PENERAPAN GRUP MULTIPLIKATIF ATAS $\mathbb{Z}_p^*$ DALAM PEMBUATAN TANDA TANGAN DIGITAL ELGAMAL

Rininda Ulfa Arizka[1], Agus Maman Abadi[2]

[1,2]*Jurusan Pendidikan Matematika,Universitas Negeri Yogyakarta*

Abstrak

Tujuan penulisan ini adalah untuk mengetahui penerapan grup multiplikatif atas $\mathbb{Z}_p^*$ dalam pembuatan tanda tangan digital ElGamal. Tanda tangan digital dapat digunakan untuk melakuakn pembuktian secara matematis bahwa data tidak mengalami modifikasi secara ilegal, sehingga bisa digunakan sebagai salah satu solusi untuk melakukan verifikasi data. Pembuatan tanda tangan digital pada umumnya didasari atas sistem kriptografi kunci publik. Salah satu sistem kriptografi kunci publik adalah sistem kriptografi ElGamal. Proses pembuatan tanda tangan digital ElGamal melalui proses *hashing*, yaitu perhitungan nilai *hash* dari suatu dokumen. Dengan menggunakan fungsi *hash* ini, maka dokumen yang terdiri dari banyak karakter bisa dimampatkan menjadi ukuran yang pendek, yakni berupa kode. Selanjutnya, teori grup multiplikatif atas $\mathbb{Z}_p^*$ digunakan pada proses pembuatan kunci. Kemudian dokumen yang dikirimkan akan diverifikasi menggunakan kunci publik dan nilai *hash*nya.

Kata kunci : Grup multiplikatif, fungsi *hash*, kriptografi, kunci publik, tanda tangan digital ElGamal.

PENDAHULUAN

Dewasa ini, perkembangan ilmu dan teknologi telah mempengaruhi segala aspek kehidupan, tak terkecuali aspek komunikasi, seperti dalam pengiriman pesan. Semakin berkembangnya teknologi, pengiriman suatu pesan juga menjadi kurang aman. Tidak menutup kemungkinan saat proses pengiriman pesan tersebut ada pihak ketiga yang ingin merubah dari pesan tersebut. Salah satu cara untuk mempertahankan kerahasiaan dari pesan tersebut, maka pesan yang akan dikirimkan disandikan menjadi kode-kode yang tidak dipahami, sehingga bila ada pihak ketiga yang ingin merubah akan kesulitan dalam menterjemahkan isi pesan yang sebenarnya. Namun, hanya dengan menyandikan pesan tersebut, tidak menutup kemungkinan pesan dirubah oleh pihak ke tiga. Untuk memperkuat kerahasiaan serta keaslian dari pesan tersebut, maka berkembanglah tanda tangan digital. Penerima pesan akan percaya bahwa pesan yang dikirimkan masih otentik, karena telah dibubuhkan tanda tangan pada pesan tersebut. Selanjutnya, untuk mengatasi permasalahan di atas, dapat diselesaikan dengan kiptografi.

Kriptografi tidak hanya menyediakan alat untuk keamanan pesan, tetapi juga sekumpulan teknik yang berguna (Rinaldi, 2006 :2). Sistem kriptografi ElGamal dikembangkan pertama kali oleh Taher Gamal pada tahun 1984. Sampai saat ini sistem kriptografi ini masih dipercaya sebagai metode untuk pengamanan pesan. Berdasarkan uraian diatas,dalam penulisan ini, akan dibahas tentang bagaimana menjaga keotentikan suatu dokumen, yaitu dengan cara pembuatan tanda tangan digital dengan menggunakan sistem kriptografi ElGamal atas $\mathbb{Z}_p^*$, dengan $\mathbb{Z}_p^*$ = {1, 2, 3, 4, ..., *p*-1} adalah himpunan bilangan bulat modulo *p* yang saling prima dengan *p*.

