Penerapan Kriptografi Kunci Publik El Gamal dalam Tanda Tangan Digital

William Juniarta Hadiman
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Bandung, Indonesia
13516026@std.stei.itb.ac.id

***Abstract*—Dalam pengiriman informasi di internet, ketakutan dapat muncul ketika pesan yang diberikan dari pengirim ke penerima merupakan pesan yang palsu yang dapat menimbulkan perpecahan. Maka penting untuk mengetahui apakah pengirim sebenarnya dari suatu pesan adalah seseorang yang asli salah satu cara menggunakan algoritma kunci publik el-gamal untuk tanda tangan digital**

Keywords—El-gamal; kriptografi; tanda tangan digital

I. PENDAHULUAN

Pada zaman-zaman sekarang, peradaban manusia terus maju. Hal ini juga terjadi pada teknologi. Teknologi adalah salah satu hal yang memiliki perkembangan signifikan beberapa tahun belakangan ini dan menjadi sangat penting dalam kehidupan manusia. Teknologi ini sangat memudahkan kehidupan manusia. Salah satu bentuk dari teknologi yang penting digunakan dalam kehidupan sekarang adalah pertukaran informasi.

Manusia hidup memiliki suatu keterbatasan. Dalam bumi yang sangat besar ini, sulit untuk memberikan suatu informasi secara fisik ke negara-negara di luar. Oleh karena itu pertukaran Informasi dalam teknologi sangat memudahkan manusia untuk beraktivitas. Dari kegiatan perkantoran, telepon memudahkan manusia untuk melakukan perbaruan terhadap harga barang, kemudian dari sekolah yang saat ini sedang mengadakan kegiatan di rumah karena adanya pandemi COVID-19, sangat terbantu dengan adanya pertukaran informasi yang tidak tergantung dari jarak dengan teknologi ini.

Namun, banyaknya informasi yang berlalu lalang dalam internet membuat berbagai orang yang tidak baik menginginkan informasi yang dapat menguntungkan dirinya sendiri seperti informasi keuangan bank, informasi personal seseorang, dan informasi lainnya. Oleh karena itu, perlu adanya pengamanan terhadap data yang berlalu lalang di internet. Teknik untuk pengamanan data dinamakan KRIPTOGRAFI.

Dalam cabang kriptografi sendiri, terdapat berbagai macam cara untuk pengamanan data. Salah satu yang akan kita lihat adalah kriptografi kunci publik. Contoh dalam kriptografi kunci publik adalah algoritma el gamal.

II. KRIPTOGRAFI KUNCI PUBLIK

A. Definisi Kriptografi dan Kriptografi Kunci Publik

Kriptografi adalah suatu cabang ilmu yang mempelajari teknik matematika. Tujuannya adalah untuk menjaga aspek penting dalam pertukaran informasi seperti integritas data, kerahasiaan, dan otentikasi. Dengan adanya Kriptografi ini, data pesan yang kita kirimkan kepada orang lain tidak dapat diketahui dan dimanfaatkan oleh pihak ketiga.

Kriptografi kunci publik sendiri adalah suatu jenis dari kriptografi sendiri dimana kunci publik sendiri adalah bagian didalamnya. Dalam kriptografi kunci publik, terdapat 2 macam kunci yang digunakan yaitu kunci publik dan kunci privat. Dengan adanya 2 macam kunci ini, menjamin keamanan kunci yang tidak diketahui oleh orang luar meskipun dikirimkan melalui jalur yang kurang aman.

B. Terminologi

Berikut adalah terminologi dari kriptografi kunci publik sendiri.

1) Plaintext (pesan) : Suatu data yang yang berisi informasi yang dapat dimengerti maknanya. Dalam dunia informasi, pesan dapat berupa teks, gambar, maupun video

2) Ciphertext : Suatu data pesan yang sudah diubah sedemikian rupa sehingga tidak dapat dimengerti baik oleh siapapun

3) Sender (pengirim) : Pihak yang mengirimkan pesan kepada orang lain

4) Receiver (penerima) : Pihak yang menerima pesan dari orang lain

5) Enkripsi : Proses untuk mengubah plainteks menjadi cipherteks

6) Dekripsi : Proses untuk mengubah cipherteks menjadi plainteks

7) Penyadap : Pihak ketiga yang ingin mengetahui dan memanfaatkan informasi dari pengirim ke penerima

8) Kunci : Suatu data yang digunakan sebagai parameter dalam suatu enkripsi ataupun dekripsi

9) Hash : suatu data dengan jumlah data yang tetap tujuannya untuk keteraturan dan menyimpanan data ke memory yang lebih sedikit.

C. Kunci

Sesuai dengan terminologi sebelumnya, kunci adalah suatu data yang digunakan sebagai parameter dalam suatu enkripsi ataupun dekripsi. Dalam kriptografi, ada 2 macam kunci yang digunakan yaitu kunci simetri ataupun kunci publik.

