Departemen Teknik Komputer
Universitas Diponegoro
2023

KRIPTOGRAFI B

Kriptografi & E-commerce 1

Presented by : Bellia Dwi Cahya Putri, S.T., M.T

RPS

Dapat memahami hubungan antara Kripto-grafi dan *e-Commerce*
Dapat menjelaskan Aplikasi kriptografi dalam *e-commerce,* Dapat memahami konsep dan fungsi, serta dapat mengerjakan soal-soal yang berkaitan dengan Tanda tangan digital*,* tanda tangan buta*,* Kontrak Digital*,* Sertifikat Digital*, dan* Protokol SET untuk transaksi dengan kartu kredit

Mgu ke -	Topik pembahasan
1	Kontrak Perkuliahan; Pendahuluan tentang Kriptografi; Kriptografi Kunci Rahasia dan Kunci Publik
2	Algoritma Kriptografi Klasik 1 (Caesar Cipher, Vigenere Cipher, Matrix Encryption, dan Vernam Cipher)
3	Algoritma Kriptografi Klasik 2 (Sandi Affine, Sandi Hill, Sandi One-Time Pad, Sandi Rotor)
4	Block Cipher (ECB, CBC, CFB, OFB, dan Feistel Cipher)
5	Enkripsi RSA (Rivest-Shamir-Adleman), pembangkitan kunci, dan dekripsinya
6	Enkripsi El-Gamal dan Rabin-Williams Cryptosystem
7	Data Encryption Standard (DES)
8	Advanced Encryption Standard (AES)
9	Steganografi: Sejarah dan Teknik-tekniknya
10	Kriptografi dan Fungsi Hash Satu Arah (One-way Hash)
11	Algoritma Message Digest-5 (MD5)
12	Kriptografi dan E-Commerce 1 (Kontrak Digital, tanda tangan digital, dan Blind Signature)
13	Kriptografi dan E-Commerce 2 (Sertifikat Digital dan Pembayaran Menggunakan Kartu Kredit)
14	Keamanan Data dan Komputer; Kapita Selekta Kriptografi

Topik

- Review Kriptografi
- E-commerce
- Relasi antara kriptografi dan e-commerce
- Aplikasi kriptografi di e-commerce
- Kontrak digital
- Digital signature
- Blind signature

Review Kriptografi

- Kriptografi

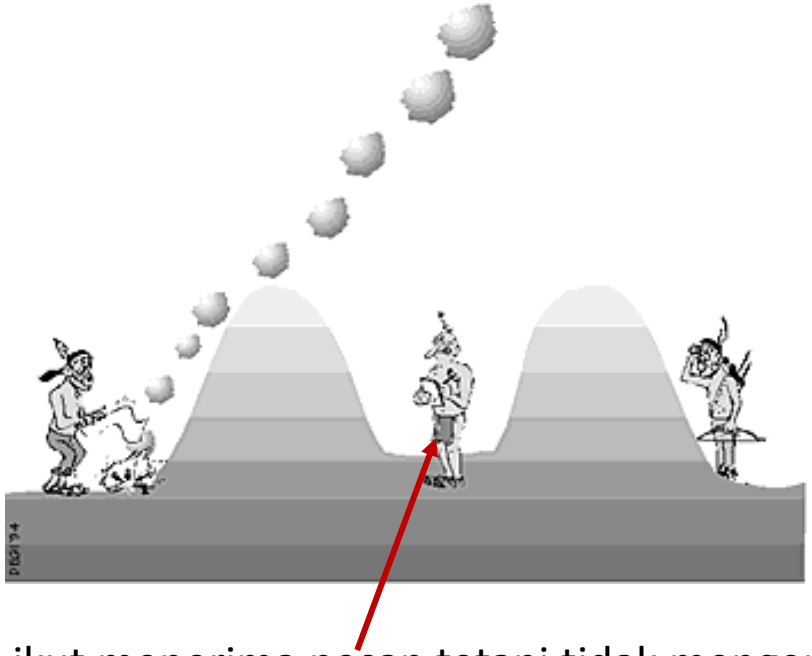
ilmu yang mempelajari bagaimana menjaga agar data/pesan tetap aman saat dikirimkan tanpa mengalami ganggunan dari pihak ketiga

- Semakin banyak aplikasi yang muncul memanfaatkan teknologi jaringan dan ada beberapa yang menuntut pengiriman data yang aman
- Beberapa pengaplikasian kriptografi yang sudah memengaruhi kehidupan manusia antara lain:
  - ATM
  - HP
  - Komputer
  - Internet
  - dsb

- Layanan yang disediakan kriptografi antara lain:

1. Kerahasiaan (confidentiality)

Layanan untuk menjaga isi pesan dari siapapun yang tidak berhak untuk membacanya.

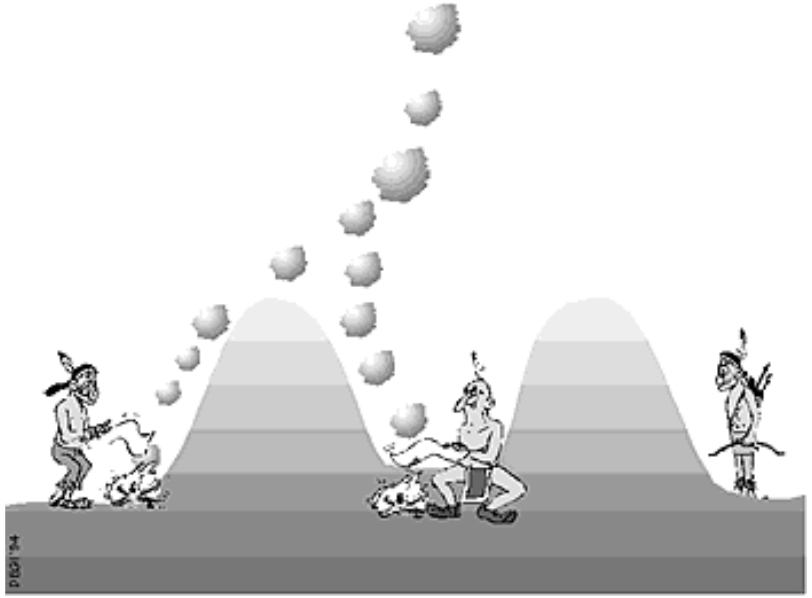


Dia ikut menerima pesan tetapi tidak mengerti

Sumber : Tutun Juhana (EL)

