KLIK: Kajian Ilmiah Informatika dan Komputer
ISSN 2723-3898 (Media Online)
Vol 3, No 4, Februari 2023
Hal 384-392
https://djournals.com/klik

Strategi Otentikasi Dokumen Pada Email Menggunakan Digital Signature dengan Algoritma Schnorr

Lisda Juliana Pangaribuan[1,*], Catra Indra Cahyadi[2], Jaidup Banjarnahor[1], Berlin Barus[1], Bertha N Siahaan[1]

[1]Universitas Mandiri Bina Prestasi, Medan, Indonesia
[2] Politeknik Penerbangan Medan, Medan, Indonesia
Email: [1,*]lisdajuliana@gmail.com, [2]catraindracahyadi@gmail.com, [3]marbun2005@gmail.com, [4]karbreti68@gmail.com, [5]berthasiahaan9@gmail.com
Email Penulis Korespondensi: lisdajuliana@gmail.com

Abstrak−Email adalah fasilitas internet untuk mengirim surat elektronik. Meskipun ada webmail yang menyediakan keamanan standar tapi untuk dokumen attachment e-mail dalam pengiriman e-mail banyak terjadi penyadapan, pemalsuan ,penyusupan dan spamming sebab itu perlu adanya strategi pengamanan dokumen yang baik supaya informasi yang dikirim otentik dan hanya diterima oleh penerima yang berhak saja. Otentikasi adalah identifikasi yang dilakukan masing-masing pihak yang berkomunikasi supaya pengirim dan penerima informasi saling percaya, Meskipun sudah dilakukan otentikasi pesan tetapi kedua belah pihak masih mungkin untuk saling menyerang. Penelitian ini bertujuan untuk menerapkan digital signature dalam menguji keutuhan dan otentikasi dokumen attachment pada email menggunakan algoritma Schnorr. Untuk verifikasi digital signature digunakan Fungsi hash SHA-1. Hasil pengujian menunjukkan bahwa isi dokumen attachment email akan menghasilkan Message Digest yang berbeda jika bilangan prima yang diinput berbeda sehingga para kriptanalis sulit memecahkannya. Perbedaan Message Digest terjadi karena bilangan prima yang berbeda menyebabkan perbedaan kunci privat dan kunci publik karena pasangan kunci privat dan kunci publik yang sinkron, pengirim dan penerima diverifikasi dengan benar. Jika ada perubahan dengan pergantian, dan pemindahan satu karakter saja dari isi dokumen akan menghasilkan perubahan Message Digest yang sangat signifikan. Jika ada yang mengubah isi dokumen maupun kunci akan membuat hasil dari proses verifikasi tidak benar, maka penerima informasi mengetahui bahwa dokumen yang diterimanya sudah tidak. Metode Schnorr merupakan strategi yang dapat memberikan keamanan dokumen attachment pada e-mail lebih baik daripada keamanan yang diterapkan e-mail standard.

Kata Kunci: Tandatangan Digital; Metode Schnorr; Kriptografi; Otentikasi; Hash SHA-1

Abstract−Email is an internet facility for sending electronic mail. Although there is a webmail that provides standard security but for e-mail attachment documents when sending e-mail there are lots of eavesdropping, forgery, infiltration,and spamming so needed security of email. Authentication is identification carried out by each communicating party so sender and recipient of information trust each other. Although message authentication has been carried out, it is still possible for both parties to attack each other. This study aims to apply digital signatures in testing the integrity and authentication of document attachments email using the schnorr algorithm. SHA-1 hash function is used for verification, Results show that contents of email attachment will produce a different Message Digest if prime numbers are different, so cryptanalysts can't solve it. Differences in Message Digest occur because different prime numbers cause differences in private keys and public keys. Private key and public key pairs are synchronous so sender and recipient are verified correctly. If there are changes or removed just one character from contents of document will result in a very significant Message Digest change. If someone changes contents of document or key, so verification process to be incorrect and recipient of information knows that document he received is no longer valid. Schnorr method is a strategy to provide document attachment security in emails that is better than security applied to standard emails.

Keywords: Digital Signature; Schnorr Methode; Cryptography; Autentication; Hash SHA-1

1. PENDAHULUAN

E-mail adalah perangkat surat elektronik yang banyak digunakan oleh masyarakat khususnya pengguna internet,[1] baik yang menggunakan webmail gratis, maupun menyediakan sendiri mail server atau menyewa melalui ISP. Ada banyak dokumen yang dikirim melalui email bersifat rahasia diantaranya notifikasi transaksi bank, tagihan kartu kredit dan transaksi e-commerce sebab itu isi dokumen ini hanya boleh diketahui oleh pihak yang berhak[2]. Pengiriman dokumen melalui internet mempunyai risiko di bidang keamanan. Walaupun ada vendor webmail yang menyediakan keamanan standar sejenis Pretty Good Privacy (PGP) [3] , namun belum diterapkan keamanan pada dokumen attachment e-mail sehingga masih banyak kasus yang terjadi tentang tidak amannya pemakaian e-mail misalnya terkena sniffing, replay attack, phising, spoofing, pembobolan, dan man in the midle attack.[4] Dengan kata lain dalam pengiriman dokumen e-mail sering terjadi penyadapan, pemalsuan ,penyusupan, spamming dan mailbomb [5] untuk itu perlu adanya strategi pengamanan dokumen yang baik supaya informasi yang dikirim otentik dan hanya diterima oleh penerima yang berhak saja.[6]. Keamanan dokumen harus memenuhi 4(empat) aspek utama yaitu kerahasiaan (confidentiality), integritas (integrity), Nir-penyangkalan (non-repudiation) dan otentikasi(authentication) [7] [8].

