Jurnal Matematika Integratif.
Vol. 15, No. 1 (2019), pp. 39-44.

p-ISSN:1412-6184, e-ISSN:2549-903
doi:10.24198/jmi.v15.n1.20960.39-44

# Modifikasi Protokol Tanda Tangan Digital ElGamal Menggunakan General Linear Group

Maxrizal Maxrizal, Syafrul Irawadi

**STMIK Atma Luhur**
**Jl. Jendral Sudirman, Kel. Selindung Baru,**
**Kec. Pangkal Balam, Pangkal Pinang, Kepulauan Bangka Belitung**
**maxrizal@atmaluhur.ac.id, syafrul@atmaluhur.ac.id**

**Abstrak**

Protokol tanda tangan digital ElGamal mengaplikasikan ring $\mathbb{Z}_p$ pada kunci asimetri dan fungsi hash. Pada makalah ini, konsep ring $\mathbb{Z}_p$ akan digantikan dengan konsep general linear group $GL(n, \mathbb{Z}_p)$ yaitu himpunan semua matriks yang berukuran $n \times n$ atas lapangan berhingga $\mathbb{Z}_p$ dengan syarat determinan matriks tak nol. Hasil menunjukkan bahwa modifikasi protokol tanda tangan digital ElGamal dapat dibentuk dengan memodifikasi algoritma pembangkit pasangan kunci, algoritma penandatangan dokumen dan algoritma verifikasi dokumen. Modifikasi protokol yang diusulkan juga lebih unggul karena dapat bekerja pada nilai $g$ yang bukan merupakan generator pada grup siklik $\mathbb{Z}_p$. Selain itu, modifikasi protokol yang diusulkan mampu mendeteksi lebih sensitif terhadap perubahan messege digest yang diubah oleh pihak-pihak yang tak berhak.

*Kata Kunci*: modifikasi protokol tanda tangan digital ElGamal, general linear group, ring $\mathbb{Z}_p$

**Abstract**

*The ElGamal digital signature protocol applies the ring $\mathbb{Z}_p$ to the asymmetry key and hash function. In this paper, the concept of the ring $\mathbb{Z}_p$ will be replaced to the general linear group $GL(n, \mathbb{Z}_p)$ concept, which is the set of all $n \times n$-sized matrices over a finite field $\mathbb{Z}_p$ with non-zero matrix determinant requirements. The results show that the modification of the ElGamal digital signature protocol can be formed by modifying the key pair generator algorithm, document signing algorithm, and document verification algorithm. The proposed protocol modification is also superior because it can work on a value of $g$ which is not a generator in the cyclic group $\mathbb{Z}_p$. The proposed protocol modification is capable of detecting more sensitive changes in messege digest that are changed by unauthorized parties.*

*Keywords*: modification of the ElGamal digital signature protocol, general linear group, ring $\mathbb{Z}_p$

*2000 Mathematics Subject Classification*: 11T71, 94A60,14G50, 68P25
Received: 2019-02-20, Revisions: 2019-05-27, Accepted: 2019-06-18

## 1. Pendahuluan

Perkembangan informasi dan teknologi di era revolusi teknologi 4.0 telah membentuk suatu konsep baru dalam kehidupan manusia yaitu internet pada segala bidang kehidupan (The Internet of Things). Perkembangan ini didukung oleh kepentingan transformasi big data yang dikumpulkan melalui internet dan disebarkan ke seluruh penjuru dunia. Revolusi teknologi 4.0 ini adalah suatu terobosan yang bertujuan untuk memudahkan aktifitas manusia. Akan tetapi, pertukaran data melalui internet secara massif ternyata memiliki kelemahan dari aspek authentication dan integrity suatu data. Pihak penerima data akan memiliki keraguan atas data yang diterima dari pihak pengirim data. Keaslian data dan kemungkinan campur tangan pihak-pihak yang tidak berhak selalu menjadi poin penting dari pertukaran data melalui internet.

Untuk itu, bidang matematika melalui kajian aljabar terapan (kriptografi) memberikan suatu solusi pertukaran data melalui internet dengan penggunaan protokol tanda tangan digital (digital signature). Konsep ini menggunakan prinsip kriptografi asimetris dan fungsi hash, dengan tujuan untuk meyakinkan penerima pesan bahwa pesan yang dikirim asli dan dikirim dari pengirim yang benar.

