Implementasi Algoritma Schnorr Untuk Tanda Tangan Digital

Implementation Of Schnorr Algorithm For Digital Signatures

Robi Adi Saputra[1], Agus Sidiq Purnomo[2]

[1,2]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Mercu Buana Yogyakarta
Jl. Wates Km. 10 Yogyakarta 55753, Indonesia
Email: robby.adhy@gmail.com[1], sidiq@mercubuana-yogya.ac.id[2]

ABSTRAK

Tanda tangan merupakan alat yang digunakan untuk melegalkan atau sebagai penanda bahwa suatu dokumen adalah asli dari pihak pertama (pembuat) atau bukan. Hal tersebut berlaku pada dokumen nyata dalam hal ini dokumen cetak atau tertulis. Selanjutnya bagaimana jika dokumen ataupun file tersebut bersifat digital. Pada saat ini media digital bukan hal awam lagi, hampir semua aktivitas bisnis maupun sehari-hari sudah menggunakan internet. Maka dari itu perlu adaya pengganti tanda tangan yang dibuat dalam bentuk digital untuk melegalkan dokumen digital.
Dalam penelitian ini digunakan algoritma schnorr. Algoritma schnorr merupakan pengembangan dari algoritma El-gamal sehingga sistem keamanan dari El-gamal terdapat pada schnorr. Pembuatan tanda tangan dengan mengubah informasi yang terdapat pada file ke dalam bentuk ASCII kemudian diubah kebentuk message digest menggunakan fungsi hash. Dengan menggunakan algoritma schnorr sign dan private key dihasilkan tanda tangan dari file tersebut. Proses verifikasi tanda tangan menggunakan public key dan file signature menggunakan algoritma schnorr verify. Jika nilai verifikasi sama dengan proses sign maka data dapat dikatakan asli. Sebaliknya jika hasil dari proses verifikasi tidak sama dengan proses sign maka data tersebut sudah mengalami perubahan informasi atau kunci yang dimasukkan tidak sesuai. Tanda tangan digital yang dihasilkan dari setiap file berbeda-beda walaupun dengan kunci yang sama. Besar kecilnya bilangan dalam pembentukan kunci juga mempengaruhi hasil dari tanda tangan digital. Penambahan fungsi hash sangat membantu untuk menambah keamanan pada tanda tangan digital.

Kata kunci: Kriptografi, Tanda Tangan Digital, Algoritma Schnorr

ABSTRACT

A signature is a tool used to legalize or as a marker that a document is original from the first party (the author) or not. This applies to real documents in this case print or written documents. What if the document or file is digital. At this time digital media is not a layman anymore, almost all business activities and daily use the internet. Therefore it is necessary to have a signature replacement made in digital form to legalize digital documents.
In this study used schnorr algorithm. The schnorr algorithm is a development of the El-gamal algorithm so that the security system of El-gamal is in Schnorr. Making a signature by changing the information contained in the file into ASCII then changed the form of message digest using hash function. By using schnorr sign algorithm and private key generated signature from the file. Signature verification process using public key and signature file using schnorr verify algorithm. If the verification value is equal to the sign process then the data can be said to be genuine. Conversely, if the result of the verification process is not the same as the sign process then the data has undergone a change of information or the key entered is not appropriate.
Digital signatures generated from each file vary though with the same key. The size of the number in the key formation also affects the result of a digital signature. The addition of hash functions is helpful to add security to digital signatures.

***Keywords**: Cryptography, Digital Signature, Schnorr Algorithm*

1. PENDAHULUAN

Untuk menjaga keabsahan dan originalitas suatu data tanda tangan dijadikan sebagai suatu persyaratan mutlak agar data tersebut dapat dijadikan sebagai alat bukti. Dalam era digital hampir semua dokumentasi dan informasi dibuat dalam bentuk digital. Data digital tersebut

tersebar dan saling bertukar melalui jaringan *internet*. Tidak sedikit orang yang menggunakan fasilitas *internet* untuk melakukan transaksi proses bisnis dan bersosial dengan pengguna lainnya.

Keamanan data pada lalu lintas jaringan adalah suatu hal yang diinginkan semua orang untuk menjaga privasi, supaya data yang dikirim aman dari gangguan orang yang tidak bertanggung jawab, yang disembunyikan menggunakan algoritma kriptografi (Arius, 2008).

