Penggunaan Metode Ong-Schnorr-Shamir Pada Pembuatan Tanda Tangan Digital

Muhammad Andhika Virgiawan*[1], Gunawan Pria Utama[2]
[1,2]Universitas Budi Luhur; jl. Ciledug Raya, 021-5853753
e-mail: *[1]andikavirgiawan91@gmail.com,
[2]Gunawan.priautama@budiluhur.ac.id

Abstrak

Penyampaian informasi pada suatu perusahaan besar menjadi sesuatu hal yang perlu dijaga keutuhan dan kerahasiaannya, informasi yang penting dan bersifat rahasia jika jatuh ketangan pihak orang yang tidak bertanggungjawab menjadi sebuah petaka. Digital signature atau tanda tangan digital merupakan sebuah mekanisme otentikasi yang memungkinkan pembuat pesan menambahkan sebuah kode yang bertindak sebagai tanda tangannya dan juga memungkinkan penerima pesan untuk menguji keaslian dan keutuhan pesan. Skema (scheme) yang dapat digunakan untuk melakukan proses tanda tangan digital terhadap suatu pesan (message) juga ada bermacam-macam, salah satu skemanya adalah skema Ong-Schnorr-Shamir. Penelitian ini menggunakan metode Ong-Schnorr-Shamir yang diimplementasikan kedalam sistem. Hasil penelitiannya bahwa metode tersebut dapat digunakan dan berhasil 100% didalam menyamarkan pesan dan membuat tanda tangan digital.

***Kata kunci** : tanda tangan digital, Pesan, Otentikasi dan Ong-Schnorr-Shamir*

Abstract

The submission of information to a large company becomes something that needs to be kept intact and confidential, information that is important and confidential if it falls on the part of the person who is not responsible for being a disaster. Digital signature or digital signatures is an authentication mechanism that allows a message creator to add a code that acts as a signature and also allows the recipient of a message to test the authenticity and integrity of the message. The scheme that can be used to perform the digital signature process of a message is also an assortment, one of the schemes is Ong-Schnorr-Shamir scheme. This study used the Ong-Schnorr-Shamir method that was implemented into the system. The results of his research that the method can be used and successfully 100% in disguise the message and create digital signatures..

***Keywords :** Digital Signature, Message, Authenticity and Ong-Schnorr-Shamir*

1. PENDAHULUAN

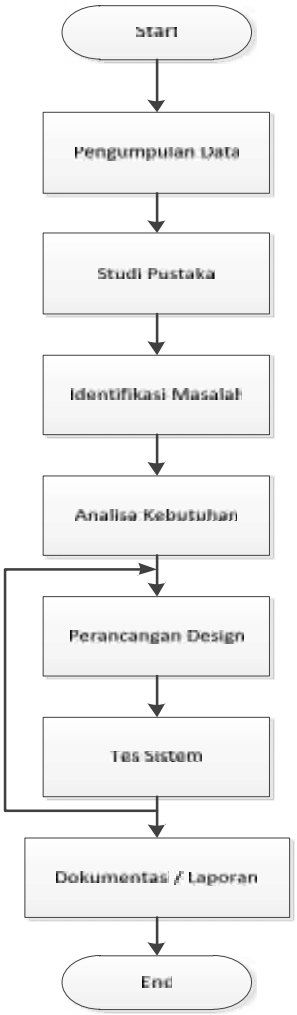
Pada saat sekarang ini banyak sekali oknum-oknum yang tidak bertanggungjawab dalam memanfaatkan sebuah informasi untuk mendapatkan keuntungan secara pribadi yaitu dengan cara menyadap sebuah informasi penting pada perusahaan dan mengancam perusahaan tersebut agar informasi tersebut tidak menjadi konsumsi publik. Pertumbuhan teknologi informasi juga sangat pesat baik itu dibidang akademis, kesehatan dan bidang-bidang lainnya. Salah satu bidang teknologi informasi yang dapat digunakan untuk melindungi data-data atau informasi-informasi penting pada sebuah perusahaan adalah Ong-Schnorr-Shamir. Ong-Schnorr-Shamir Memiliki Dua Buah Skema, Yaitu Skema Tanda Tangan Digital (Digital Signature) Dan Skema Saluran Tersembunyi (Subliminal Channel) [1]. Skema Digital Signature Dapat Digunakan Untuk Menjaga Keaslian Pesan Dan Keutuhan Pesan. Skema Digital Signature Akan Membentuk Digital Signature Dari Suatu Pesan. Proses Verifikasi Dilakukan Terhadap Pesan Dan Digital

