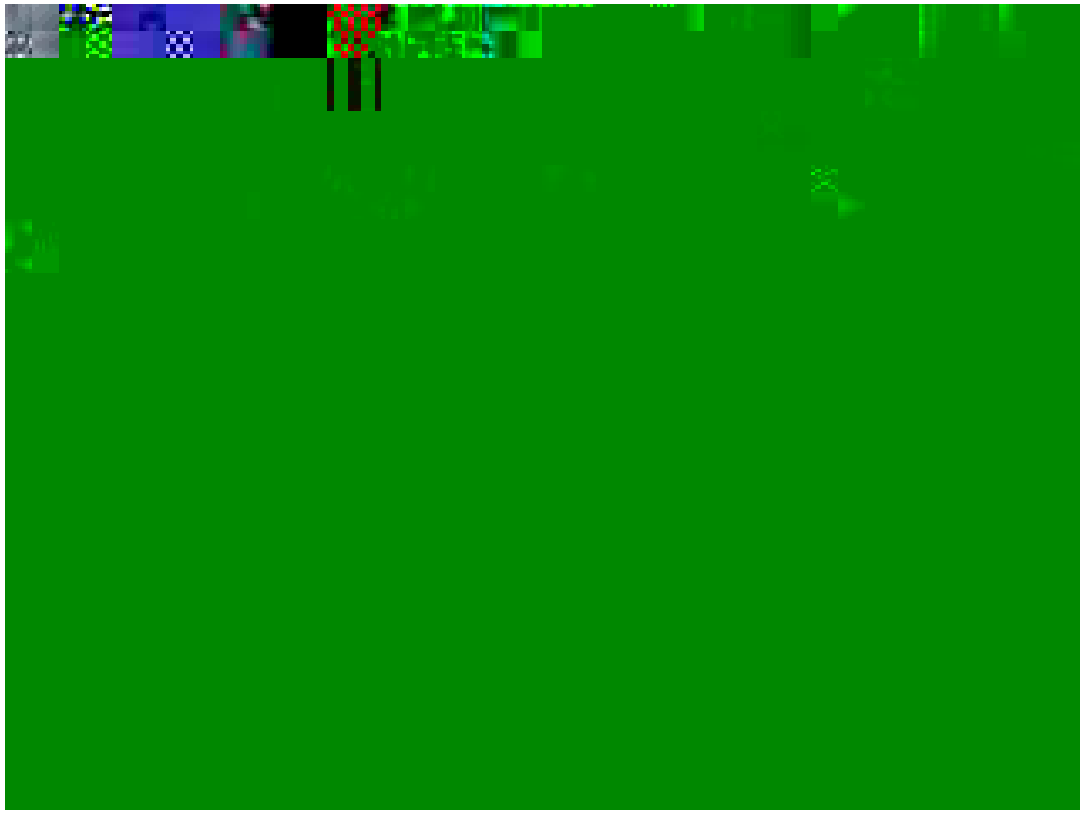
HAWFHZDOHAHANGOMKLGFCVWFLBOCPRKFGNHOFNIN
SPGNLHMPFVBEFWMVFWTBWRHSFZRWKFQMVHPAFWIK
DOHAHANGPFEWNFPFNKLHMPFGLBAMGFCXKFQMOCFV
AVKANIAVHSFZRNCODGAFOHYUVGWFOFGFXEGFMLFWIT
HEFWTBVCPAYQOBLHMPFVBPVADOVWGNFWOCKARVKA
RQOBRGGFFWCHFVGVYUDORVGVYCFWABAPVSVGCHGCI
DRFIFHBAPVQRVOCKAFWSGHSNIHSOBDHFVNGFWDGRGF
WGNHANFCVIDGSWZ

Plain-image



Cipher-image

Plain-video



Cipher-video

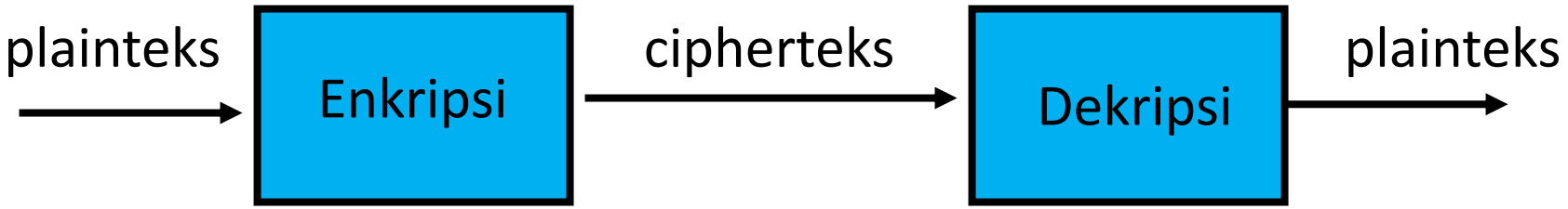
5. **Enkripsi** (*encryption*) dan **dekripsi** (*decryption*)

- Enkripsi: proses menyandikan plainteks menjadi cipherteks.

