KAPALAMADA: Jurnal Multidisipliner

http://azramedia-indonesia.azramediaindonesia.com/index.php/kapalamada/index
DOI: https://doi.org/10.62668/kapalamada.v3i01.1108
Email : info@azramediaindonesia.com

Open Access

DIGITAL SIGNATURE SECURITY LEARNING ANIMATION DESIGN USING THE ONG-SCHNORR-SHAMIR METHOD

Deny Adhar[*1], Risman[2], Linda Wahyuni[3], Ahmad Sabir[4]
[1,3] Universitas Potensi Utama, Indonesia
[2]Institut Teknologi dan Bisnis CARNEGEI, Indonesia
[4]Universitas Mercu Buana, Indonesia
Corresponding Author: adhardeny@gmail.com

Info Article
Received :
10 Januari 2023
Revised :
07 Februari 2024
Accepted :
02 Maret 2024
Publication :
31 Maret 2024

Keywords:
Learning Media, Digital Signature, Ong-Schnorr-Shamir Method
Kata Kunci :
Media Pembelajaran, *Digital Signature, Metode Ong-Schnorr-Shamir*

Abstract: *This research is entitled Digital Signature Security Learning Animation Design Using Ong-Schnorr-Shamir Method. The purpose of the research is to know the design of digital signature security learning animation using ong-schnorr-shamir method. Digital signature is an authentication mechanism that allows the author of a message to add a code that acts as its signature. There are also various schemes that can be used to process digital signatures on a message. One of the schemes is the Ong-Schnorr-Shamir scheme. The Ong-Schnorr-Shamir scheme is a digital signature scheme based on sequentially linearized equations. This digital signature scheme uses polynomials modulo n. The security of this scheme is based on the difficulty of solving polynomial equations. The version of the scheme described here is based on quadratic polynomials.*

Abstrak: Penelitian ini berjudul Desain Animasi Pembelajaran Keamanan Tanda Tangan Digital Menggunakan Metode Ong-Schnorr-Shamir. Tujuan penelitian adalah untuk mengetahui desain animasi pembelajaran keamanan tanda tangan digital menggunakan metode ong-schnorr-shamir. Tanda tangan digital (digital signature) adalah suatu mekanisme otentikasi yang memungkinkan pembuat pesan menambahkan sebuah kode yang bertindak sebagai tanda tangannya. 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. Skema Ong-Schnorr-Shamir merupakan skema tanda tangan digital yang berdasarkan pada persamaan linier sekuensial (sequentially linearized equations). Skema tanda tangan digital ini menggunakan polinomial modulo n. Keamanan dari skema ini didasarkan pada kesulitan untuk memecahkan persamaan polinomial. Versi dari skema yang dideskripsikan pada pembahasan kali ini adalah berdasarkan polinominal kuadratik.

INTRODUCTION

Tanda tangan digital (digital signature) adalah suatu 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.

Ong-Schnorr-Shamir memiliki dua buah skema, yaitu skema tanda tangan digital (digital signature) dan skema saluran tersembunyi (subliminal channel). 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 dekripsi yang menyamarkan pesan asli.

METHOD

Ong-Schnorr-Shamir Digital Signature Scheme

Berikut adalah prosedur kerja skema tanda tangan digital Ong-Schnorr-Shamir:[3]

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 (Bob)
2. Hitung nilai h dengan rumus berikut.