Signature Untuk Menguji Keaslian Dan Keutuhan Pesan. Bila Verifikasi Sukses, Maka Pesan Masih Asli Dan Utuh. Skema Subliminal Channel Hampir Sama Dengan Skema Digital Signature. Perbedaannya Adalah Skema Subliminal Channel Memiliki Proses Enkripsi dan Dekripsi Yang Menyamarkan Pesan Asli [2]. Kajian serupa juga telah dilakukan oleh Addinur Hatta Sembiring [3] yang berjudul Perancangan Aplikasi Dokumen Undeniable Digital Signature dengan Algoritma Ong-Schnorr-Shamir. pada penelitiannya menguji dokumen-dokumen undeniable yaitu dokumen yang perlu verifikasi tanda tangan digital. hasil pada penelitiannya adalah sebuah aplikasi yang dapat memberikan tanda tangan digital pada masing-masing dokumen. Begitu juga kajian yang dilakukan oleh Herdita Fajar Isnaini dan K.Karyati [4] yang berjudul Penerapan Skema Tanda Tangan Schnorr pada Pembuatan Tanda Tangan Digital. Hasil dari kajian nya adalah adalah didapatkan algoritma – algoritma dari skema tanda tangan Schnorr, yaitu algoritma pembentukan kunci publik dan kunci privat, algoritma pembuatan tanda tangan, serta algoritma verifikasi tanda tangan**.**

2. METODE PENELITIAN

2.1 Metode Penelitian

Pada penelitian ini menggunakan metode sebagai berikut :



Gambar 1 metode penelitian

a. Pengumpulan Data
   Pada tahap ini adalah mengumpulkan data-data dari sebuah pokok permasalahan dari topik yang diangkat oleh penulis, yaitu dengan Observasi yang terdiri dari wawancara
b. Studi Pustaka
   Setelah data – data yang dibutuhkan terkumpul, selanjutnya adalah mencari data atau fakta yang *real* melalui studi pustaka
c. Identifikasi Masalah
   Dari data nyata yang tekumpul maka selanjutnya dapa diidentifikasi suatu masalah dan permasalahannya yang ada dengan pembatasan
d. Analisa Kebutuhan
   Dari hasil identifikasi masalah yang diatas, selanjutnya baru dapat dilakukan analisa kebutuhan yang menunjang dalam perancangan system tanda tangan digital menggunakan metode Ong-Schnorr-Shamir ini berdasarkan tinjauan pustaka, yaitu meliputi kebutuhan materi tanda tangan digital, dan kriptografi, teori perancangan sistem atau program yang *interaktif* serta *template* atau *platform* dimana perancangan akan dilakukan
e. Perancangan Desain
   Pada tahap ini adalah merancang tampilan tatap muka pengguna yang mudah digunakan menurut kaidah interaksi manusia dengan komputer dan konten-konten yang ada didalamnya seperti, struktur menu, tombol.
f. Tes Sistem
   Pada tahap ini adalah mengujikan apa saja yang telah diteliti kemudian dirancang kedalam bentuk model program. Jika belum sesuai dan atau masih ada kekurangan dalam perancangan model program ini dapat ditambah dalam rancangannya bahkan dirancang ulang pada tahap perancangan disain untuk mendapatkan hasil yang sesuai
g. Dokumentasi / pembuatan Laporan
   Tahap dokumentasai atau pembuatan laporan adalah memaparkan hasil penelitian yang dilakukan dari tahap awal hingga akhir dan diimplementasikan kedalam bentuk laporan jurnal.

