Aplikasi Teori Bilangan dalam Tanda Tangan Digital dengan DSA

Yonatan Viody (13518120)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
yonatanviody@gmail.com

***Abstract*—Zaman sekarang sudah banyak data digital yang ada. Setiap data digital harus dijaga keasliannya dengan tanda tangan digital. Pembuatan dan verifikasi tanda tangan digital dapat dilakukan dengan banyak algoritma. Salah satunya adalah DSA. DSA memiliki beberapa persyaratan yang harus dipenuhi agar dapat dijaga keamanannya.**

***Keywords*—DSA, tanda tangan digital, persyaratan, keamanan**

I. PENDAHULUAN

Bilangan bulat adalah dasar dari teori bilangan. Dalam kehidupan sehari-hari, kita sering memanfaatkan bilangan bulat untuk mengatasi persoalan yang ada, baik secara sadar maupun tidak sadar. Contohnya adalah dalam penggunaan uang. Pada dasarnya, nominal uang adalah bilangan bulat. Dalam kegiatan jual-beli, kita sering memanfaatkan operasi yang ada pada bilangan bulat untuk menghitung harga belanjaan yang ada.

Seiring berkembangnya zaman, teori bilangan dimanfaatkan untuk berbagai hal, contoh seperti penyederhanaan perhitungan, kriptografi, dan lain-lain. Karena pemanfaatannya yang cukup banyak, teori bilangan pun menjadi salah satu teori yang harus diketahui oleh orang-orang pada zaman sekarang. Oleh karena itu, teori bilangan diajarkan pada beberapa mata kuliah di beberapa universitas. Salah satunya adalah di ITB pada mata kuliah Matematika Diskrit.

Kriptografi adalah hal yang umum ada dalam dunia digital, terutama pada era informasi ini. Komunikasi yang kita lakukan biasa bersifat rahasia sehingga kita tidak ingin agar orang lain mengetahuinya selain beberapa orang. Hal ini mudah diatasi untuk komunikasi secara langsung. Namun bagaimana untuk komunikasi melalui dunia digital? Di sinilah kriptografi bekerja. Komunikasi yang terjadi dirahasiakan sementara pada proses transmisi dan diungkapkan rahasianya saat sampai pada penerima yang seharusnya. Tidak hanya sampai di situ, kriptografi digunakan juga untuk menjaga kerahasiaan suatu data seperti tanda tangan digital.

Tanda tangan digital telah banyak digunakan oleh perusahaan-perusahaan berbasis digital untuk menjaga keaslian data digital yang dimilikinya. Banyak perusahaan berbasis permainan digital, contohnya Sony, menggunakan tanda tangan digital untuk menentukan permainan apa saja yang diterima oleh platform-nya untuk mencegah *cracking* dan lain-lain. Untuk menjaga keaslian suatu tanda tangan digital, digunakan konsep teori bilangan untuk pembuatannya. Salah satu cara membuat tanda tangan digital adalah dengan menggunakan algoritma yang bernama *Digital Signature Algorithm* (DSA). Pada dasarnya, algoritma ini aman untuk menjaga keaslian tanda tangan digital selama kita memenuhi persyaratan yang ada. Namun, karena kurangnya pengetahuan akan algoritma ini dan syaratnya, serta teori bilangan, tanda tangan digital yang dihasilkan bisa dikatakan menjadi tidak aman. Hal ini sudah terbukti oleh kasus *cracking* Playstation 3 milik perusahaan Sony yang terjadi karena perusahaan Sony tidak mengetahui persyaratan yang terdapat dalam algoritma DSA ini. Karena kelalaian yang dilakukan Sony ini, beberapa orang berhasil memecahkan tanda tangan digital Playstation 3 dan dapat membuat tanda tangan digital sendiri yang diterima oleh Playstation 3 dengan memanfaatkan teori bilangan. Oleh karena itu, penulis ingin mencoba menjelaskan algoritma DSA untuk tanda tangan digital dan menjelaskan alasan mengapa persyaratan yang ada harus dipenuhi.

