Tanda Tangan Digital

Bahan Kuliah Keamanan Data

Sevi **Nurafni**

Fakultas Sains dan Teknologi
Universitas Koperasi Indonesia 2025

- Ingat kembali empat layanan keamanan yang disediakan oleh kriptografi:
    1. Kerahasiaan pesan (confidentiality/secrecy)
    2. Keaslian pesan (*data integrity*).
    3. Otentikasi (authentication)
    4. Anti-penyangkalan (*non-repudiation*).

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

Tanda Tangan

- Sejak zaman dahulu, tanda-tangan sudah digunakan untuk otentikasi dokumen cetak.

- Tanda-tangan mempunyai karakteristik sebagai berikut:
    1. Tanda-tangan adalah bukti yang otentik.
    2. Tanda tangan tidak dapat dilupakan.
    3. Tanda-tangan tidak dapat dipindah untuk digunakan ulang.
    4. Dokumen yang telah ditandatangani tidak dapat diubah.
    5. Tanda-tangan tidak dapat disangkal.

Hari: Senin, Tanggal 12 September 2016

Waktu: 14.00 Wib

Tempat: Aula

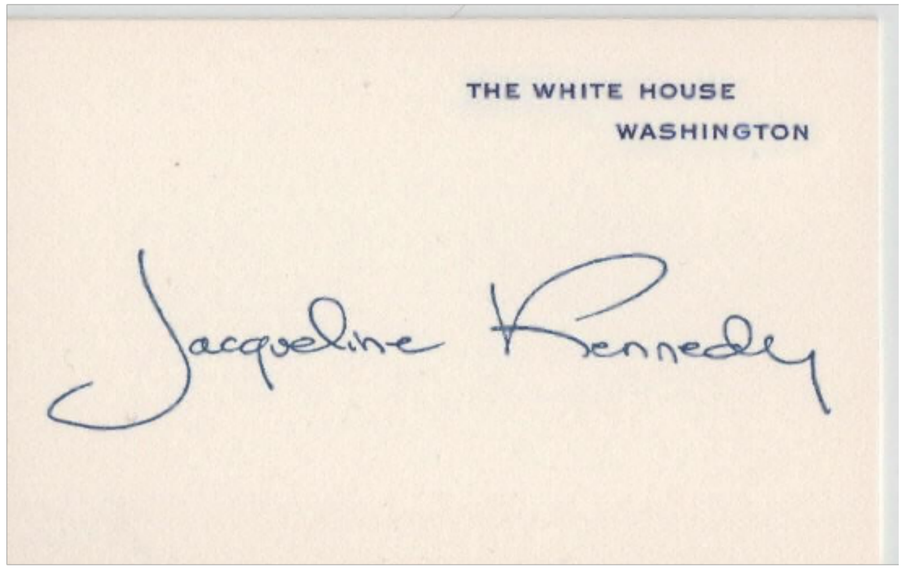
Demikian kami buat surat ini dengan sebenarnya. Harap semua peserta untuk hadir sesuai jadwal yang telah disebutkan di atas. Terima kasih.

Tertanda tangan

Mr Mukidi

Master of Ceremony
Doktor Mukidi, Mpd

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



digitized signature

- Tanda-tangan digital adalah *nilai kriptografis* yang bergantung pada isi pesan dan kunci.
- Tanda-tangan seseorang pada dokumen cetak selalu sama, apa pun isi dokumennya.
- Sedangkan tanda-tangan digital selalu berbeda-beda antara satu pesan dengan pesan lain, dan/atau antara satu kunci dengan kunci yang lain.

Paris, 31 Desember 2018

Halo Alice

Sudah lama kita tidak berjumpa sejak lulus SMA. Saya sekarang tinggal di Paris sejak tahun 2016. Saya bekerja di sebuah perusahaan IT yang bernama Solution Express. Perusahaan ini memberikan layanan keamanan informasi berbasis cloud computing. Saya menjadi menejer Quality Control. Klien kami umumnya adalah bank-bank yang membutuhkan keamanan data nasabah.

Oh ya, saya belum menanyakan bagaimana keadaanmu sekarang. Di mana kamu bekerja atau malah melanjutkan studi S2 di mana? Saya ingat kamu dulu jago sekali pelajaran kimia. Apakah kamu masih menekuni bidang kimia saat ini?