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

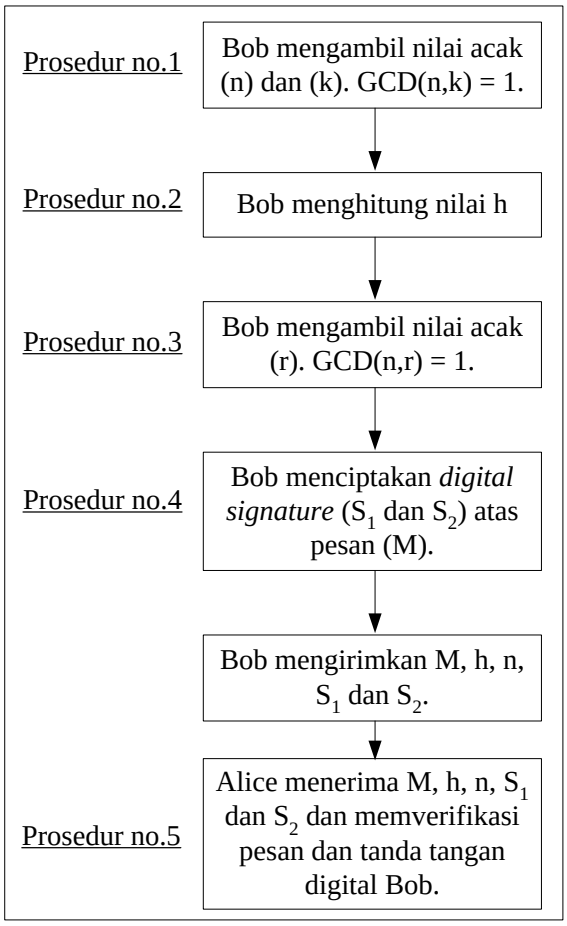
3. Tentukan sebuah bilangan integer acak (r).
   a. n dan r harus relatif prima, artinya nilai GCD(n, r) = 1.
   b. r merupakan kunci publik, artinya nilai r boleh diketahui oleh pihak lain.
4. Hitung S1 dan S2 terhadap pesan (M). (S1 dan S2 merupakan signature oleh Bob) dengan rumus berikut.

$$S_1 = {}^{1}/_{2} * (M/r + r) \bmod n$$
$$S_2 = {}^{k}/_{2} * (M/r - r) \bmod n \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2)$$

5. Alice memverifikasi pesan dan tanda tangan digital Bob dengan menggunakan rumus berikut.

$$S_1^2 + h \cdot S_2^2 \equiv M \pmod n \quad \ldots\ldots\ldots\ldots\ldots\ldots(3)$$

Skema prosedur dapat dilihat pada gambar 2.1 berikut ini.



Gambar 2.1 Skema prosedur Ong-Schnorr-Shamir Digital Signature

Sebagai contoh, pesan yang akan dikirimkan adalah huruf ‘A’, maka prosedur yang dilakukan dalam skema ini adalah:

1) Bob memilih n = 393541 dan k = 20.
2) Bob menghitung nilai h.

   h = -(k-1)2 mod n

   h = -(1/20)2 mod 393541

h = -0.0025

3) Bob memilih r = 16.
4) Hitung S1 dan S2 (digital signature dari Bob)

   M = Kode ascii dari huruf 'A' = 65.

   S1 = 1/2 * (65/16 + 16) mod 393541

   S1 = 10.03125

   S2 = 20/2 * (65/16 - 16) mod 393541

   S2 = -119.375

5) Alice memverifikasi pesan dan tanda tangan dari Bob.

   n = 393541, h = -0.0025, r = 16

   M = Kode ascii dari huruf 'A' = 65

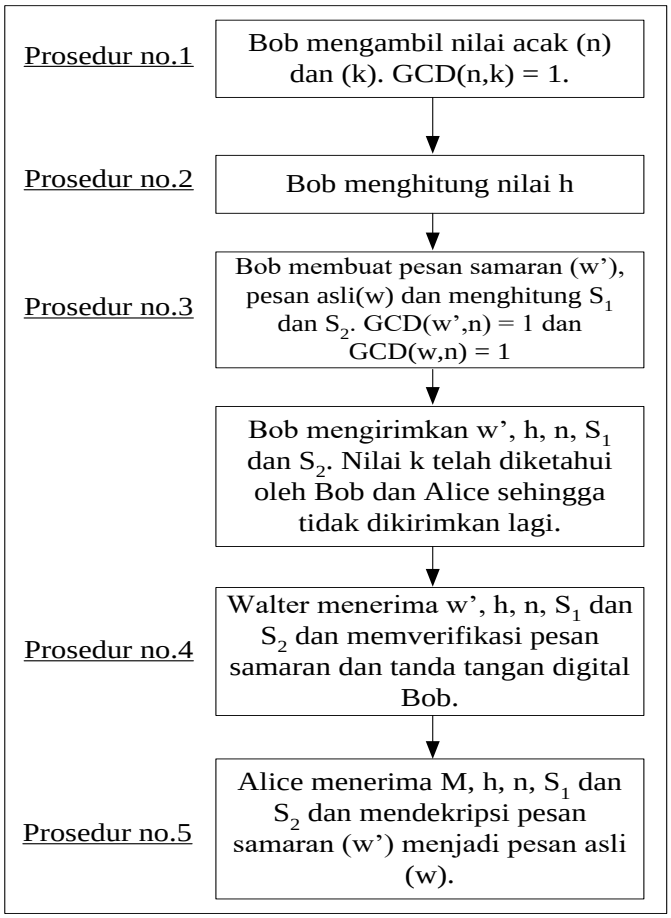
   S1 = 10.03125, S2 = -119.375

   (10.03125)^2 + -0.0025 . (-119.375)^2 = 65

   65 = 65 (True)