Pada penelitian terdahulu, Fitriyah mengatakan adanya pemalsuan tanda tangan surat bebas covid oleh petugas penerimaan pasien di salah satu puskesmas di Mojokerto yang berdampak ke sanksi pidana sebab itu diperlukan tanda tangan digital pada fasilitas pelayanan kesehatan karena tanda tangan digital memiliki sistem enkripsi yang aman, dapat menghindari risiko pemalsuan tanda tangan atau penyalahgunaan pihak yang tidak bertanggungjawab, ramah lingkungan, efisien dan dilindungi oleh penjamin[9].

Beberapa penelitian terdahulu terkait otentikasi dan tandatangan digital seperti penelitian Puspitasari [10] mengatakan tanda tangan digital bukanlah tanda tangan yang di-digitalisasi dengan scanner namun suatu nilai kriptografis

yang bergantung pada dokumen asli dan pengirimnya. Pada tanda tangan digital ditambahkan sebuah kode yang dihasilkan dari enkripsi *message digest* dengan fungsi hash.

Untuk menjamin keaslian serta legalitas suatu dokumen digunakan tanda tangan digital. *Digital Signature* adalah suatu cara menjamin keaslian suatu dokumen elektronik serta menjaga supaya pengirim dokumen dalam suatu waktu tidak dapat menyangkal bahwa dialah pengirim dokumen itu. Dalam penerapannya *Digital Signature* menggunakan algoritma dan teknik-teknik kriptografi kunci publik yang menggunakan dua buah kunci, yaitu kunci untuk membentuk tanda tangan digital atau mengenkripsi ke bentuk lain sehingga tidak dapat dipahami, dan kunci untuk verifikasi tanda tangan digital ataupun mengembalikan pesan ke bentuk semula [11].

Kriptografi merupakan seni mengenai metode mengamankan dokumen supaya hanya penerima aslinya yang dapat membaca informasi dan memahaminya sehingga informasi yang bersifat rahasia dan dikirim melalui jaringan internet tidak dapat diketahui serta dimanfaatkan oleh pihak yang tidak berkepentingan [8].

Lorien dan Wellem memadukan *QR code* dan *digital signature* untuk memastikan keaslian dan integritas dokumen dan dapat mencegah pemalsuan dokumen. Semua dokumen yang mencantumkan *QR code* yang tidak di-generate oleh sistem berhasil diidentifikasi sebagai dokumen palsu.[12]. Penelitian lain mengatakan Metode Schnorr adalah pengembangan dari metode El-Gamal sehingga sistem keamanan El-Gamal terdapat pada Schnorr. Pembuatan Tanda Tangan Schnorr dimulai dari pembentukan kunci, pembuatan tandatangan dengan menambahkan nilai hash, serta proses verifikasinya[13]. Walaupun tanda tangan digital metode Schnorr disebut aman tapi keamanan masih bergantung pada kerahasiaan kunci privat agar tidak bisa diketahui orang lain. Dan dibutuhkan suatu cara untuk mempermudah penentuan nilai prima p dan q yang memenuhi p-1= (0 mod p) [14], maka dalam penelitian ini bilangan prima di *generate* secara acak dengan algoritma Fast Exponentiation.

Menurut Prabowo [15] Digital signature merupakan suatu teknologi digital yang disisipkan pada sebuah dokumen untuk menjaga autentifikasinya. Salah satu cara untuk membuat *digital signature* pada dokumen digital adalah menggunakan fungs hash. Pada penelitian ini algoritma hash yang digunakan adalah SHA-256, sedangkan algoritma kunci publiknya yaitu algoritma Rivest-Shamir-Adleman (RSA). *Riset* tersebut mengimplementasikan *digital signature* dengan fungsi hash algoritma SHA-256 dan algoritma RSA dapat memberikan layanan keamanan dokumen pada sertifikat tanah digital untuk mencegah terjadinya pemalsuan dan manipulasi dokumen oleh orang yang tidak berhak.

Otentikasi adalah identifikasi oleh masing-masing pihak yang berkomunikasi untuk memperoleh kepercayaan penuh antara pengirim dan penerima informasi, Meskipun sudah dilakukan otentikasi pesan tetapi kedua belah pihak masih mungkin untuk saling menyerang. [16].

Solusi untuk mengatasi masalah keamanan pengiriman dokumen via internet adalah *digital signature*, maka penelitian ini dilakukan dengan tujuan untuk menerapkan *digital signature* dalam menguji keutuhan dan otentikasi dokumen *attachment* pada email dengan algoritma Schnorr supaya kerahasiaan, integritas, dan keasliannya terjaga dan untuk melakukan verifikasi *digital signature* digunakan Fungsi hash SHA-1.

Algoritma Schnorr adalah algoritma yang digunakan untuk otentikasi dan tandatangan digital yang mengambil efek melalui perhitungan logaritma diskrit dan menggunakan bilangan prima dalam pembentukan kuncinya proses[17].

Sedangkan fungsi hash adalah cara untuk menghasilkan sebuah digital “fingerprint” ukuran kecil dari data yang acak. Fungsi ini mencampurkan data untuk menghasilkan fingerprint yang disebut sebagai nilai hash (hash value).

SHA di golongkan menjadi 4 bagian yaitu: SHA-1,SHA-256, SHA-384, dan SHA-512. Secure Hash Algorithm (SHA-1) dapat di implementasikan pada *Digital Signature*. SHA-1 dikatakan aman karena proses SHA-1 dihitung secara infisibel untuk menemukan informasi yang sesuai sehingga diperoleh pencerna informasi.[18]

2. METODOLOGI PENELITIAN

2.1 Langkah-Langkah Penelitian

Penelitian ini dimulai dengan identifikasi masalah yaitu dengan mengirim dokumen email, kemudian menganalisis kebutuhan kebutuhan sistem yang akan dirancang, lalu membangun sistem kemudian melakukan pengujian terhadap sistem. Penelitian ini mengunakan algoritma Schnorr Authentication dan Digital Signature dengan melakukan langkah-langkah : pembentukan kunci, pembuatan tanda tangan yang disertai perhitungan nilai hash lalu verifikasi [14]

a. Pihak1 (woman) mengirim dokumen

Langkah-langkah yang dilakukan pihak1 (woman)

a. Woman mengetik pesan
b. Woman melakukan proses pembentukan kunci, pihak yang di otentikasi dan pihak yang diverifikasi tanda tangan digitalnya dengan cara memilih nilai variabel, menghitung nilai variabel atau sedang melakukan pengiriman.