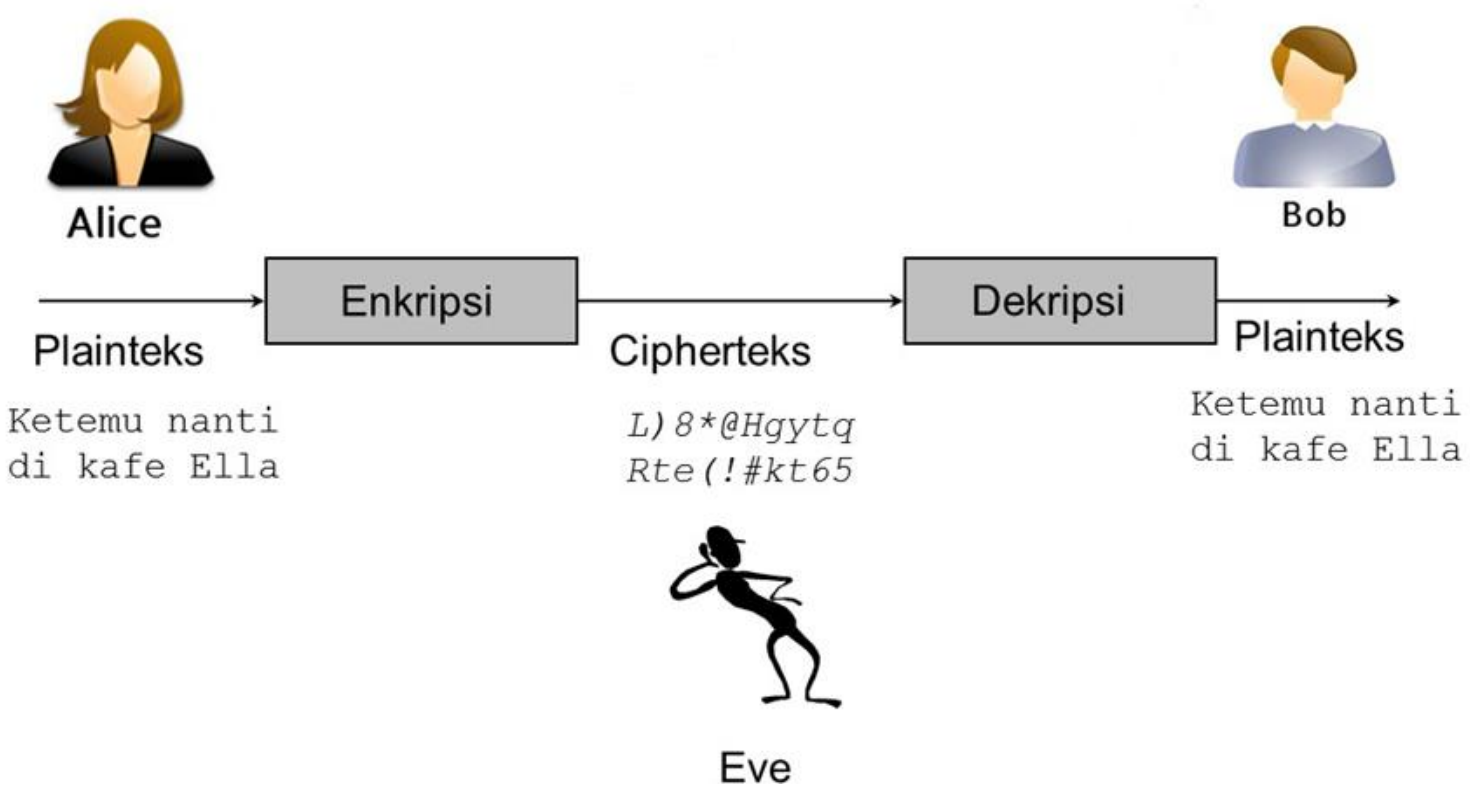
  Nama lain: *enciphering*

- 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

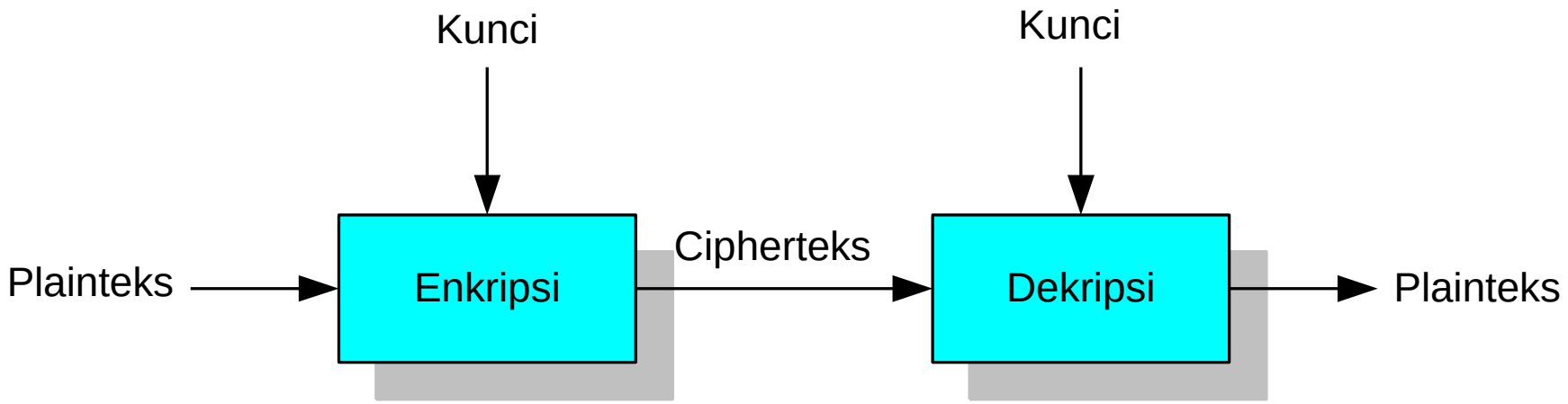


6. Kunci

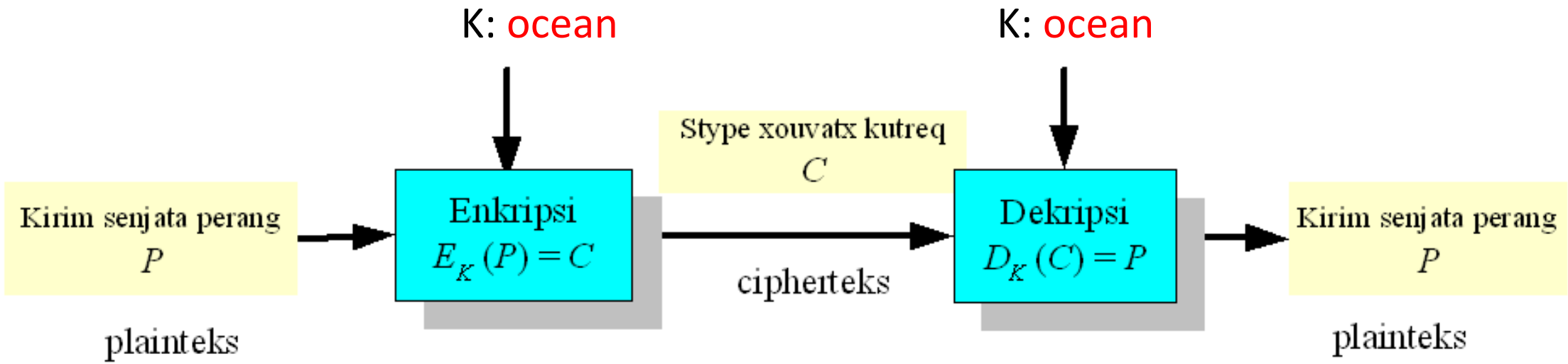
- Agar enkrpsi dan dekripsi hanya dapat dilakukan oleh dua pihak yang berkomunikasi, maka diperlukan **kunci** rahasia.