Oke deh, jika kamu jalan-jalan ke Eropa jangan lupa mampir ke kota Paris. Nanti saya akan ajak

kamu mengunjungi Menara Eiffel. Bisa naik sampai ke atas lho.

Salam dari temanmu di Paris Bob

-- BEGIN SIGNATURE—

13706B6D42442620B2FD1098BD4D54ADFA9F7DC27576954ADCE5E5FC901

-- END SIGNATURE--

KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI
LEMBAGA LAYANAN PENDIDIKAN TINGGI WILAYAH IV
Alamat Jalan Khp Hasan Mustopa Nomor 38 Kota Bandung 40124
Telepon (022) 7275630
Laman https://lldikti4.id/

Nomor : 7348/LL4/PT/2025 22 Mei 2025
Perihal : Pemberitahuan Pendataan Dosen untuk Publikasi Artikel Ilmiah

Yth. Pimpinan Perguruan Tinggi
di Lingkungan LLDIKTI Wilayah IV

Dalam rangka meningkatkan kompetensi dosen dalam menulis dan mempublikasikan artikel ilmiah, serta mendorong peningkatan jumlah dan kualitas publikasi ilmiah di lingkungan perguruan tinggi, LLDIKTI Wilayah IV berkomitmen untuk memperkuat sinergi antara berbagai pihak.

Berdasarkan hasil analisis yang telah dilakukan, salah satu kendala utama yang dihadapi dalam pengajuan usulan Jabatan Akademik Dosen adalah terbatasnya jumlah publikasi ilmiah yang memenuhi syarat. Oleh karena itu, LLDIKTI Wilayah IV akan menjalin kolaborasi dan fasilitasi sebagai bentuk dukungan terhadap para dosen dalam proses publikasi karya ilmiah.

Sehubungan dengan hal tersebut, kami mohon kesediaan Saudara untuk menugaskan dosen di lingkungan perguruan tinggi yang Saudara pimpin agar mengisi formulir pendataan dosen yang berminat mengikuti program fasilitasi publikasi artikel ilmiah melalui tautan berikut: https://forms.gle/XnyZGWCdsYJ5TAvZ8

Untuk informasi lebih lanjut, Bapak/Ibu dapat menghubungi narahubung:
- Bapak Idik Nursidik (0821-1546-4615)
- Ibu Yeni Rospiani (0852-2053-8908)

Demikian surat ini kami sampaikan. Atas perhatian dan kerja sama yang baik, kami ucapkan terima kasih

Kepala Lembaga Layanan
Pendidikan Tinggi Wilayah IV,

Lukman
NIP 197805112003121002

Bagaimana Cara Menandatangani pesan?

Ada dua cara yang dilakukan untuk menandatangani pesan:

1. Mengenkripsi pesan
2. Menggunakan kombinasi fungsi *hash* (*hash function*) dan kriptografi kunci-publik

Penandatanganan dengan Cara Mengenkripsi Pesan

a. Enkripsi menggunakan algoritma kriptografi kunci-simetri

- Pesan yang dienkripsi dengan algoritma simetri sudah memberikan solusi untuk otentikasi pengirim karena kunci simetri hanya diketahui oleh pengirim dan penerima.
- Namun cara ini tidak menyediakan cara untuk melakukan anti-penyangkalan (*non-repudiation*).
- Jika Alice menyangkal telah mengirim pesan kepada Bob, maka Bob tidak punya cara untuk membantah sangkalan Alice. Alice dapat saja menuduh bahwa pesan tersebut dibuat oleh Bob sendiri karena hanya Alice dan Bob yang mengetahui kunci untuk enkripsi dan dekripsi.
- **Kesimpulan**: menandatangani pesan dengan kriptografi kunci simetri tidak dapat dilakukan.

- Agar kriptografi kunci-simeteri dapat mengatasi masalah penyangkalan, maka diperlukan pihak ketiga yang dipercaya oleh pengirim penerima.
- Pihak ketiga ini disebut penengah (*arbitrase*).
- Misalkan BB (*Big Brothers*) adalah otoritas arbitrase yang dipercaya oleh Alice dan Bob.
- BB memberikan kunci rahasia K_A kepada Alice dan kunci rahasia K_B kepada Bob.
- Hanya Alice dan BB yang mengetahui K_A, begitu juga hanya Bob dan BB yang mengetahui K_B.