Ong-Schnorr-Shamir Subliminal Channel Scheme

Skema prosedur dapat dilihat pada gambar 2.2 berikut ini.



Gambar 2.2 Skema prosedur Ong-Schnorr-Shamir *Subliminal Channel*

Sebagai contoh, pesan yang akan dikirimkan adalah huruf ‘A’, maka prosedur yang dilakukan dalam skema ini adalah:

1) Bob memilih n = 393541 dan k = 20.
2) Bob menghitung nilai h.
   h = -(k-1)2 mod n
   h = -(1/20)2 mod 393541
   h = -0.0025
3) Misalkan pesan asli (w) = ‘K’ dan pesan samaran (w’) = ‘H’, maka hitung S1 dan S2 (digital signature dari Bob)
   w = Kode ascii dari huruf 'K' = 75
   w' = Kode ascii dari huruf 'H' = 72
   S1 = 1/2 * (72/75 + 75) mod 393541
   S1 = 37.98
   S2 = 20/2 * (72/75 - 75) mod 393541
   S2 = -740.4
4) Walter memverifikasi tanda tangan dan pesan samaran (w’) dari Bob.
   w' = Kode ascii dari huruf 'H' = 72
   S1 = 37.98, S2 = -740.4
   w' = (37.98)^2 + -0.0025 . (-740.4)^2
   72 = 72 (True)
5) Alice mendekripsi pesan samaran (w’) menjadi pesan asli(w).
   w' = Kode ascii dari huruf 'H' = 72
   S1 = 37.98, S(2) = -740.4
   w = 72 / (37.98 + -740.4/20)
   w = 75 (Karakter dari kode ascii 75 = 'K')

Pesan dan digital signature dari metode Ong-Schnorr-Shamir subliminal channel dapat diverifikasi keasliannya dengan menggunakan Ong-Schnorr-Shamir digital signature scheme. Perbedaannya hanya terletak pada metode dekripsi yang dimiliki oleh Ong-Schnorr-Shamir subliminal channel.

RESULTS AND DISCUSSION

Perancangan Animasi Pembelajaran Kemananan Digital Signature dengan Metode Ong-Schnorr-Shamirdibangun dengan menggunakan bahasa pemrograman Microsoft Visual Basic 6.0 diintegrasikan dengan aplikasi Macromedia Flash MX. Fungsi dari

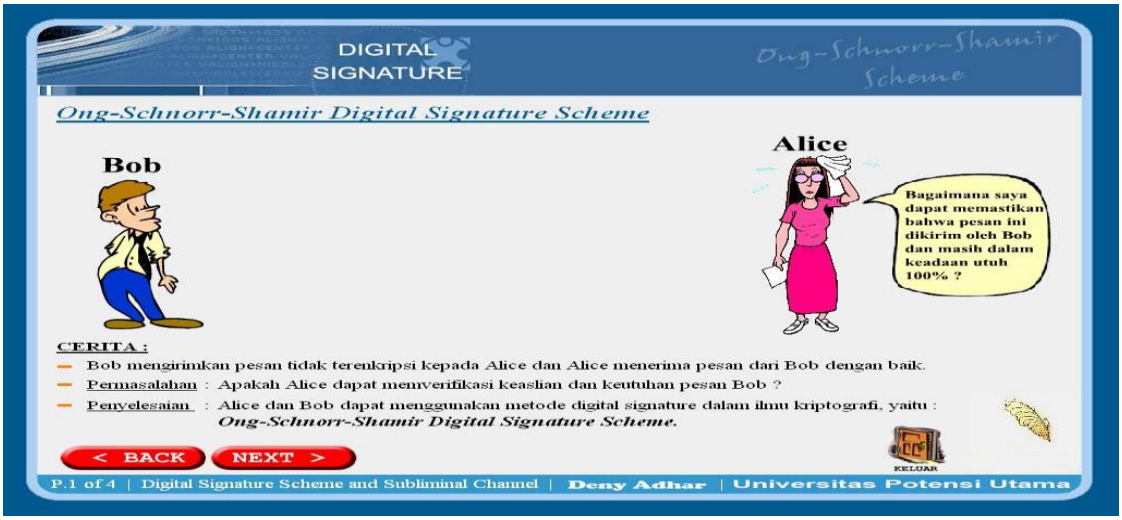
aplikasi Flash MX adalah untuk membuat beberapa slide animasi dan tombol yang terintegrasi ke bahasa pemrograman Microsoft Visual Basic 6.0. Berikut adalah pembahasan perancangan prosedur kerja perangkat lunak dan perancangan slide animasi dan tombol pada aplikasi Flash MX.