- Kunci adalah parameter yang digunakan di dalam enkripsi dan dekripsi
  Simbol: K (K dapat berupa integer, string, alphanumeric, dsb)

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



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


K: ocean
K: ocean
Kirim senjata perang
P
plainteks
Enkripsi
$E_K(P) = C$
Stype xouvatx kutreq
C
cipherteks
Dekripsi
$D_K(C) = P$
Kirim senjata perang
P
plainteks

7. *Cipher*

- Algoritma untuk enkripsi dan dekripsi pesan
- Aturan (rule) untuk *enchipering* dan *dechipering,* 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)

$E(p) = (p + k) \bmod 26$ (fungsi matematika)

$D(c) = (c - k) \bmod 26$ (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: $C \times \mathcal{K} \rightarrow \mathcal{M}$

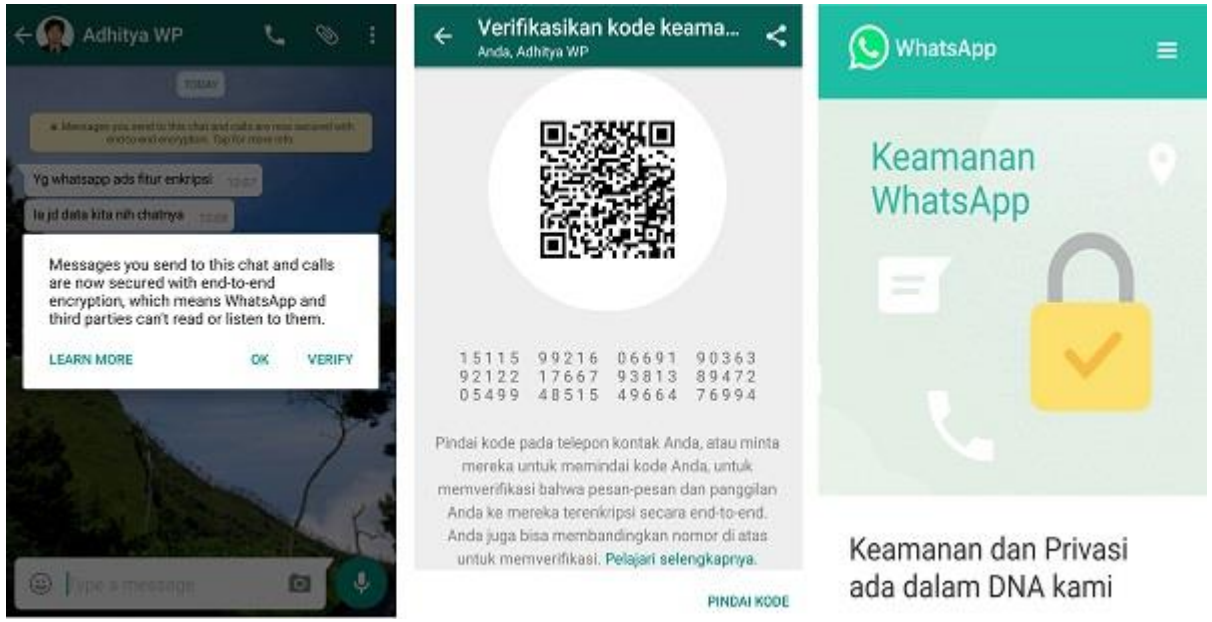
Contoh: Caesar cipher (ingat kembali materi di dalam kuliah Matdis ☺)

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

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*.

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□□ □]Hlm;□□□□A□□□□□ □ A□□□ A□□□□ N□□□□□A □□□ N□□ G□ □ OG,□ □□□ A□□ □ jk□ □□ □ N□□ G□□□H□□□E□ □G □□ □□□E□ □□N□□□□ □□□ □A□ □S□□ □□□ □G2*I~b2*1BE□ □G2#$]−

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

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**.

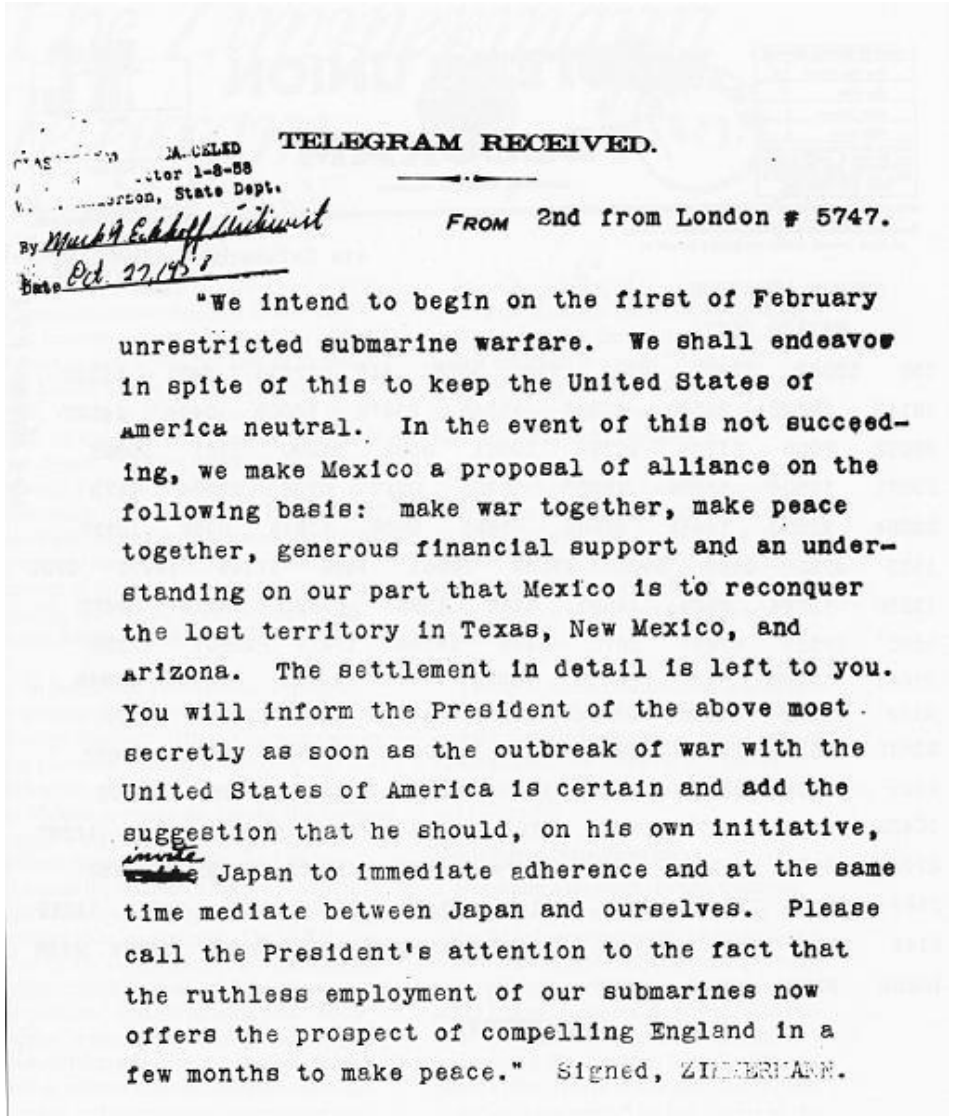
- Al-Kindi menulis buku tentang seni memecahkan kode, buku yang berjudul '*Risalah fi Istikhraj al-Mu'amma* (*Manuscript for the Deciphering Cryptographic Messages*)

- 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

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.