Jika Alice bekirim pesan *M* kepada Bob, maka langkah-langkahnya adalah sebagai berikut:

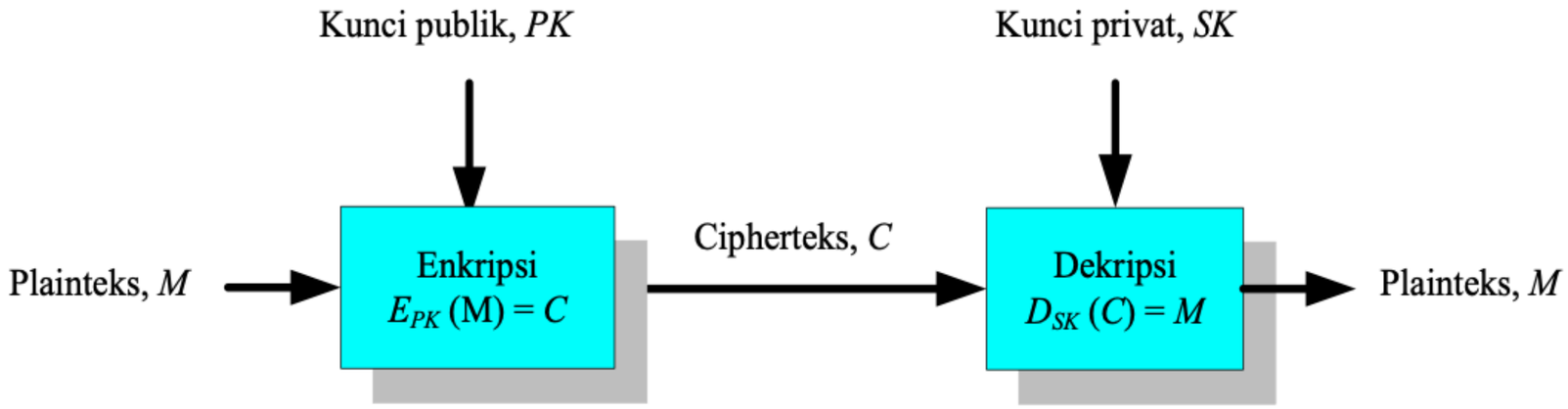
1. Alice mengenkripsi pesan *M* untuk Bob dengan K_A, lalu mengirim cipherteksnya ke BB.
2. BB melihat bahwa pesan dari Alice, lalu mendekripsi pesan dari Alice dengan K_A.
3. BB membuat pernyataan *S* bahwa ia menerima pesan dari Alice, lalu menambahkan pernyataan tersebut pada plainteks dari Alice.
4. BB mengenkripsi bundel pesan (*M* + *S*) dengan K_B, lalu mengirimkannya kepada Bob.
5. Bob mendekripsi bundel pesan dengan K_B. Ia dapat membaca pesan dari Alice (*M*) dan pernyataan (*S*) dari BB bahwa Alice yang mengirim pesan tersebut.

- 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?

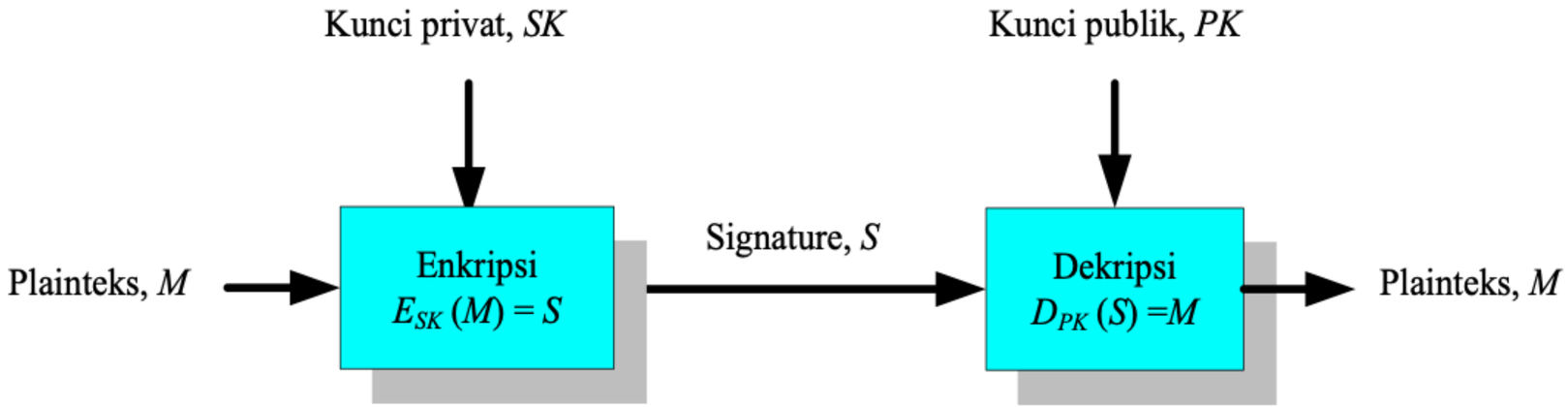
- **Kelemahan**: pelibatan pihak ketiga dalam penandatanganan pesan membuatnya menjadi lebih rumit, tidak praktis, dan tidak *efficient* sehingga tidak digunakan di dalam praktek dunia nyata.
- Solusinya adalah menandatangani pesan dengan menggunakan kriptografi kunci-publik