b. Pihak2 (man) mengirim dokumen

Langkah-langkah yang dilakukan pihak2 (man)

a. Man menerima kunci publik
b. Man melakukan proses otentikasi dan memverifikasi tanda tangan digital dari woman dengan memilih nilai variabel, menghitung nilai variabel atau sedang melakukan pengiriman.

c. Algoritma Pembentukan kunci [19]

a. Pilih 2 buah bilangan prima p dan q, dan sebuah nilai a, dimana GCD(q, p-1) <> 1 dan (a^q) mod p = 1 (1)
Rumus (1) diselesaikan dengan menggunakan algoritma Fast Exponentiation.
b. Pilih sebuah nilai s, dimana s < q. dan s adalah kunci privat
c. Hitung nilai v dengan rumus berikut:
v = a^(-s) mod p maka v adalah kunci publik (2)
Rumus (2) diselesaikan dengan menggunakan algoritma Extended Euclidean.

d. Algoritma otentikasi [13]
a. Pihak1 (woman) memilih sebuah nilai r (r < q).
b. Pihak1 (woman) menghitung: x = a^r mod p (3)
Rumus (3) diselesaikan dengan menggunakan algoritma Fast Exponentiation.
c. Pihak1 (woman) mengirim x kepada Pihak2 (man).
d. Pihak2 (man) memilih sebuah nilai e (e diantara 0 sampai (2^t-1)) (4)
dan mengirim e kepada Pihak1 (woman) .
e. Pihak1 (woman) menghitung: y = (r + se) mod q (5)
dan mengirim y kepada Pihak2 (man).
f. Pihak2 (man) melakukan verifikasi berikut: x = ((a^y).(v^e)) mod p (6)
Jika nilai x sesuai, maka verifikasi dan otentikasi berhasil.

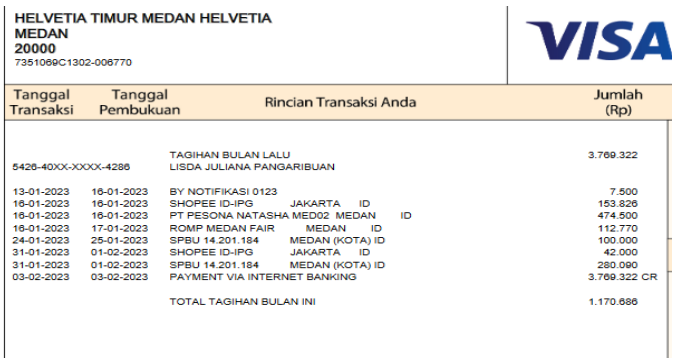
e. Algoritma Digital Signature [14]
a. Pihak1 (woman) memilih sebuah nilai r (r < q) dan menghitung: x = a^r mod p
b. Pihak1 (woman) menggabungkan (concatenate) M dan x dan menghitung nilai hash dari hasil penggabungan tersebut.
e = H(M, x) (7)
Hasil penggabungan M dengan x dimasukkan ke fungsi hash SHA-1[11]
c. Pihak1 (woman) menghitung: y = (r + se) mod q
d. Digital signature adalah e dan y. Pihak1 (woman) mengirimkan tanda tangan bersama pesan.
e. Pihak2 (man) menghitung: x' = ((a^y).(v^e)) mod p (8)
f. Pihak2 (man) menggabungkan (concatenate) M dan x' dan melakukan verifikasi dengan rumus: e = H(M,x')(9)

f. **Algoritma Rabin Miller**.
Untuk mengetahui apakah bilangan yang dipilih pada algoritma Pembentukan kunci itu bilangan prima atau bukan digunakan algoritma Rabin Miller. Adapun algoritma Rabin Miller tersebuat adalah : [20] [21]
a. Input : n (n adalah angka prima yang akan di uji)
b. Misalkan $n - 1 = 2^s d$ dimana $d \in N$ dan $s \in N$. Pilih bilangan bulat acak a dengan $2 \leq a \leq n - 2$
c. Hitung : $X \equiv a^d \pmod n$
Jika $X \equiv \pm 1 \pmod n$ maka tampilkan pesan " n adalah Prima".
Jika s=1 maka tampilkan pesan " n bukan bilangan prima".
Jika tidak, tetapkan r=1 dan lanjutkan ke langkah 4)
d. Hitung : $X \equiv a^{2r\,d} \pmod n$
Jika $x \equiv 1 \pmod n$ maka tampilkan pesan " n bukan prima".
Jika $x \equiv -1 \pmod n$ maka tampilkan pesan "n adalah prima".
Jika tidak, atur r = r+1 dan lanjutkan ke langkah 5)
e. Jika r = s-1, lanjutkan ke langkah 6), jika tidak, lanjutkan ke langkah 4)
f. Hitung : $X \equiv a^{2s-1} d \pmod n$
Jika $x \neq -1 \pmod n$ maka "n bukan prima " dan Jika $x \equiv -1 \pmod n$ maka "n adalah prima".