II. HIMPUNAN

Himpunan adalah koleksi dari elemen-elemen dan identitasnya ditentukan oleh $x, x \in S$. Himpunan memiliki elemen yang unik, tetapi koleksi dari elemen-elemen yang tidak unik disebut sebagai himpunan ganda. Banyaknya elemen pada himpunan disebut dengan istilah kardinal (notasinya $|S|$, artinya kardinal dari himpunan S). Himpunan yang tidak memiliki elemen disebut sebagai himpunan kosong (dengan simbol $\emptyset$). Pada umumnya, himpunan dapat ditulis dalam notasi sebagai berikut:

$$\{x \mid syarat\ yang\ harus\ dipenuhi\ dari\ x\}$$

Ada beberapa simbol baku yang digunakan untuk merepresentasikan himpunan-himpunan unik:

1. $P = himpunan\ bilangan\ bulat\ positif = \{1,2,3, \dots\}$
2. $N = himpunan\ bilangan\ natural = \{1,2,3, \dots\}$
3. $Z = himpunan\ bilangan\ bulat = \{\dots, -1,0,1, \dots\}$
4. $Q = himpunan\ bilangan\ rasional$
5. $R = himpunan\ bilangan\ riil$
6. $C = himpunan\ bilangan\ kompleks$

Operasi dasar pada himpunan adalah sebagai berikut:

1. Gabungan
   Misal terdapat himpunan A dan B, maka gabungan antara A dan B adalah himpunan baru dengan elemen-elemen dari

A dan B, yang dapat dinyatakan dalam notasi $A \cup B$.

2. Irisan
   Misal terdapat himpunan A dan B, maka irisan antara A dan B adalah himpunan baru dengan elemen-elemen yang ada pada A dan B, yang dapat dinyatakan dalam notasi $A \cap B$.

3. Komplemen
   Misal terdapat himpunan A, maka komplemen dari A adalah himpunan baru dengan elemen-elemen yang tidak ada pada A, yang dapat dinyatakan dalam notasi $\bar{A}$.

4. Beda Setangkup
   Misal terdapat himpunan A dan B, maka beda setangkup antara A dan B adalah himpunan baru dengan elemen-elemen dari A dan B, tetapi tidak pada keduanya, yang dapat dinyatakan dalam notasi $A \oplus B$.

5. Selisih
   Misal terdapat himpunan A dan B, maka selisih A dengan B adalah himpunan baru dengan elemen-elemen dari A yang dikurang elemen-elemen yang ada di B, yang dapat dinyatakan dalam notasi $A - B$.

6. Perkalian
   Misal terdapat himpunan A dan B, maka perkalian A dengan B adalah himpunan baru dengan elemen-elemen berupa pasangan (x, y) dengan x elemen dari A dan y elemen dari B, yang dapat dinyatakan dalam notasi $A \times B$.

III. Relasi dan Fungsi

Relasi adalah penghubung antara dua elemen. Relasi dapat dinyatakan dalam bentuk himpunan dengan elemen berisi dua *tuple* sebagai berikut:

$$R = \{(A, B), (C, D)\}$$

Himpunan di atas menunjukkan adanya relasi antara A dengan B dan C dengan D. Dari sini relasi dapat dinyatakan dalam bentuk perkalian himpunan A (dalam kasus ini $\{A, C\}$) dengan himpunan B (dalam kasus ini $\{B, D\}$), yaitu $A \times B$.

Fungsi adalah relasi yang khusus antara dua himpunan, dengan salah satu himpunan berlaku sebagai domain dan himpunan lainnya sebagai kodomain. Fungsi disebut juga sebagai pemetaan karena memetakan nilai pada domain menjadi suatu nilai pada kodomain. Notasi fungsi adalah sebagai berikut:

$$f: A \rightarrow B$$

Fungsi ada bermacam-macam, salah satunya adalah fungsi rekursif. Fungsi rekursif adalah fungsi yang mengacu pada dirinya sendiri. Fungsi rekursif terdiri dari dua bagian:

1. Basis
   Basis adalah bagian fungsi rekursif yang berisi nilai awal. Bagian ini berfungsi untuk menghentikan proses rekursif.
2. Rekurens
   Rekurens adalah bagian fungsi rekursif yang berisi definisi fungsi dan argumennya. Argumen fungsi yang terdapat pada rekurens harus mengarahkan fungsi ke nilai awalnya, yaitu basis.