1) Kunci simetri : kunci yang digunakan untuk melakukan enkripsi dan dekripsi sama

2) Kunci publik : kunci yang digunakan untuk melakukan enkripsi dan dekripsi berbeda

D. Kunci Publik dan Kunci Privat

1) Definisi

Dalam menggunakan kriptografi kunci publik, akan ada 2 macam kunci yaitu kunci publik dan kunci privat. Kunci publik adalah kunci yang tidak disembunyikan atau dengan kata lain, orang lain yang ingin tahu kunci tersebut, boleh mengetahuinya. Sedangkan kunci privat adalah kunci yang disembunyikan, tidak boleh diketahui oleh orang lain.

2) Penggunaan

Kunci publik digunakan saat pengirim akan melakukan enkripsi untuk dikirimkan kepada penerima. Enkripsi akan mengikuti proses matematika :

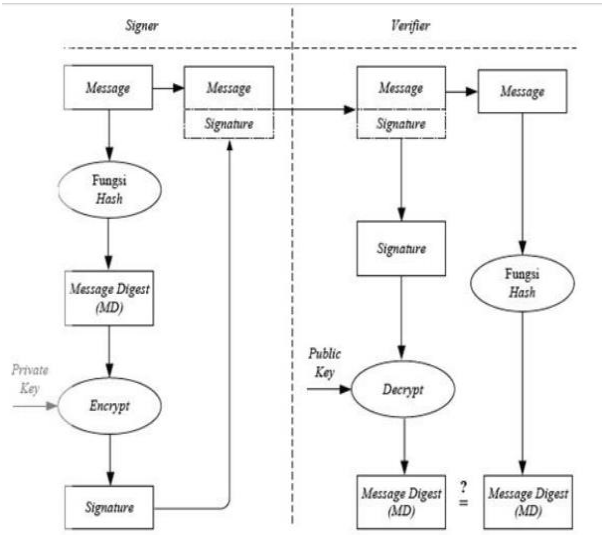
$$\mathbf{E_{KunciPublik}(Plainteks) = Ciphterteks}$$

Kunci privat digunakan saat penerima akan mekakukan dekripsi untuk mengethaui pesan yang dikirimkan oleh pengirim. Dekripsi akan mengikuti proses matematika :

$$\mathbf{D_{KunciPrivat}(Cipherteks) = Plainteks}$$

E. Tanda Tangan Digital

Tanda tangan digital sama seperti tanda tangan pada umumnya dan bertujuan untuk memberikan tanda suatu entitas untuk mengikat identitas menjadi satu bagian informasi. Proses tanda tangan digital sebagai berikut.



III. PENERAPAN DALAM TANDA TANGAN DIGITAL

Proses pembuatan algoritma tanda tangan digital menggunakan el-gamal adalah sebagai berikut

1. Membentuk kunci
    a. Pilih suatu bilangan prima p
    b. Pilih 2 buah bilangan prima g dan s, yang memenuhi syarat diantara 1 sampai p-1
    c. Hitung nilai $v = g^s \bmod p$
    d. P dan v bisa dipublikasi tetapi jangan publikasi nilai s
2. Proses Penandatanganan
    a. Menghitung nilai hash (Message digest)
        i. Pesan dipotong menjadi blok pesan, dengna 1 blok persan terisi dengna 1 buah karakter
        ii. Konversi masing-masing karakter ke dalam ASCII
        iii. Lakukan perhitungan MD = $(m_1 + m_2 + m_3 + ... + m_{akhir}) \bmod 256 + 1$
    b. Menghitung nilai kriptografis dokumen
        i. Pilih nilai e yang relatif prima dengan p-1
        ii. Hitung nilai
            1. $R = g^e \bmod p$
            2. $T = (MD - sR)e^{-1} \bmod (p-1)$
        iii. Bubuhkan (R, T) pada dokumen. R dan T ini adalah nilai kriptografis.
    c. Kirimkan dokumen
3. Proses Verivikasi Tanda Tangan Visual
    a. Hitung nilai MD
    b. Cek nilai R ada dalam rentang 1 sampai dengan p-1
    c. Hitung nilai $v^R R^T$ kongruen dengan $g^{MD} \bmod p$

Jika nilai perhitungan mod p terpenuhi, maka dokumen berasal dari pengirim yang asli

IV. KESIMPULAN

1) Teknik Kriptografi dapat mengatasi keamanan dari pesan yang dikirimkan

2) Tanda tangan digital dapat menjamin keaslian dari pengiriman pesan

3) Algoritma kunci publik el gamal dapat digunakan untuk tanda tangan digital

REFERENCES

[1] https://tematika.uajm.ac.id/index.php/tematika/article/view/83/64

[2] http://repository.amikom.ac.id/files/Publikasi_06.12.1748.pdf

[3] https://jurnal.unimed.ac.id/2012/index.php/cess/article/view/4037

[4] http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2017-2018/Pengantar-Kriptografi-(2018).pdf

[5] https://journal.unnes.ac.id/nju/index.php/sji/article/view/6115/4910

[6] https://jurnaleeccis.ub.ac.id/index.php/eeccis/article/view/95/94