Algoritma yang digunakan untuk merancang perangkat lunak ini dibagi menjadi 2 (dua) bagian, yaitu:

1. Skema Ong-Schnorr-Shamir Digital Signature, terbagi menjadi:
   a. Algoritma Pembuatan Tanda Tangan Digital.
   b. Algoritma Verifikasi Tanda Tangan Digital.
   c. Algoritma Menyimpan File Digital Signature pada Aplikasi.
   d. Algoritma Membuka File Digital Signature pada Aplikasi.
2. Skema Ong-Schnorr-Shamir Subliminal Channel, terbagi menjadi:
   a. Algoritma Pembuatan Tanda Tangan Digital.
   b. Algoritma Verifikasi Tanda Tangan Digital.
   c. Algoritma Dekripsi.
   d. Algoritma Menyimpan File Subliminal Channel pada Aplikasi.
   e. Algoritma Membuka File Subliminal Channel pada Aplikasi.

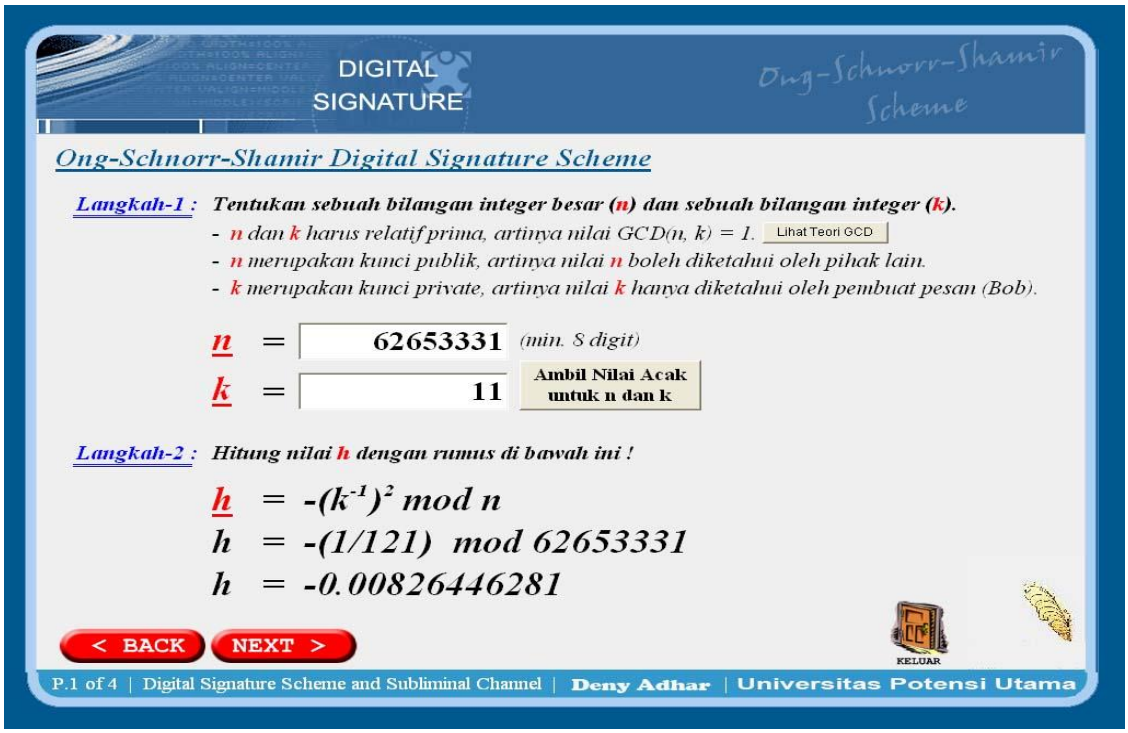
Untuk melihat dan menguji output perangkat lunak, maka dibahas beberapa contoh penerapan skema digital signature dan subliminal channel pada subbab ini. Contoh penerapan skema digital signature pada perangkat lunak adalah sebagai berikut:

Untuk melihat dan menguji *output* perangkat lunak, maka dibahas beberapa contoh penerapan skema *digital signature* dan *subliminal channel* pada subbab ini. Contoh penerapan skema *digital signature* pada perangkat lunak adalah sebagai berikut:



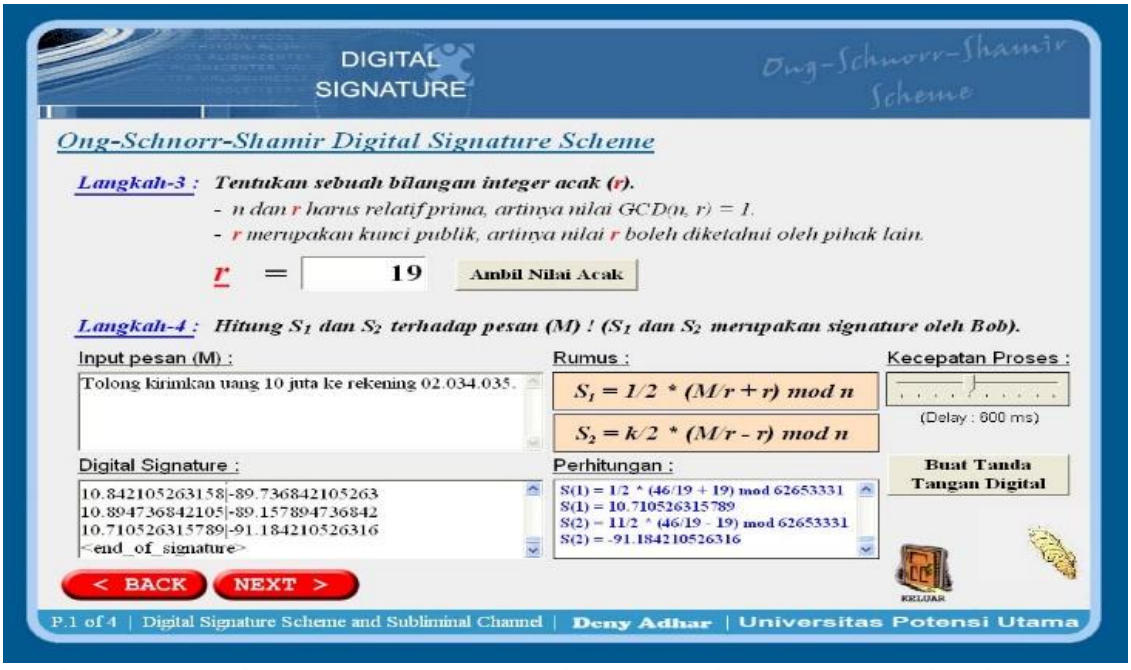
Gambar 3.1 Tampilan Pendahuluan Ong-Schnorr-Shamir

Ambil nilai n = 62653331 dan nilai k = 11. Tampilan input dapat dilihat pada gambar 3.2.



