



Bahan Kuliah IF4020 Kriptografi

A digital signature asserts identity and proves integrity - that's never been more critical.

# *Digital Signature Standard (DSS)*

**Oleh: Rinaldi Munir**

Program Studi Teknik Informatika

STEI-ITB

2023

# Pendahuluan

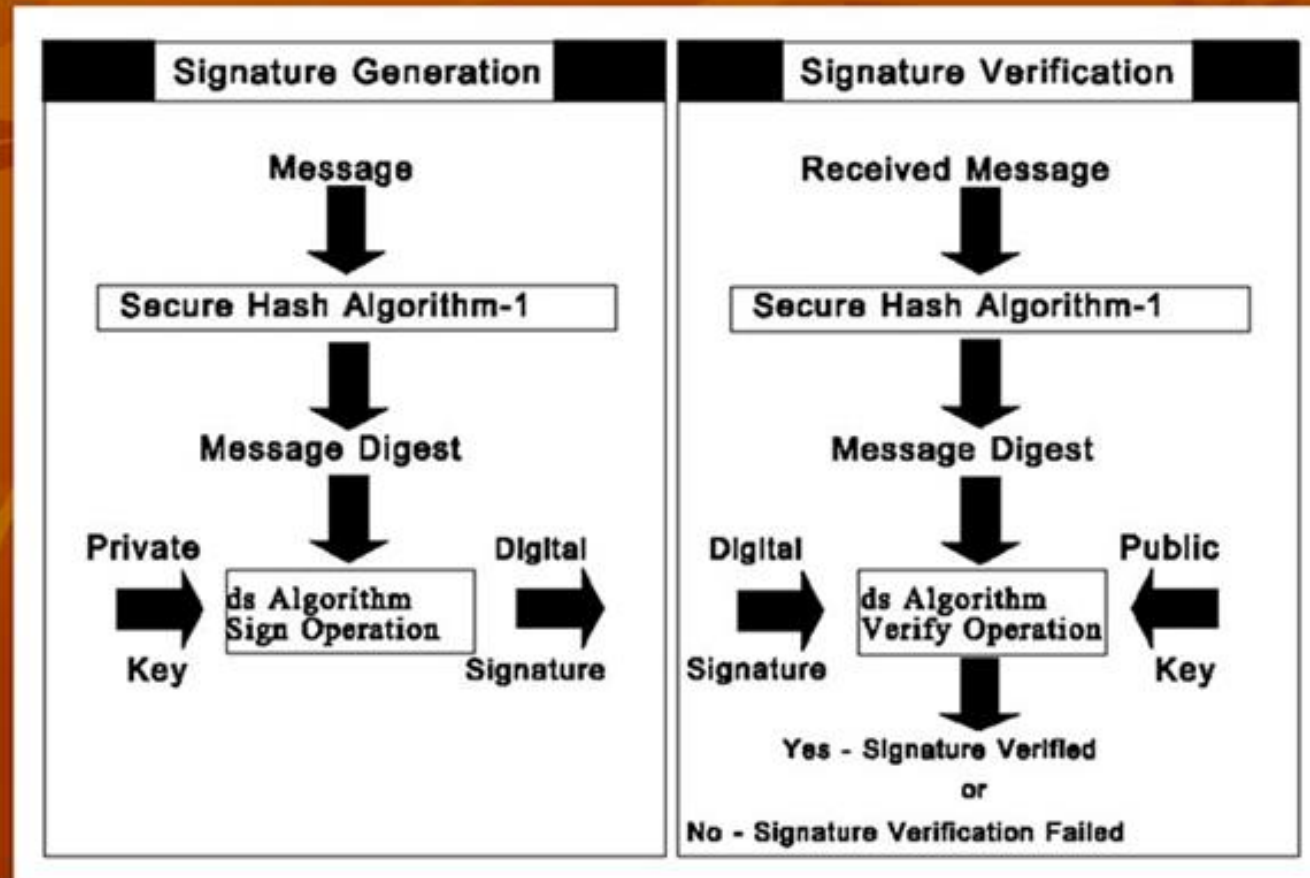
- DSS adalah bakuan (standard) untuk tanda-tangan digital.
- Diresmikan pada bulan Agustus 1991 oleh NIST (*The National Institute of Standard and Technology*)
- DSS terdiri dari dua komponen:
  1. Algoritma tanda-tangan digital: *Digital Signature Algorithm (DSA)*.
  2. Fungsi *hash* standard: *Secure Hash Algorithm (SHA-1)*.