b. Enkripsi mengunakan algoritma kriptografi kunci-publik

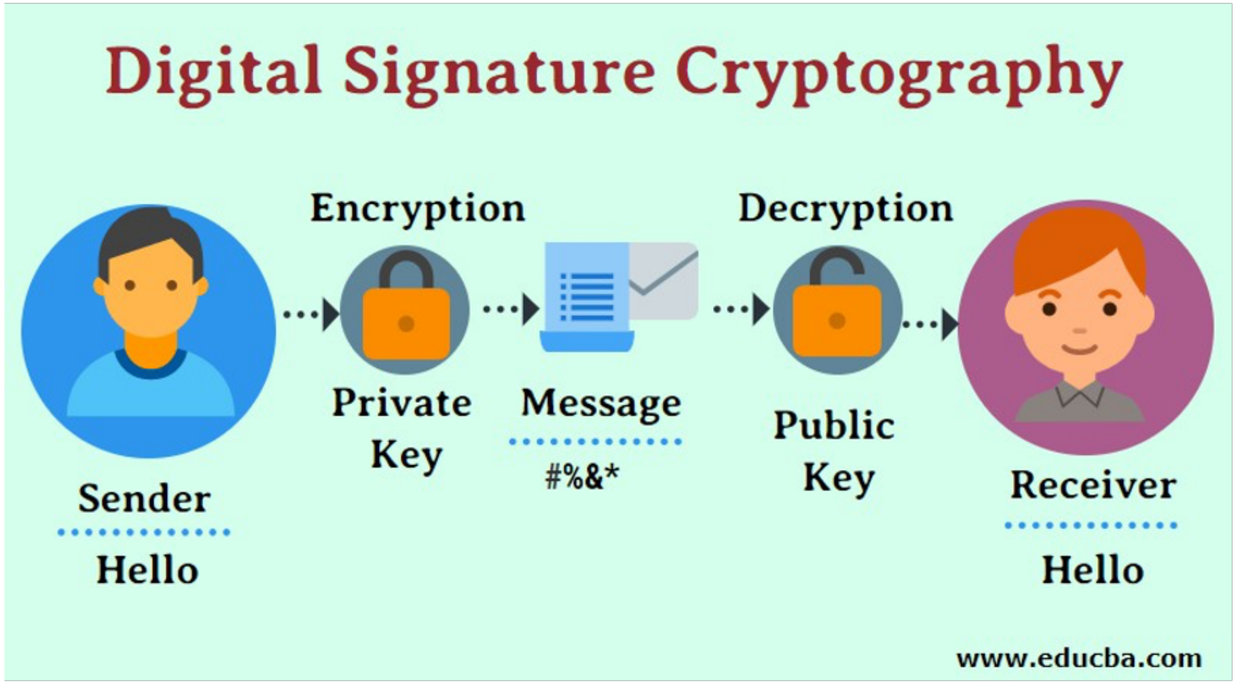
- Pesan dienkripsi dengan kunci publik penerima
- Pesan didekripsi dengan kunci privat penerima
- Cara ini tidak memberikan bukti otentifikasi karena?