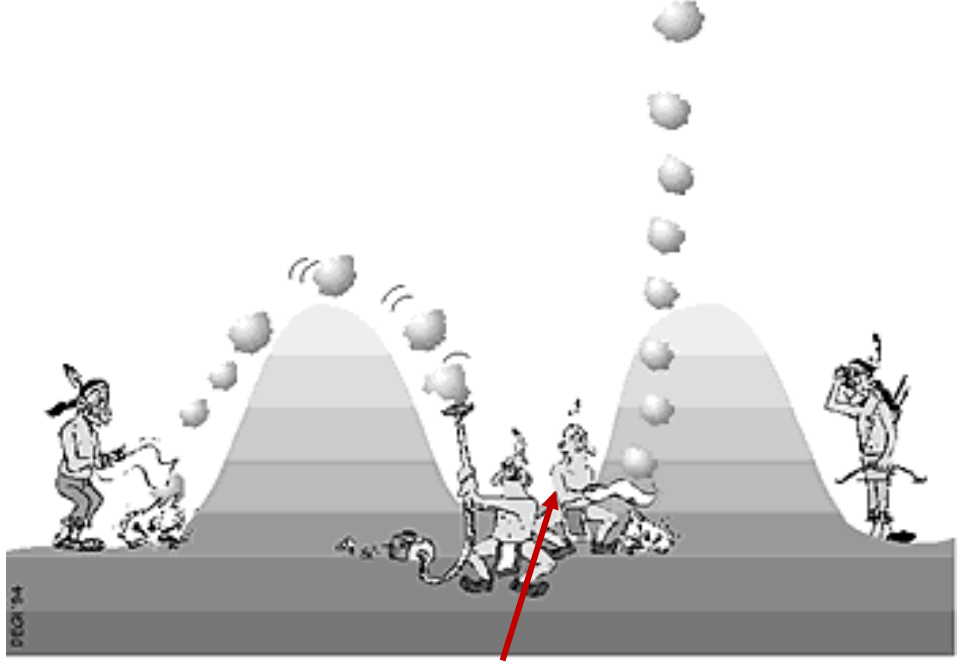
2. Integritas data (data integrity)

Layanan yang menjamin bahwa pesan masih asli/utuh atau belum di manipulasi selama pengiriman



3. Otentikasi (authentication)

Layanan untuk mengidentifikasi kebenaran pihak-pihak yang berkomunikasi dan mengindentifikasi kebenaran sumber pesan. “apakah pesan benar-benar berasal dari pengirim yang benar?”

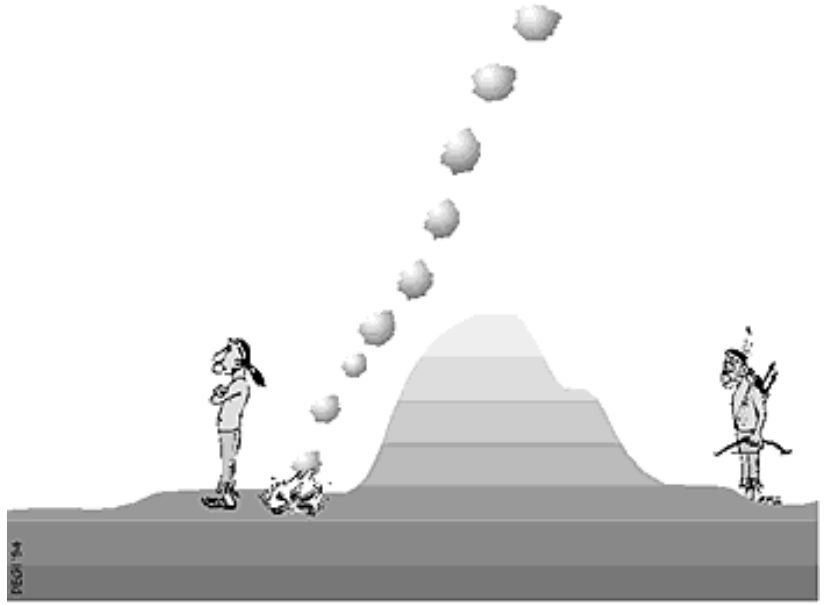


Dia bisa mengkalim kalau dia adalah si pengirim

Sumber : Tutun Juhana (EL)

4. Nir-penyangkalan (Non-repudiation)

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



- Proses utama pada kriptografi → enkripsi dan dekripsi
- Istilah dalam kritpografi → plainteks, cipherteks, enkripsi, dekripsi, kunci, kriptanalis, penyadap (enemy, adversary, intruder, interceptor, bad guy, man-in-the-middle, hacker, cracker, sniffer, dsb)

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

Kriptografi pada zaman Mesir Kuno

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

https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2022-2023/01-Pengantar-Kriptografi-(2023).pdf

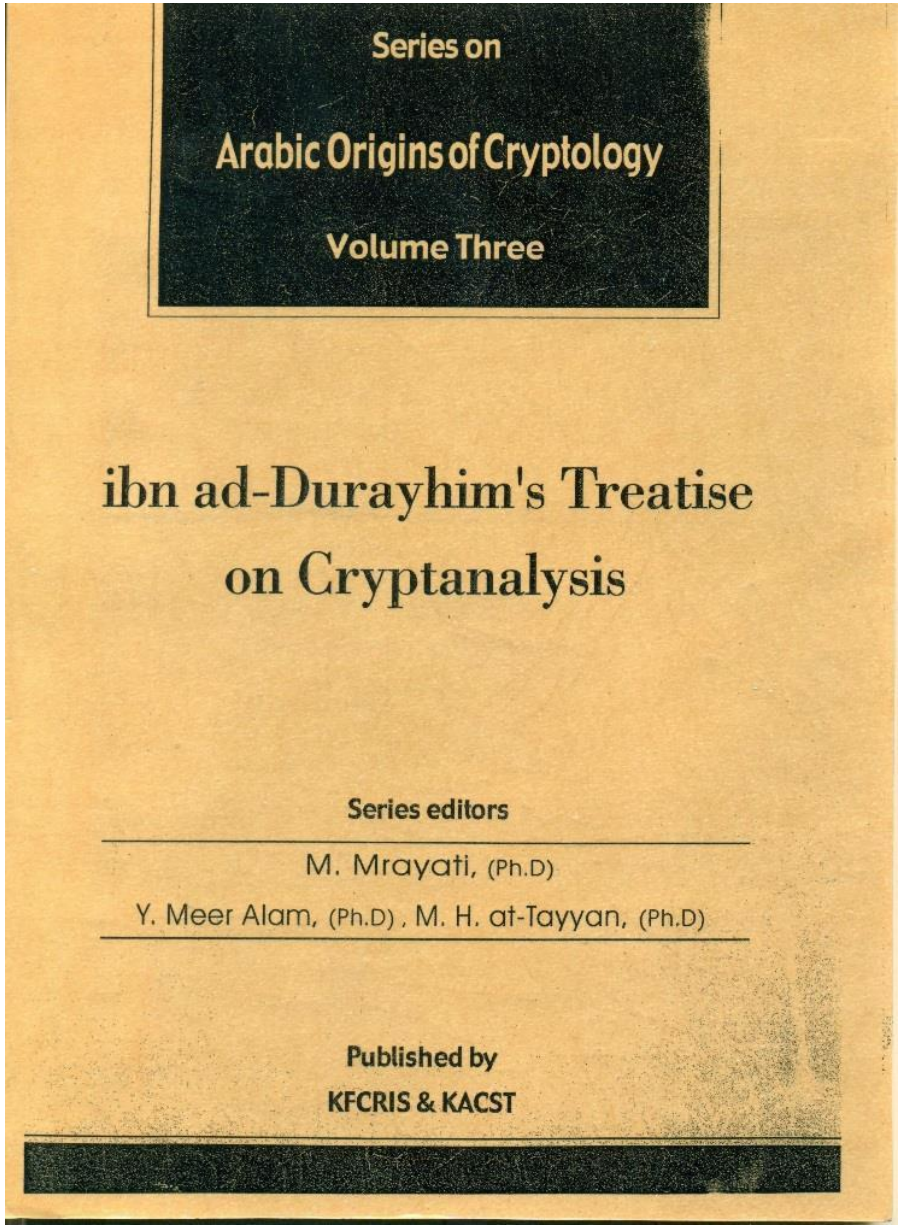
Kriptografi pada Zaman Yunani dan Romawi Kuno