Salah satu konsep protokol tanda tangan digital yang masih dipakai sampai sekarang adalah protokol tanda tangan digital ElGamal. Proses penandatangan digital data (pesan) dimulai dengan proses pembuatan algoritma pembangkit kunci oleh pihak pengirim pesan yaitu $v = g^s \bmod p$, dengan $p$ adalah bilangan prima. Kemudian diperoleh kunci publik $(v, g, p)$ dan kunci privat $(s)$. Selanjutnya, pihak pengirim pesan menghitung tanda tangan dengan rumus $r = g^e \bmod p$ dan $t = (z - sr)\, e^{-1} \bmod (p-1)$, dengan $z = messege\ \ digest$ dan $(e, p-1) = 1$. Tanda tangan $(r, t)$ dan kunci publik $(v, g, p)$ siap dikirim ke pihak penerima pesan. Setelah pesan bertandatangan digital diterima oleh pihak penerima pesan, nilai hash $z$ dihitung. Selanjutnya, pihak penerima pesan cukup memverifikasi tanda tangan dengan menghitung nilai $v^r r^t \equiv g^z \bmod p$. Jika persamaan $v^r r^t \equiv g^z \bmod p$ berlaku, maka data (pesan) yang diterima terjamin keasliannya [1], [2].

Secara matematis, protokol tanda tangan digital ElGamal masih menggunakan konsep bilangan bulat (integer), yaitu menggunakan ring $\mathbb{Z}_p$. Untuk itu, pada makalah ini akan diusulkan suatu modifikasi dengan menggantikan ring $\mathbb{Z}_p$ menjadi himpunan matriks-matriks yang dinamakan general linear group $GL(n, \mathbb{Z}_p)$ yaitu himpunan semua matriks yang berukuran $n \times n$ atas lapangan berhingga (finite field) $\mathbb{Z}_p$ yang memiliki determinan tak nol [3]-[5]. Selanjutnya, diperoleh fakta bahwa kekuatan protokol tanda tangan digital ElGamal terletak pada pemilihan $g$ sebagai generator dari grup siklik $\mathbb{Z}_p$. Jika dipilih $g$ yang bukan generator dari grup siklik $\mathbb{Z}_p$ maka terdapat kemungkinan tanda tangan yang tidak asli oleh pihak-pihak yang tidak berhak (penyadap pesan). Untuk itu, pada makalah ini akan digunakan konsep general linear group agar ruang verifikasi dokumen pada penerima pesan menjadi lebih besar sehingga lebih sensitif atas perubahan $z = messege\ digest$ oleh pihak-pihak yang tidak berhak. Pemilihan konsep general linear group juga diharapkan dapat memperbaiki protokol tanda tangan digital ElGamal sehingga tidak perlu memastikan bahwa protokol bisa bekerja dengan baik jika ada elemen generator pada grup siklik $\mathbb{Z}_p$.

## 2. Metode Penelitian

Penelitian ini merupakan penelitian studi pustaka. Referensi [1], [2] menjelaskan protokol tanda tangan digital ElGamal dan variannya. Selanjutnya, pada referensi [5] menjelaskan konsep general linear grup pada sistem kripto RSA. Selanjutnya, peneliti mengadopsi referensi diatas dan [3], [4] untuk memodifikasi protokol tanda tangan digital ElGamal menggunakan konsep general linear group $GL(n, \mathbb{Z}_p)$. Peneliti juga harus memastikan syarat tambahan agar protokol tanda tangan digital ElGamal ini dapat diaplikasikan atas $GL(n, \mathbb{Z}_p)$. Syarat tambahan bisa berupa manipulasi persamaan-persamaan aljabar pada algoritma pembangkit pasangan kunci, penandatangan dokumen dan verifikasi dokumen. Hal ini dilakukan dengan

tujuan agar modifikasi protokol tanda tangan digital ElGamal yang diusulkan dapat bekerja dengan baik.