g. **Algoritma SHA-1** [13]
a. Buat dua *buffer* dan masing-masing *buffer* terdiri dari lima kata sebesar 32 bit kata pertama yaitu A, B, C, D, E sedangkan kata kedua adalah H0, H1, H2, H3, dan H4. 80 kata berikutnya adalah W0, W1, ..., W79 yang memakai sebuah variabel sementara yaitu TEMP.
b. Input pesan, M lalu buat pesan ke dalam N 512 bit blok yaitu M(1), M(2), ..., M(n) dengan cara : 32 bit pertama dari blok pesan ditunjukkan ke M0 (i) , lalu 32 bit berikutnya adalah M1 (i) dan selanjutnya berlaku hingga M15 (i)
c. Inisialisasi Nilai Hash (dalam bentuk hex) :
d. H0 = 67452301 ; H3 = 10325476 ; H1 = EFCDAB89 ; H4 = C3D2E1F0
e. Lakukan proses M1, M2, ..., Mn dengan membagi Mi ke dalam 16 kata W0, W1, ..., W15 dimana W0 merupakan left most.
f. Hitung : For t = 16 to 79
Wt = S1 (Wt-3 xor Wt-8 xor Wt-14 xor Wt-16)
g. Inisialisasi 5 variabel A, B, C, D, E dengan nilai Hash : A = H0 ; B = H1; C = H2; D = H3; E = H4
h. Hitung : For t = 0 to 79
TEMP = S5 (A) + ft(B,C,D) + E + Wt + Kt ; E = D; D = C; C = S30(B); B = A; A = TEMP
i. Hitung Nilai Hash : H0 = H0 + A ; H1 = H1 + B ; H2 = H2 + C; H3 = H3 + D ; H4 = H4 + D ;
Hasil dari pencerna pesan sebesar 160 bit dari pesan, M adalah : H0 H1 H2 H3 H4

3. HASIL DAN PEMBAHASAN

Autektikasi Dokumen dan Digital Signature.pada penelitian ini dilakukan dengan beberapa kali pengujian terhadap beberapa dokumen yang berbeda. Dalam penelitian ini objek yang dilakukan sebagai uji coba adalah dokumen attachment yang dikrim lewat email namun isi dokumen yang digunakan hanyalah dokumen email yang berisi teks. Untuk menjamin keasliannya dokumen yang dikirim dibubuhi tanda tangan digital. Adapun dokumen tersebut dapat dilihat pada Gambar 1.



HELVETIA TIMUR MEDAN HELVETIA
MEDAN
20000
7351069C1302-006770

VISA

Tanggal Transaksi	Tanggal Pembukuan	Rincian Transaksi Anda	Jumlah (Rp)
		TAGIHAN BULAN LALU	3.769.322
5426-40XX-XXXX-4286		LISDA JULIANA PANGARIBUAN	
13-01-2023	16-01-2023	BY NOTIFIKASI 0123	7.500
16-01-2023	16-01-2023	SHOPEE ID-IPG JAKARTA ID	153.826
16-01-2023	16-01-2023	PT PESONA NATASHA MED02 MEDAN ID	474.500
16-01-2023	17-01-2023	ROMP MEDAN FAIR MEDAN ID	112.770
24-01-2023	25-01-2023	SPBU 14.201.184 MEDAN (KOTA) ID	100.000
31-01-2023	01-02-2023	SHOPEE ID-IPG JAKARTA ID	42.000
31-01-2023	01-02-2023	SPBU 14.201.184 MEDAN (KOTA) ID	280.090
03-02-2023	03-02-2023	PAYMENT VIA INTERNET BANKING	3.769.322 CR
		TOTAL TAGIHAN BULAN INI	1.170.686

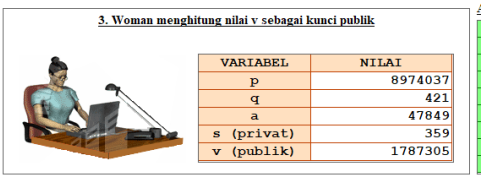
Gambar1 . Dokumen pada Email

Tahap pengujian pertama sekali yang dilakukan Proses Pembentukan kunci dimana kunci yang dihasilkan adalah kunci privat dan kunci publik. Kunci privat diselesaikan dengan algoritma Fast Exponentiation, sedangkan untuk mengetahui kunci publik diselesaikan dengan Extended Euclidean. Kunci dibentuk dengan memilih 2 buah bilangan prima, untuk mengetahui bilangan acak yang dipilih adalah prima digunakan algoritma Rabin Miller. Kedua bilangan prima yang dipilih harus memiliki sebuah faktor prima yang sama dan untuk mengetahui bilangan prima tersebut memiliki faktor prima yang sama digunakan Algoritma Greatest Common Divisor (GCD).

Setelah kunci privat dan kunci publik dibentuk maka dilakukan proses otentikasi. Pada proses ini akan diverifikasi keaslian (otentikasi) salah satu pihak dalam saluran komunikasi. Jika verifikasi *TRUE*, maka dokumen dikirim dan diterima oleh pihak yang benar. Langkah terakhir adalah proses *Digital Signature*, dimana pihak 1 mengirim dokumen yang telah dibubuhi tanda tangan dan hasilnya menjadi *Message Digest* . Untuk verifikasi tanda tangan digital tersebut digunakan fungsi hash SHA-1. Jika nilai penggabungan variabel dan informasi sama dengan nilai hash maka tanda tangan digital tersebut autentik.

3.1 Proses Pembentukan Kunci

Pada proses ini pihak 1 menentukan bilangan prima p,q dan nilai a. Pada pengujian nilai prima p = 8974037 dan q = 421 maka nilai a = 47849. , sedangkan nilai s (kunci private) = 359 maka nilai v (kunci publik) = 1787305. Kunci privat dipegang oleh pihak1 (woman), sedangkan kunci publik diberikan kepada pihak2 (man). Pada sistem hasil pembentukan kunci dapat dilihat pada Gambar 2.