PEMBAHASAN

Berikut akan dibahas mengenai langkah – langkah pembuatan tanda tangan digital ElGamal atas grup $\mathbb{Z}_p^*$. Untuk lebih jelasnya akan dibahas pengantar tentang grup multiplikatif serta fungsi *hash*.

Grup Multiplikatif atas $\mathbb{Z}_p^*$

Grup multiplikatif merupakan suatu grup yang dikenai dengan operasi perkalian (*). Pada penulisan ini, dikhususkan dalam grup multiplikatif $\mathbb{Z}_p^*$. Dimana grup multiplikatif atas $\mathbb{Z}_p^*$ akan sangat berperan dalam proses pembuatan tanda tangan digital, karena bilangan-bilangan yang digunakan dalam pembuatan tanda tangan digital merupakan elemen-elemen yang ada pada grup $\mathbb{Z}_p^*$. Selain itu, pada proses pembentukan kunci dipilih suatu bilangan g yang merupakan generator dari grup $\mathbb{Z}_p^*$.

Fungsi *Hash* Satu Arah

Dalam kriptografi, terdapat sebuah fungsi yang digunakan untuk aplikasi keamanan, seperti otentifikasi dan integritas pesan. Fungsi tersebut ialah fungsi *hash*. Fungsi *Hash* adalah fungsi yang menerima masukan string yang panjangnya sembarang dan menkonversikannya menjadi string keluaran yang panjangnya tetap (Rinaldi, 2006 : 217). Fungsi *hash* bisa menerima inputan string apa saja. Jika string menyatakan pesan (*message*), maka sembarang pesan *M* yang ukurannya bebas, dimampatkan dengan fungsi *hash* melalui persamaan berikut.

$$MD = H(M) \qquad (1)$$

dengan *MD* adalah nilai *hash* atau *message diges*t dari fungsi *hash H* dengan masukan pesan *M* .

Ada beberapa cara dalam perhitungan suatu *message digest*. Penulis menggunakan operasi aritmatika yang dapat dikerjakan, misalnya menjumlahkan semua nilai huruf pada pesan, yang sebelumnya pesan sudah dikonversi ke dalam kode ASCII. Kemudian dikenakan operasi modulo 256 pada jumlahan tersebut. Kemudian menambahkan 1 pada nilainya. Dituliskan pada persamaan (2).

$$MD = [(m_1 + m_2 + \cdots + m_n) \bmod 256] + 1 \qquad (2)$$

Berikut diberikan ilustrasi bagaimana mencari nilai *hash* dari suatu dokumen.
Misalkan terdapat pesan singkat yang berisi : “Semnas MIPA UNY”
Berdasarkan pesan tersebut, akan dicari nilai *MD* (*Message digest*) nya. Langkah pertama yaitu, memecah pesan menjadi beberapa blok . Lalu masing-masing blok dikonversikan ke dalam kode ASCII. Untuk hasil konversinya, dapat dilihat pada tabel berikut.

Tabel 1. Konversi Karakter Pesan Ke Kode ASCII

i	***m_i***	**karakter**	**ASCII**	***i***	***m_i***	**karakter**	**ASCII**
1	m_1	S	83	9	m_9	I	73
2	m_2	e	101	10	m_{10}	P	80
3	m_3	m	109	11	m_{11}	A	65
4	m_4	n	110	12	m_{12}	<spasi>	32
5	m_5	a	97	13	m_{13}	U	85
6	m_6	s	115	14	m_{14}	N	78
7	m_7	<spasi>	32	15	m_{15}	Y	89
8	m_8	M	77				

Melihat Tabel 1, dapat diketahui bahwa banyaknya karakter n = 15. Lalu menjumlahkan semua karakter yang sudah dikonversi ke dalam kode ASCII menggunakan persamaan (2).

$$\begin{aligned} MD &= [(m_1 + m_2 + \cdots + m_{15}) \bmod 256] + 1 \\ &= [(83 + 101 + \cdots + 89) \bmod 256] + 1 \\ &= [1226 \bmod 256] + 1 \\ &= 203 \end{aligned}$$

Jadi nilai *hash* dari pesan singkat tersebut adalah 203.