## 3. Hasil dan Pembahasan

3.1. ***General Linear Group.*** General linear group $GL(n, F_q)$ didefinisikan sebagai himpunan semua matriks yang berukuran $n \times n$ atas lapangan berhingga (finite field) dengan syarat determinan matriks tak nol. Secara matematis, dinotasikan $GL(n, F_q)$=$\{A\,(|A)$ adalah matriks berukuran $n \times n$ dengan entri-entri $F_q$ dan $\det(A) \neq 0\}$. Pada penelitian ini, dipilih $F_q = \mathbb{Z}_p$ sehingga diperoleh $GL(n, \mathbb{Z}_p)$. Karena $p$ prima maka elemen invers dari elemen-elemen tak nol selalu ada atas modulo $p$ [3][5].

3.2. **Protokol Tanda Tangan Digital ElGamal.** Protokol tanda tangan digital ElGamal dikembangkan menggunakan prinsip bilangan prima $p$ yang besar. Protokol ini dimulai dengan algoritma pembangkit kunci dan penandatangan digital oleh pihak pengirim pesan [1], [2]. Selanjutnya pihak penerima pesan hanya melakukan verifikasi data. Secara umum, protokol tanda tangan digital ElGamal disajikan pada tabel berikut:

Tabel 1. Skema protokol tanda tangan digital ElGamal

| | | |
|---|---|---|
| Pihak Pengirim Pesan | Pembangkit pasangan Kunci | $v = g^s \bmod p$<br>Kunci publik $(v, g, p)$<br>Kunci privat $(s)$ |
| | Penandatanganan dokumen | $r = g^e \bmod p$<br>$t = (z - sr)\, e^{-1} \bmod (p-1)$<br>Syarat $(e, p-1)$=1 |
| Pihak Penerima Pesan | Memverifikasi dokumen | $v^r r^t \equiv g^z \bmod p$ |

3.3. **Modifikasi Protokol Tanda Tangan Digital ElGama.** Berdasarkan protokol tanda tangan digital ElGamal, ring $\mathbb{Z}_p$ akan digantikan dengan $GL(n, \mathbb{Z}_p)$ untuk menghasilkan modifikasi yang diusulkan. Langkah pertama, dibentuk persamaan matriks $V = (gG)^s \bmod p$. Perhatikan bahwa $G \in GL(n, \mathbb{Z}_p)$ dan $g \in \mathbb{Z}_p$ sehingga $V \in GL(n, \mathbb{Z}_p)$. Dengan demikian, diperoleh kunci publik $(V, gG, p)$ dan kunci privat $(s)$. Langkah kedua, dibentuk tiga persamaan berikut yaitu $r = g^e \bmod p$, $R = rG^e \bmod p$, dan $t = e^{-1}(-sr + z) \bmod (p-1)$, dengan $z = messege\ digest$ dan $FPB(e, p-1) = 1$. Perhatikan bahwa telah diperoleh tanda tangan digital $(r, R, t)$.

Langkah ketiga, merumuskan fungsi matematika untuk memverifikasi tanda tangan digital, yaitu:

$$\begin{aligned}
V^r R^t &= ((gG)^s)^r (rG^e)^t \\
&= ((gG)^s)^r (g^e G^e)^t \\
&= ((gG)^s)^r ((gG)^e)^t \\
&= (gG)^{sr} ((gG)^e)^t \\
&= (gG)^{sr} (gG)^{et} \\
&= (gG)^{sr} (gG)^{ee^{-1}(-sr+z)} \\
&= (gG)^{sr} (gG)^{-sr} (gG)^z \\
&= (gG)^z
\end{aligned}$$

Perhatikan bahwa berlaku $g^e G^e = \underbrace{g.g\cdots g}_{e\ faktor}.\underbrace{G.G\cdots G}_{e\ faktor} = \underbrace{gG.gG\cdots gG}_{e\ faktor} = (gG)^e$ . Hal ini karena $g \in \mathbb{Z}_p$, sehingga perkalian suatu matriks dan suatu bilangan bulat (integer) bersifat komutatif. Selanjutnya, perhatikan persamaan $(gG)^{-sr} = \left((gG)^{-1}\right)^{sr}$. Hal ini menunjukan bahwa $G^{-1}$ harus selalu ada dan konsep general linear group menjamin eksistensi dari $G^{-1}$. Jika $G \in GL(n, \mathbb{Z}_p)$ maka $\det(G) \neq 0$ sehingga pasti selalu memiliki invers atas $\mathbb{Z}_p$. Jadi, diperoleh persamaan matematika untuk memverifikasi tanda tangan digital yaitu $V^r R^t = (gG)^z \bmod p$.