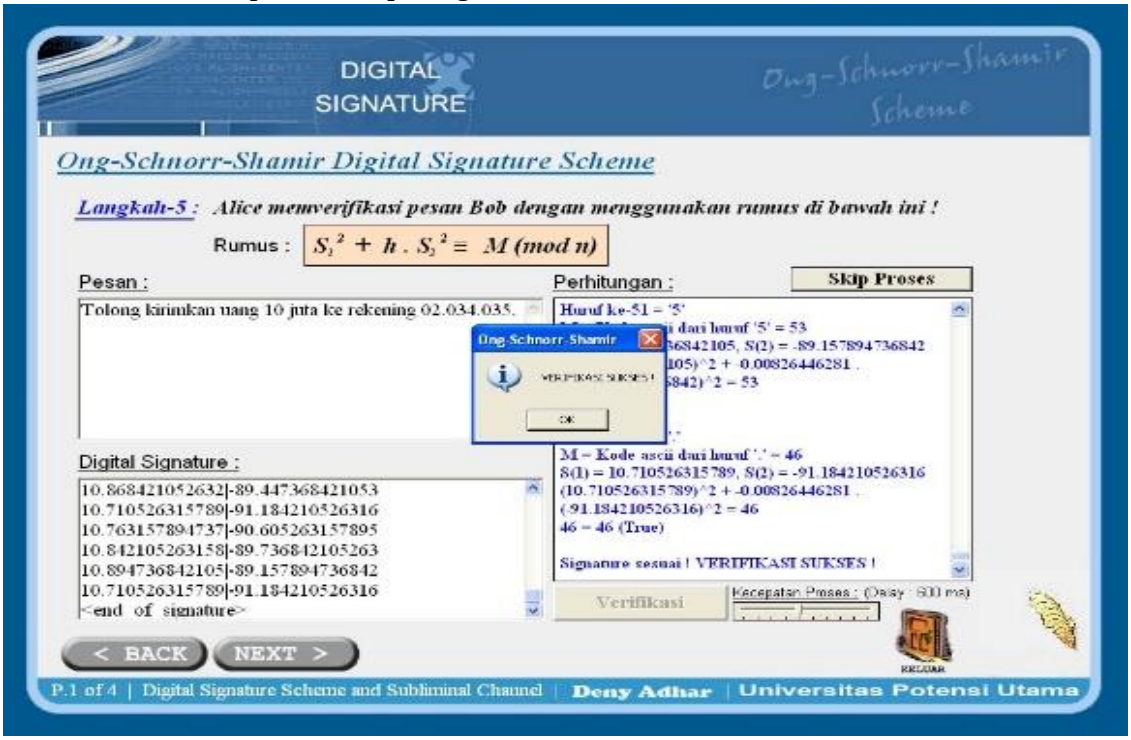
Gambar 3.2 Tampilan Input n, k & Perhitungan Nilai h pada Ong-Schnorr-Shamir

Ambil nilai r = 18 dan pesan = ‘Tolong kirimkan uang 10 juta ke rekening 02.034.035.’. Tampilan input dapat dilihat pada gambar 3.3.



Gambar 3.3 Tampilan Input r, Pesan & Pembuatan Tanda Tangan Digital pada Ong-Schnorr-Shamir