Tanda Tangan Digital ElGamal

Tanda tangan digital merupakan alat yang digunakan untuk menjaga keotentikan dari suatu dokumen. Yang dimaksud tanda tangan digital disini bukanlah tanda tangan yang di-digitalisasi menggunakan alat *scanner*, namun suatu nilai kriptografis yang bergantung pada pesan dan pengirim pesan. Hal ini kontras dengan tanda tangan pada dokumen biasa, yang hanya bergantung pada pengirim, dan selalu sama untuk semua dokumen. Dengan tangan digital, maka integritas data dapat dijamin, disamping itu dapat digunakan untuk membuktikan keabsahan pengirim, dan nirpenyangkalan.

Tanda tangan digital merupakan suatu mekanisme yang memungkinkan pembuat pesan menambahkan sebuah kode-kode yang bertindak sebagai tanda tangannya. Jadi, tanda tangan digital dapat menjamin integritas dan sumber dari sebuah pesan. Tanda tangan digital berkembang dari suatu sistem kriptografi kunci publik. Salah satu sistem kriptografi yang digunakan ialah sistem kriptografi ElGamal. Suatu sistem kriptografi yang didasarkan pada masalah logaritma diskret. Langkah – langkah pembuatan tanda tangan digital ElGamal secara rinci dapat dilihat pada Gambar 1.

Parameter buatan yang bersifat publik	
Seorang pihak yang dapat dipercaya memilih dan kemudian mempublikasikan sebuah bilangan prima besar *p* dan akar primitif g modulo *p*	
Pengirim (*Signer*)	**Penerima (*verifier*)**
Pembuatan Kunci	
Memilih kunci privat *s*, $1 \leq s \leq p-1$ Menghitung $v = g^s mod\ p$ Mempublikasikan kunci publik (p, g,v)	
Proses Penandatanganan	
Menghitung MD dari pesan Memilih *e*, yang relatif prima dengan *p* -1 Menghitung : $R = g^e mod\ p$ dan $T = (MD - sR)e^{-1} mod\ (p-1)$	
Proses Verifikasi	
	Mengecek bahwa $1 \leq R \leq p-1$ terpenuhi Menghitung $v^R R^T$mod *p*, kemudian diperiksa bahwa $v^R R^T \equiv g^{MD}$ mod *p*

Gambar 1. Algoritma Tanda Tangan Digital ElGamal (Hoffstein, Jill, and Silverman, 2008 :443)

Contoh penggunaan tanda tangan digital pada suatu dokumen.

Misalkan Bapak Gunawan dan Bapak Masfuri, merupakan dosen di suatu universitas, akan menyampaikan suatu dokumen penting kepada bagian penyerahan nilai mahasiswa. Beliau menitipkan kepada salah seorang mahasiswa mereka untuk disampaikan pada bagian penilaian

mahasiswa. Dikarenakan isi dokumen penting, maka kedua dosen tersebut memberikan tanda tangan pada dokumen tersebut. Berikut isi dari dokumen tersebut.

> Dengan ini, diberitahukan bahwa mahasiswa kami yang bernama Wahyu Nur Habibi dengan NIM 07305141001 telah menyelesaikan ujian TA, dan mendapatkan nilai 86,5 dengan indeks A. Demikian telah dilakukan penilaian secara menyeluruh.

Dokumen tersebut telah ditandangani oleh dua orang, ini berarti terdapat dua kunci publik yang akan diberikan kepada pihak penilaian mahasiswa. Di bawah ini adalah proses pembentukan kunci oleh Bapak Gunawan dan Bapak Masfuri.

