Seminar Nasional Teknologi Komputer & Sains (SAINTEKS)
SAINTEKS 2020
ISBN: 978-602-52720-7-3
Februari 2020
Hal 627 - 630

Analisa Sistem Keamanan Biometrik Dengan Otentikasi Pada *ECDSA* Algorithm

Hanna Willa Dhany

Sains dan Teknologi, Sistem Komputer Universitas Pembangunan Pancabudi Medan, Medan, Indonesia.
E-mail: hdhany@dosen.pancabudi.ac.id

Abstrak−Hanya pemilik informasi lah yang dapat mengubah sebuah informasi. Maka perlu dilakukan sebuah pengamanan yang ketat agar informasi tersebut tetap terjaga kerahasiaannya. Dalam dunia *cyber* yang lebih trend saat ini, ancaman akan keamanan data sudah sangat beresiko besar. Kebanyakan orang-orang yang telah memiliki kemampuan untuk melakukan penyusupan dalam sistem keamanan dan penyusup itu melakukan cara apapun agar mendapatkan data atau informasi yang diinginkan oleh pelaku kejahatan *cyber*. Keamanan dalam pertukaran data sangatlah penting dalam penggunaan internet. Maka dari itu perlu adanya tindakan dalam melakukan pengamanan terhadap pesan agar terjaga kerahasaiaannya dai hal-hal yang tidak diinginkan termasuk adanya psnyusup yang ingin mengambil data tersebut. Seperti halnya saat ini dalam pengiriman data banyak terjadi perubahan dan penukaran data yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab dan mengambil keuntungan. Apabila ada seseorang yang tidak berhak meniru atau mengambil dengan cara melakukan pemalusn suatu pesan yang ada sehingga orang menerima informasi tersebut, menyangka pesan tersebut berasal dariorang yang seharusnya menjadi penerima pesan. Di dalam pengiriman pesan melalui email sangat dibutuhkan keamanan agar menjaga keutuhan pesan. Kriptografi kurva eliptik termasuk kedalam sistem kriptografi kunci publik yang mendasarkan keamanannya.

Kata kunci : Kriptografi, Otentikasi pesan, *ECDSA*, Enkripsi, Dekripsi.

1. PENDAHULUAN

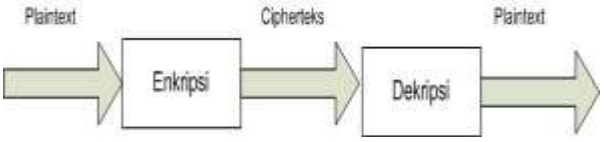
Beberapa tipe kunci yang dimiliki oleh tandatangan digital yang paling sering digunakan yaitu RSA, DSA, ECDSA. ECDSA merupakan kurva eliptik analog dari DSA. Standar ANSI menerimanya ditahun 1999, dan IEEE dan NIST standar diterima ditahun 2000. Melihat latar belakang di atas, maka Penelitian ini membahas tentang sebuah keamanan dalam pengiriman pesan agar terjaga kerahasiaannya dari orang yang ingin mengambil informasi data secara paksa.

2. METODE PENELITIAN

Kriptografi merupakan metode dalam menjaga keamanan pesan yang dilakukan menggunakan cara penyandian dengan melakukan cara perubahan bentuk agar tidak bisa diketahui sama sekali. Perkembangan kriptografi dilakukan dengan berbagai cara sehingga tidak hanya dalam mengubah atau menyandikan pesan saja, tetapi dalam aspek-aspek keamanan lainnya juga.

Enkripsi (*Encryption*) merupakan proses perubahan pesan yang asli atau tidak ada sandi (*plaintext)* ke bentuk yang tidak diketahui orang lain *(chipertext),* dekripsi (*Decryption*) merupakan proses pengubahan pesan yang tidak diketahui tadi menjadi pesan yang dapat diketahui atau dapat terbaca. Proses ini dilakukan dengan penerapan kunci-kunci yang terdapat pada kriptografi.

Kriptografi dapat dibedakan menjadi kriptografi kunci simetri (*Symmetric-key Cryptography*) dan kriptografi kunci asimetri (*Asymmetric-key Cryptography*). Proses enkripsi dan dekripsi dapat dilihat pada gambar 1.



Gambar 1. Proses Enkripsi dan Dekripsi

Pada pesan N yang melakukan atau mengekripsikan menajdi pesan D dengan penerapan kunci L, sedangkan pada proses didekripsi yang melakukan atau menggunakan kunci L dan melakukan pada pesan D yang sudah dienkripsi dan menghasilkan pesan awal yaitu N.