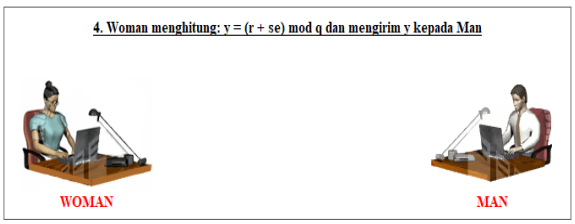
3. Woman menghitung nilai v sebagai kunci publik

VARIABEL	NILAI
p	8974037
q	421
a	47849
s (privat)	359
v (publik)	1787305

Gambar 2. Hasil Pembentukan Kunci

3.2 Proses Otentikasi

Pada proses otentikasi, diperoleh nilai r,x dan e. Adapun nilai r = 317 dan nilai x= 1892924 yang dikirimkan pihak1 (woman) kepada pihak2 (man), lalu pihak2 (man) memperoleh nilai e= 50101314 yang kemudian akan diberikan kepada pihak1 (woman), sehingga menghasilkan nilai y= 410 yang akan dikirim kembali ke pihak2 (man). Adapaun hasil otentikasi pada sistem dapat dilihat pada Gambar 3.



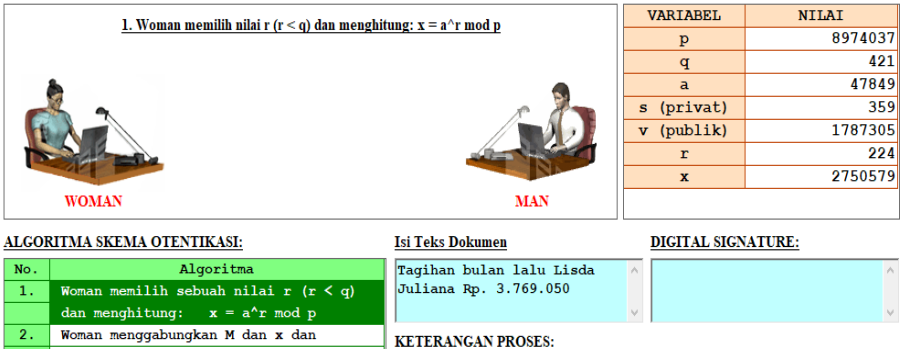
VARIABEL	NILAI
q	421
a	47849
s (privat)	359
v (publik)	1787305
r	317
x	1892924
e	50101314
y	410

Gambar 3. Hasil Otentikasi

Dari nilai yang peroleh, Man melakukan verifikasi dengan rumus (6) sehingga hasil x = (47849^410 mod 8974037) = 1892924 (TRUE). Hasil perhitungan operasi (((a^y).(v^e)) mod p) sama dengan nilai x. Proses otentikasi berhasil. Hal ini menunjukkan bahwa dokumen diterima dari orang yang benar.

3.3 Proses Digital Signature

Kutipan isi dokumen yang dikirim melalui email pada Gambar1 berupa teks yang digunakan sebagai uji coba adalah : "Tagihan bulan lalu Lisda Juliana Rp. 3.769.050". Hasil perhitungan fungsi hash dapat dilihat pada Gambar 4.



Gambar 4. Isi Dokumen Dan Perhitungan Fungsi Hash

Pihak1(woman) menginput nilai r= 224, maka diperoleh nilai x= 2750579, kemudian Woman menggabungkan M dan x dan menghitung nilai hash: e = H(M, x) , maka diperoleh:

e(1) = H(842750579) = 57564948 ; e(2) = H(972750579) = 49675567

e(3) = H(1032750579) = 53526669 ; e(4) = H(1052750579) = 56706557

e(5) = H(1042750579) = 50705069 ; e(6) = H(972750579) = 49675567

e(7) = H(1102750579) = 68525252 ; e(8) = H(322750579) = 50515048

e(9) = H(982750579) = 68664852 ; e(10) = H(1172750579) = 55545548

e(11) = H(1082750579) = 69504965 ; e(12) = H(972750579) = 49675567

e(13) = H(1102750579) = 68525252 ; e(14) = H(322750579) = 50515048

e(15) = H(1082750579) = 69504965 ; e(16) = H(972750579) = 49675567

e(17) = H(1082750579) = 69504965 ; e(18) = H(1172750579) = 55545548

e(19) = H(322750579) = 50515048 ; e(20) = H(762750579) = 66496554

e(21) = H(1052750579) = 56706557 ; e(22) = H(1152750579) = 49555153

e(23) = H(1002750579) = 50564955 ; e(24) = H(972750579) = 49675567

e(25) = H(322750579) = 50515048 ' e(26) = H(742750579) = 54546953

e(27) = H(1172750579) = 55545548 ; e(28) = H(1082750579) = 69504965

e(29) = H(1052750579) = 56706557 ; e(30) = H(972750579) = 49675567

e(31) = H(1102750579) = 68525252 ; e(32) = H(972750579) = 49675567

e(33) = H(322750579) = 50515048 ; e(34) = H(822750579) = 56525269

e(35) = H(1122750579) = 48545549 ; e(36) = H(462750579) = 69505770

e(37) = H(512750579) = 50684950 ; e(38) = H(462750579) = 69505770

e(39) = H(552750579) = 52556568 ; e(40) = H(542750579) = 67696650

e(41) = H(572750579) = 68496970 ; e(42) = H(462750579) = 69505770

e(43) = H(482750579) = 48484948 ; e(44) = H(532750579) = 67545051

e(45) = H(482750579) = 48484948 ; e(46) = H(462750579) = 69505770

Woman menghitung nilai y dengan rumus (5) maka diperoleh hasil :

y(1) = 106 ; y(2) = 352 ; y(3) = 73 ; y(4) = 54 ; y(5) = 301 ; y(6) = 352 ; y(7) = 305

y(8) = 339 ; y(9) = 23 ; y(10) = 32 ; y(11) = 400 ; y(12) = 352 ; y(13) = 305 ; y(14) = 339

y(15) = 400 ; y(16) = 352 ; y(17) = 400 ; y(18) = 32 ; y(19) = 339 ; y(20) = 358 ; y(21) = 54