Pihak I (Bapak Gunawan)

Bapak Gunawan memilih bilangan besar p_1 = 15137 , dan g_1 = 3. Serta ia memilih s_1 = 14121. Bapak Gunawan melakukan perhitungan dengan menggunakan persamaan 3.7, kemudian diperoleh $v_1 = 3^{14121} mod\ 15137$.= 15011. Kunci privat s_1 adalah 14121 , dan kunci publik yang diberikan adalah **(p_1, g_1, v_1) = (15137, 3, 15011)**. Berdasar dari isi dokumen tersebut diperoleh nilai *hash*nya (*MD*) yaitu 111. Dan dipilih nilai e_1 = 13217. Selanjutnya adalah proses pembuatan tanda tangan. Pertama bapak Gunawan melakukan perhitungan $R_1 = {g_1}^{e_1} mod\ p_1$ = 3^{13217}mod 15137 = 5003. Kemudian diperoleh $T_1 = (MD - s_1 R_1)\ {e_1}^{-1}$ mod (p_1-1) = (111- 14121.5003)13217^{-1} mod 15136 = 12332. Jadi tanda tangan milik Bapak Gunawan adalah **(R_1, T_1) = (5003,12332).**

Pihak II (Bapak Masfuri)

Dan Bapak Masfuri memilih bilangan besar p_2 = 17011 , dan g_2 = 2. Serta ia memilih s_2 = 16982. Dengan menggunakan persamaan 3.7 Bapak Masfuri akan memperoleh $v_2 = 2^{16982} mod\ 17011 = 4688$. Dengan begitu, kunci privat s_2 adalah 16982 , dan kunci publik yang diberikan adalah **(p_2, g_2, v_2) = (17011,2,4688)**. Berdasar dari isi dokumen tersebut diperoleh nilai *hash*nya yaitu 111. Dan dipilih nilai e_2 = 13313 . Pertama bapak Masfuri melakukan perhitungan $R_2 = {g_2}^{e_2} mod\ p_2$ = 2^{13313}mod 17011 = 8603. Kemudian diperoleh $T_2 = (MD - s_2 R_2)\ {e_2}^{-1}$ mod (p_2-1) = (111- 16982.8603)13313^{-1} mod 17010 = 16885. Jadi tanda tangan milik Bapak Masfuri adalah **(R_2, T_2) = (8603,16885).**

Verifikasi oleh Pihak III (Bagian Penilaian Mahasiswa)

Nilai *hash(MD)* dari dokumen = 111

1. Tanda tangan I (Bp. Gunawan)
   Diperoleh (R_1, T_1) = (5003,12332).
   Kunci publik = (p_1, g_1,v_1) = (15137,3,15011)
   Lalu menghitung ${v_1}^{R_1} {R_1}^{T_1} mod\ p = 15011^{5003}\ 5003^{12332}$ mod 15137 = 5783. Pihak III juga menghitung ${g_1}^{MD}$ mod p_1 = 3^{111} mod 15137 = 5783. Karena ${v_1}^{R_1} {R_1}^{T_1} \equiv {g_1}^{MD}$ mod p_1 , maka verifikasi telah dilakukan.

2. Tanda tangan II (Bp. Masfuri)
   Diperoleh (R_2,T_2) = (8603,16885).
   Kunci publik = (p_2,g_2,v_2) = (17011,2,4688)
   Lalu menghitung ${v_2}^{R_2} {R_2}^{T_2} mod\ p_2 = 4688^{8603} 8603^{16885}$mod 17011 = 12240. Pihak III juga menghitung ${g_2}^{MD}$ mod p_2 = 2^{111} mod 17011 =12240. Karena ${v_2}^{R_2} {R_2}^{T_2} \equiv {g_2}^{MD}$ mod p_2 , maka verifikasi telah dilakukan.

Karena saat proses verifikasi cocok, maka dapat dikatakan bahwa dokumen yang akan diberikan kepada bagian penilaian mahasiswa tersebut sah, berasal dari Bapak Gunawan dan Bapak Masfuri, tanpa ada pengubahan isi dokumen dari pihak lain.