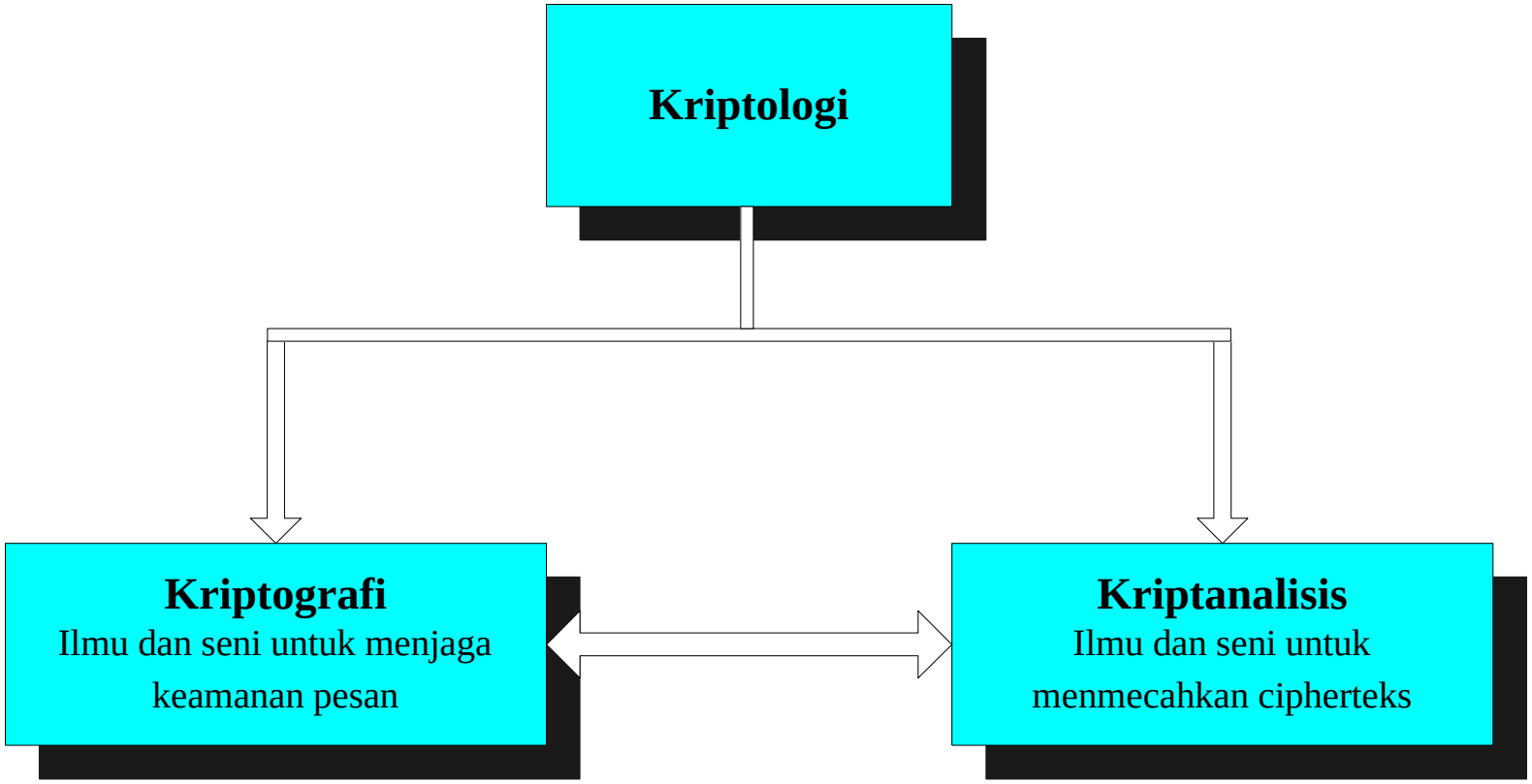
FROM 2nd from London # 5747.

"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, ZIMMERMANN.