IV. Teori Bilangan

Bilangan bulat adalah bilangan yang tidak mempunyai pecahan desimal seperti 0, 2, dan -3. Bilangan bulat direpresentasikan dengan simbol himpunan **Z**. Bilangan bulat memiliki beberapa sifat dan properti sebagai berikut:

1. Komutatif
   Misal $a, b \in \boldsymbol{Z}$, maka berlaku:
   $$a + b = b + a$$
   $$a \cdot b = b \cdot a$$

2. Asosiatif
   Misal $a, b, c \in \boldsymbol{Z}$, maka berlaku:
   $$(a + b) + b = a + (b + c)$$
   $$(a \cdot b) \cdot b = a \cdot (b \cdot c)$$

3. Distributif
   Misal $a, b, c \in \boldsymbol{Z}$, maka berlaku:
   $$(a + b) \cdot c = a \cdot c + b \cdot c$$

4. Identitas
   Misal $a \in \boldsymbol{Z}$, maka berlaku:
   $$a + 0 = 0 + a$$
   $$a \cdot 1 = 1 \cdot a$$

5. Habis Membagi
   Misal $a, b \in \boldsymbol{Z}$, maka a habis membagi b jika b terdiri dari perkalian a dengan suatu bilangan bulat.
   $$a \mid b \; jika \; b = ac, c \in \boldsymbol{Z} \; dan \; a \neq 0$$

6. Pembagi Bersama Terbesar (*greatest common divisor*)
   Misal $a, b, c \in \boldsymbol{Z}$, maka pembagi bersama terbesar a dan b adalah bilangan bulat terbesar yang habis membagi a dan b, misal c.
   $$GCD(a, b) = c$$

7. Relatif Prima
   Misal $a, b \in \boldsymbol{Z}$, maka a dan b dikatakan relatif prima jika:
   $$GCD(a, b) = 1$$

8. Aritmatika Modulo
   Misal $a, b \in \boldsymbol{Z}$ dan sisa a bagi b adalah r, maka $a \; mod \; b = r$.
   $$a = b \cdot q + r$$
   $$a \; mod \; b = r$$

   Aritmatika modulo sendiri memiliki beberapa sifat khusus sebagai berikut:
   - Penjumlahan dan Pengurangan
     $$(a \pm b) \; mod \; c = \big((a \; mod \; c) \pm (b \; mod \; c)\big) \; mod \; c$$
   - Perkalian
     $$(a \cdot b) \; mod \; c = \big((a \; mod \; c)(b \; mod \; c)\big) \; mod \; c$$

9. Kongruen

Misal $a, b, m \epsilon \boldsymbol{Z}$ dan $m|a-b$, maka a kongruen dengan b mod m.

$$a \equiv b \; mod \; m$$

10. Inverse
    Misal $a \epsilon \boldsymbol{Z}$, maka x dikatakan sebagai inverse dari a jika:
    - $a + x = 0 \rightarrow x = -a$ (*additive inverse*)
    - $a \cdot x = 1 \rightarrow x = a^{-1}$ (*multiplicative inverse*)
    - $a \cdot x \equiv 1 \; mod \; n$ (*modular inverse a mod n*)

Bilangan prima adalah bilangan bulat positif yang hanya habis dibagi satu atau bilangannya sendiri. Semua bilangan bulat positif terdiri dari perkalian satu atau lebih bilangan prima. Contoh bilangan prima adalah 2, karena 2 hanya habis dibagi 1 dan 2. Syarat dari bilangan prima dapat dinyatakan notasi berikut:

$$p \; adalah \; prima \; jika \; a \mid p, \;\; b \mid p, a = 1, dan \; b = p$$

V. Algoritma Euclidean

Teorema Euclidean mengatakan bahwa jika $a, b \epsilon \boldsymbol{Z}$, a dapat dinyatakan dalam bentuk:

$$a = b \cdot q + r, \qquad q, r \epsilon \boldsymbol{Z}$$

sehingga $GCD(a, b)$ dapat dinyatakan dalam persamaan berikut:

$$GCD(a, b) = GCD(b \cdot q + r, b) = GCD(b, r)$$

Dari teorema di atas, algoritma untuk mencari $GCD(a, b)$ yang dikemukakan Euclidean dapat dinyatakan oleh persamaan fungsi rekursif sebagai berikut:

$$GCD(a, b) = \begin{cases} a, & a = b \\ GCD(b, r), & a = b \cdot q + r \; dan \; q, r \epsilon \boldsymbol{Z} \end{cases}$$

dengan syarat peletakan $a \geq b$.