2.2 Digital Signature

Tanda tangan digital (*digital signature*) adalah suatu mekanisme otentikasi yang memungkinkan pembuat pesan menambahkan sebuah kode yang bertindak sebagai tanda tangannya. Tanda tangan dihasilkan berdasarkan pesan yang ingin ditandatangani dan berubah-ubah sesuai dengan pesan [5]. Tanda tangan digital dikirimkan bersama-sama dengan pesan kepada penerima. Tanda tangan digital memungkinkan penerima informasi untuk menguji terlebih dahulu keaslian informasi yang didapat dan juga untuk meyakinkan bahwa data yang diterimanya itu dalam keadaan utuh. Oleh karena itu, tanda tangan digital kunci publik (*public key digital signature*) menyediakan layanan *authentication* (keaslian) dan *data integrity* (keutuhan data). Selan itu, tanda tangan digital juga menyediakan layanan *non-repudiation*, yang artinya melindungi pengirim dari sebuah klaim yang menyatakan bahwa dia telah mengirim informasi padahal tidak [6]. Tanda tangan digital memberikan pelayanan yang tujuannya sama dengan tanda tangan (berupa tulisan tangan biasa). Tetapi, bagaimanapun juga, tanda tangan berupa tulisan tangan relatif lebih mudah ditiru/dipalsukan oleh orang lain. Sedangkan, tanda tangan digital hampir tidak mungkin dipalsukan, bahkan bisa berfungsi ganda, yaitu sekaligus dapat memperlihatkan sekilas isi informasi mengenai identitas yang menandatangani. Bahkan, beberapa orang lebih cenderung menggunakan tanda tangan digital daripada menggunakan enkripsi biasa.
Proses enkripsi informasi biasanya menggunakan kunci publik. Tetapi pada konsep tanda tangan digital, informasi justru dibubuhi tanda tangan digital (dienkripsi) dengan kunci rahasia yang dimiliki sumber. Apabila informasi tadi bisa diverifikasi (didekripsi) dengan kunci publik sumber yang telah tersebar, ini berarti bahwa informasi tersebut adalah benar-benar asli dari sumber. Konsep tanda tangan digital dapat dilihat pada gambar 2 berikut:

Gambar 2. Konsep tanda tangan digital

Pertama-tama teks biasa akan diberi tanda tangan digital menggunakan kunci privat, kemudian teks yang telah dibubuhi tanda tangan tersebut dikirim kepada pihak lain. Kemudian oleh pihak penerima akan dicek keaslian tanda tangan digital tersebut menggunakan kunci publik sehingga pesan atau teks tersebut dapat dibuka menjadi teks biasa.

2.3 Ong-Schnorr-Shamir Scheme

Skema Ong-Schnorr-Shamir merupakan salah satu skema tanda tangan digital yang terdapat dalam ilmu kriptografi. Skema tanda tangan digital Ong-Schnorr-Shamir diciptakan oleh H.Ong, C.P.Schnorr dan A.Shamir [7] Selain skema tanda tangan digital, Ong-Schnorr-Shamir juga memiliki skema *subliminal channel* (saluran tersembunyi). Skema ini diciptakan oleh Gustavus.

2.3.1 Ong-Schnorr-Shamir Digital Signature Scheme

Berikut adalah prosedur kerja skema tanda tangan digital Ong-Schnorr-Shamir:

1. Tentukan sebuah bilangan *integer* besar (*n*) dan sebuah bilangan *integer* (*k*).
   a. *n* dan *k* harus relatif prima, artinya nilai GCD(*n*, *k*) = 1.
   b. *n* merupakan kunci publik, artinya nilai *n* boleh diketahui oleh pihak lain.
   c. *k* merupakan kunci privat, artinya nilai k hanya diketahui oleh pembuat pesan (X).
2. Hitung nilai *h* dengan rumus berikut.