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

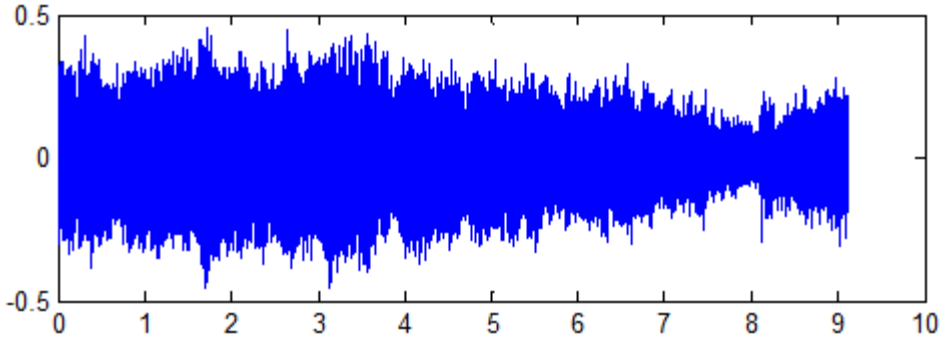
Modern Cryptography

- 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

2. Audio



3. Gambar (*image*)

4. Video

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

Kriptografi pada zaman Mesir Kuno

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

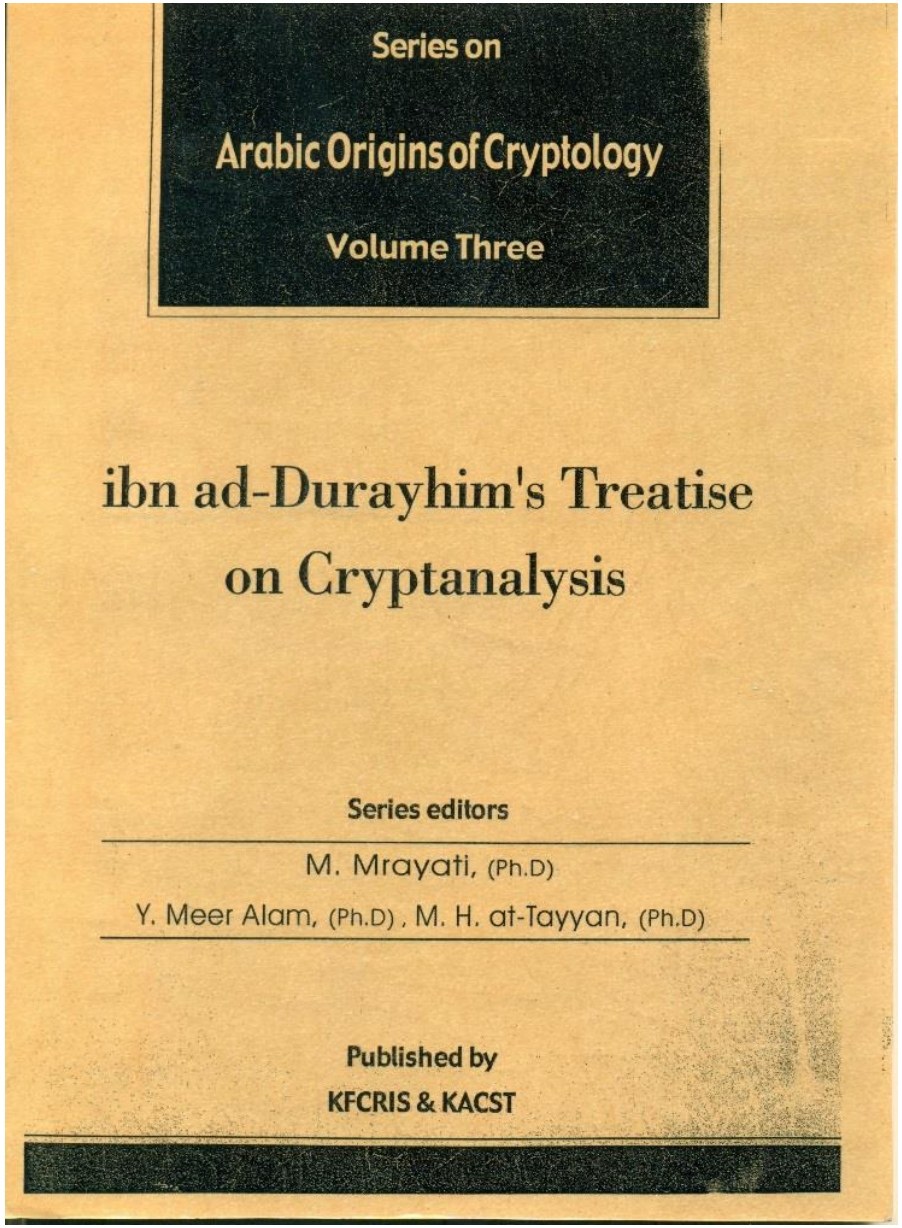
Kriptografi pada Zaman Yunani dan Romawi Kuno

- 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 cryptanalysis.
(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 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 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 (sebuah cipherteks yang isinya rencana membunuh Ratu Elizabeth I) pada Abad Pertengahan berhasil dipecahkan oleh Thomas Phelippes, seorang pemecah kode (*codebreaker*).