Sehingga hal ini perlu adanya pengganti tanda tangan yang dibuat dalam bentuk digital untuk melegalkan dokumen digital.

Secara umum, skema tanda tangan digital menawarkan kriptografi analog tanda tangan tulisan tangan, yang pada kenyataannya memberikan jaminan keamanan yang jauh lebih kuat. Tanda tangan digital berfungsi sebagai alat yang ampuh dan sekarang diterima sebagai ikatan hukum di banyak negara, dapat digunakan untuk sertifikasi kontak atau dokumen notaris, untuk otentikasi individu atau perusahaan, dan sebagai komponen protokol yang lebih kompleks. Tanda tangan digital memungkinkan distribusi dan transmisi kunci publik yang aman sehingga memiliki arti yang sangat nyata, berfungsi sebagai pondasi untuk semua kriptografi kunci publik (Katz, 2010).

Rumusan masalah dalam penelitian ini dibagi menjadi empat diantaranya adalah : (1) Bagaimana proses pembuatan tanda tangan digital? (2) Informasi apa saja yang dapat digunakan dalam pembuatan tanda tangan digital pada sebuah *file*? (3) Bagaimana hasil dari penerapan algoritma *Schnorr* pada pembuatan tanda tangan digital? (4) Apakah perangkat lunak dapat digunakan untuk pengamanan data?

Selabjutnya penelitian ini bertujuan untuk : (1) Memahami proses pembuatan tanda tangan digital menggunakan algoritma *schnorr*. (2) Memperkuat keamanan pada pembuatan tanda tangan digital dari informasi yang diperoleh dari sebuah *file*. (3) Tanda tangan digital yang dihasilkan dapat berfungsi sebagai mana mestinya, seperti halnya tanda tangan manual pada dokumen kertas. (4) Menghasilkan perangkat lunak yang dapat digunakan dalam pengamanan data pada sebuah *file*.

Hasil dari penelitian ini diharapkan dapat memberikan manfaat diantaranya : (1) Dapat memahami bagaimana pembuatan tanda tangan digital. (2) Dapat memastikan keasliannya dari tanda tangan yang dihasilkan berdasarkan informasi yang didapat dari *file* dapat terenkripsi dengan baik. (3) Tanda tangan digital dapat dijadikan sebagai pengganti tanda tangan manual pada sebuah dokumen tertulis. (4) Mengasilkan perangkat lunak untuk membuat tanda tangan digital pada dokumen digital.

2. TINJAUAN PUSTAKA

Beberapa penelitian yang terkait antara lain seperti pada penelitian mengenai perancangan sistem pencarian publikasi ilmiah berbasis semantik yang menggunakan metadata berupa entry bibtex sebagai kriteria pencarian. Pada sistem tersebut, digital signature digunakan untuk identifikasi sumber data dan mencegah duplikasi data. Data *bibtex*, yang diperoleh dari penyedia layanan data publik seperti CiteSeer, Google Scholar dan lain lain. serta dari data milik sendiri, akan dikonversi ke bentuk metadata dalam hal ini *Resource Description Framework* (RDF) dan juga diproses menggunakan fungsi hashing dan enkripsi untuk membuat *digital signature*. Hasil pemrosesan ini kemudian disatukan ke dalam bentuk data RDF yang nantinya akan digunakan di repository metadata (Lestriandoko & Wirahman, 2008).

Selanjutnya penelitian mengenai *new signcryption* yang didasarkan pada tanda tangan digital algoritma *schnorr*. *New signcryption* (*schnorr signcryption)* diimplementasikan dalam logika tunggal pada kedua enkripsi *public key* dan tanda tangan digital, penelitian ini menghasilkan proses komputasi yang singkat dengan keamanan yang tinggi jika dengan menggunakan kedua fungsi kriptografi secara individual (Savu, 2012).

Keamanan dokumen digital juga dapat menggunakan teknik watermaking, teknik ini memberikan proteksi terhadap penggunaan tidak sah dari materi digital, namun untuk menghilangkan kecurigaan dari pihak yang tidak memiliki hak akses terhadap materi digital watermaking dapat digunakan invisible watermaking (Sukarno, 2013).