Tandatangan digital atau Digital Signature yaitu suatu tandatangan yang dibubuhkan pada pesan digital. Dengan begitu nilai pada tandatangan digital terdapat perbedaan yang bergantung dengan data yang ditandatangani. Dengan tandatangan digital maka kerahasiaan data dapat dijamin, dan digunakan dalam pembuktian dalam asal pesan keaslian pengirim.

Fungsi hash yang sederhana mempunyai macam jenis fungsi secara komputasi, tapi apabila digunakan dalam masalah kriptografi, fungsi hash selalu dikombinasi dalam berbagai metode lainnya. Kemungkinan dalam penggunaan yang sering digunakan dari fungsi kriptografi hash adalah dalam membuat tanda tangan digital. Karena fungsi hash paling sering dipakai dalam pengujian untuk mendapatkan nilai fungsi hash yang dikalkulasikan tanda tangan yang mendapatkan hasil nilai hash yang lebih kecil ketimbang dokumen aslinya.

Daripada itu, dapat diberikan sebuah saran tanpa membeberkan isi dari saran yang ada didalamnya. Cara ini dilakukan untuk penerapan tanggal dalam sebuah dokumen atau file kareana dengan diterapkannya fungsi hash, orang-

ISBN: 978-602-52720-7-3
Februari 2020
Hal 627 - 630

orang dapat memberikan tanggal di dalam dokumen tanpa harus melihat isi dari dokumen tersebut pada setiap proses pemberian tanggal.

ECDSA merupakan kurva elliptic analog yang berasal dari DSA. Parameter domain ECDSA terdiri dari merupakan pilihan yang tepat dengan kurva elliptik E yang memiliki bidang yang tak terhingga dari Fq ke karateristik p, dan sebuah titik dasar G € E(Fq).

3. ANALISA DAN PEMBAHASAN

Pada penelitian yang dillakukan terhadap suatu system terdapat tahap-tahap dalam pembuatan yang harus di jelaskan terlebih dahulu, yaitu sebagai berikut :

1. Melakukan tahap persiapan, yaitu menganalisa hal-hal yang dibutuhkan dalam mendukung implementasi dari sistem. Persiapan yang dilakukan meliputi aspek software dan hardware yang digunakan.
2. Melakukan tahap pengujian, yaitu dengan menguji setiap fungsi yang ada pada sistem apakah berhasil atau tidaknya suatu system yang telah diuji sebelumnya.

Berikut ini adalah tampilan dari Analisa Sistem Keamanan Otentikasi Pesan dengan Menggunakan ECDSA.

Gambar 2. Tampilan pengiriman pesan

Kunci rahasia merupakan kunci yang digunakan saat enkripsi untuk mengaksesnya hanya boleh pemilik kunci dan tidak ada yang boleh mengetahuinya, sedangkan kunci publik dapat disebar luaskan dan diwajibkan untuk dibagikan kepada publik. Pada pembagian kunci publik ini dilakukan dengan cara manual, yang dilakukan dengan cara download dari beberapa web yang di buat oleh seseorang, dan dapat dilakukan juga dengan cara mengirim kunci pribadi tersebut ke sebuah server kunci yang dapat menyimpan kunci publik ke berabagai orang-orang. Setelah tersimpan pada server kunci maka semua orang dapat mendownloas atau mencari kunci publik tersebut walaupun milik orang lain sesuka hati kapanpun dan dimana saja.

Saat mendekrip chipertext perlu menggunakan kunci rahasia yang dikirim ke pemiliknya, agar pemilik bisa menandatangani file ataudokumen yang dikirimkan kepada orang yang berhak menerimanya. Kunci ini digunakan orang untuk mengenkripsi file yang dituju kepada pemilik kunci, agar dapat memeriksa keaslian file atau dokumen yang telah ditandatangani oleh pemilik kunci rahasia.

Gambar 3. Private/Public Key

Fandy akan mengirim email yang berisi informasi kepada rekan kerjanya. Sebelum Fandy dapat mengekrip pesannya, dia harus memiliki public key. Dengan menggunakan public key itu maka Fandy dapat mengenkripsi pesan. Pesan tersebut dalam bentuk terenkripsi. Selain rekan kerja Fandy tidak seorang pun yang dapat mendekripsi teks itu, karena hanya rekan kerjanya lah yang memiliki private keynya. Bila private key jatuh ketangan orang lain, maka orang itu juga dapat mendekripsi apapun yang ada di dalam email yang telah terenkripsi yang telah dikirim kepadanya.