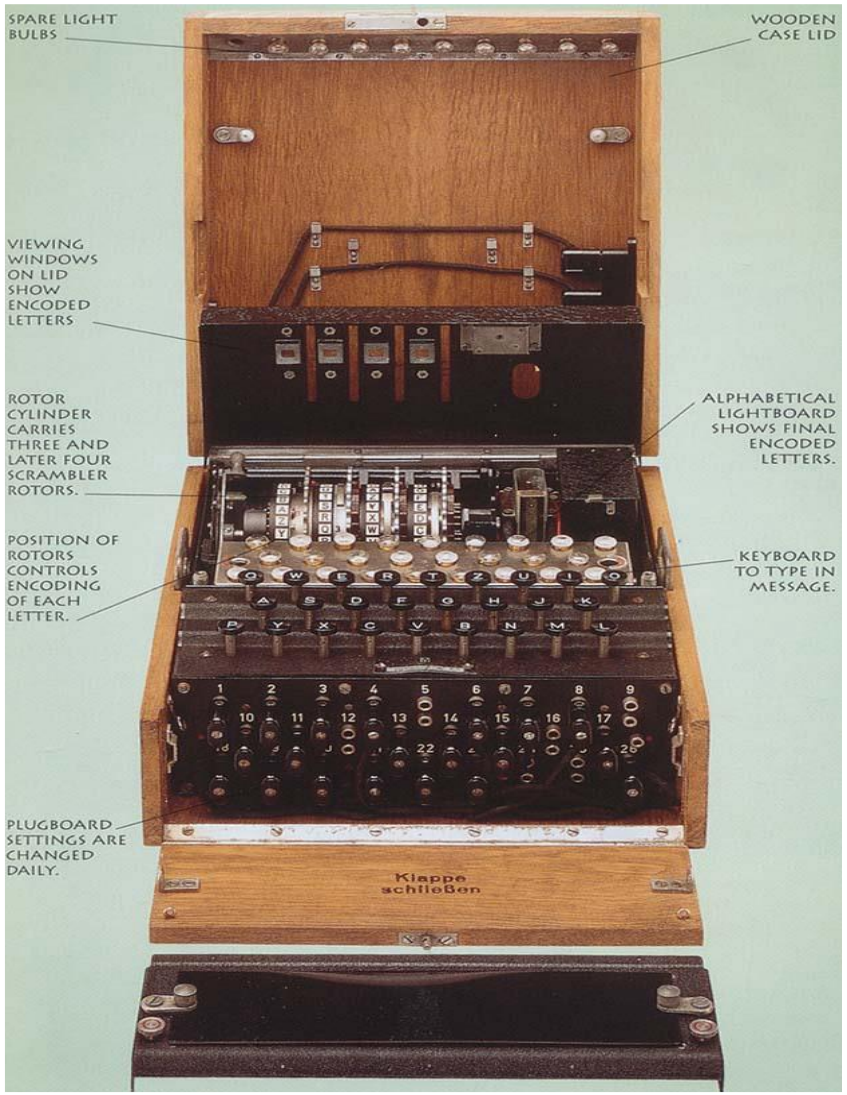
Queen Mary

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

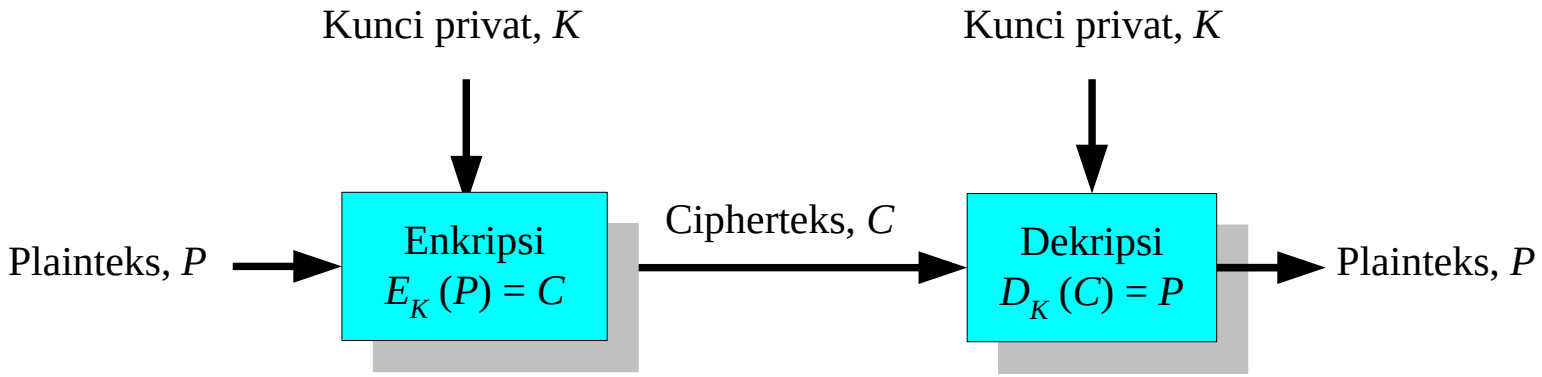


Enigma

Tiga (3) Jenis Algoritma Kriptografi

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

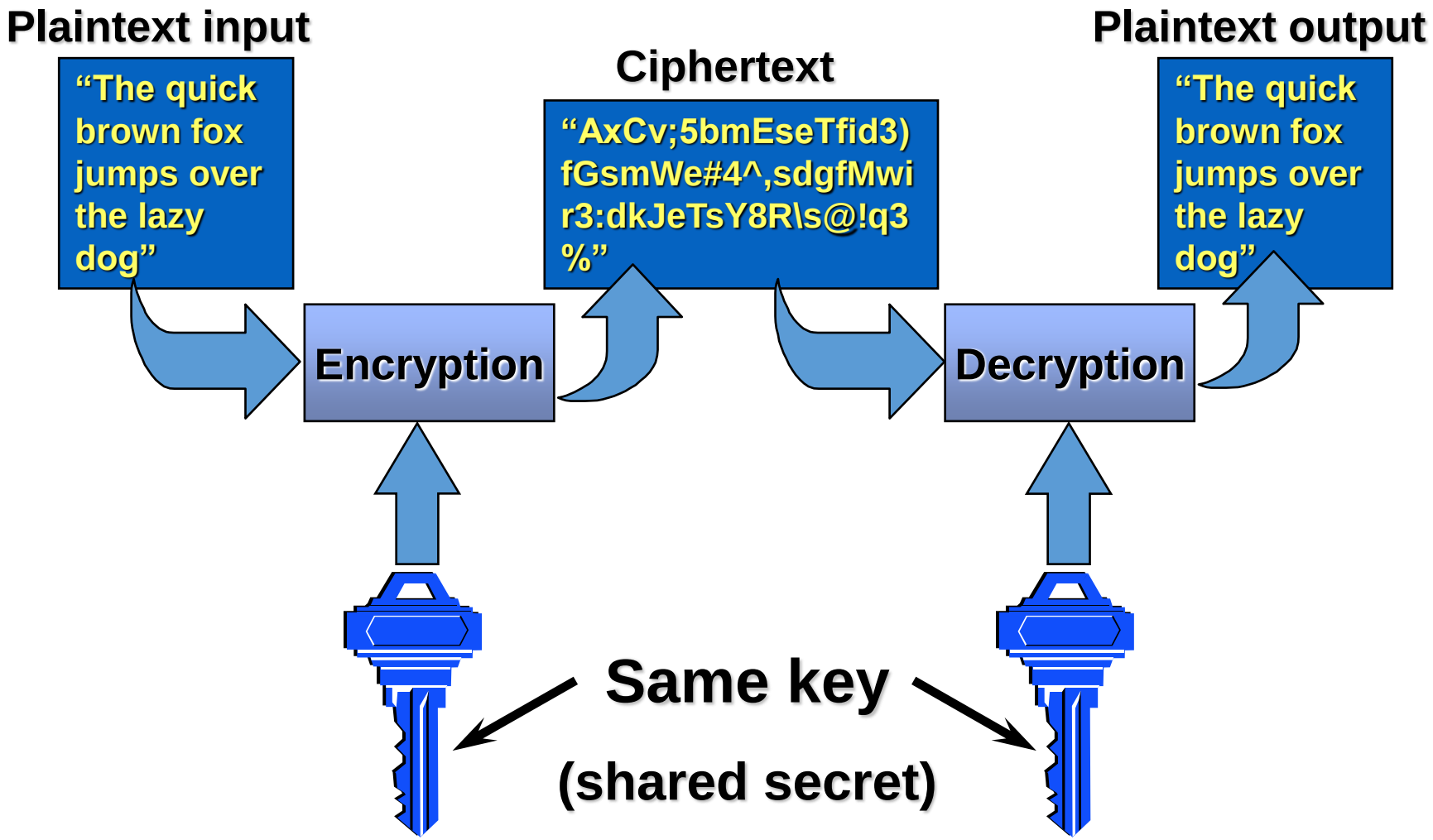
- Kunci enkripsi = kunci dekripsi, harus dijaga privat (rahasia) atau *secret*
- Sudah ada sejak ribuan tahun yang hingga tahun 1976