Berdasarkan uraian diatas, diperoleh modifikasi protokol tanda tangan digital ElGamal yang diusulkan seperti tabel dibawah ini:

Tabel 2. Skema modifikasi protokol tanda tangan digital ElGamal yang diusulkan

| | | |
|---|---|---|
| Pihak Pengirim Pesan | Pembangkit pasangan Kunci | $v = gG^s \bmod p$<br>Kunci publik $(v, gG, p)$<br>Kunci privat $(s)$ |
| | Penandatanganan dokumen | $r = g^e \bmod p$<br>$R = rG^e \bmod p$<br>$t = (z - sr)\, e^{-1} \bmod (p-1)$<br>Syarat $(e, p-1)$=1 |
| Pihak Penerima Pesan | Memverifikasi dokumen | $V^r R^t = (gG)^z \bmod p$ |

Berdasarkan tabel diatas, titik awal modifikasi protokol yang diusulkan adalah memilih matriks $G$ agar memiliki invers.. Untuk memastikan eksistensi $G^{-1}$, maka dipilih matriks $G \in GL(n, \mathbb{Z}_p)$. Selanjutnya, diberikan tabel perbandingan protokol tanda tangan digital ElGamal dan modifikasi protokol tanda tangan digital ElGamal yang diusulkan.

Tabel 3. Skema perbandingan protokol tanda tangan digital ElGamal dan protokol yang diusulkan

| | Protokol tanda tangan digital ElGamal | Modifikasi protokol yang diusulkan |
|---|---|---|
| Diaplikasikan pada Pembangkit pasangan kunci | Ring $\mathbb{Z}_p$<br>$v = g^s \bmod p$<br>Kunci publik $(v, g, p)$<br>Kunci privat $(s)$ | General linear group $GL(n, \mathbb{Z}_p)$<br>$V = (gG)^s \bmod p$<br>Kunci publik $(V, gG, p)$<br>Kunci privat $(s)$ |
| Penandatangan dokumen | $r = g^e \bmod p$<br>$t = (z - sr)\, e^{-1} \bmod (p-1)$<br>Syarat $(e, p-1) = 1$<br>Tanda tangan $(r, t)$ | $r = g^e \bmod p$<br>$R = rG^e \bmod p$<br>$t = (z - sr)\, e^{-1} \bmod (p-1)$<br>Syarat $(e, p-1) = 1$<br>Tanda tangan $(r, R, t)$ |
| Memverifikasi dokumen | $v^r r^t \equiv g^z \bmod p$<br>Berupa integer | $V^r R^t = (gG)^z \bmod p$<br>Berupa matriks $n \times n$ |

Kekuatan protokol tanda tangan digital ElGamal terletak pada pemilihan elemen $g$ yang merupakan generator dari grup siklik $\mathbb{Z}_p$ . Jika dipilih $g$ bukan generator dari grup siklik $\mathbb{Z}_p$ maka akan memungkinkan penandatangan yang tidak sah dari pihak-pihak yang tidak berhak. Selanjutnya, modifikasi protokol tanda tangan digital ElGamal yang diusulkan ternyata dapat membantu memberikan ruang verifikasi yang lebih besar sehingga lebih sensitif atas perubahan $z = messege\ digest$ oleh pihak-pihak yang tidak berkepentingan. Perhatikan bahwa dalam proses verifikasi dokumen oleh penerima pesan, yang diperiksa adalah matriks yang berukuran $n \times n$, bukan lagi berupa integer.

3.4. **Contoh Protokol Tanda Tangan Digital ElGamal (g bukan generator $\mathbb{Z}_p$). Algoritma Pembangkit Pasangan Kunci**
Alice akan mengirim dokumen digital melalui jaringan internet ke Bob. Alice memilih $g = 2$, $s = 4$ dan $p = 31$. Jelas bahwa bukan merupakan generator pada grup siklik $\mathbb{Z}_{31}$. Selanjutnya, Alice menghitung $v = g^s \bmod p = 16$. Alice memperoleh kunci publik $(v = 16, g = 2, p = 31)$ dan kunci privat $(s = 4)$.