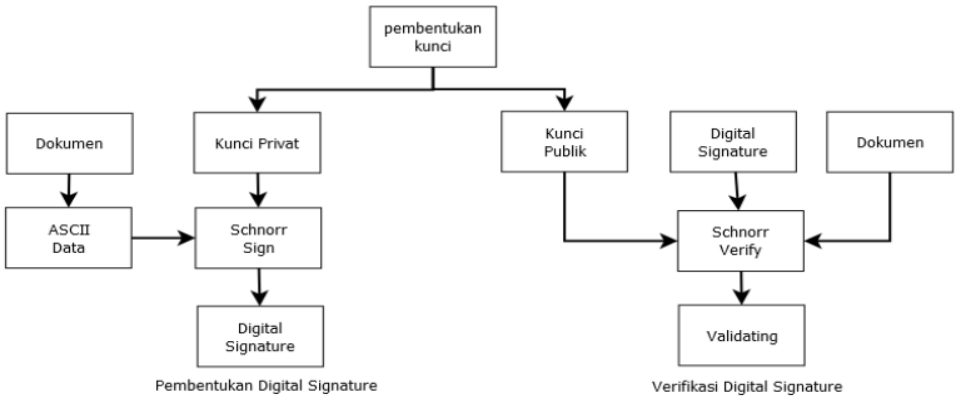
Sebuah studi kasus tentang penggunaan *DSP board* untuk membangun saluran komunikasi yang aman. *DSP board* dibangun sebagai kriptosistem perangkat keras untuk meningkatkan keamanan data yang dikirimkan menggunakan sistem komunikasi bergerak. Dengan menerapkan *Schnorr Signcryption scheme* pada DSP, selanjutnya kinerjanya dievaluasi dengan menghitung waktu yang dikonsumsi dengan proses enkripsi/dekripsi. Dari penelitian ini ada usulan mengenai sebuah model yang disempurnakan untuk menerapkan beberapa DSP dengan menggunakan teknik perpipaan dan paralelisasi untuk mengurangi

waktu yang dikonsumsi dalam keseluruhan proses (Elshobaky, et al., 2015).

Selanjutnya dalam penelitian ini digunakan algoritma schnorr yang ditujuakan untuk mengamankan file digital. *Schnorr signature* adalah tanda tangan digital yang dihasilkan oleh algoritma tanda tangan *Schnorr*. Keamanannya didasarkan pada kekurangan beberapa masalah logaritma diskrit tertentu. *Schnorr signature* merupakan skema tanda tangan digital yang paling sederhana untuk menjadi aman dalam *random oracle model* (Schnorr, 1990).

3. METODOLOGI PENELITIAN

Secara umum proses pembuatan tanda tangan digital dapat digambarkan melalui diagram alir pada Gambar 1.



Gambar 1. Diagram alir pembuatan tanda tangan digital

Pembuatan Kunci

Dalam pembuatan kunci ini bilangan yang dibutuhkan adalah bilangan prima berukuran besar. Hal ini dimungkinkan agar kunci yang dihasilkan juga bernilai besar. Algoritma pembuatan kunci adalah sebagai berikut:

Algoritma Pembuatan Kunci
```
Input   : Bilangan Prima {P, Q}; Bilangan Integer(A);
          Private key(S); % Nilai S < Q
Output  : Kunci Pulik { A,P,Q,V }; Private key(S)
if GCD(Q,P-1) ~= 1
   print P dan Q
end if
if A^Q mod P = 1
   print A
end if
V = A^(-S) mod P.
```

Dari proses pembuatan kunci ini didapat 2 buah kunci yaitu *private key* (S) dan *public key* (V). *Private key* akan digunakan untuk pembuatan tanda tangan digital, sedangkan *public key* akan digunakan untuk verifikasi data.

Schnorr Sign

Setelah didapat *public key* (*V*) *private key* (*S*) dan nilai ASCII (*M*) maka selanjutnya adalah proses pembuatan tanda tangan. Adapun algoritma *sign* adalah sebagai berikut:

Algoritma *Schnorr Sign Digital Signature*
```
Input : M, Private key(S), public key(A,P,Q,V)
Output: E,Y{Signature}
Pilih R {1 ≤ R ≤ Q}  % R adalah random
E = Hash(M|A^R mod P)
Y = (R + S × E) mod Q
```

Dengan menerapkan algoritma *schnorr sign*, maka *signature* dapat diperoleh dari E dan Y.