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

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

- FEAL
- RC4
- SEAL
- Panama
- dll



Sumber: Cryptography in E-Commerce

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

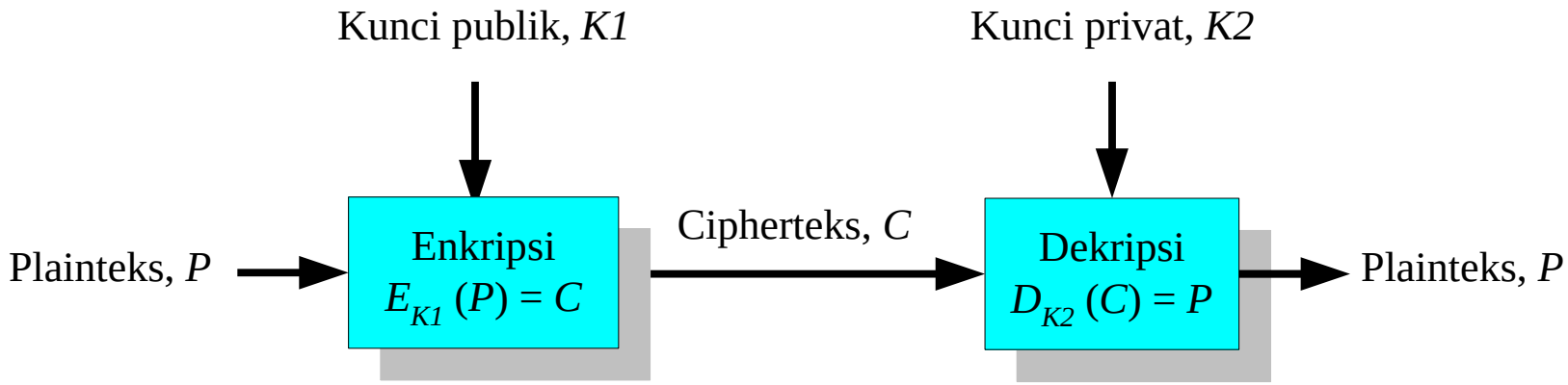
- Kunci enkripsi ≠ kunci dekripsi (K1 ≠ K2)

  Kunci enkripsi → tidak rahasia (*public key*)

  Kunci dekripsi → rahasia (*private key*)