VI. Teorema Euler dan Fermat

Teorema Euler mengatakan bahwa jika $m \in \boldsymbol{P}$, $a \in \boldsymbol{Z}$, dan m dan a relatif prima, maka berlaku:

$$a^{\phi(m)} \equiv 1 \; mod \; m$$

dengan $\phi(m)$ adalah fungsi totient Euler dengan bentuk persamaan:

$$\phi(m) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

Dari teorema Euler, muncullah teorema Fermat, yang mengatakan bahwa jika p adalah bilangan prima dan $a \in P$ dengan $a \; mod \; p \neq 0$, maka berlaku:

$$a^{p-1} \equiv 1 \; mod \; m$$

VII. Chinese Remainder Theorem

Suatu sistem persamaan kongruen akan memiliki solusi dalam bentuk persamaan kongruen. Misalkan terdapat k persamaan kongruen sebagai berikut:

$$x \equiv a_1 \; mod \; n_1$$
$$x \equiv a_2 \; mod \; n_2$$
$$\ldots$$
$$x \equiv a_k \; mod \; n_k$$

maka akan memiliki solusi dengan bentuk persamaan kongruen berikut:

$$x \equiv b \; mod \; (n_1 \cdot n_2 \cdot \ldots \cdot n_k)$$

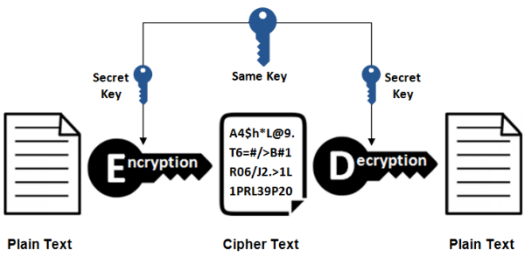
VIII. Kriptografi

Kriptografi adalah ilmu yang mempelajari teknik-teknik untuk menyembunyikan makna asli dari suatu pesan. Kriptografi biasanya digunakan untuk menjaga keamanan informasi, seperti pada aplikasi *messaging*. Kriptografi menamakan suatu pesan sebagai *plaintext* dan hasil pemrosesan pesan tersebut sebagai *ciphertext*.

Pada kriptografi, terdapat dua proses penting yaitu dekripsi dan enkripsi. Enkripsi adalah proses mengubah *plaintext* menjadi *ciphertext*, sedangkan dekripsi adalah proses mengembalikan *ciphertext* menjadi *plaintext*. Pada umumnya, suatu proses enkripsi memiliki proses dekripsi. Namun, ada juga yang proses enkripsi-nya tidak bisa dikembalikan sehingga disebut sebagai *one-way encryption* atau fungsi hash.

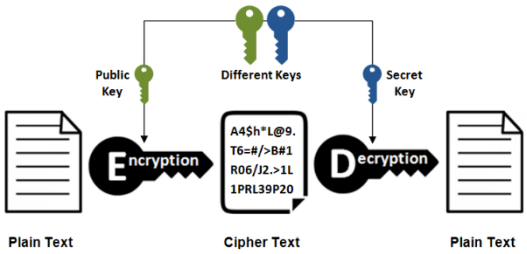
Kriptografi memiliki tiga cabang utama, yaitu:

1. Kriptografi Simetri
   Kriptografi simetri adalah kriptografi dengan proses enkripsi dan dekripsi menggunakan kunci yang sama. Skema kriptografi simetri dapat dilihat pada gambar diagram di bawah ini:



Gambar 1 Skema Kriptografi Simetri
Sumber: https://www.ssl2buy.com/wiki/wp-content/uploads/2015/12/Symmetric-Encryption.png

2. Kriptografi Kunci-Publik
   Kriptografi kunci-publik adalah kriptografi dengan proses enkripsi dan dekripsi menggunakan kunci yang berbeda. Dalam cabang ini, proses enkripsi menggunakan kunci yang disebut kunci privat (*private key*) dan proses dekripsi menggunakan kunci publik (*public key*). Skema kriptografi kunci-publik dapat dilihat pada gambar diagram di bawah ini:



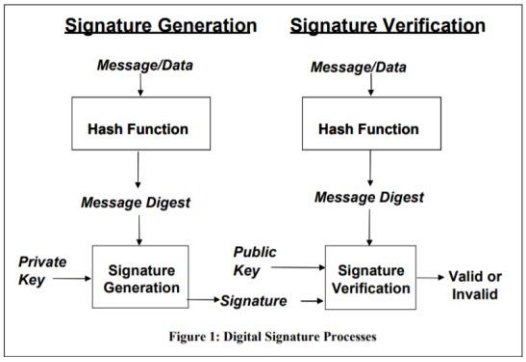
Gambar 2 Skema Kriptografi Kunci-Publik
Sumber: https://www.ssl2buy.com/wiki/wp-content/uploads/2015/12/Asymmetric-Encryption.png

3. Protokol Kriptografi
   Protokol kriptografi adalah protokol jaringan yang menggunakan algoritma kriptografi simetri dan kunci-publik. Contoh dari protokol kriptografi adalah skema Transport Layer Security (TLS) yang digunakan hampir dalam semua *Web Browser*.

VIIII. TANDA TANGAN DIGITAL

Tanda tangan digital adalah tanda tangan untuk data digital. Tanda tangan digital bukanlah tulisan tanda tangan yang di-digitisasi. Tanda digital berfungsi untuk mendeteksi keaslian suatu data digital yang telah ditanda tangan.

Proses pembuatan dan verifikasi tanda tangan digital dapat dilihat pada gambar diagram di bawah ini:



Gambar 3 Skema Pembuatan dan Verifikasi Tanda Tangan Digital
Sumber:
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

Dari gambar di atas, ada 2 langkah utama dalam pembuatan tanda tangan digital, yaitu enkripsi pesan dengan *hash function* dan dilanjutkan dengan kriptografi kunci-publik. Ada banyak algoritma kriptografi kunci-publik yang digunakan untuk tanda tangan digital, di antaranya adalah RSA, DSA, dan ECDSA. Makalah ini hanya akan membahas mengenai DSA.

Seperti yang dikatakan sebelumnya, tanda tangan digital berfungsi untuk memastikan keaslian suatu data digital, bukan untuk menjaga kerahasiaan suatu pesan. Hal ini disebabkan karena penggunaan *hash function* yang hanya berlaku satu arah sehingga pesan asli harus diketahui untuk proses verifikasi. Proses verifikasi tanda tangan digital ada bermacam-macam dan tergantung dengan algoritma pembuatan tanda tangan yang digunakan.

X. ANALISIS DSA

DSA atau *Digital Signature Algorithm* adalah salah satu algoritma kriptografi kunci-publik untuk tanda tangan digital dan merupakan salah satu komponen dari DSS (*Digital Signature Standard*).

Parameter DSA terdiri atas:

1. p – bilangan prima dengan panjang bit L
2. q – bilangan prima yang merupakan faktor dari $(p-1)$ dengan panjang bit N
3. g – angka generator dengan nilai
   $$g = h^{\frac{p-1}{q}} \bmod p \quad (1.1)$$
   dengan $h < p-1$ sehingga terpenuhi pertidaksamaan $1 < g < p$
4. x – kunci privat yang dihasilkan secara *random* pada interval $[1, q-1]$
5. y – kunci publik dengan nilai
   $$y = g^x \bmod p \quad (1.2)$$
6. k – angka unik untuk setiap pesan yang dihasilkan secara *random* pada interval $[1, q-1]$
7. m – pesan/data yang akan ditandatangani

Dari parameter di atas, yang menjadi bagian dari kunci publik adalah parameter p, q, g, y, dan m. Sedangkan sisanya adalah bagian dari kunci privat.

Untuk parameter p dan q, besar L dan N berhubungan dan telah ditentukan pada DSS sebagai berikut:

- $L = 1024, N = 160$
- $L = 2048, N = 224$
- $L = 2048, N = 256$
- $L = 3072, N = 256$

Dengan parameter DSA yang telah tersedia, kita dapat memulai proses pembuatan tanda tangan digital dengan rumus sebagai berikut:

$$r = (g^k \bmod p) \bmod q \quad (1.3)$$
$$s = \left(k^{-1}(H(m) + x \cdot r)\right) \bmod q \quad (1.4)$$

dengan $H(x)$ berupa *hash function*.