y(22) = 6 ; y(23) = 34 ; y(24) = 352 ; y(25) = 339 ; y(26) = 241 ; y(27) = 32 ; y(28) = 400

y(29) = 54 ; y(30) =352 ; y(31) = 305 ; y(32) = 352 ; y(33) = 339 ; y(34) = 52 ; y(35) = 332

y(36) = 168 ; y(37) = 256 ; y(38) = 168 ; y(39) = 170 ; y(40) = 262 ; y(41) = 324 ; y(42) = 168

y(43) = 169 ; y(44) = 154 ; y(45) = 169 ; y(46) = 168

Digital Signature adalah e dan y, maka *Message Digest* yang dikirim pihak1 (woman) kepada pihak2 (man) adalah:

|57564948,106|49675567,352|53526669,73|56706557,54|50705069,301|49675567,352|68525252,305|50515048,339|68664852,23|55545548,32|69504965,400|49675567,352|68525252,305|50515048,339|69504965,400|49675567,352|69504965,400|55545548,32|50515048,339|66496554,358|56706557,54|49555153,6|50564955,34|49675567,352|50515048,339|54546953,241|55545548,32|69504965,400|56706557,54|49675567,352|68525252,305|49675567,352|50515048,339|56525269,52|48545549,332|69505770,168|50684950,256|69505770,168|52556568,170|67696650,262|68496970,324|69505770,168|48484948,169|67545051,154|48484948,169|69505770,168

3.4 Proses verifikasi Digital Signature

Man melakukan perhitungan verifikasi menggunakan rumus (8) diperoleh hasil : x'(1) = 2750579. Kemudian Man menggabungkan M dan x' dan melakukan verifikasi menggunakan rumus (9). Hasil verifikasi dapat dilihat pada Tabel1.

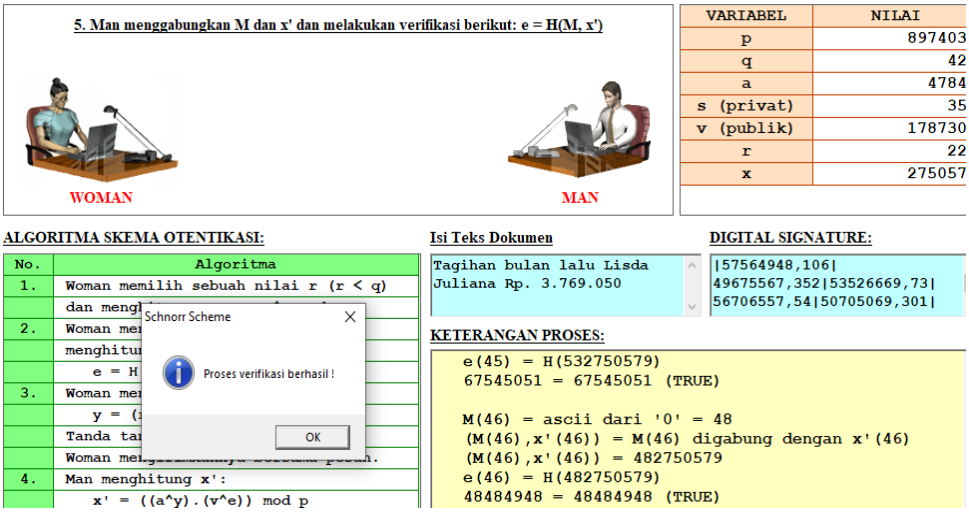
Tabel 1. Hasil verifikasi Digital Sigature

Index	(M,x')	Nilai Hash (H)	e	Keterangan
1	842750579	57564948	57564948	TRUE
2	972750579	49675567	49675567	TRUE
3	1032750579	53526669	53526669	TRUE
4	1052750579	56706557	56706557	TRUE
5	1042750579	50705069	50705069	TRUE
6	972750579	49675567	49675567	TRUE
7	1102750579	68525252	68525252	TRUE
8	322750579	50515048	50515048	TRUE
9	982750579	68664852	68664852	TRUE
10	172750579	55545548	55545548	TRUE
11	1082750579	69504965	69504965	TRUE
12	972750579	49675567	49675567	TRUE
13	1102750579	68525252	68525252	TRUE
14	322750579	50515048	50515048	TRUE
15	1082750579	69504965	69504965	TRUE
16	972750579	49675567	49675567	TRUE
17	1082750579	69504965	69504965	TRUE
18	1172750579	55545548	55545548	TRUE
19	322750579	50515048	50515048	TRUE
20	762750579	66496554	66496554	TRUE
21	1052750579	56706557	56706557	TRUE
22	1152750579	49555153	49555153	TRUE
23	1002750579	50564955	50564955	TRUE
24	972750579	49675567	49675567	TRUE
25	322750579	50515048	50515048	TRUE
26	742750579	54546953	54546953	TRUE
27	1172750579	55545548	55545548	TRUE
28	1082750579	69504965	69504965	TRUE
29	1052750579	56706557	56706557	TRUE
30	972750579	49675567	49675567	TRUE
31	1102750579	68525252	68525252	TRUE
32	972750579	49675567	49675567	TRUE
33	322750579	50515048	50515048	TRUE
34	822750579	56525269	56525269	TRUE
35	1122750579	48545549	48545549	TRUE
36	462750579	69505770	69505770	TRUE
37	512750579	50684950	50684950	TRUE
38	462750579	69505770	69505770	TRUE

39	552750579	52556568	52556568	TRUE
40	542750579	67696650	67696650	TRUE
41	572750579	68496970	68496970	TRUE
42	462750579	69505770	69505770	TRUE
43	482750579	48484948	48484948	TRUE
44	532750579	67545051	67545051	TRUE
45	482750579	48484948	48484948	TRUE
46	462750579	69505770	69505770	TRUE

Dari Tabel1 dapat dilihat bahwa hasil perhitungan operasi H(M, x') sama dengan nilai e maka proses verifikasi Digital Signature TRUE atau berhasil diverifikasi. Itu artinya bahwa tanda tangan dan informasi pada dokumen asli dan belum mengalami perubahan.