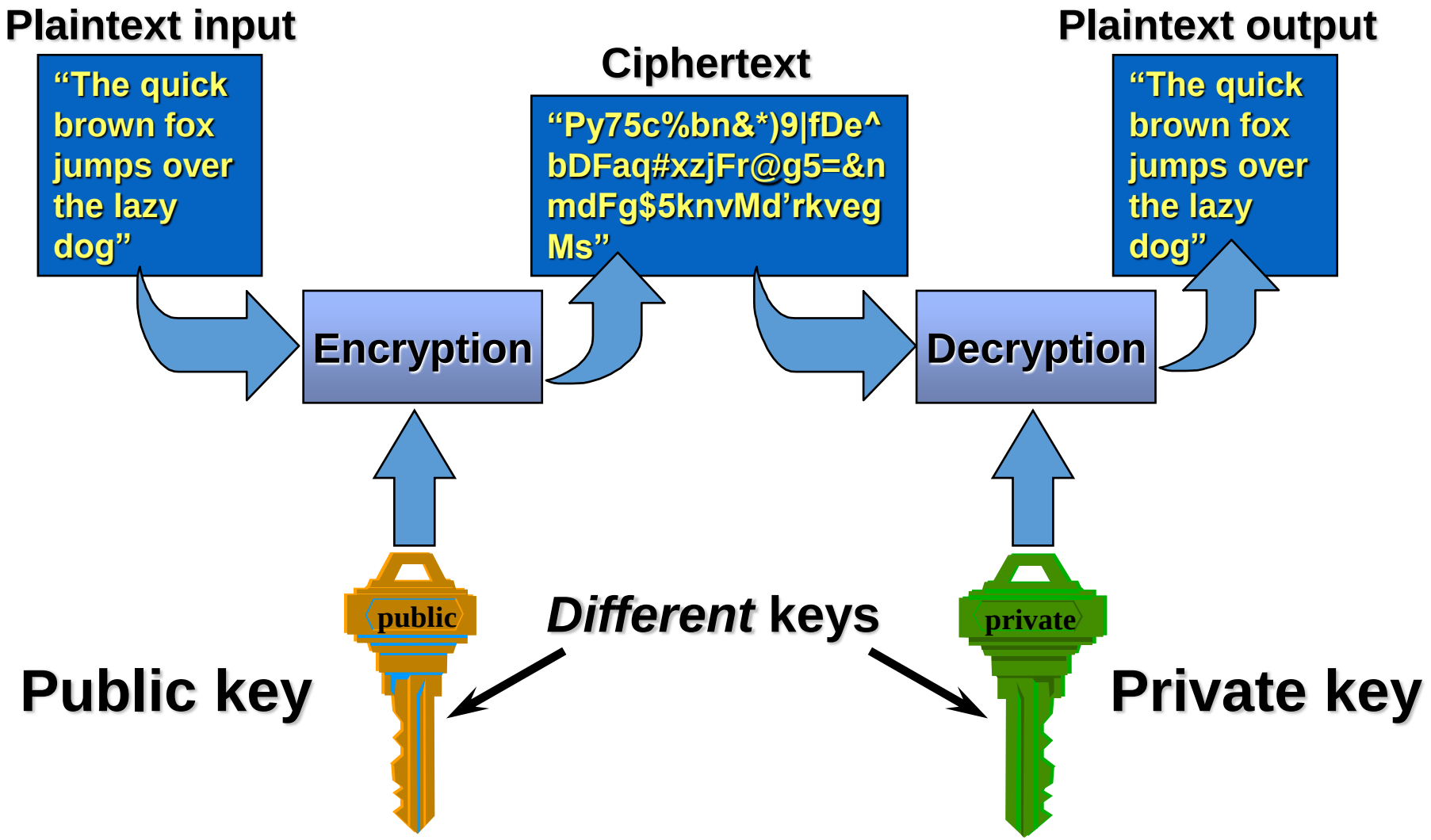
- Mulai ditemukan sejak tahun 1976

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



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

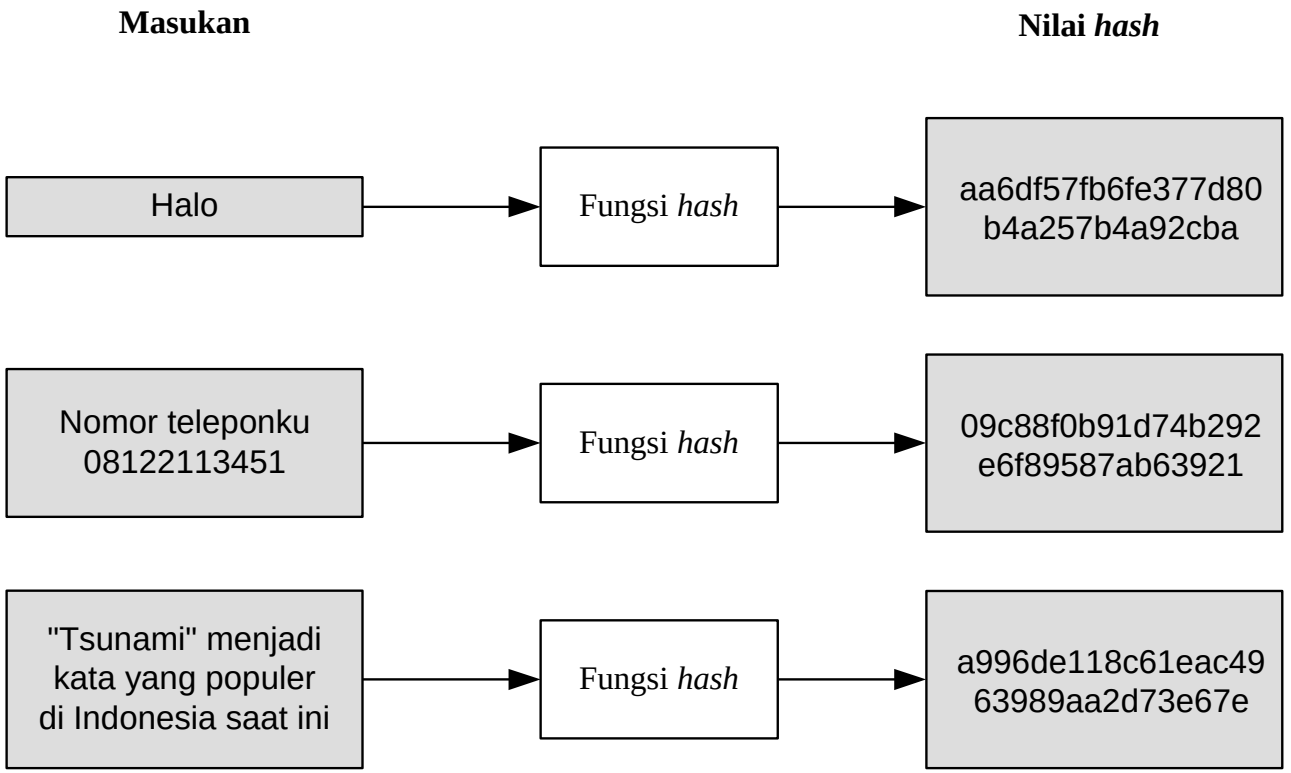
- Rabin
- EPOC
- Mc Eliece
- XTR
- ECC (*Elliptic Curve Cryptography*)



Sumber: Cryptography in E-Commerce

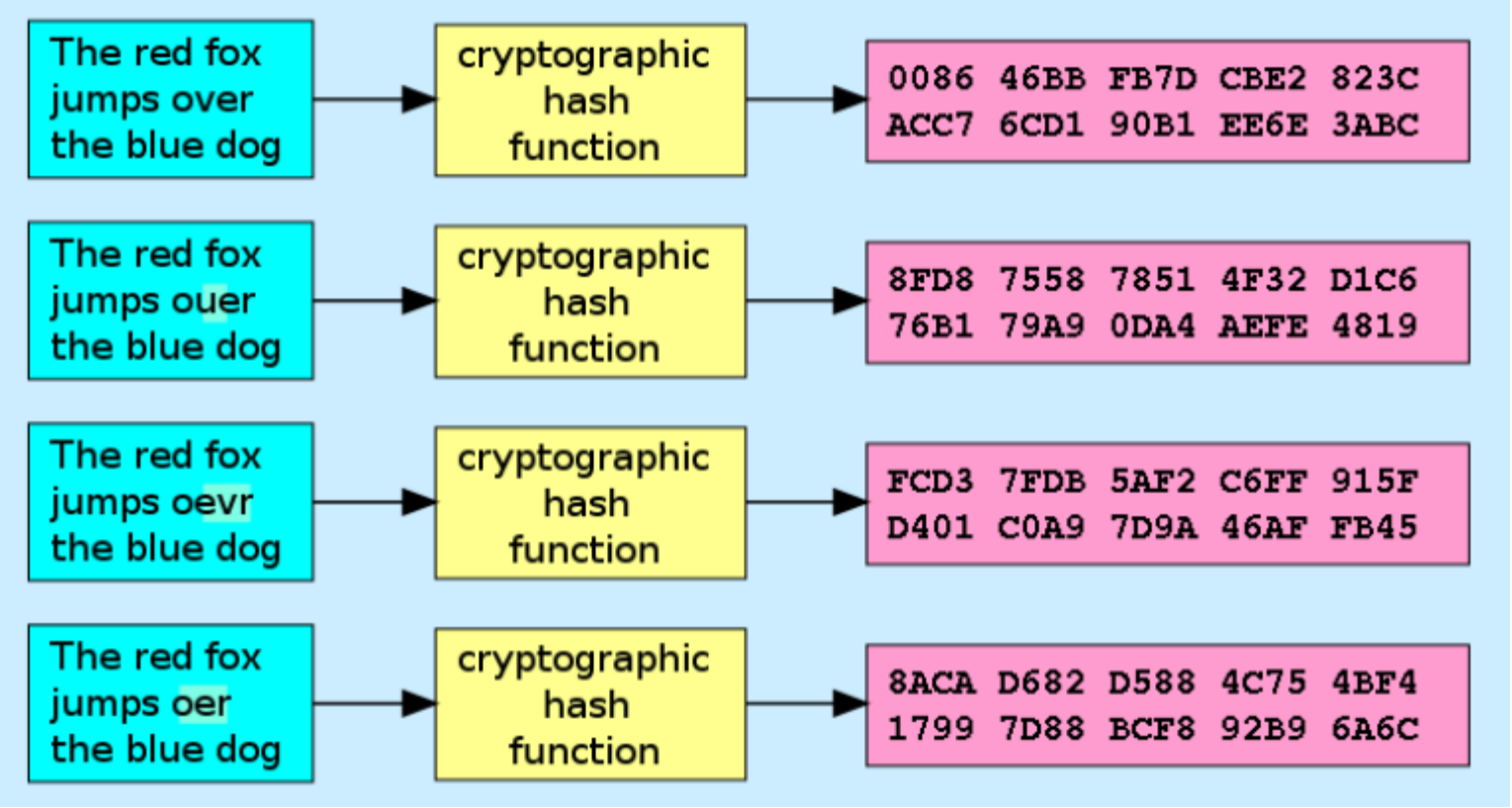
3. Fungsi Hash

- 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)

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