$$h = -(k^{-1})^2 \bmod n$$

3. Tentukan sebuah bilangan *integer* acak (*r*).
   a. *n* dan *r* harus relatif prima, artinya nilai GCD(*n*, *r*) = 1.
   b. *r* merupakan kunci publik, artinya nilai *r* boleh diketahui oleh pihak lain.
4. Hitung S_1 dan S_2 terhadap pesan (M). (S_1 dan S_2 merupakan *signature* oleh pembuat pesan (X)) dengan rumus berikut.

$$S_1 = {}^{I}/_{2} * (M/r + r) \bmod n$$

$$S_2 = {}^{k}/_{2} * (M/r - r) \bmod n$$

5. Pihak penerima pesan Y memverifikasi pesan dan tanda tangan digital oleh pembuat pesan X dengan menggunakan rumus berikut.

$$S_1^2 + h \cdot S_2^2 \quad M \pmod n$$

2.3.2 Ong-Schnorr-Shamir Subliminal Channel Scheme

Ong-Schnorr-Shamir Subliminal Channel Scheme menggunakan sebuah bentuk sandi didalam pengiriman pesan. Dimana pesan yang hendak dikirim akan dienkripsi terlebih dahulu. Dan penerima pesan harus memiliki kuncinya untuk membuka pesan tersebut.

Berikut adalah prosedur kerja skema Ong-Schnorr-Shamir *Subliminal Channel*:

1. Tentukan sebuah bilangan *integer* besar (*n*) dan sebuah bilangan *integer* (*k*).
   a. *n* dan *k* harus relatif prima, artinya nilai GCD(*n*, *k*) = 1.
   b. *n* merupakan kunci publik, artinya nilai *n* boleh diketahui oleh pihak lain.
   c. *k* merupakan kunci privat. Nilai *k* diketahui oleh pembuat pesan (X) dan pihak yang akan mendekripsi pesan samaran (Y).
2. Hitung nilai *h* dengan rumus berikut.

$$h = -(k^{-1})^2 \bmod n$$

3. Buat pesan asli (*w*), pesan samaran (*w*') dan hitung S_1 dan S_2 !
   a. Pesan samaran (*w*') diciptakan untuk menyamarkan pesan asli. Nilai variabel *w*, *w*' dan *n* harus relatif prima (GCD(*w*', *n*) = 1 dan GCD(w,n) = 1).
   b. S_1 dan S_2 merupakan *signature* oleh pembuat pesan (X)
   c. Pembuat pesan (X) akan mengirimkan S_1, S_2 dan *w*' kepada Z dan Y.

$$S_1 = {}^{1}/_{2} * (w'/w + w) \bmod n$$

$$S_2 = {}^{k}/_{2} * (w'/w - w) \bmod n$$

4. Z memverifikasi pesan samaran dan tanda tangan digital X (*w*') dengan menggunakan rumus berikut.

$$w' = S_1^2 + h \cdot S_2^2 \pmod n$$

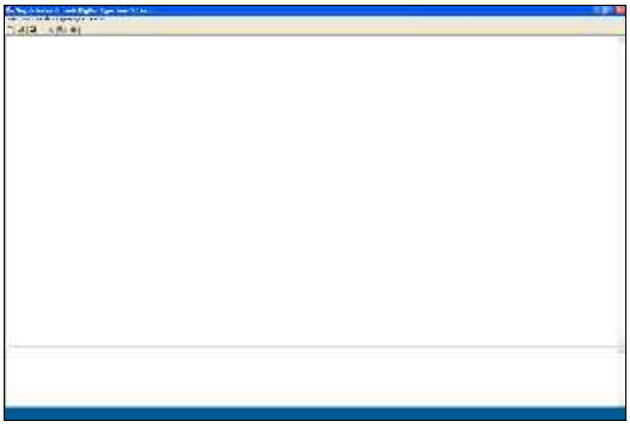
5. Y mendekripsi pesan samaran X (*w*') dengan menggunakan rumus berikut. Y juga dapat memverifikasi keutuhan pesan Bob dengan menggunakan rumus yang dipakai oleh X.