Selanjutnya proses pembentukan digital signature hingga verifikasi dapat dilihat pada Gambar5. Dari gambar5 dapat diketahui bahwa semua karakter isi dokumen pada email yang dikirim berhasil diverifikasi.



Gambar 5. Proses verifikasi Digital Signature

Dengan cara yang sama dilakukan beberapa kali percobaan dan hasil pengujian yang diperoleh yang dapat dilihat pada Tabel2. dan Tabel 3. Dari Tabel2 diketahui bahwa bilangan prima yang berbeda akan menghasilkan kunci privat dan kunci publik yang berbeda. Pada proses otentikasi dapat dilihat bahwa semua nilai x= (a^y).(v^e)) mod p). Hal itu berarti dari 5 uji coba pembentuk kunci yang dilakukan, semua proses dapat diverifikasi dengan baik. Maka pihak yang berkomunikasi atau yang mengirim dan menerima dokumen adalah orang yang tepat.

Tabel 2. Hasil Pengujian Proses Pembentukan Kunci dan Proses Otentikasi Schnorr

NO	Proses Pembentukan kunci					Proses Otentikasi				
	p	q	a	s (kunci private)	v (kunci publik)	r	X	e	y	(a^y).(v^e)) mod p)
1	8974037	421	47849	359	1787305	317	**1892924**	50101314	410	**1892924**
2	796759	97	68457	24	33091	64	**745650**	56309102	41	**745650**
3	203051	31	81242	19	193986	18	**169961**	18971024	12	**169961**
4	691871	43	61783	37	55814	31	**5116**	421171	29	**5116**
5	691871	43	61783	37	55814	31	**5116**	421171	29	**5116**

Dari Tabel2 dapat diketahui bahwa isi dokumen yang sama pada email apabila nilai variabel bilangan prima yang diinput berbeda akan menghasilkan Message Digest yang berbeda sehingga para kriptanalis sulit memecahkannya. Perbedaan hasil Message Digest terjadi karena perbedaan bilangan prima yang di input menyebabkan perbedaan kunci privat dan kunci publik yang dibentuk. Hasil Pengujian Digital Signature beberapa teks dapat dilihat pada Tabel 3.
Tabel3 juga menunjukkan bahwa semua hasil uji dari isi dokumen dengan kunci yang berbeda, dapat diveryfikasi dengan benar. Hal ini dapat dilihat dari semua nilai e=H(Mx') atau hasil penggabungan M dan x' sama dengan nilai hash SHA-1. Dengan demikian Digital Signature yang dihasilkan berupa Message Digest ini menunjukkan bahwa informasi dan tanda tangan digital yang dikirim benar-benar asli .

Dari Tabel 3 dapat dilihat bahwa perubahan dengan pergantian, dan pemindahan yang terdiri dari satu karakter saja akan menghasilkan perubahan Digital Signature yang sangat signifikan. Dengan kata lain keamanan dokument attachment yang dikirim melalui email terjamin keamanannya.

Tabel3. Hasil Pengujian Digital Signature Metode Schnorr

r	X	Isi Dokumen	MESSAGE DIGEST	e	H (Mx')
224	2750579	Tagihan bulan lalu Lisda Juliana Rp. 3.769.050.	|57564948,106|49675567,352|53526669,73|56706557,54|50705069,301|49675567,352|68525252,305|50515048,339|68664852,23|55545548,32|69504965,400|49675567,352|68525252,305|50515048,339|69504965,400|49675567,352|69504965,400|55545548,32|50515048,339|66496554,358|56706557,54|49555153,6|50564955,34|49675567,352|50515048,339|54546953,241|55545548,32|69504965,400|56706557,54|49675567,352|68525252,305|49675567,352|50515048,339|56525269,52|48545549,332|69505770,168|50684950,256|69505770,168|52556568,170|67696650,262|68496970,324 |69505770,168 |48484948,169 |67545051,154 |48484948,169 |69505770,168	69505770	69505770
46	65516	BY NOTIFIKASI 0123	|69695453,26 |56675249,48 |53504949,36 |65707070,83 |65665257,36 |52506651,78 |70495349,66 |55656849,23 |70495349,66 |67515049,84 |54706752,67 |67546652,16 |70495349,66 |53504949,36 |55666965,16 |68695055,11 |56515566,29 |68514852,78 |69544968,1 |67656654,9 |49516955,8 |48695768,3 |54495366,13 |48516567,7	68514852	68514852
25	94469	BY NOTIFIKASI 0123	|69555169,8|65516949,6|69555169,8|70555267,17 |49536766,15 |65706757,4 |69555169,8 |49516955,8 |69655050,20 |65545265,5 |51525750,6 |52535367,22 |51535654,14 |52675656,12 |53666856,13	52535367	52535367
35	99997	PAYMENT VIA INTERNET BANKING 3.769.322	||69665448,27|53514870,28|49536667,32 |66486655,6 |65565357,15 |50695753,35 |51574856,12 |52675656,12|65565357,15|51574856,12 |49536667,32 |66486655,6|53514870,28|50705648,5|49536667,32|53514870,28|66486655,6|65565357,15|66655555,30|52675656,12|49536667,32|54555553,3|51574856,12|49536667,32|67546748,8 |65565357,15 |48545150,41 |49676868,35 |67517049,10 |66505056,24 |67565569,0 |49676868,35 |48545150,41 |65695469,8 |65695469,8	65695469	65695469
35	99997	PAYMENT VIA INTERNET BANKING 2.769.322	|51535654,14|52675656,12|53666856,13|69665448,27 |53514870,28 |49536667,32 |66486655,6 |65565357,15 |50695753,35 |51574856,12 |52675656,12|65565357,15 |51574856,12 |49536667,32 |66486655,6 |53514870,28 |50705648,5|49536667,32|53514870,28|66486655,6|65565357,15|66655555,30|52675656,12|49536667,32|54555553,3|51574856,12|49536667,32|67546748,8|65565357,15|65695469,8 |49676868,35 |67517049,10 |66505056,24 |67565569,0 |49676868,35 |48545150,41 |65695469,8 |65695469,8	65695469	65695469