# *Digital Signature Algorithm (DSA)*

- *DSA* termasuk ke dalam algoritma kriptografi kunci-publik.
- *DSA* tidak dapat digunakan untuk enkripsi pesan; *DSA* dispesifikasikan khusus untuk tanda-tangan digital saja.
- *DSA* mempunyai dua fungsi utama:
  1. Pembangkitan tanda-tangan (*signature generation*),
  2. Pemeriksaan keabsahan tanda-tangan (*signature verification*).

- *DSA* dikembangkan dari algoritma *ElGamal*.
- *DSA* menggunakan dua buah kunci, yaitu kunci publik dan kunci privat.
- Pembentukan tanda-tangan menggunakan kunci privat, sedangkan verifikasi tanda-tangan menggunakan kunci publik.
- *DSA* menggunakan fungsi *hash SHA-1 (Secure Hash Algorithm)* untuk menghasilkan *message digest* yang berukuran 160 bit (*SHA*-sudah dijelaskan pada materi kuliah sebelumnya).

# Digital Signature Standard (DSS)



Sumber: <https://signx.wondershare.com/knowledge/digital-signature-algorithm.html>

# Parameter DSA

1.  $p$ , bilangan prima, panjangnya  $L$  bit,  $512 \leq L \leq 1024$  dan  $L$  harus kelipatan 64. Parameter  $p$  bersifat publik.
2.  $q$ , bilangan prima 160 bit, merupakan faktor dari  $p - 1$ . Dengan kata lain,  $(p - 1) \bmod q = 0$ . Parameter  $q$  bersifat publik.
3.  $g = h^{(p-1)/q} \bmod p$ ,  $h < p - 1$  sedemikian sehingga  $h^{(p-1)/q} \bmod p > 1$ . Parameter  $g$  bersifat publik.
4.  $x$ , kunci privat, adalah bilangan bulat kurang dari  $q$ .
5.  $y = g^x \bmod p$ , kunci publik.
6.  $m$ , pesan yang akan diberi tanda-tangan.

# Pembangkitan Sepasang Kunci

1. Pilih bilangan prima  $p$  dan  $q$ , yang dalam hal ini  $(p - 1) \bmod q = 0$ .
2. Hitung  $g = h^{(p-1)/q} \bmod p$ , yang dalam hal ini  $1 < h < p - 1$  dan  $h^{(p-1)/q} \bmod p > 1$ .
3. Tentukan kunci privat  $x$ , yang dalam hal ini  $x < q$ .
4. Hitung kunci publik  $y = g^x \bmod p$ .