$$w = \frac{w'}{S_1 + k^{-1} * S_2}$$

3. HASIL DAN PEMBAHASAN

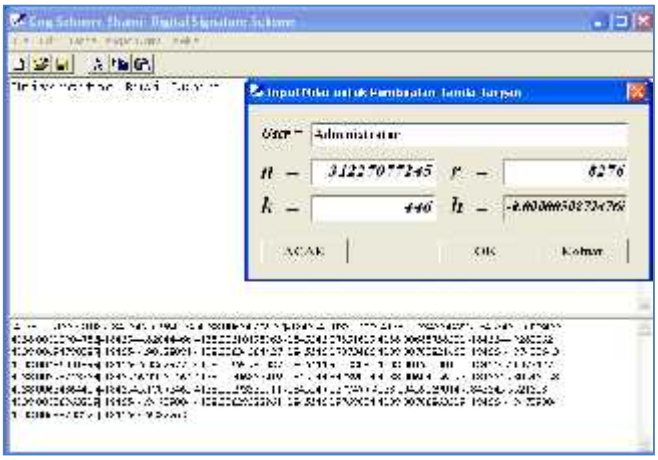
3.1 Proses Ong-Schnorr-Shamir Digital Signature Scheme

Langkah pertama adalah membuka aplikasi yang tampak pada gambar 3 berikut



Gambar 3. Form teks editor form digital signature scheme

Kemudian kita beri pesan dan input nilai untuk pembuatan digital signature



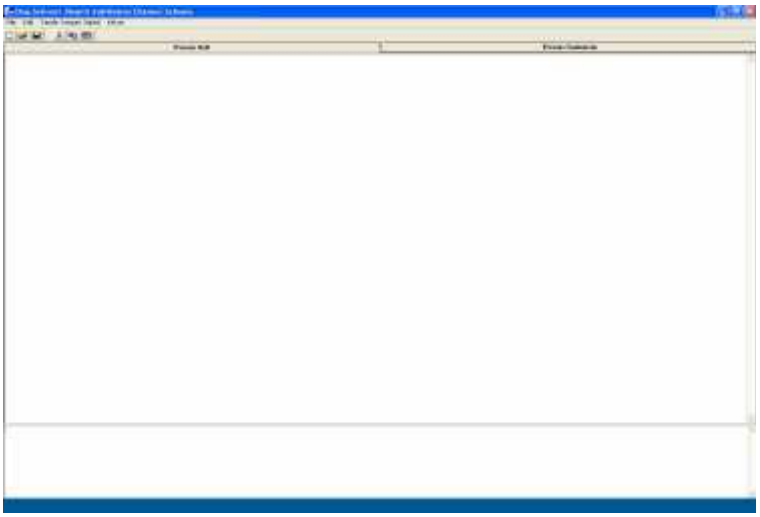
Gambar 4. Penginputan pesan dan pembuatan tanda tangan

Langkah berikutnya jika verifikasi digital signature berhasil akan muncul pesan seperti gambar 5

Gambar 5. Verifikasi signature sukses

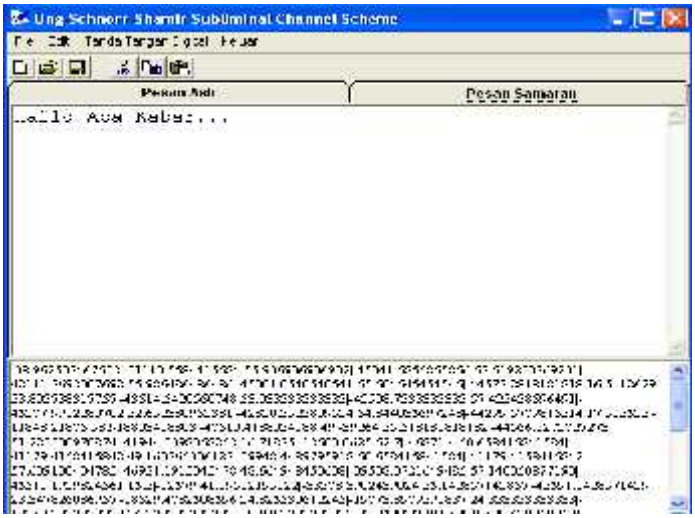
3.2 Ong-Schnorr-Shamir-Subliminal Channel Scheme