**Algoritma Tanda Tangan Digital**
Asumsikan data digital Alice adalah $z = 13$. Alice memilih $e = 17$ dan menghitung $r = g^e \bmod p = 4$ serta $t = (z - sr)\, e^{-1} \bmod p = 21$. Alice memperoleh tanda tangan digital $(r = 4, t = 21)$. Alice mengirimkan kunci publik dan tanda tangan digital ke Bob.

**Algoritma Verifikasi Pesan**
Bob menerima kunci publik dan tanda tangan digital dari Alice. Berdasarkan perhitungan **fungsi hash**, Bob mendapatkan $z = 13$ dari dokumen yang ia terima. Bob menghitung

$$v^r r^t \bmod p = g^z \bmod p = 8$$

Karena persamaan $v^r r^t \bmod p \equiv g^z \bmod p$ berlaku, maka pesan yang dikirim oleh Alice ke Bob masih terjamin keasliannya. Bob yakin pesan atau dokumen tersebut benar-benar berasal dan dibuat oleh Alice.

**Serangan Pada Tanda Tangan Digital**
Asumsikan terdapat pihak yang tidak berhak yang menyadap pesan Alice, sebelum pesan itu diterima Bob dan mengubah fungsi hash dokumen menjadi $z = 18$. Selanjutnya, pihak penyadap seolah-olah sebagai Alice mengirimkan pesan ke Bob dan mengunakan kunci publik Alice. Bob melakukan $v^r r^t \bmod p = g^z \bmod p = 8$. Perhatikan bahwa pesan telah diubah dan telah ditandatangani oleh pihak penyadap. Tetapi Bob tidak bisa mendeteksi perubahan pesan karena secara matematis dihasilkan nilai yang sama yaitu $v^r r^t \bmod p = g^z \bmod p = 8$. Jadi, pada protokol tanda tangan digital ElGamal, jika $g$ bukan generator pada grup siklik $\mathbb{Z}_p$ maka terdapat kemungkinan tanda tangan yang tidak asli oleh pihak-pihak yang tidak berhak (penyadap pesan).

3.5. **Contoh Modifikasi Protokol Tanda Tangan Digital ElGamal yang Diusulkan (g bukan generator $\mathbb{Z}_p$). Algoritma Pembangkit Pasangan Kunci**
Asumsikan Alice menggunakan data yang sama dengan Contoh 3.4 $(g = 2, s = 4, p = 31)$. Selanjutnya, Alice membentuk $G = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix} \in GL\,(3, \mathbb{Z}_{31})$. Selanjutnya, Alice menghitung

$$V = (gG)^s \bmod p = \begin{bmatrix} 13 & 2 & 13 \\ 13 & 13 & 2 \\ 2 & 13 & 13 \end{bmatrix} \bmod 31$$

. Alice memperoleh kunci publik

$$\left( V = \begin{bmatrix} 13 & 2 & 13 \\ 13 & 13 & 2 \\ 2 & 13 & 13 \end{bmatrix}, gG = \begin{bmatrix} 2 & 4 & 6 \\ 6 & 2 & 4 \\ 4 & 6 & 2 \end{bmatrix}, p = 31 \right)$$

dan kunci privat $(s = 4)$.

**Algoritma Tanda Tangan Digital Pesan**
Asumsikan data yang akan dikirim oleh Alice adalah $z = 13$. Alice memilih $e = 17$ karena $(e, p - 1) = (17, 30) = 1$. Selanjutnya Alice menghitung,

$$r = g^e \bmod p = 4$$

$$R = rG^e \bmod p = \begin{bmatrix} 1 & 27 & 14 \\ 14 & 1 & 27 \\ 27 & 14 & 1 \end{bmatrix}$$

$$t = (z - sr)\, e^{-1} \bmod (p - 1) = 21$$

Alice memperoleh tanda tangan digital $(r, R, t) = \left(4, \begin{bmatrix} 1 & 27 & 14 \\ 14 & 1 & 27 \\ 27 & 14 & 1 \end{bmatrix}, 21\right)$. Alice mengirimkan kunci publik dan tanda tangan digital ke Bob.