- 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.

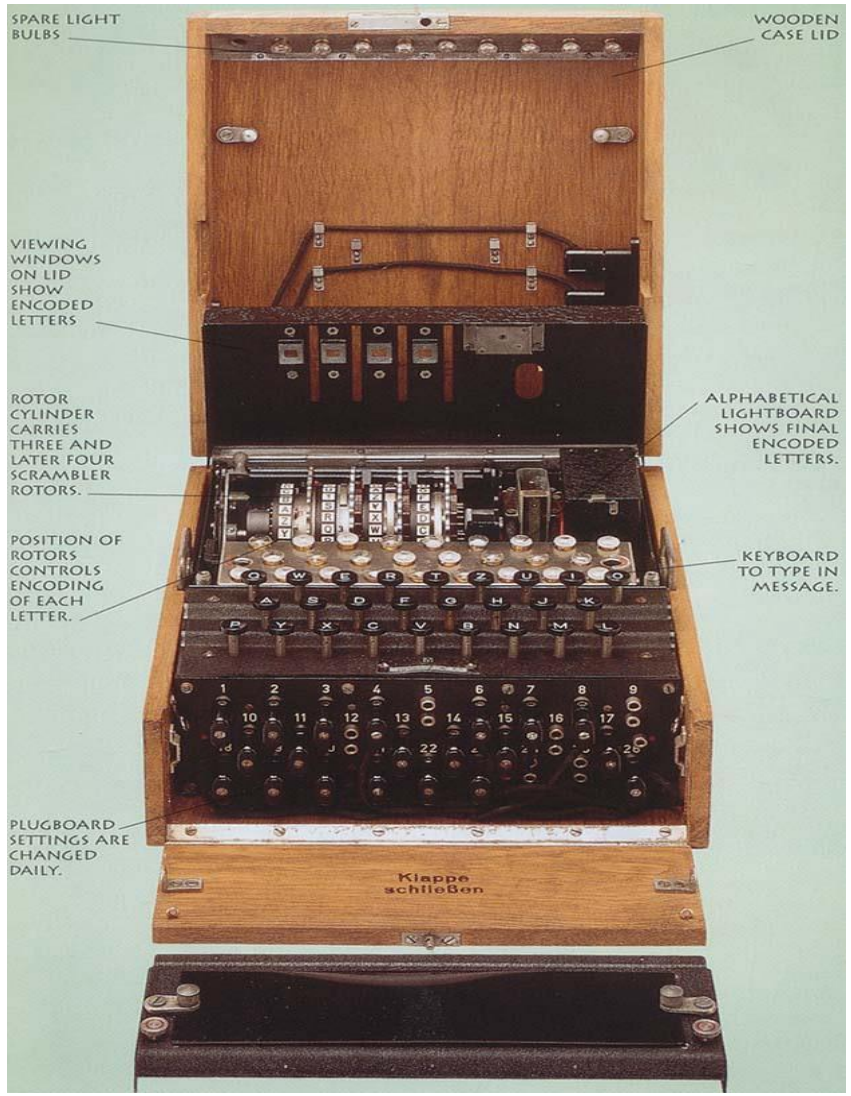
- Pada Abad ke-17, sejarah kriptografi pernah mencatat korban di Inggris.

- 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

E-commerce

- Merupakan model bisnis yang memungkinkan perusahaan atau individu bisa membeli atau menjual barang melalui internet (online).
- Hampir semua produk, termasuk jasa, tersedia di internet dari mulai makanan, musik, buku, produk rumah tangga, tiket pesawat, investasi bisa dibeli lewat e-commerce.

https://money.kompas.com/read/2021/09/11/191943626/pengertian-e-commerce-dan-bedanya-dengan-marketplace?page=all#google_vignette

Relasi kriptografi & e-commerce

- Keberhasilan atau kegagalan operasi e-commerce bergantung pada berbagai faktor, termasuk namun tidak terbatas pada model bisnis, tim, pelanggan, investor, produk, dan keamanan transmisi dan penyimpanan data.
- Keamanan data menjadi concern utama sejak serangkaian serangan "cracker“ terjadi.
- Keamanan adalah pemikiran setiap pengusaha e-commerce yang meminta, menyimpan, atau mengkomunikasikan informasi apa pun yang mungkin bahaya/sensitif jika hilang.
- Salah satu cara paling efektif untuk memastikan keamanan dan integritas data adalah enkripsi.

https://cyber.harvard.edu/ecommerce/encrypt.html

- Jenis enkripsi yang relevan dengan e-commerce:

Encryption type	Description	Common algorithms and uses
Symmetric key	Uses a single key to encrypt and decrypt data.	DES, Triple DES, RC2; used for encrypting large amounts of data.
Asymmetric key	Uses a mathematically related public/private key pair; also known as public key encryption.	RSA enables secure key exchange. Diffie/Hellman explains the concept of key exchange.
One way	A one-way encryption algorithm produces ciphertext that cannot be taken BACK to the original plaintext.	Used for signing data and transactions.
Hash function	A smaller numerical representation of the plaintext.	A hash of a message is encrypted using one way encryption to become the signature for that message.
Applied encryption	Uses a combination of symmetric, asymmetric, and one-way encryption for enhanced security.	Email, credit card encoding, S/MIME and SSL protocols, SETs, payment gateways.