Pada fungsi Ong-Schnorr-Shamir-Subliminal Channel Scheme terdapat fungsi untuk menyamarkan pesan, pesan asli akan disembunyikan dan yang tampak hanya pesan samaran. Untuk tampilan Ong-Schnorr-Shamir-Subliminal Channel Scheme seperti pada gambar 6 berikut.



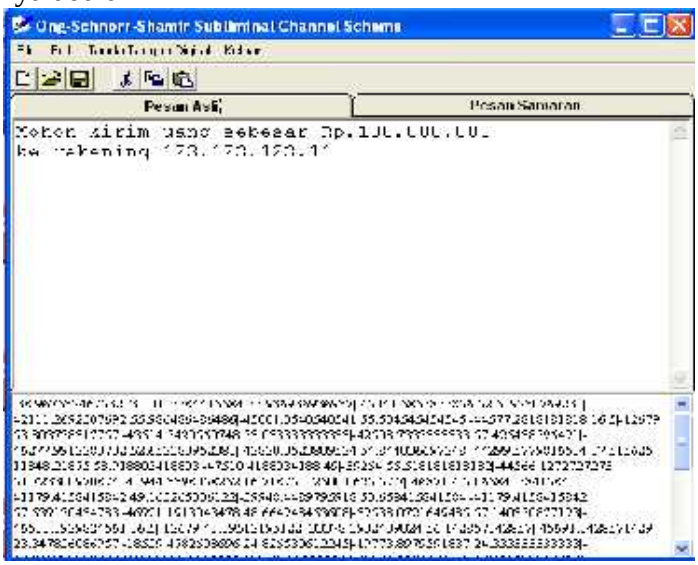
Gambar 6. Verifikasi signature sukses

Kemudian kita buat pesan samaran



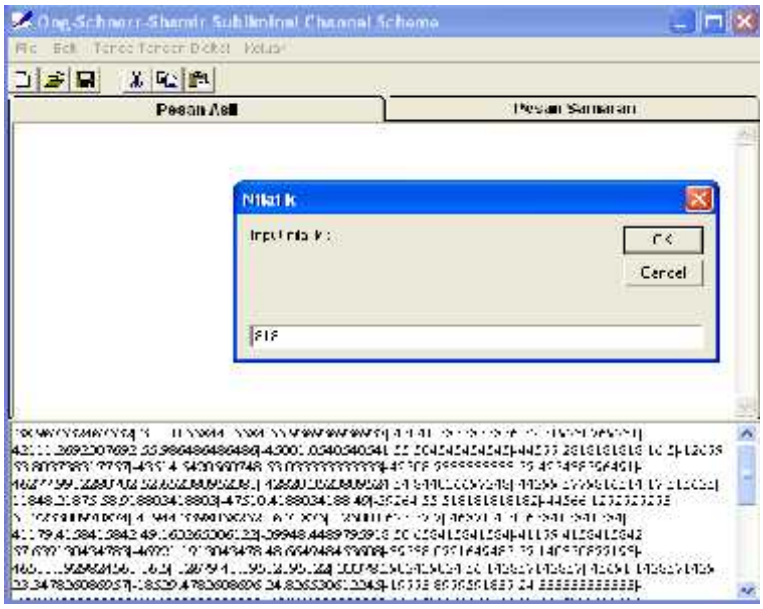
Gambar 7. Pesan samaran

Sedangkan pesan aslinya adalah



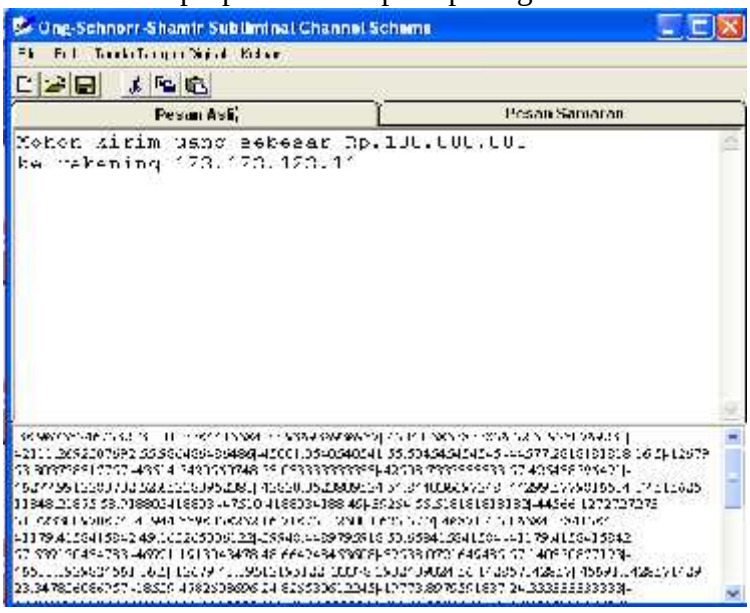
Gambar 8. Pesan asli

Penerima pesan untuk membuka file asli maka perlu memasukan nilai k seperti pada gambar 9 berikut



Gambar 9. Input nilai k

Jika nilai k benar, maka akan tampil pesan asli seperti pada gambar 10



Gambar 10. Pesan asli yang berhasil ditampilkan

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, algoritma yang telah diimplementasikan serta diujikan, maka dapat ditarik kesimpulan sebagai berikut :

1. Untuk menyamarkan pesan yang hendak dikirim maka dapat menggunakan Ong-Schnorr-Shamir-Subliminal Channel Scheme. Dimana pesan yang asli akan disembunyikan dan pihak yang tidak diinginkan hanya dapat melihat pesan samaran
2. Untuk membuat pesan menggunakan digital signature dapat menggunakan Ong-Schnorr-Shamir Digital Signature Scheme