**Algoritma Verifikasi Pesan**

Bob menerima kunci publik dan tanda tangan digital dari Alice. Berdasarkan perhitungan *fungsi hash*, Bob mendapatkan $z = 13$ dari dokumen yang ia terima. Bob menghitung

$$V^r R^t \bmod p = (gG)^z \bmod p = \begin{bmatrix} 12 & 16 & 20 \\ 20 & 12 & 16 \\ 16 & 20 & 12 \end{bmatrix}$$

Karena persamaan $V^r R^t \bmod p = (gG)^z \bmod p$ berlaku, maka pesan yang dikirim oleh Alice ke Bob masih terjamin keasliannya.

**Serangan Pada Tanda Tangan Digital**

Asumsikan terdapat pihak yang tidak berhak ternyata menyadap pesan dan mengubah data $z$ menjadi $z = 18$. Selanjutnya, pihak penyadap seolah-olah sebagai Alice mengirimkan pesan ke Bob dan mengunakan kunci publik Alice. Bob menghitung $V^r R^t \bmod p = \begin{bmatrix} 12 & 16 & 20 \\ 20 & 12 & 16 \\ 16 & 20 & 12 \end{bmatrix}$ dan $(gG)^z \bmod p = \begin{bmatrix} 3 & 18 & 18 \\ 18 & 3 & 18 \\ 18 & 18 & 3 \end{bmatrix}$ Perhatikan bahwa berlaku $V^r R^t \bmod p \neq (gG)^z \bmod p$. Hal ini menandakan bahwa pesan telah diubah dan ditandatangani oleh pihak-pihak yang tidak berhak (pihak penyadap pesan). Tetapi Bob bisa mendeteksi perubahan pesan karena secara matematis dihasilkan nilai yang tak sama. Jadi, Bob yakin bahwa pesan yang ia terima bukan pesan asli yang dikirim Alice.

Perhatikan bahwa modifikasi protokol tanda tangan digital ElGamal yang diusulkan ternyata mampu bekerja pada elemen yang bukan merupakan generator dari grup siklik $\mathbb{Z}_p$. Protokol ini juga mampu mendeteksi perubahan messege digest lebih sensitif terhadap serangan oleh pihak-pihak yang tak berhak, sehingga pesan yang tidak asli terdeteksi.

## 4. Simpulan

Dari hasil dan pembahasan yang telah dipaparkan, diperoleh kesimpulan bahwa protokol tanda tangan digital ElGamal pada ring $\mathbb{Z}_p$ dapat digantikan menggunakan konsep general linear group $GL(n, \mathbb{Z}_p)$ yaitu himpunan semua matriks yang berukuran $n \times n$ atas lapangan berhingga (finite field) $\mathbb{Z}_p$ dengan syarat determinan matriks tak nol. Modifikasi protokol yang diusulkan juga lebih unggul karena dapat bekerja pada nilai $g$ yang bukan merupakan generator pada grup siklik $\mathbb{Z}_p$. Selain itu, modifikasi protokol yang diusulkan mampu mendeteksi lebih sensitif terhadap perubahan messege digest yang diubah oleh pihak-pihak yang tak berhak.

## Daftar Pustaka

[1] T. ElGamal, 1985, A Public Key Cryptosystem and A Signature Based on Descrete Logarithms, *IEEE Trans. Inf. Theory*, vol. 31, no. 4, pp. 469472.

[2] O. Khadir, 2015, Insecure primitive elements in an ElGamal signature protocol, *J. Discret. Math. Sci. Cryptogr.*, vol. 18, no. 3, pp. 237245.

[3] D. S. Dummit and R. M. Foote, 2004, Abstract Algebra, 3rd ed. *John Wiley & Sons Inc.*

[4] H. Anton and C. Rorres, 2004, Elementary Linear Algebra: Applications Version. *Wiley eGrade.*

[5] A. D. Hartanto, D. Junia, and E. Palupi, 2016, Konstruksi Sistem Kripto Menggunakan General Linear Group, *Pros. Semin. Nas. Aljabar USD 2016*, pp. 203214.