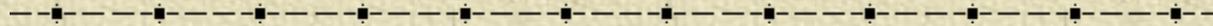
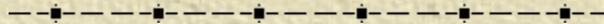


# *Digital Signature Standard (DSS)*



Bahan Kuliah  
IF4020 Kriptografi



# 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 yang disebut *Digital Signature Algorithm (DSA)*.
  2. Fungsi *hash* standard yang disebut *Secure Hash Algorithm (SHA)*.

# *Digital Standard Algorithm (DSA)*

---

- ✦ *DSA* termasuk ke dalam algoritma kriptografi kunci-publik.
- ✦ *DSA* tidak dapat digunakan untuk enkripsi; *DSA* dispesifikasikan khusus untuk tanda-tanagn digital.
- ✦ *DSA* mempunyai dua fungsi utama:
  1. Pembentukan 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 rahasia privat, sedangkan verifikasi tanda-tangan menggunakan kunci publik pengirim.
  - ✦ DSA menggunakan fungsi *hash SHA (Secure Hash Algorithm)* untuk mengubah pesan menjadi *message digest* yang berukuran 160 bit (sudah dijelaskan pada kuliah minggu lalu).

# Parameter DSA

---

1.  $p$ , adalah bilangan prima dengan panjang  $L$  bit, yang dalam hal ini  $512 \leq L \leq 1024$  dan  $L$  harus kelipatan 64.  
Parameter  $p$  bersifat publik dan dapat digunakan bersama-sama oleh orang di dalam kelompok.
2.  $q$ , bilangan prima 160 bit, merupakan faktor dari  $p - 1$ . Dengan kata lain,  $(p - 1) \bmod q = 0$ . Parameter  $q$  bersifat publik.
3.  $g = h^{(p-1)/q} \bmod p$ , yang dalam hal ini  $h < p - 1$  sedemikian sehingga  $h^{(p-1)/q} \bmod p > 1$ . Parameter  $g$  bersifat publik.
4.  $x$ , adalah bilangan bulat kurang dari  $q$ . Parameter  $x$  adalah kunci privat.
5.  $y = g^x \bmod p$ , adalah 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  $y = g^x \bmod p$ .

Jadi, prosedur di atas menghasilkan:

kunci publik dinyatakan sebagai  $(p, q, g, y)$ ;  
kunci privat dinyatakan sebagai  $(p, q, g, x)$ .

# Pembangkitan Tanda-tangan(*Signing*)

---

1. Ubah pesan  $m$  menjadi *message digest* dengan fungsi hash SHA,  $H$ .
2. Tentukan bilangan acak  $k < q$ .
3. Tanda-tangan dari pesan  $m$  adalah bilangan  $r$  dan  $s$ .  
Hitung  $r$  dan  $s$  sebagai berikut:

$$r = (g^k \bmod p) \bmod q$$

$$s = (k^{-1} (H(m) + x * r)) \bmod q$$

4. Kirim pesan  $m$  beserta tanda-tangan  $r$  dan  $s$ .

# Verifikasi Keabsahan Tanda-tangan (*Verifying*)

---

1. Hitung

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

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

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

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

2. Jika  $v = r$ , maka tanda-tangan sah, yang berarti bahwa pesan masih asli dan dikirim oleh pengirim yang benar.

# Contoh Perhitungan *DSA*

---

## *a. Prosedur Pembangkitan Sepasang Kunci*

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

$$p = 59419$$

$$q = 3301 \text{ (memenuhi } 3301 * 18 = 59419 - 1)$$

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

$$g = 18870 \quad \text{(dengan } h = 100)$$

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

$$x = 3223$$

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

$$y = 29245$$

---

*b. Prosedur Pembangkitan Tanda-tangan (Signing)*

1. Hitung nilai *hash* dari pesan, misalkan  $H(m) = 4321$
2. Tentukan bilangan acak  $k < q$ .

$$k = 997$$

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

3. Hitung  $r$  dan  $s$  sebagai berikut:

$$r = (g^k \pmod{p}) \pmod{q} = 848$$

$$s = (k^{-1} (H(m) + x * r)) \pmod{q}$$

$$= 7957694475 \pmod{3301} = 183$$

4. Kirim pesan  $m$  dan tanda-tangan  $r$  dan  $s$ .

---

*c. Prosedur Verifikasi Keabsahan Tanda-tangan*

1. Hitung

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

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

$$u_1 = (H(m) * w) \pmod{q} = 2026549 \pmod{3301} = 3036$$

$$u_2 = (r * w) \pmod{q} = 397712 \pmod{3301} = 1592$$

$$v = ((g^{u_1} * y^{u_2}) \pmod{p}) \pmod{q} = 848 \pmod{3301} = 848$$

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