3. Untuk pengiriman pesan dalam karakter yang banyak maka proses pembuatan digital signature semakin lama sehingga perlu pembatasan jumlah karakter.

DAFTAR PUSTAKA

[1] Hassan M. Elkamchouchi, Ali E. Takieldeen, and Mahmoud A. Shawky, "An Advanced Hybrid Technique for Digital Signature Scheme", *5th International Conference on Electrical and Electronics Engineering (ICEEE 2018)*, 5 May 2018

[2] Aziz, A. A. (2009). Implementasi tanda tangan digital menggunakan metode ong-schnorr-shamir dan euclidean pada teks. *Skripsi*. Fakultas Sains dan Teknologi UIN Syarief Hidayatullah

[3] A.H.Sembiring, 2017, Perancangan Aplikasi Dokumen Undeniable Digital Signature Dengan Algoritma Ong-Schnorr-Shamir, *Jurnal Pelita Informatika*, Vol.16. no.4. pp. 363-367

[4] Herdita F.I and K.Karyati. 2017. Penerapan Skema Tanda Tangan Schnorr pada Pembuatan Tanda Tangan Digital. PYTHAGORAS: *Jurnal Pendidikan Matematika*, Vol. 12. No. 1. pp. 57-64

[5] Hisham A.Eltaib. 2020. Hybrid Signature Scheme Integrating Elliptic Curve Cryptosystem withOng, Schnorr, and Shamir Digital Signature Scheme. *Journal of Physics* : Conference Series.

[6] Jain, R. (2011). *Digital signature*. *Makalah*. Washington University.

[7] Ong, Schnorr, and Shamir, "An Efficient Signature Scheme Based on Quadratic Equations," proceedings of the 16'th symposium on theory of computing, pp. 208–216, 1984.