Persamaan untuk nilai k dapat diperoleh dari persamaan (1.4) dengan proses sebagai berikut:

$$s = \left(k^{-1}(H(m) + x \cdot r)\right) \bmod q$$
$$s = (k^{-1} \bmod q)\left((H(m) + x \cdot r) \bmod q\right)$$
$$s \cdot k \equiv (H(m) + x \cdot r) \bmod q$$
$$k \equiv \left(s^{-1}(H(m) + x \cdot r)\right) \bmod q$$

Ingat bahwa $1 \leq k \leq q-1$, sehingga:

$$k = \left(s^{-1}(H(m) + x \cdot r)\right) mod\ q \quad (1.5)$$

Dalam menghitung nilai s, ada kemungkinan bahwa nilai $k\ mod\ q$ tidak memiliki invers modulo sehingga digunakan cara alternatif untuk menghitung nilai invers modulo dari $k\ mod\ q$ dengan menggunakan teorema fermat (berlaku karena q adalah bilangan prima:

$$k^{q-1}\ mod\ q = 1$$

maka:

$$k^{q-2}\ mod\ q = \ k^{-1}\ mod\ q$$

Proses verifikasi tanda tangan digital dilakukan dengan persamaan:

$$w = s^{-1}\ mod\ q \quad (1.6)$$
$$u_1 = (H(m) \cdot w)\ mod\ q \quad (1.7)$$
$$u_2 = (r \cdot w)\ mod\ q \quad (1.8)$$
$$v = \left((g^{u_1} y^{u_2})\ mod\ p\right) mod\ q \quad (1.9)$$

dengan verifikasi bahwa:

$$v = r \quad (1.10)$$

Proses verifikasi tanda tangan digital dengan DSA ini memanfaatkan konsep teori bilangan, pembuktiannya adalah sebagai berikut:

- Substitusi persamaan (1.2) ke (1.9)

$$v = \left((g^{u_1}(g^x\ mod\ p)^{u_2})\ mod\ p\right) mod\ q$$

- Sederhanakan persamaan

$$v = \left((g^{u_1}(g^x)^{u_2})\ mod\ p\right) mod\ q$$
$$v = \left((g^{u_1} g^{x \cdot u_2})\ mod\ p\right) mod\ q$$
$$v = \left((g^{u_1 + x \cdot u_2})\ mod\ p\right) mod\ q$$

- Substitusi persamaan (1.7) dan (1.8) ke persamaan

$$v = \left(\left(g^{(H(m) \cdot w)\ mod\ q + x \cdot ((r \cdot w)\ mod\ q)}\right) mod\ p\right)\ mod\ q$$
$$v = \left(\left(g^{(H(m) \cdot w)\ mod\ q + (x \cdot r \cdot w)\ mod\ q}\right) mod\ p\right)\ mod\ q$$
$$v = \left(\left(g^{(H(m) \cdot w + x \cdot r \cdot w)\ mod\ q}\right) mod\ p\right)\ mod\ q$$
$$v = \left(\left(g^{((H(m) + x \cdot r) \cdot w)\ mod\ q}\right) mod\ p\right)\ mod\ q$$

- Substitusi persamaan (1.6) ke persamaan

$$v = \left(\left(g^{\left((H(m) + x \cdot r) \cdot (s^{-1}\ mod\ q)\right)\ mod\ q}\right)\ mod\ p\right)\ mod\ q$$
$$v = \left(\left(g^{\left((H(m) + x \cdot r) \cdot s^{-1}\right)\ mod\ q}\right)\ mod\ p\right)\ mod\ q$$

- Dari persamaan (1.5), kita mengetahui bahwa $(H(m) + x \cdot r) \cdot s^{-1} = k$, sehingga:

$$v = \left((g^{k\ mod\ q})\ mod\ p\right)\ mod\ q$$

- Dari persamaan (1.3), kita mengetahui bahwa $(g^k\ mod\ p)\ mod\ q = r$ dan ingat bahwa $1 \leq k \leq q - 1$, sehingga:

$v = r$ (terbukti)

Sebelumnya, telah dikatakan bahwa DSA memiliki persyaratan nilai k untuk setiap pembuatan tanda tangan digital tidak boleh sama untuk data yang berbeda. Hal ini disebabkan karena nilai x dapat diperoleh jika nilai k selalu sama.