Schnorr Verify

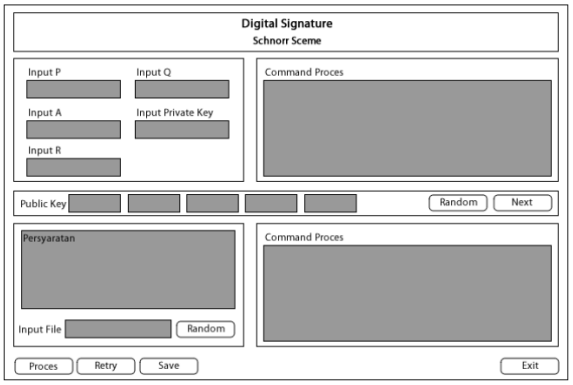
Untuk dapat memverifikasi *signature* seseorang harus memiliki *public key* Jika *public key* telah diterima maka proses verifikasi dapat dilakukan. Adapun algoritma *schnorr verify* adalah sebagai berikut :

Algoritma *Schnorr Verify Digital Signature*
```
Input : M, E, Y, A, dan public key(A,P,Q,V)
Output: diterima
X` = Hash(M|A^Y × V^E) mod P
if X`≡ Y mod Q then
    diterima = true
else
    diterima = false
end if
```

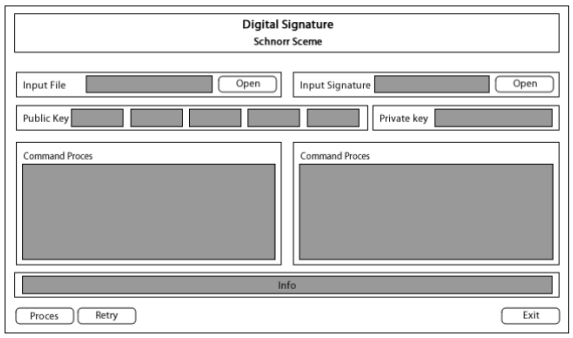
Dengan menerapkan algoritma *schnorr verify*, jika nilai *Y mod Q* sama dengan *X`* maka *signature* adalah asli.

Perancangan Perangkat Lunak

Desain perancangan antar muka pembuatan *signature* dapat dilihat pada Gambar 2.



Gambar 2. Perancangan antar muka pembuatan *signature*



Gambar 3. Perancangan antar muka *signature verify*

Sedangkan desain perancangan antar muka *signature verify* dapat dilihat pada Gambar 3.

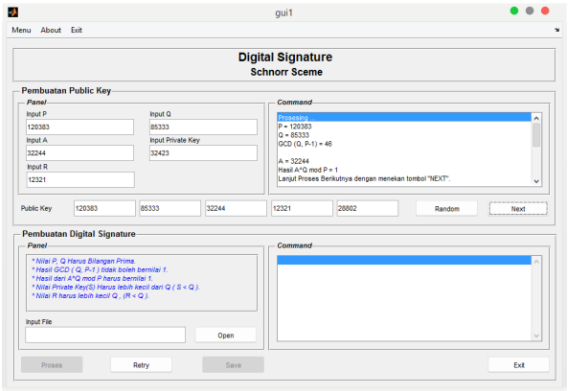
4. PEMBAHASAN

Sampel data yang digunakan adalah berupa *file* citra, *file* teks (dengan ekstensi seperti '*.doc' dan '*.pdf'. Dalam pembuatan tanda tangan digital bilangan yang digunakan adalah bilangan prima sebagai penentu *public key* dan *private key*. Tanda tangan digital dari sebuah *file* tersebut disimpan dalam bentuk *file* matrik(berekstensi *'*.mat'*). *File signature* tersebut nantinya akan digunakan untuk validasi *file* yang bersangkutan untuk mengetahui keaslian *file* tersebut.Pengujian validasi dilakukan dengan cara mengubah nilai variabel dari *public key* maupun *private key*. Selain itu pengujian dilakukan pada *file* yang sudah mengalami perubahan informasi.