Berdasarkan di atas , seorang mahasiswa yang diberi kepercayaan untuk mengantarkan dokumen tersebut, ternyata mengubah isi dari dokumen tersebut. Adapun mahasiswa tersebut hanya mengubah bagian dari isi surat saja. Di bawah ini adalah surat yang telah diubah oleh mahasiswa tersebut.

> Dengan ini, diberitahukan bahwa mahasiswa kami yang bernama Dimas Setya Aji dengan NIM 07305141091 telah menyelesaikan ujian TA, dan mendapatkan nilai 86,5 dengan indeks A. Demikian telah dilakukan penilaian secara menyeluruh.

Setelah memperoleh dokumen dari mahasiswa tersebut, bagian Penilaian Mahasiswa akan memverifikasi tanda tangan pada milik Bapak Gunawan = (R_1, T_1) = (5003, 12332) dan Bapak Masfuri = (R_2, T_2) = (8603, 16885).

Verifikasi oleh Pihak III (Bagian Penilaian Mahasiswa)
Nilai *hash(MD)* dari dokumen = 254

1. Tanda tangan I (Bp. Gunawan)
   Diperoleh (R_1, T_1) = (5003, 12332).
   Kunci publik = (p_1, g_1 ,v_1) = (15137, 3, 15011)
   Lalu menghitung $v_1^{R_1} R_1^{T_1} mod\ p_1 = 15011^{5003}\, 5003^{12332} \bmod 15137 = 5783$. Selanjutnya juga dihitung $g_1^{MD} \bmod p_1 = 3^{254} \bmod 15137 = 14150$. Karena $v_1^{R_1} R_1^{T_1} \not\equiv g_1^{MD} \bmod p_1$, verifikasi tanda tangan tidak cocok.

2. Tanda tangan II (Bp. Masfuri)
   Diperoleh (R_2, T_2) = (8603, 16885).
   Kunci publik = (p_2, g_2,v_2) = (17011, 2, 4688)
   Lalu menghitung $v_2^{R_2} R_2^{T_2} mod\ p_2 = 4688^{8603}\, 8603^{16885} \bmod 17011 = 12240$. Selanjutnya dihitung $g_2^{MD} \bmod p_2 = 2^{254} \bmod 17011 = 4128$. Karena $v_2^{R_2} R_2^{T_2} \not\equiv g_2^{MD} \bmod p_2$, maka verifikasi tanda tangan tidak cocok.

Karena saat proses verifikasi tidak cocok, maka dapat dikatakan bahwa dokumen yang akan diberikan kepada bagian penilaian mahasiswa tersebut tidak sah, berasal dari Bapak Gunawan dan Bapak Masfuri, dan diindikasikan telah terjadi pengubahan isi dokumen yang dikirimkan.

KESIMPULAN

Berdasarkan pada pembahasan diatas dapat disimpulkan bahwa grup multiplikatif atas $\mathbb{Z}_p^*$dapat diterapkan pada pembuatan tanda tangan digital ElGamal. Proses penting pada tanda tangan digital ElGamal yaitu proses pembentukan kunci, proses penandatanganan serta proses verifikasi.

Pembahasan selanjutnya yang dapat dikaji mengenai metode untuk menghitung nilai *hash* yang aman dari *collision.* Sehingga bisa lebih aman dari usaha kriptanalis dalam mengubah isi dari dokumen yang dikirimkan.

DAFTAR PUSTAKA

Buchmann, Johannes A. 2000. Introduction to Cryptography. New York : Springer- Verlag.

Hoofstein, Phiper, and Silverman., 2008, *An Introduction to Mathematical Cryptography*, Springer, New York.

Iskandar, Kusrini, Sismoro, Heri. 2004. *Struktur Data dan Pemrograman dengan Pascal*. Yogyakarta :Andi offset.

Munir Rinaldi. 2006. Kriptografi. Bandung: Informatika Bandung.

Stinson, D.R., 2006, *Cryptography Theory and Practice*, Chapman & Hall/CRC, Boca Raton, Florida.