https://www.seotrance.com/ecommerce-implementation/module4/encryption-methods-types.php

KONTRAK DIGITAL, DIGITAL SIGNATURE, BLIND SIGNATURE

Kontrak Digital

- Kontrak elektronik adalah perjanjian yang dirumuskan secara online. Para pihak berinteraksi satu sama lain dalam format digital, bukan secara langsung (kertas&pena) atau melalui telepon
- Undang-undang federal seperti UU ESIGN menjadikan kontrak digital sama mengikatnya dengan kontrak tradisional, namun memerlukan pelacakan dan pencatatan yang tepat.
- Beberapa unsur-unsur penting kesepakatan antara dua individu atau perusahaan untuk menciptakan kewajiban bersama yang mengikat:

1. Komitmen : kedua belah pihak terikat oleh kontrak.
2. Tidak dapat dipalsukan : Tanda tangan kontrak harus dapat dibuktikan keasliannyaTanda tangan kontrak harus dapat dibuktikan keasliannya

- Solusi agar kepercayaan antar kedua pihak semakin kuat, bisa menggunakan pihak ketiga (arbitrator)

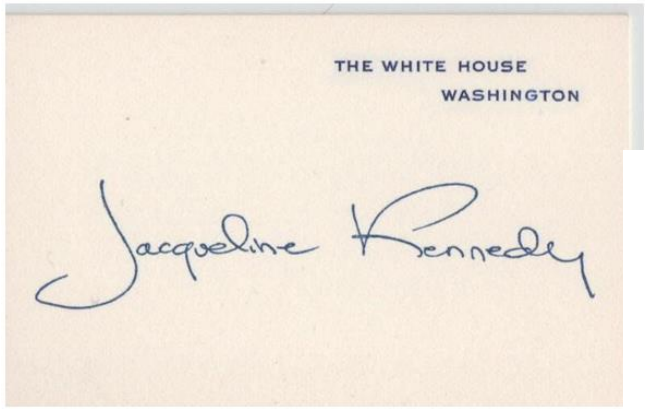
Digital Signature

- Masih ingat 4 layanan kriptografi?

1. Kerahasiaan pesan
2. Integritas/keaslian pesan
3. Otentikasi
4. Anti-penyangkalan

- Layanan 1 dilakukan dengan enkripsi/dekripsi pesan
- Layanan 2 dilakukan dengan fungsi hash
- Layanan 3 dan 4 dilakukan dengan tanda tangan digital (digital signature)

- Fungsi tanda tangan pada dokumen kertas juga diterapkan untuk otentikasi pada data digital (pesan, dokumen elektronik).
- Tanda-tangan digital di dalam konteks kriptografi tidak sama dengan tandatangan yang di-digitisasi (digitized signature) dengan cara dipindai atau difoto.



digitized signature

digitized signature

https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2022-2023/28-Tanda-tangan-digital-2023.pdf

- Tanda-tangan digital adalah nilai kriptografis yang bergantung pada isi pesan dan kunci.
- Tanda-tangan seseorang pada dokumen cetak selalu sama, apapun isi dokumennya.
- Sedangkan tanda-tangan digital selalu berbeda-beda antara satu pesan dengan pesan lain, dan/atau antara satu kunci dengan kunci yang lain.
- 2 proses dalam tanda-tangan digital
    1. Menandatangani pesan (signing) : memberi tanda tangan digital
    2. Memverifikasi pesan (verification) : memeriksa ke-absahan digital signature

- Bagaimana cara menandatangani pesan?

Ada 2 cara, yaitu:

1. Mengenkripsi pesan – khusus untuk pesan rahasia
2. Menggunakan kombinasi fungsi hash dan kunci public – untuk pesan yang tidak perlu rahasia

Penandatanganan dengan Mengenkripsi Pesan

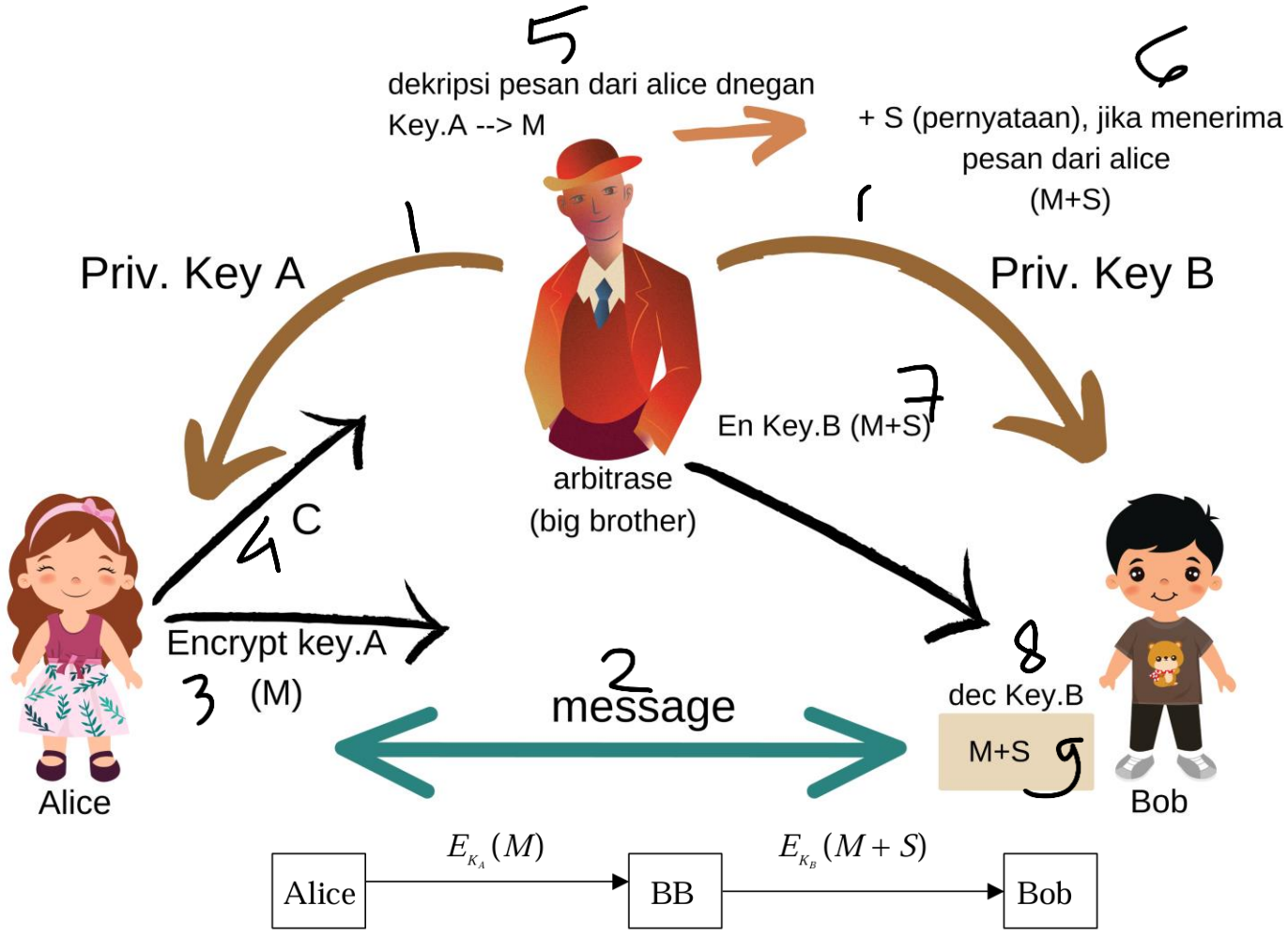
- Enkripsi menggunakan algoritma kriptografi kunci-simetri