Proses verifikasi dapat dilihat pada gambar 4

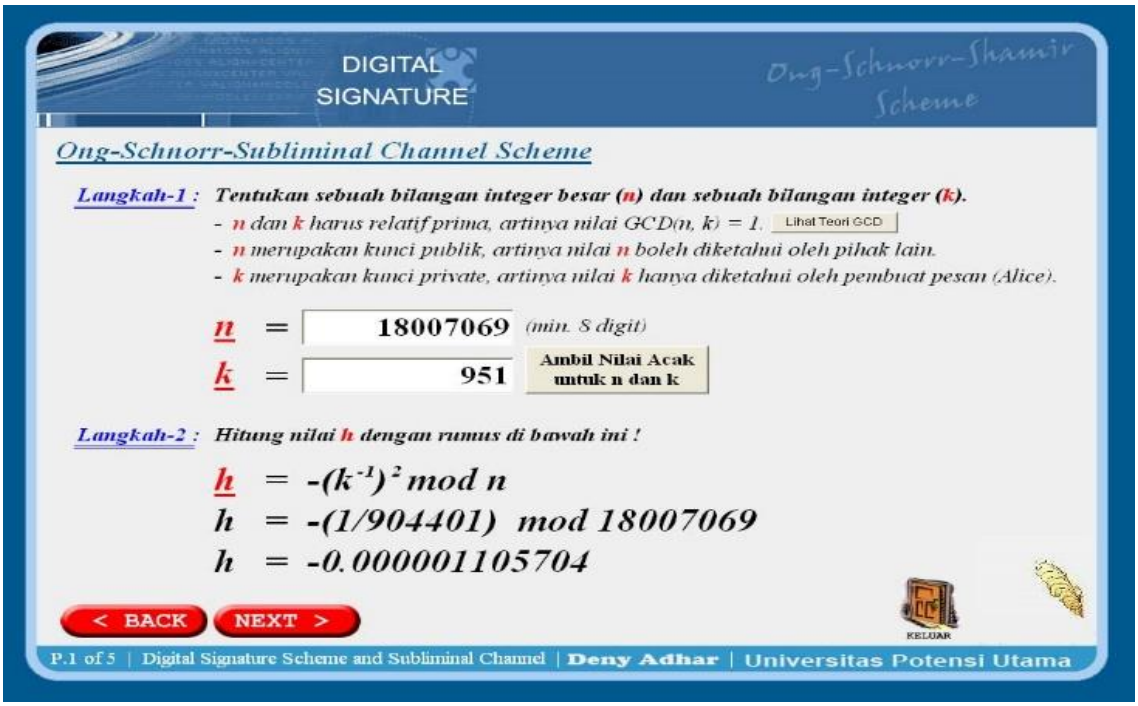


Gambar 3.4 Tampilan Verifikasi Pesan & Tanda Tangan Digital pada Ong-Schnorr-Shamir

Pembelajaran penerapan skema digital signature pada perangkat lunak adalah sebagai berikut:

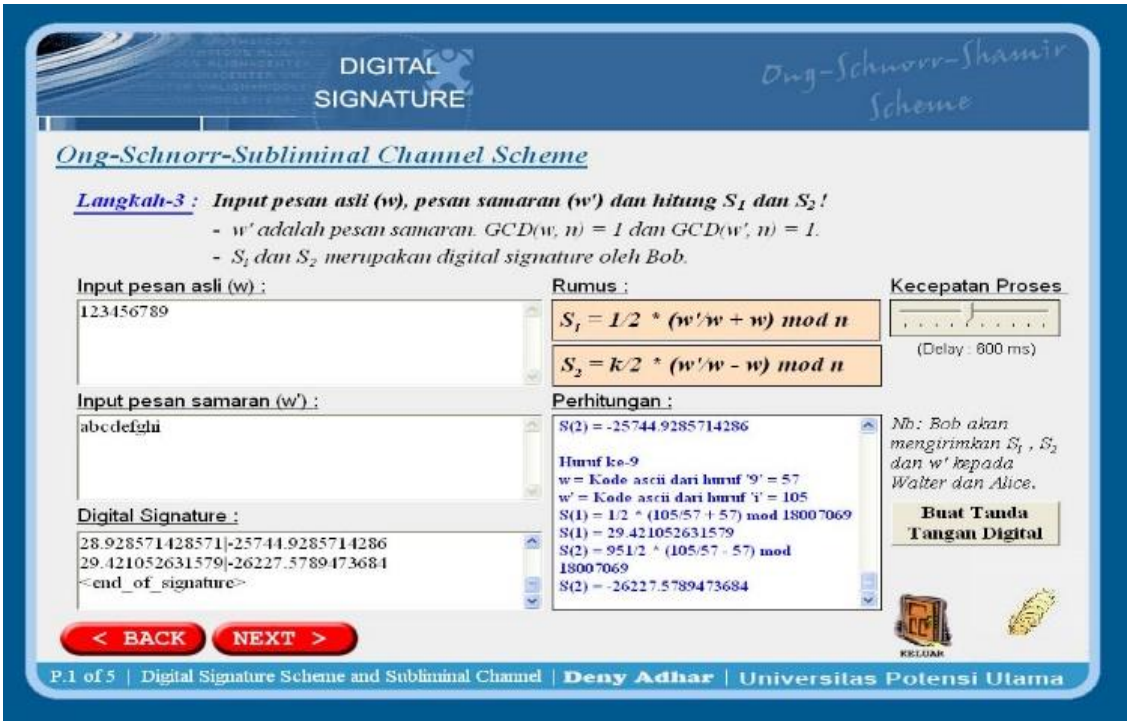
Gambar 3.5 Tampilan Pendahuluan Ong-Schnorr-Shamir SCS

Ambil nilai n = 18007069 dan nilai k = 951. Tampilan input dapat dilihat pada gambar 3.6.



Gambar 3.6 Tampilan Input n, k dan Perhitungan Nilai h pada Ong-Schnorr-Shamir SCS

Misalkan pesan asli = ‘123456789’ dan pesan samaran = ‘abcdefghi’. Tampilan input dapat dilihat pada gambar 3.7.