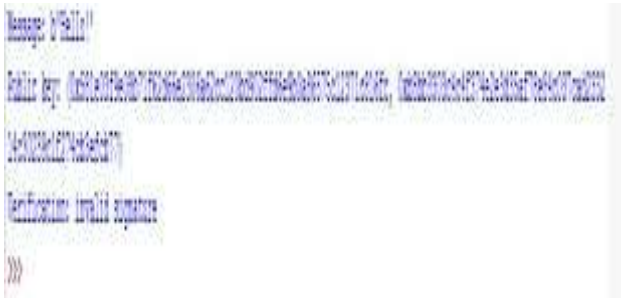
Ada kemungkinan bahwa yang mengirimkan pesan itu bukanlah Fandy, namun orang lain berpura-pura menjadi Fandy. Oleh karena itu ada baiknya bila Fandy juga menandatangani pesannya. Untuk menambahkan digital signature,

ISBN: 978-602-52720-7-3
Februari 2020
Hal 627 - 630

harus menggunakan private key. Pada saat menerima pesan, rekan kerja Fandy harus memverifikasi bahwa digital signature yang terdapat disana benar-benar asli milik Fandy dengan menggunakan public key milik Fandy. Dengan begitu rekan kerja Fandy boleh merasa yakin bahwa pesan itu benar-benar dikirim oleh Fandy.

Gambar 4. Penerapan Digital Signature

Jika dalam pengiriman pesan terjadi perubahan pesan maka verifikasi tidak berhasil, karena nilai dari signature akan berubah dan tidak sama dengan nilai signature pada saat pengiriman. Berikut tampilan verifikasi salah.



Gambar 5. Verivikasi Signature

Gambar 6. Tampilan Output Program

4. KESIMPULAN

Dari berbagai penjelasan yang telah di uraikan dalam laporan ini, maka dapat disimpulkan dengan adanya analisa program ini, dapat mengurangi tindakan dari pihak yang bukan haknya untuk mengubah pesan dan membuat pesan yang akan dikirim tidak asli lagi. Analisa program ini, seseorang yang mengirimkan pesan text dan data yang dienkripsi dengan ECDSA terjaga dari perubahan yang dilakukan seorang penyadap dalam proses pengiriman pesan. Verifikasi yang salah menyimpulkan bahwa adanya manipulasi terhadap pesan yang diterima dan terjadinya ketidak cocokan pesan yang akan dikirim kepada si penerima.

Penulis menyarankan pengembangan penelitian lebih lanjut terhadap otentikasi pesan dengan program yang dibuat perlu didukung dengan *hardware* dan *software* yang sesuai dengan kebutuhan programnya. Program yang diusulkan hanya membahas komunikasi dan pengiriman file yang berupa *text.* Program yang penulis buat ini hanya dapat digunakan untuk proses pengiriman pesan agar terjaga kerahasiaannya, dan pihak penerima pesan adalah pihak yang sebenarnya yang diinginkan. Program ini diharapkan nantinya dapat dikembangkan lagi sehingga memudahkan bagi semua bagian yang berhubungan dengan proses pengiriman pesan sehingga dapat menghasilkan informasi yang lengkap dan sempurna.

ISBN: 978-602-52720-7-3
Februari 2020
Hal 627 - 630

REFERENCES

[1] Adam, W. 2009. *Pemanfaatan Algoritma ECDSA (Elliptic Curve Digital Signature Algorithm) untuk Penandatanganan Digital Chipertext ElGamal Elliptic Curve Cryptography*. Ilmu Komputer. Universitas Pembangunan Nasional Veteran Jakarta. Jakarta.
[2] Hankerson, D., Menezes, A. & Vanstone, S. 2004. *Guide to Ellpitic Curve Cryptography*. Springer-Verlag: New York.
[3] Kiros , T. & Raimond, K. 2009. An Efficient Modified Elliptical Curve Digital Signature Algorithm. *Journal of EAA, vol.26.*
[4] Liao, H.-Z. & Shen,Y.-Y. 2006. On the Elliptic Curve Digital Signature Algorithm. *Tunghai Science vol. 8: 109-126.*
[5] Munir, Rinaldi., 2006, *Kriptografi*, Bandung : Penerbit Informatika.
[6] Sendi, P. A. P., Winarno, I. S.ST. M.Kom. & Rosyid, N. M. S.Kom. M.Kom. 2010. *Implementasi Algoritma ECDSA Untuk Pengamanan E-mail (Verifikasi Keaslian Pesan)*. Politeknik Elektronika Negeri Surabaya Institut Teknologi Sepuluh Nopember. Surabaya
[7] Triwinarko, A. 2010. *Elliptic Curve Digital Signature Algorithm*. Institut Teknologi Bandung. Bandung.
[8] Wizanajani, D. R. 2013. *Perbandingan Algoritma Berbasis Elliptic Curve Cryptography dengan RSA dan DSA pada Tandatangan Digital*. Teknik Informatika Institut Teknologi Bandung. Bandung.