Pesan yang dienkripsi dengan algoritma simetri sudah memberikan solusi otentikasi pengirim, karena kunci ini hanya diketehaui oleh pengirim dan penerima.

→tetapi cara ini tidak menyediakan cara untuk melakukan anti-penyangkalan (non-repudiation). Contoh kasus alice dan bob.

Sehingga, menandatangani pesan dengan kriptografi kunci simetri tdk dapat dilakukan.

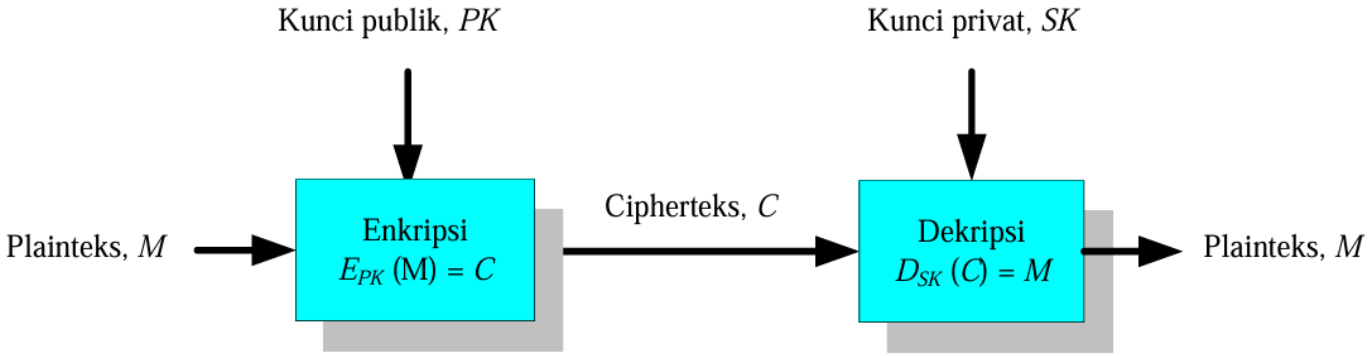
- Agar kriptografi kunci simetri dapat mengatasi masalah penyangkalan, dibutuhkan pihak ketiga (arbitrase) yang di percaya oleh pengirim/penerima.



- Jika Alice menyangkal telah mengirim pesan tersebut, maka pernyataan dari BB pada pesan yang diterima oleh Bob digunakan untuk menolak penyangkalan Alice.
- Bagaimana BB tahu bahwa pesan tersebut dari Alice dan bukan dari Charlie? Karena hanya BB dan Alice yang mengetahui kunci rahasia, maka hanya Alice yang dapat mengenkripsi pesan dengan kunci terebut.
- Kelemahan: pelibatan pihak ketiga dalam penandatanganan pesan membuatnya menjadi lebih rumit, tidak praktis, dan tidak efficient sehingga tidak digunakan di dalam praktek dunia nyata.
- Solusinya adalah menandatangani pesan dengan menggunakan kriptografi kunci public

https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2022-2023/28-Tanda-tangan-digital-2023.pdf

- Enkripsi menggunakan algoritma kriptografi kunci-public

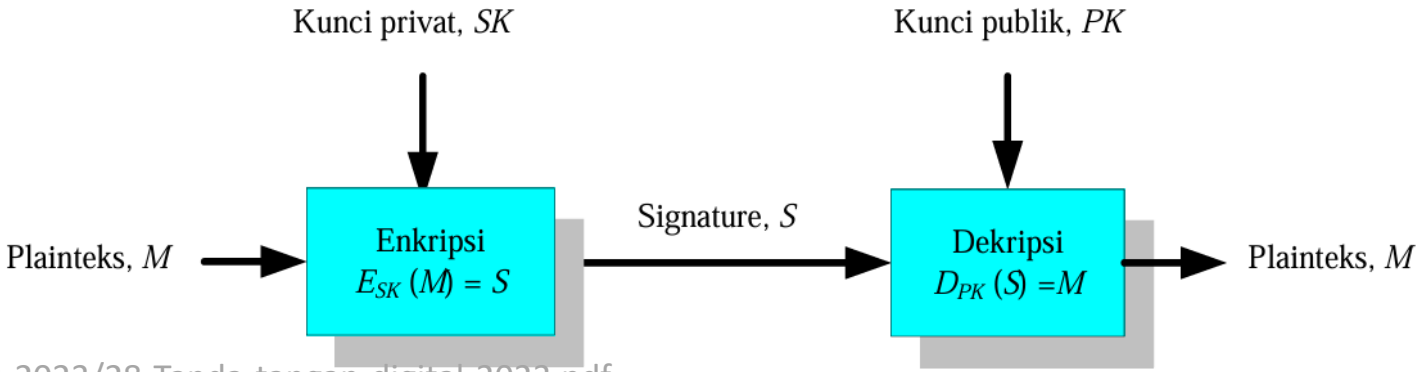


Cara ini tidak dapat mengotentikasi si pengirim pesan karena kunci public diketahui oleh siapapun. Karena itu cara ini tidak dapat digunakan untuk menandatangani pesan.