- Oleh karena itu, agar dapat berfungsi sebagai tanda-tangan digital, maka prosesnya dibalik:
  - pesan dienkripsi dengan kunci privat si pengirim.
  - pesan didekripsi dengan kunci publik si pengirim.
  - Dengan cara ini, maka kerahasiaan pesan dan otentikasi si pengirim pesan keduanya dicapai sekaligus.
  - Ide ini ditemukan oleh Diffie dan Hellman.



Kesimpulan: Jadi untuk menandatangani pesan, maka pesan dienkripsi dengan kunci privat si pengirim, penerima pesan mendekripsinya dengan kunci publik si pengirim pesan.



Sumber: https://www.educba.com/digital-signature-cryptography/

- Proses menandatantangani pesan (*signing* oleh pengirim):

  $S = E_{SK}(M)$

- Proses memverifikasi tanda-tangan (*verification* oleh penerima):

  $M = D_{PK}(S)$

Keterangan:

SK = *secret key* = kunci privat pengirim

PK = *public key* = kunci publik pengirim

E = fungsi enkripsi;

M = pesan;

D = fungsi dekripsi

S = *signature* = cipherteks (hasil enkripsi pesan)

Jadi, mengenkripsi pesan dengan menggunakan kunci privat sama artinya dengan menandatangani pesan. Mendekripsi pesan dengan kunci publik sama artinya dengan memverifikasi tanda-tangan. Dengan cara seperti ini, tidak lagi dibutuhkan pihak penengah (arbitrase).

- Beberapa algoritma kunci-publik dapat digunakan untuk menandatangani pesan dengan cara mengenkripsinya, asalkan algoritma tersebut memenuhi sifat:

$$D_{SK}(E_{PK}(M)) = M \text{ dan } D_{PK}(E_{SK}(M)) = M ,$$

Keterangan:

PK = kunci publik ;

E = fungsi enkripsi;

SK = kunci privat (*secret key*).

D = fungsi dekripsi; *M* = pesan

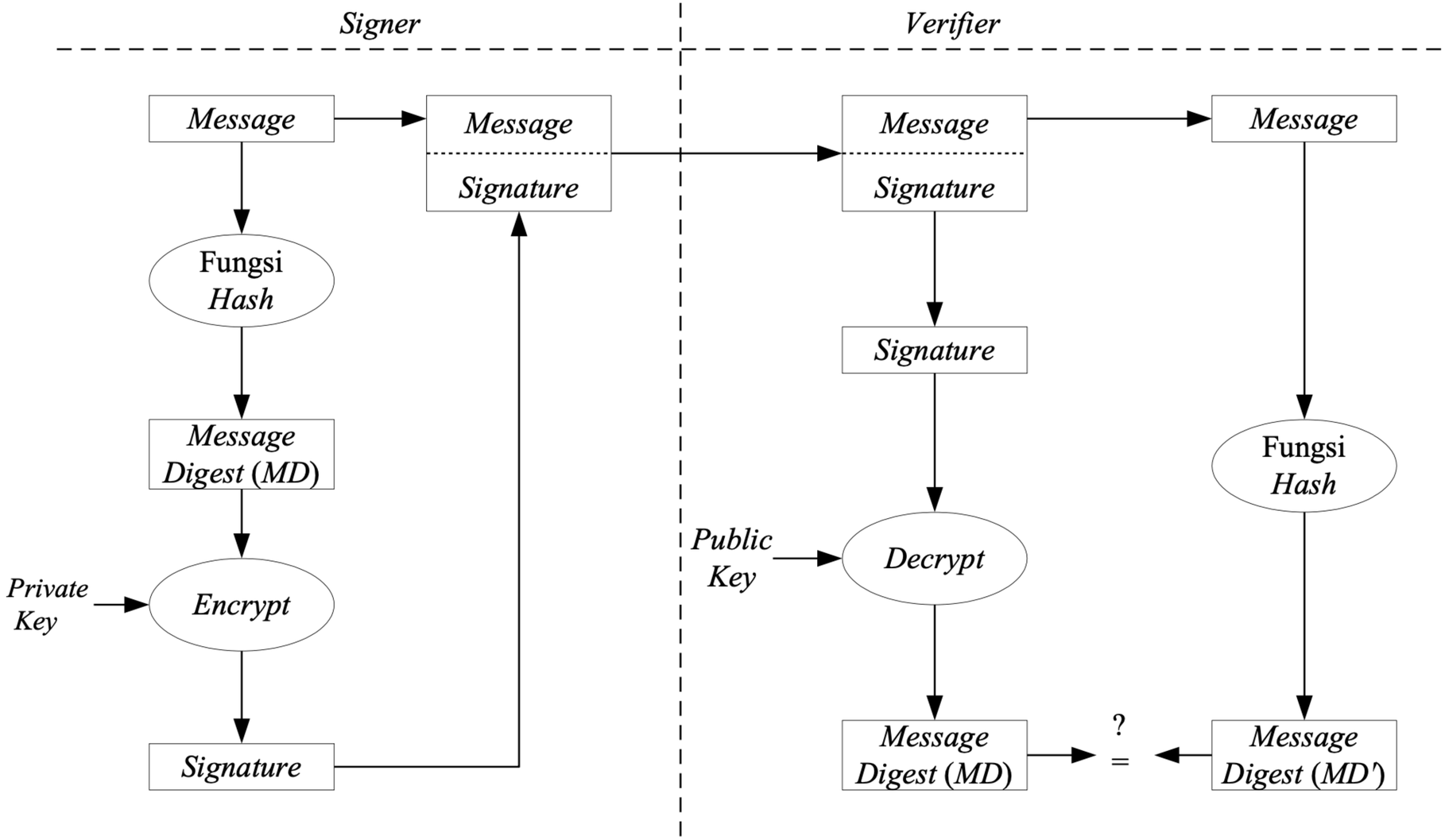
Contoh algoritma yang memenuhi sifat ini adalah RSA, karena persamaan enkripsi dan dekripsi identik (dapat dipertukarkan)