Sebagai contoh pembuatan kunci dilakukan dengan menginputkan bilangan prima yang diinisialisasikan sebagai berikut:

P = 120383
Q = 85333
A = 32244
R = 12321
S = 32423

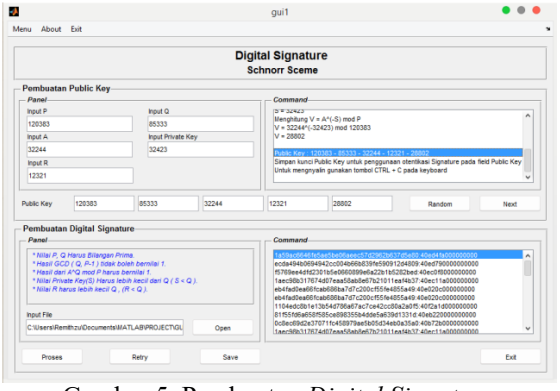
Pembuatan kunci dapat dilihat pada Gambar 4.



Gambar 4. Pembuatan kunci

Dari bilangan prima tersebut dan *private key* (*S*), didapat nilai V = 28802 sehingga kunci dapat dituliskan sebagai berikut:
Public key = 120383 – 85333 – 32244 – 12321 – 28802
Private key = 32423

Setelah proses pembuatan kunci selesai, selanjutnya adalah proses pembuatan tanda tanga digital dari *public key, private key* dan *file* yang akan dienkripsi seperti pada Gambar 5.

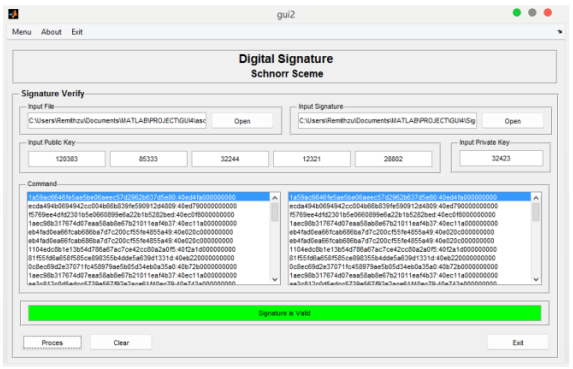


Gambar 5. Pembuatan *Digital Signature*

Untuk proses verifikasi diperlukan beberapa persyaratan yaitu harus memiliki *public key, private key* dan *file* beserta *digital signature,* kemudian proses verifikasi dapat dilakukan. Berikut ini adalah tampilan dari *form* verifikasi ditunjukkan pada Gambar 6.

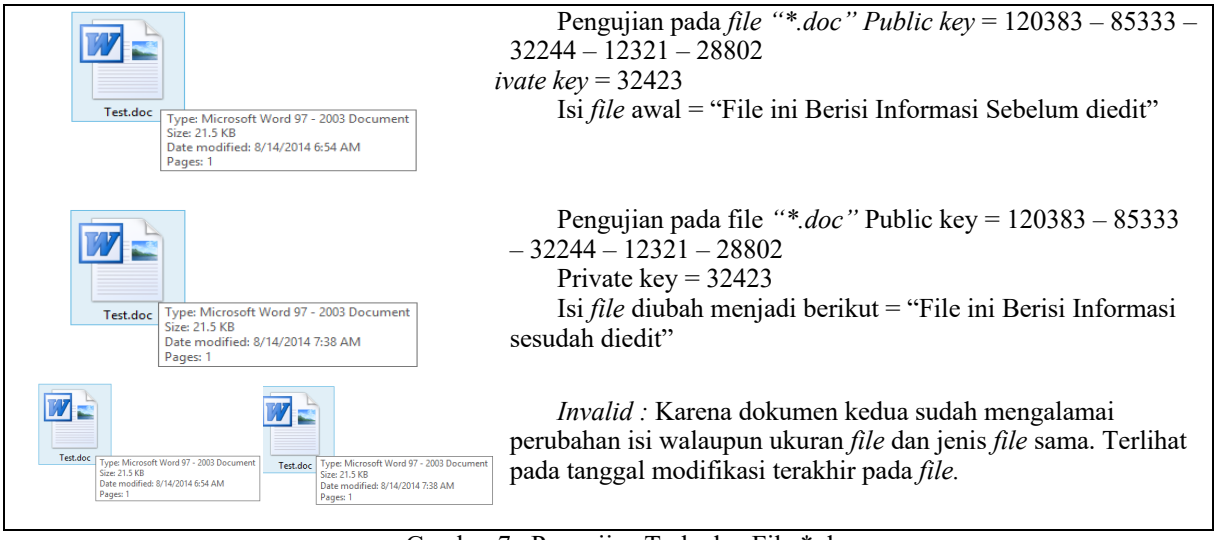
Jika *file* tidak diubah dan kunci tidak salah, maka pada saat proses verifikasi maka *signature* yang dibawa dan *signature* yang ada pada *file* hasilnya akan sama.