Dari persamaan (1.5), didapat persamaan k untuk pesan ke-i

$$k_i = \left(s_i{}^{-1}(H(m_i) + x \cdot r_i)\right) mod\ q \quad (1.11)$$

Jika kita memiliki dua buah tanda tangan digital dengan k yang sama, maka berlaku:

$$k_1 = k_2 = k$$

dan

$$\left(s_1{}^{-1}(H(m_1) + x \cdot r_1)\right)\ mod\ q = \left(s_2{}^{-1}(H(m_2) + x \cdot r_2)\right)\ mod\ q$$

sehingga kita bisa mencari nilai x sebagai berikut:

- Tukar s_1 ke ruas kiri dan s_2 ke ruas kanan

$$\left(s_2(H(m_1) + x \cdot r_1)\right)\ mod\ q = \left(s_1(H(m_2) + x \cdot r_2)\right)\ mod\ q$$

- Distribusi perkalian s_1 dan s_2

$$(s_2 \cdot H(m_1) + x \cdot r_1 \cdot s_2)\ mod\ q = (s_1 \cdot H(m_2) + x \cdot r_2 \cdot s_1)\ mod\ q$$

- Kelompokkan semua nilai dengan variabel x

$$(x \cdot r_1 \cdot s_2 - x \cdot r_2 \cdot s_1)\ mod\ q = \left(s_1 \cdot H(m_2) - s_2 \cdot H(m_1)\right)\ mod\ q$$

- Kelompokkan koefisien x

$$\left(x \cdot (s_2 \cdot r_1 - s_1 \cdot r_2)\right)\ mod\ q = \left(s_1 \cdot H(m_2) - s_2 \cdot H(m_1)\right)\ mod\ q$$

- Nyatakan nilai x dalam bentuk persamaan kongruen

$$a_1 = s_1 \cdot H(m_2) - s_2 \cdot H(m_1)$$
$$a_2 = s_2 \cdot r_1 - s_1 \cdot r_2$$
$$x \equiv (a_1 \cdot a_2{}^{-1}) mod\ q$$

Ingat bahwa $1 \leq x \leq q - 1$, sehingga:

$$x = (a_1 \cdot a_2{}^{-1})\ mod\ q \quad (1.12)$$

dengan

$$a_1 = s_1 \cdot H(m_2) - s_2 \cdot H(m_1)$$
$$a_2 = s_2 \cdot r_1 - s_1 \cdot r_2$$

Dengan demikian, kita bisa membuat tanda tangan digital palsu yang tetap diterima oleh sistem verifikasi yang ada.

Contoh kasus sederhana untuk persoalan di atas adalah sebagai berikut. Misalkan kita memiliki dua pesan yaitu "Aku Cinta Matematika Diskrit" dan "Aku Mahasiswa UGM". Kedua pesan diubah menjadi representasi bilangan bulatnya:

- $m_1 = 688950441963592677899829496721048$ $131692816040425946345920840427892$
- $m_2 = 222611893993102567632408358157883742$ 14477

Lalu kita membuat parameter DSA lainnya dengan nilai sebagai berikut:

- $p = 898846567431158419739209390410128671$ $870870018417134413756367950214637558084$ $774121391020720897901181334917147746064$ $320386587791470217392044382118708259021$ $305087768662008204517910565636082374570$ $571813373385429247571677308581644298993$ $094589259580372212750055646276165834681$ $484518577384242552187592472466021270 73$
- $q = 993034308002953055245871866033232306$ 025414532589
- $g = 849569904470082581364207859089129094$ $634029249204946608679311253439481033200$ $148612345089159996450686964670420075$ $004225895425840439900555893716203169687$ $755098958013394466305660597952264078982$ $971346338587703144220494081146911016633$ $062113605022115984334537652696902467$ $561968598262889844018349454295970618655$ 658471
- $x = 277311068442250596887216137487069617$ 99821553671
- $y = 543855215872208984960751237360526090$ $781623503737955158212619344537517497490$ $880207004498868843342581916509624787540$ $419293262047671797848321742146456946311$ $123491059752010580443819990172655746870$ $657566490260580595839517173681153614688$ $536593053817300484538468322303783619739$ $139870615653372469167132263983269407 48$
- $k = 938907239186660776053935055487596351$ 308675599320