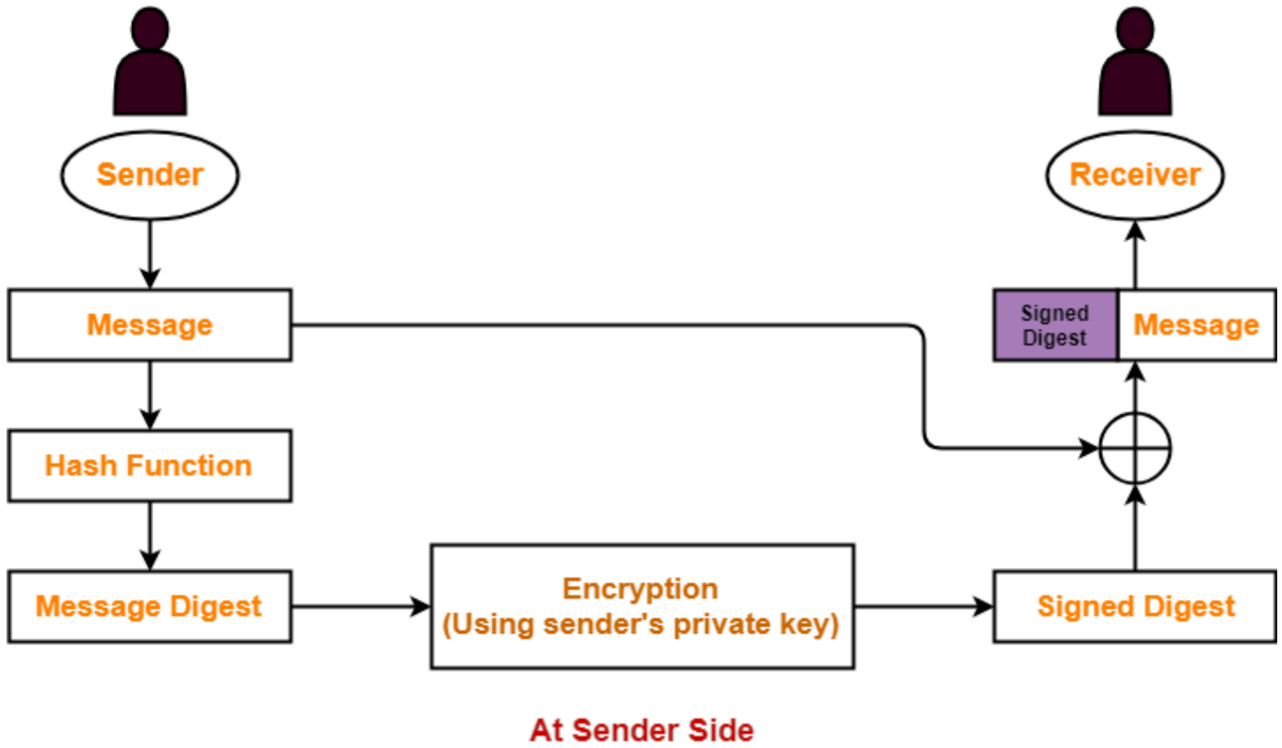
Penandatanganan dengan Menggunakan Kombinasi Kriptografi Kunci-Publik dan Fungsi Hash