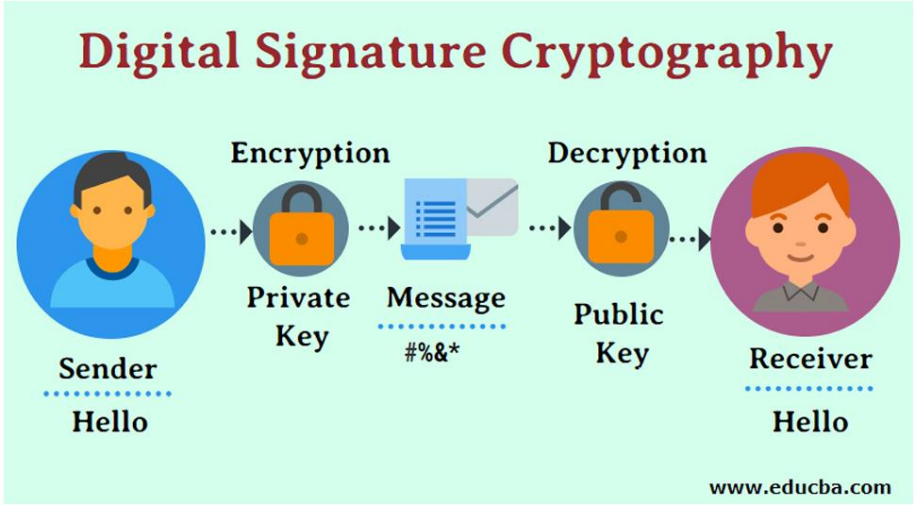
Oleh karenaitu, agar dapat berfungsi sebagai tanda-tangan digital, maka prosesnya dibalik:

-pesan dienkripsi dengan kunci privatsi pengirim

-pesan didekripsi dengan kunci public si pengirim



- Kesimpulan: Jadi untuk menandatangani pesan,maka pesan dienkripsi dengan kunci privat si pengirim, penerima pesan mendekripsinya dengan kunci public si pengirim pesan.
- Dengan cara seperti ini, tidak lagi dibutuhkan pihak penengah (arbitrase).
- Contoh algoritma yang memenuhi sifat ini adalah RSA, karena persamaan enkripsi dan dekripsi identik(dapat dipertukarkan)

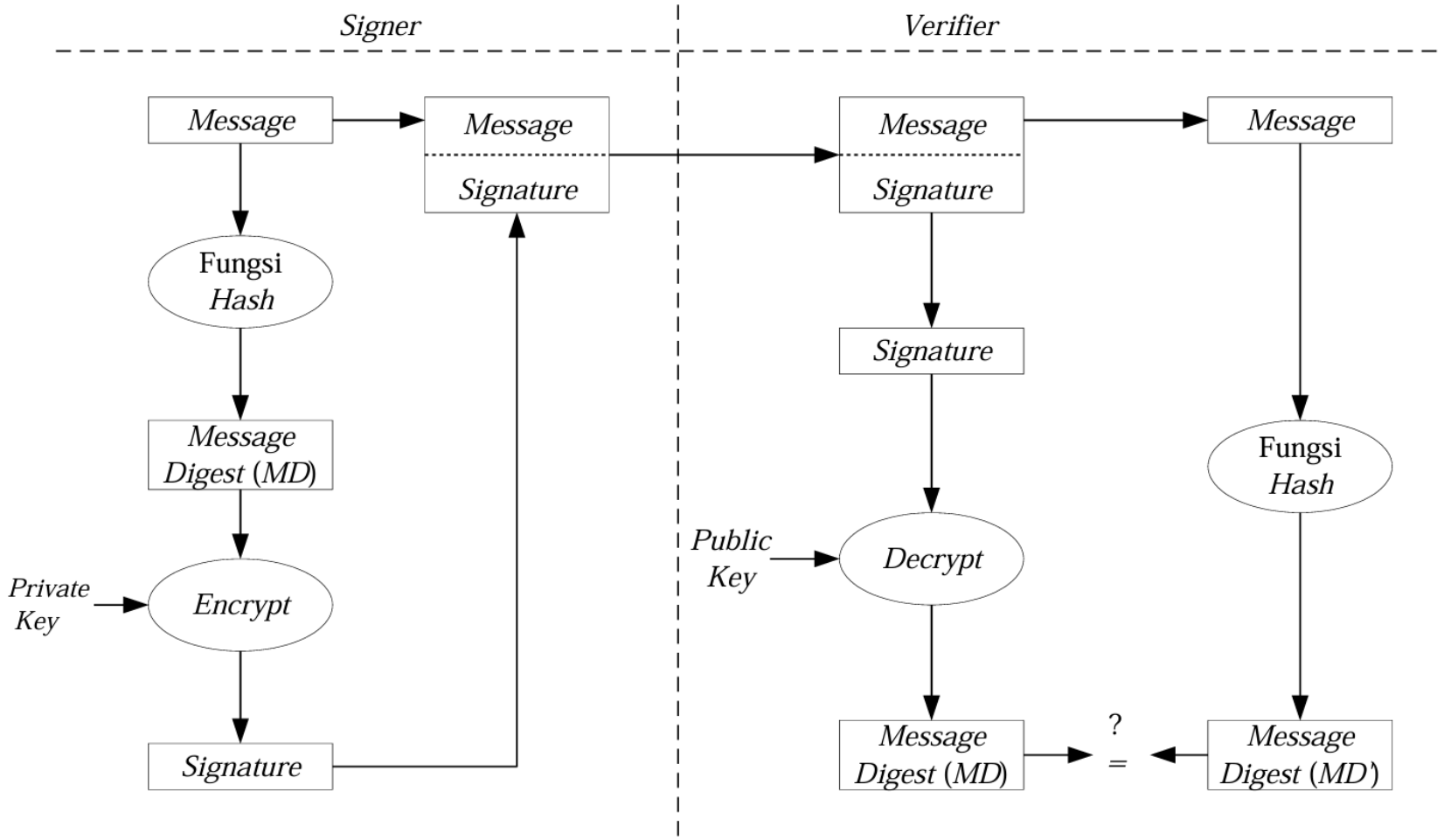


Enkripsi/dekripsi biasa dengan RSA:
- Enkripsi: $c = m^e \bmod n$
- Dekripsi: $m = c^d \bmod n$