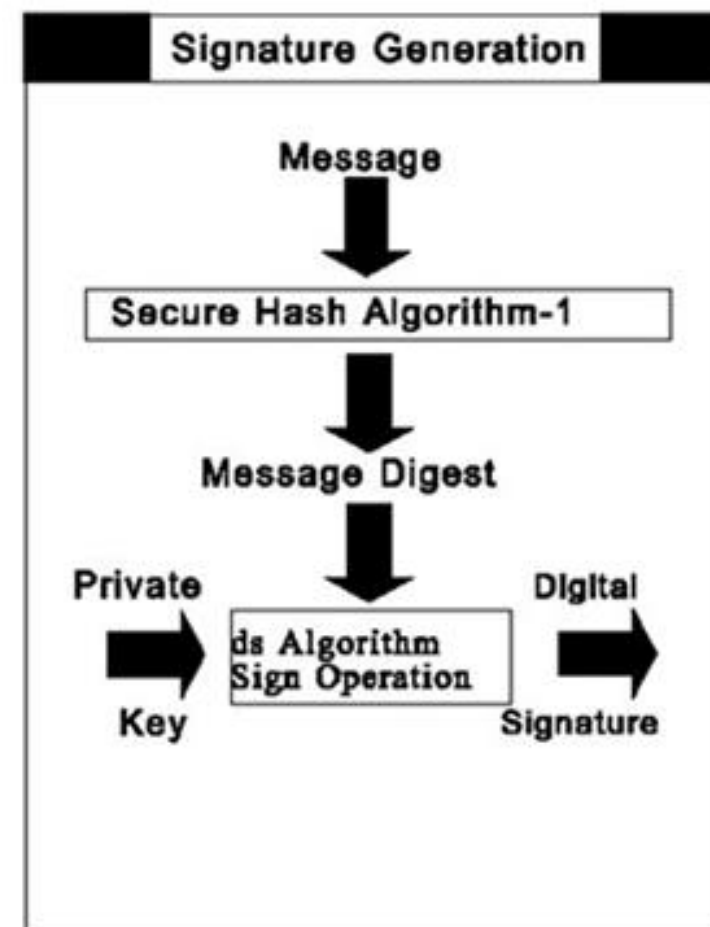
Prosedur di atas menghasilkan:

parameter publik:  $(p, q, g, y)$

parameter privat:  $x$

# Pembangkitan Tanda-tangan (*Signing*)

1. Hitung *message digest* pesan  $m$  dengan fungsi *hash* SHA-1,  $H(m)$ .
2. Tentukan bilangan acak  $k < q$ .
3. Tanda-tangan dari pesan  $m$  adalah bilangan  $r$  dan  $s$ . Hitung  $r$  dan  $s$  sebagai berikut (kunci privat =  $x$ ):  
$$r = (g^k \bmod p) \bmod q$$
$$s = (k^{-1} (H(m) + x \cdot r)) \bmod q$$
4. Kirim pesan  $m$  beserta tanda-tangan  $r$  dan  $s$ .





# Verifikasi Keabsahan Tanda-tangan (*Verifying*)

1. Hitung *message digest* pesan  $m$  dengan fungsi hash SHA-1,  $H(m)$ .
2. Verifikasi tanda-tangan,  $r$  dan  $s$ , sebagai berikut (kunci publik =  $y$ ): :