Ketidak cocokan *signature* bisa disebabkan dari beberapa faktor yaitu bisa terjadi karena perubahan isi, perubahan format, ketidaksaamaan kunci, perubahan ukuran. Kemungkinan lain bisa terjadi perubahan *signature* oleh pihak ketiga sehingga informasi yang diterima pihak kedua dari pihak pertama sudah diambil alih oleh pihak ketiga.



Gambar 6. Verifikasi data uji

Sebagai contoh pengujian pada file "Test.doc" yang belum ada perubahan dan sudah ada perubahan. Hasil dapat ditunjukkan pada Gambar 7.



Gambar 7. Pengujian Terhadap File *.doc

5. KESIMPULAN

Berdasarkan hasil pengujian yang telah dilakukan dapat disimpulkan :

1. Dalam pembuatan kunci bilangan yang pilih yaitu merupakan bilangan prima dan bilangan prima tersebut harus bilangan prima besar. Hal ini dimungkinkan agar kunci yang dihasilkan unik dan besar pula. Sehingga apabila dilakukan *cracking* agar lebih sulit.
2. Informasi yang dapat dipakai dalam pembuatan tanda tangan hanya sebatas informasi atribut yang terdapat pada *file*, untuk data yang terdapat pada file seperti teks pada dokumen *office* tidak dapat dibaca, sehingga *signature* yang dihasilkan kurang kuat.
3. Dalam pembuatan *digital signature* kunci yang dibuat sangat mempengaruhi proses pembuatan *digital signature*, sehingga perlu ditambahkan fungsi *hash* untuk menambah keamanan pada informasi yang dienkripsi.
4. Perubahan pada *file* maupun pada kunci dapat mengakibatkan hasil dari proses verifikasi tidak sesuai dengan yang semestinya dengan kata lain hasil verifikasi dari *file* yang bersangkutan tidak cocok. Sehingga hal ini dapat dikatakan *file* tersebut sudah tidak asli atau tidak dapat dipercaya.

Sedangkan saran untuk penelitian selanjutnya yaitu perlu dikembangkan aplikasi yang dapat membaca seluruh data informasi yang terdapat dari suatu file agar mendapat keamanan yang lebih baik.

DAFTAR PUSTAKA

Arius, D., 2008. *Pengantar Ilmu Kriptografi.* Yogyakarta: Andi.

Elshobaky, A., Rasslan, M. & Guirguis, S., 2015. *Implementation of Schnorr Signcryption Algorithm on DSP. International Journal of Security and Its Applications,* Volume Vol.9, No.11 , pp. 217-230.

Katz, J., 2010. *Digital Signatures.* London: Springer.

Lestriandoko, N. H. & Wirahman, T., 2008. *Penggunaan Digital Signature Pada Metadata Untuk Pencarian Publikasi Ilmiah Berbasis Semantik.* Yogyakarta, s.n.

Savu, L., 2012. Signcryption scheme based on schnorr digital signature. *ARXIV,* Issue eprint arXiv:1202.1663.

Schnorr, C. P., 1990. *Efficient identification and signatures for smart cards, in G. Brassard, ed. Advances in Cryptology-Crypto '89, PP. 239-252,* Berlin Heidelberg: Springer-Verlag.

Sukarno, A. S., 2013. *Pengembangan Aplikasi Pengamanan Digital Memanfaatkan Algoritma Advance Encryption Standard, RSA Digital Signature dan Invisible Watermaking.* Yogyakarta, Seminar Nasional Aplikasi Teknologi Informasi (SNATI), ISSN : 1907-5022, Universitas Islam Indonesia.