Dari parameter di atas dan *hash function* berupa $H(x) = x \bmod q$, kita menghasilkan tanda tangan digital berikut:

- $r_1 = 464729590841316682205971845899908385810626626622$
- $r_2 = 464729590841316682205971845899908385810626626622$
- $s_2 = 827165561971519364720895039508524115920270534091$
- $s_2 = 128103232548709206669362601880699779923079123708$

Lalu kita buktikan bahwa nilai x dapat kita peroleh kembali dengan persamaan (1.12).

$a_1 = -126884100442973104522147416585165730452495809341544746338086690785819396598440610684344387132137$

$a_2^{-1} \bmod q = 84895120478350323385585035483483298697649698054 6$

$x = (a_1 \cdot a_2^{-1}) \bmod q = \left(a_1 \cdot (a_2^{-1} \bmod q)\right) \bmod q$
$= 277311068442250596887216137487069617998215536 71$ (terbukti)

XI. KESIMPULAN

Algoritma-algoritma kriptografi untuk tanda tangan digital, seperti DSA, memanfaatkan teori bilangan dan memiliki persyaratannya masing-masing. Persyaratan ini ada karena suatu alasan. Contohnya seperti persyaratan nilai k harus berbeda untuk setiap pesan pada DSA. Pada analisis di bab X, terbukti bahwa jika kita memiliki dua tanda tangan digital dengan nilai k yang sama, kita dapat memperoleh kunci privat untuk memecahkan dan menghasilkan tanda tangan digital yang ada dan yang diterima sistem verifikasi yang ada.

Sebab itu, jika kita ingin menggunakan algoritma tanda tangan digital, tentu kita harus mengetahui teori bilangan dan konsep yang ada agar kita tahu apakah algoritma itu bisa dikatakan aman atau tidak.

XII. UCAPAN TERIMA KASIH

Puji syukur kepada Tuhan atas rahmat-Nya yang telah diberikan sehingga penulis dapat menyelesaikan makalah yang berjudul "Aplikasi Teori Bilangan dalam Tanda Tangan Digital dengan DSA" ini. Penulis mengucapkan terima kasih kepada orang tua dan teman-teman atas dukungannya selama ini, serta Ibu Fariska selaku dosen mata kuliah Matematika Diskrit K03 dan dosen mata kuliah Matematika Diskrit lainnya atas ilmu dan bimbingan yang telah diberikan sehingga makalah ini dapat diselesaikan.

REFERENSI

[1] Paar, Christof dan Jan Pelzl. *Understanding Cryptography: A Textbook for Students and Practitioners*. 2009. New York: Springer Science & Business Media.

[2] http://www.maths.qmul.ac.uk/~pjc/notes/nt.pdf diaskses pada 21 November 2019.

[3] https://wstein.org/ent/ent.pdf diakses pada 21 November 2019.

[4] https://resources.saylor.org/wwwresources/archived/site/wp-content/uploads/2013/05/An-Introductory-in-Elementary-Number-Theory.pdf diakses pada 21 November 2019.

[5] http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2017-2018/Digital_Signature_Standard_DSS_(2018).pdf diakses pada 21 November 2019.

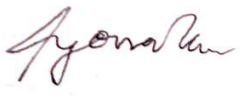
[6] http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2017-2018/Tandatangan-Digital-(2018).pdf diakses pada 21 November 2019.

[7] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf diakses pada 21 November 2019.
[8] https://www.uvm.edu/~cvincen1/files/numtheoryandcrypto.pdf diakses pada 21 November 2019.
[9] http://www.cs.yale.edu/homes/aspnes/classes/202/notes.pdf diaskes pada 29 November 2019.
[10] http://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2019-2020/Himpunan-(2019).pdf diakses pada 29 November 2019.
[11] http://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2019-2020/Relasi-dan-Fungsi-(2019).pdf diakses pada 30 November 2019.
[12] http://mathworld.wolfram.com/TotientFunction.html diakses pada 30 November 2019.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 6 Desember 2019



Yonatan Viody 13518120