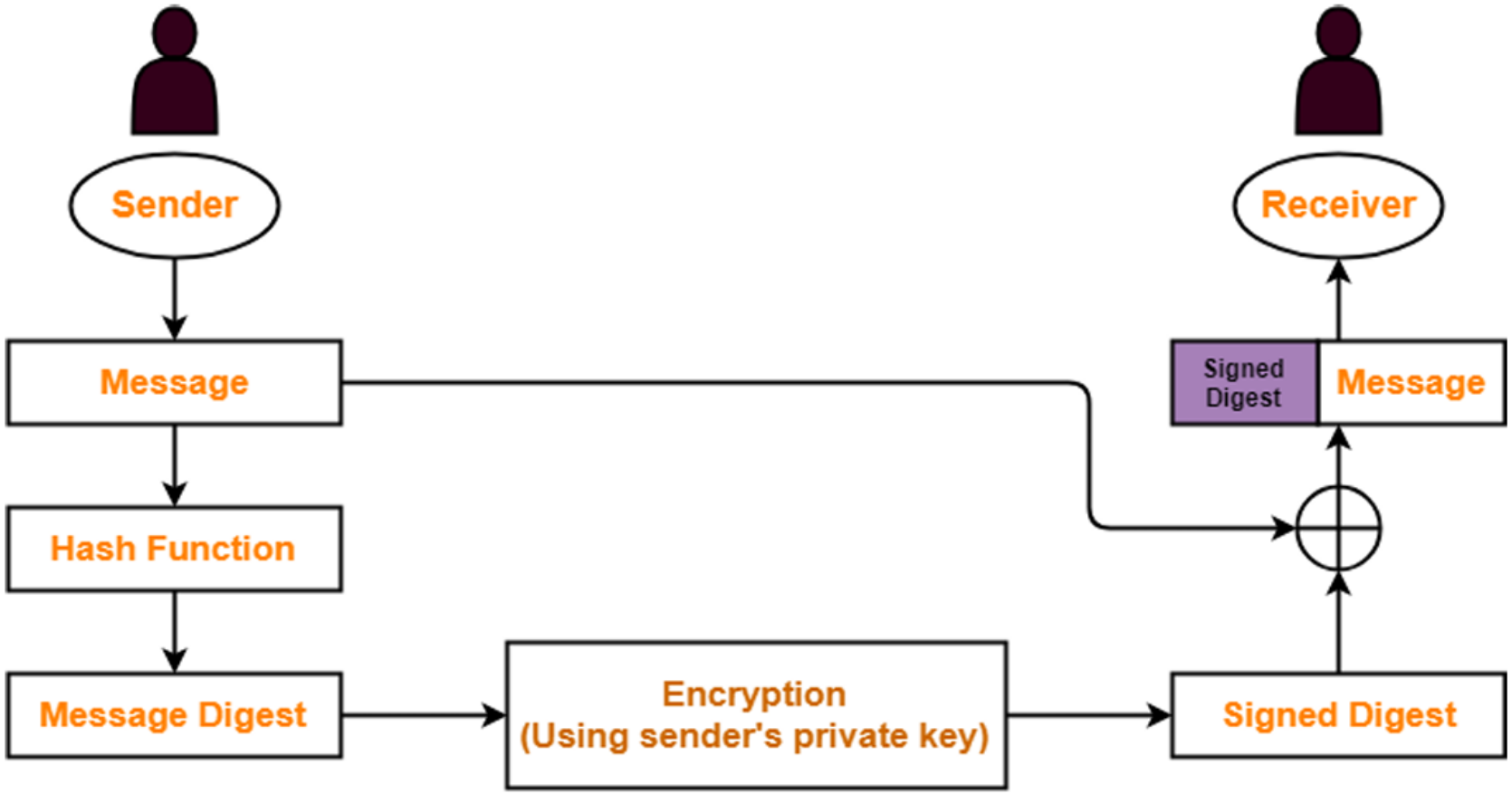
Tanda-tangan digital dengan RSA:
- Signing: $c = m^d \bmod n$
- Verification: $m = c^e \bmod n$

Penandatanganan dengan Menggunakan Kombinasi Kriptografi kunci-public dan fungsi Hash

- Penanda tanganan pesan dengan cara mengenkripsinya selalu memberikan dua fungsi berbeda: kerahasiaan pesan dan otentikasi pesan.
- Pada beberapa kasus, sering kali otentikasi yang diperlukan, tetapi kerahasiaan pesan tidak perlu. Maksudnya, pesan tidak perlu dienkripsi karena tidak rahasia, sebab yang dibutuhkan hanya keotentikan pesansaja.
- Kombinasi algoritma kunci-public dan fungsi hash dapat digunakan untuk kasus seperti ini.