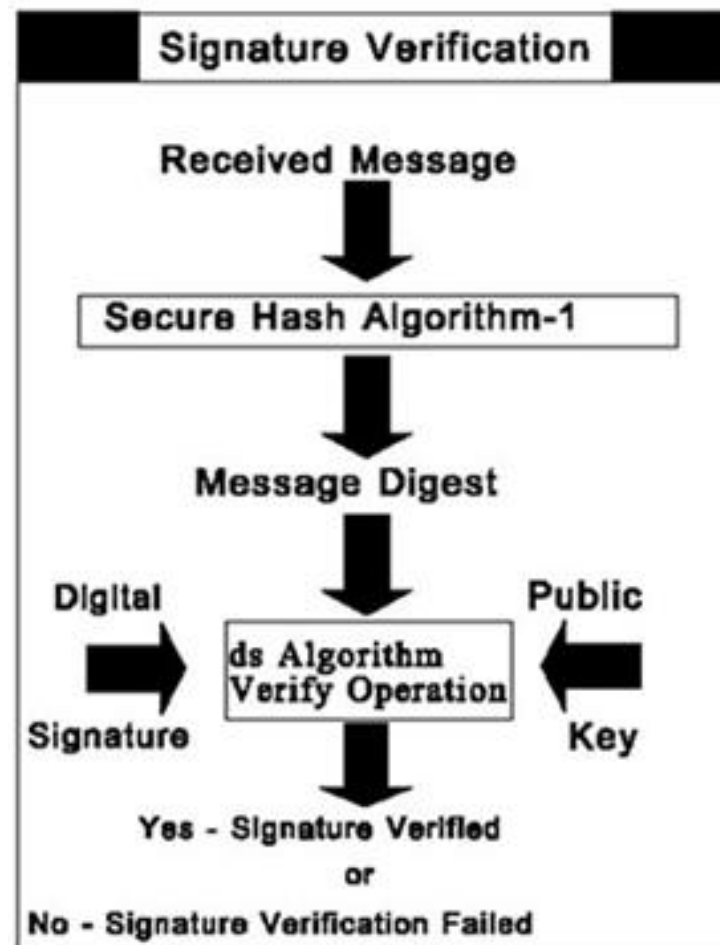
$$w = s^{-1} \bmod q$$

$$u_1 = (H(m) \cdot w) \bmod q$$

$$u_2 = (r \cdot w) \bmod q$$

$$v = ((g^{u_1} \cdot y^{u_2}) \bmod p) \bmod q$$

2. Jika  $v = r$ , maka tanda-tangan digital sah (terverifikasi), sebaliknya tidak sah.



# Contoh Perhitungan DSA

## A. Prosedur Pembangkitan Sepasang Kunci

1. Pilih bilangan prima  $p$  dan  $q$ , yang dalam hal ini  $(p - 1) \bmod q = 0$ .

$$p = 59419$$

$$q = 3301 \text{ (memenuhi } (59419 - 1) \bmod 3301 = 0 \text{ )}$$

2. Hitung  $g = h^{(p-1)/q} \bmod p$ , yang dalam hal ini  $1 < h < p - 1$  dan  $h^{(p-1)/q} \bmod p > 1$ .

$$g = 100^{(59419 - 1)/3301} \bmod (59419) = 18870 \quad \text{(dengan } h = 100\text{)}$$

3. Tentukan kunci privat  $x$ , yang dalam hal ini  $x < q$ .

$$x = 3223$$

4. Hitung kunci publik  $y = g^x \bmod p$ .

$$y = 18870^{3223} \bmod 59419 = 29245 \quad \text{(cek dengan Wolframalpha ☺)}$$

## B. Prosedur Pembangkitan Tanda-tangan (Signing)

1. Hitung nilai *hash* dari pesan  $m$ , misalkan  $H(m) = 4321$

2. Tentukan bilangan acak  $k < q$ .

$$k = 997$$

$$k^{-1} \equiv 2907 \pmod{3301}$$

parameter publik: ( $p = 59419$  ,  $q = 3301$ ,  $g = 18870$  )  
parameter privat:  $x = 3223$

3. Hitung tanda-tangan digital,  $r$  dan  $s$ , sebagai berikut:

$$r = (g^k \bmod p) \bmod q = (18870^{997} \bmod 59419) \bmod 3301 = 848$$

$$s = (k^{-1} (H(m) + x \cdot r)) \bmod q = (2907 (4321 + 3223 \cdot 848)) \bmod 3301 \\ = 7957694475 \bmod 3301 = 183$$

4. Kirim pesan  $m$  dan tanda-tangan,  $(r, s) = (848, 183)$

### C. Prosedur Verifikasi Keabsahan Tanda-tangan

1. Hitung nilai *hash* dari pesan  $m$ , misalkan  $H(m) = 4321$
2. Verifikasi tanda-tangan,  $(r, s) = (848, 183)$ , sebagai berikut:

$$s^{-1} \equiv 469 \pmod{3301}$$

$$w = s^{-1} \pmod{q} = 469 \pmod{3301} = 469$$

$$u_1 = (H(m) \cdot w) \pmod{q} = (4321 \cdot 469) \pmod{3301} = 3036$$

$$u_2 = (r \cdot w) \pmod{q} = (848 \cdot 469) \pmod{3301} = 1592$$

$$\begin{aligned} v &= ((g^{u_1} \cdot y^{u_2}) \pmod{p}) \pmod{q} = (18870^{3086} \cdot 29245^{1592}) \pmod{3301} \\ &= 3036 \cdot 848 \pmod{3301} = 848 \end{aligned}$$

parameter publik:  $(p = 59419, q = 3301,$   
 $g = 18870, y = 29245)$

3. Karena  $v = r$ , maka tanda-tangan sah.

SELAMAT BELAJAR