Gambar 3.7 Tampilan Input Pesan Asli, Pesan Samaran dan Pembuatan Tanda Tangan Digital

Proses verifikasi seperti terlihat pada gambar 3.8

Gambar 3.8 Tampilan Verifikasi Pesan Samaran dan Tanda Tangan Digital pada Ong-Schnorr-Shamir SCS

Proses dekripsi seperti terlihat pada gambar 3.9.

Gambar 3.9 Tampilan Dekripsi Pesan Samaran ke Pesan Asli pada Ong-Schnorr-Shamir SCS

CONCLUSION

Setelah menyelesaikan Perancangan Animasi Pembelajaran Kemananan Digital Signature dengan Metode Ong-Schnorr-Shamir ini, penulis menarik kesimpulan sebagai berikut:

1. Skema Ong-Schnorr-Shamir Digital Signature dapat digunakan untuk menjaga keaslian data (authentication) dan keutuhan data (data integrity).
2. Skema Ong-Schnorr-Shamir Subliminal Channel merupakan metode kriptografi yang dapat digunakan untuk menyamarkan pesan asli. Skema ini juga mendukung proses verifikasi dari skema Ong-Schnorr-Shamir Digital Signature.
3. Perangkat lunak menjelaskan secara bertahap proses kerja Ong-Schnorr-Shamir Digital Signature dan Ong-Schnorr-Shamir Subliminal Channel, sehingga dapat membantu pemahaman terhadap skema ini dan dapat digunakan untuk mendukung kegiatan belajar mengajar dalam mata kuliah kriptografi.

REFERENCES

A. H. Sembiring, (2017) “PERANCANGAN APLIKASI DOKUMEN UNDENIABLE DIGITAL SIGNATURE DENGAN ALGORITMA ONG-SCHNORR-SHAMIR,” *Pelita Inform. Budi Darma*, vol. 16, no. 4, pp. 363–367, 2017, [Online]. Available: https://ejurnal.stmik-budidarma.ac.id/index.php/pelita/article/view/552.

Fatah, A., Arif, I., Farchan, F., Sununianti, V. V., Madi, R. A., Satria, E., ... & Dewi, S. P. (2019). APPLICATION OF KNUTH-MORRIS-PRATT ALGORITHM ON WEB BASED DOCUMENT SEARCH. In *Journal of Physics: Conference Series* (Vol. 1175, No. 1, p. 012117). IOP Publishing.

H. Ong and C. P. Schnorr,(1991) “FAST SIGNATURE GENERATION WITH A FIAT SHAMIR - LIKE SCHEME,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 473 LNCS, pp. 432–440, 1991, doi: 10.1007/3-540-46877-3_38.

L. M. Adleman and G. L. Mi, (1986) “Z [F I L .,” no. 2, pp. 3–13, 1986.

M. Ikhsan, M. Kom, D. Arisandi, and M. Kom, (2020) “STRATEGI KEAMANAN PESAN MENGGUNAKAN SKEMA SUBLIMINAL CHANEL ONG-SCHNORR-SHAMIR.”

M. A. Virgiawan and G. P. Utama, (2020) “PENGGUNAAN METODE ONG-SCHNORR-SHAMIR PADA PEMBUATAN TANDA TANGAN DIGITAL,”

J. Tek. Inform. Unika St. Thomas, vol. 05, pp. 51–59, 2020.

P. Chyan, (2018) "PENERAPAN SISTEM KRIPTOGRAFI ENKRIPSI JAMAK DAN TANDA TANGAN DIGITAL DALAM MENDUKUNG KEAMANAN INFORMASI," *J. Temat.*, vol. 6, no. 1, pp. 39–46, 2018.

Putar, R., (2005), THE BEST SOURCE CODE VISUAL BASIC, PT. Elex Media Komputindo, Jakarta.

Suciadi, A., (2003), MENGUASAI PEMBUATAN ANIMASI DENGAN FLASH MACROMEDIA MX, PT.Elex Media Komputindo, Jakarta.

Y. Anshori, A. Y. Erwin Dodu, and D. M. P. Wedananta, (2019) "IMPLEMENTASI ALGORITMA KRIPTOGRAFI RIVEST SHAMIR ADLEMAN (RSA) PADA TANDA TANGAN DIGITAL," *Techno.Com*, vol. 18, no. 2, pp. 110–121, 2019, doi: 10.33633/tc.v18i2.2166.