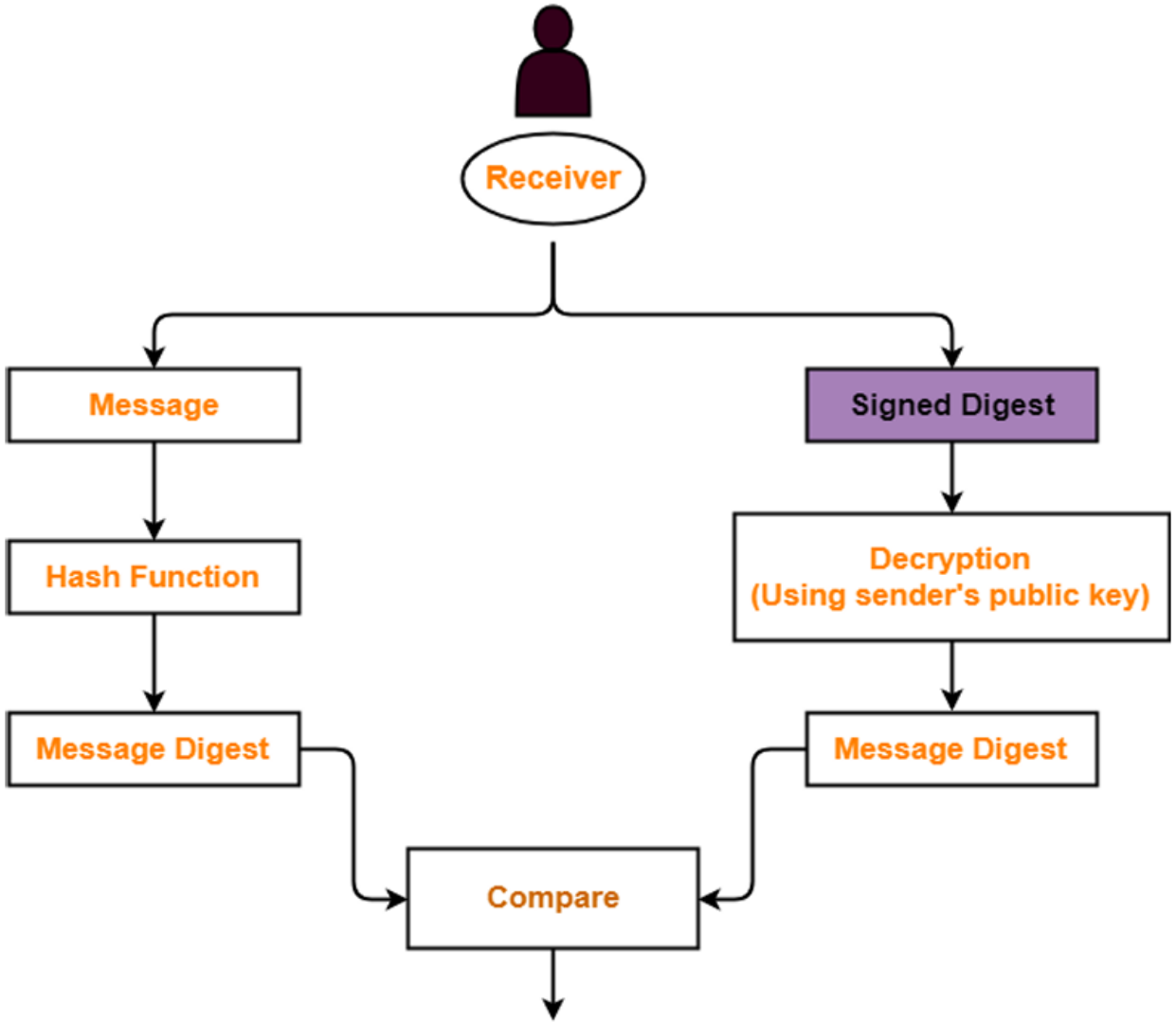


https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2022-2023/28-Tanda-tangan-digital-2023.pdf



At Sender Side

https://www.gatevidyalay.com/how-digital-signature-works-algorithm/



At Receiver Side

https://www.gatevidyalay.com/how-digital-signature-works-algorithm/

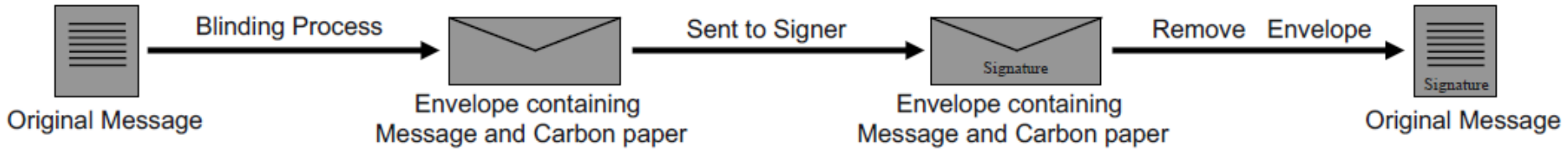
- Dua algoritma signature yang digunakan secara luas adalah RSA dan El-Gamal Signature.
- Pada RSA, algoritma enkripsi dan dekripsi identik, sehingga proses signature dan verifikasi juga identik
- Selain RSA, terdapat algoritma yang dikhususkan untuk tanda-tangan digital, yaitu Digital Signature Algorithm (DSA), yang merupakan bakuan(standard) untuk Digital Dignature Standard(DSS).
- Pada DSA, algoritma signature dan verifikasi berbeda

https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2022-2023/28-Tanda-tangan-digital-2023.pdf

Blind Signature

- Proses membutakan suatu pesan dapat diibaratkan seperti memasukkan pesan ke dalam amplop bersama dengan selembar kertas karbon.
- Tidak ada yang bisa membaca pesan melalui amplop. Tanda tangan buta dibuat pada amplop dan melewati amplop dan kertas karbon ke pesan aslinya.
- Ketika pesan dikeluarkan dari amplop, pesan itu akan ditandatangani dan penandatangan tidak akan mengetahui apa yang ditandatangani.
- Pada langkah-langkah di bawah ini, pengguna Alice menggunakan protokol tanda tangan buta untuk membuat pengguna lain, Bob, menandatangani pesan tanpa mengetahui isinya.

1. Alice mengambil pesan tersebut dan mengalikannya dengan nilai acak, yang disebut faktor pembutakan. Ini membutakan pesan sehingga isinya tidak dapat dibaca.
2. Alice mengirimkan pesan buta kepada Bob.
3. Bob secara digital menandatangani pesan yang dibutakan dan mengembalikannya ke Alice.
4. Alice membagi faktor yang membutakan, meninggalkan pesan asli yang sekarang ditandatangani oleh Bob.



https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2022-2023/28-Tanda-tangan-digital-2023.pdf

Contoh soal:

Pada proses *blind signature*, seorang pengirim (Alice) memiliki pesan 181 (desimal), kemudian nilai acak pengali yang dipilih adalah 21 (desimal).

a. Bagaimana pesan (dalam biner) setelah mengalami proses pembutaan
b. Anggap bahwa tanda-tangan dilakukan (oleh Bob) dengan algoritma *one-time pad* berupa fungsi XOR dengan kunci 2177, tentukan pesan yang telah ditandatangani oleh Bob (dalam kasus nyata, tanda tangan digital tidaklah semudah ini).
c. Menurut Anda, bagaimanakah cara Alice dapat mendekripsi pesannya kembali?

Jawab:

a. Pesan = $m = 181_d = 10110101_b$
   Nilai acak pengali = *blinding factor* = $bf = 21_d$
   Pesan setelah mengalami proses pembutaan = *blinded message* = $bm = m$ x bf
   $\boldsymbol{bm = 181 \text{ x } 21 = 3.801_d = 1110\ 1101\ 1001_b}$

b. Pesan yang ditandatangani Bob = $(bm)_b$ XOR $(\text{kunci})_b$

bm			$\mathbf{= 1110\ 1101\ 1001_b}$
kunci	=	2177_d	$\mathbf{= 1000\ 1000\ 0001_b}$
			XOR
Pesan yg di-tdt Bob			$\mathbf{= 0110\ 0101\ 1000_b}$

c. Cara Alice dapat mendekripsi pesannya kembali (memperoleh pesan asli dan tanda tangan Bob)
   1) Alice harus mendapatkan kunci (tanda tangan Bob)

Pesan yg di-tdt Bob	$\mathbf{= 0110\ 0101\ 1000_b}$
bm (Alice tahu)	$\mathbf{= 1110\ 1101\ 1001_b}$
	XOR
Kunci (=tdt Bob)	$\mathbf{= 1000\ 1000\ 0001_b = 2177_d}$

   2) **Pesan asli $m = bm / bf = 3.801/21 = 181_d$**

Ada pertanyaan?

- SEKIAN DAN TERIMAKASIH