- Penandanganan pesan dengan cara mengenkripsinya selalu memberikan dua fungsi berbeda: kerahasiaan pesan dan otentikasi pesan.

- Pada beberapa kasus, seringkali otentikasi yang diperlukan, tetapi kerahasiaan pesan tidak perlu. Maksudnya, pesan tidak perlu dienkripsi karena tidak rahasia, sebab yang dibutuhkan hanya keotentikan pesan saja.

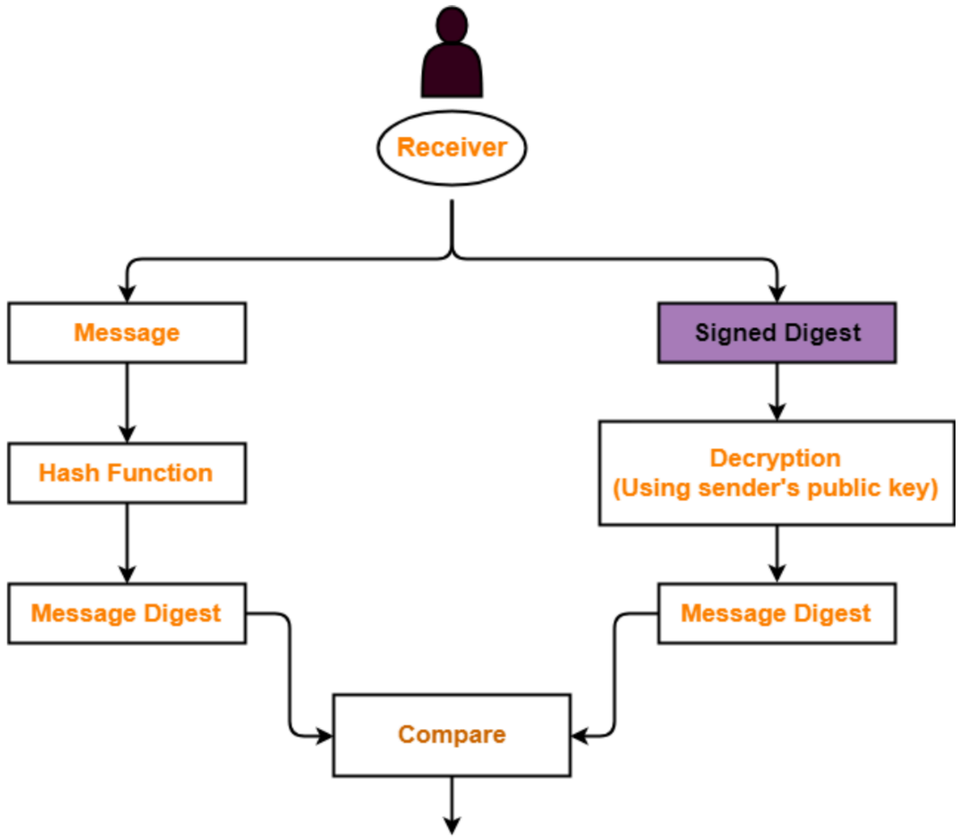
- Kombinasi algoritma kunci-publik dan fungsi *hash* dapat digunakan untuk kasus seperti ini.


Signer
Verifier
Message
Message
Signature
Message
Signature
Message
Fungsi
Hash
Signature
Message
Digest (MD)
Fungsi
Hash
Private
Key
Encrypt
Public
Key
Decrypt
Signature
?
=
Message
Digest (MD)
Message
Digest (MD')



At Sender Side

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



At Receiver Side

- Dua algoritma *signature* yang digunakan secara luas adalah *RSA* dan ElGamal 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

SELAMAT BELAJAR