4. KESIMPULAN

Peneltian ini menggunakan informasi berupa teks pada dokumen yang dikirim via email. Dari hasil pengujian yang dilakukan menggunakan Metode schnorr dapat disimpulkan bahwa isi dokumen yang sama pada email apabila nilai variabel bilangan prima yang berbeda akan menghasilkan *Message Digest* yang berbeda sehingga para kriptanalis sulit

memecahkannya karena hanya pemegang kunci privat dan kunci publik yang dapat memperoleh dokumen aslinya. Perbedaan hasil *Message Digest* terjadi karena perbedaan bilangan prima yang di input menyebabkan perbedaan kunci privat dan kunci publik yang dibentuk. Dari hasil uji dari isi dokumen dengan pasangan kunci privat dan kunci publik kunci yang sinkron, dapat diverifikasi dengan benar. Dengan demikian *Digital Signature* yang dihasilkan berupa *Message Digest* ini menunjukkan bahwa informasi dan tanda tangan digital yang dikirim benar-benar asli. Hasil percobaan juga menunjukkan bahwa perubahan dengan pergantian, dan pemindahan satu karakter saja dari isi dokumen yang dikirim akan menghasilkan perubahan digital signature yang sangat signifikan. Jika ada yang mengubah isi dokumen maupun kunci akan membuat hasil dari proses verifikasi tidak benar, maka penerima dokumen dapat mengetahui bahwa dokumen yang diterimanya sudah tidak asli dan tidak dapat dipercaya. Dari hasil pengujian diketahui dokumen attachment yang dikirim melalui email menggunakan Digital Signature dengan Metode *Schnorr* merupakan strategi yang dapat memberikan keamanan dokumen *attachment* pada e-mail yang lebih baik daripada keamanan yang diterapkan e-mail standar seperti PGP.

REFERENCES

[1] A. Supriyanto, "Pemakaian Kriptografi Kunci Publik Untuk Proses Enkripsi Dan Tandatangan Digital Pada Dokumen E-Mail," *Din. Inform.*, no. 1, 2009.

[2] L. J. Pangaribuan and D. Sitanggang, "KEAMANAN PESAN WHATSAPP MENGGUNAKAN KRIPTOGRAFI ALGORITMA GOVERNMENT STANDARD (GOST)," vol. 2, no. 1, pp. 210–217, 2022.

[3] L. J. Pangaribuan, "KRIPTOGRAFI MODERN KUNCI ASIMETRIS DENGAN METODE RSA UNTUK KEAMANAN PESAN DALAM E-MAIL," in *Konferensi Nasional Pengembangan Teknologi Informasi dan Komunikasi (KETIK)*, 2014, pp. 153–159.

[4] M. S. Ramadhan and F. P. Ariyani, "Peningkatan Keamanan Login Website Dengan Implementasi One Time Password Menggunakan Algoritma Sha1 Dan Md5 Berbasis Mobile," *Skanika*, vol. 1, no. 2, pp. 689–696, 2018.

[5] L. Juliana Pangaribuan and F. Haris Simbolon, "KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer) KRIPTOGRAFI HYBRIDA MENGGUNAKAN ALGORITMA HILL CIPHER DAN ALGORITMA RSA UNTUK KEAMANAN PENGIRIMAN INFORMASI PADA EMAIL," in *KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer)*, 2017. [Online]. Available: http://ejurnal.stmik-budidarma.ac.id/index.php/komik

[6] L. J. Pangaribuan, "Kriptografi Hybrida Agloritma Hill Cipher Dan Rivest Shamir Adleman (RSA) Sebagai Pengembangan Kriptografi Kunci Simetris (Studi Kasus : Nilai Mahasiswa Amik Mbp)," *J. Teknol. Inf. Dan Komun.*, vol. 7, no. 1, pp. 11–26, 2018.

[7] L. J. Pangaribuan, "IMPLEMENTASI KRIPTOGRAFI MENGGUNAKAN METODE HILL CIPHER," in *Seminar Nasional Inovasi dan Teknologi Informasi (SNITI)*, 2014, vol. 1, pp. 10–11.

[8] Y. Anshori, A. Y. Erwin Dodu, and D. M. P. Wedananta, "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.

[9] Y. Fitriyah, "Analisis Tingkat Kesiapan implmentasi Tanda Tangan Digital Untuk Autentikasi Dokumen Rekam Medis ELektronik di Instalasi Rawat Jalan RSUD Kota Yogyakarta," *J. Inf. Syst. Public Heal.*, vol. 7, no. 2, p. 53, 2022, doi: 10.22146/jisph.73666.

[10] Y. P. Dwi Puspitasari*, "Kriptografi Rivest Shamir Adleman (RSA) pada Tanda Tangan Digital," in *Prosiding Matematika*, 2020, pp. 14–20.

[11] A. B. Ronald Makaleo Tandiabang, Tomy Handaka Patria, "Otentikasi Dokumen Elektronik Menggunakan Tanda Tangan Digital," *Tanda Tangan Digit.*, p. 3, 2019.

[12] A. Lorien and T. Wellem, "Implementasi Sistem Otentikasi Dokumen Berbasis Quick Response (QR) Code dan Digital Signature," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 5, no. 4, pp. 663–671, 2021, doi: 10.29207/resti.v5i4.3316.

[13] I. Silaban, P. S. Ramadhan, and D. H. Pane, "Implementasi Algoritma Schnorr Untuk Tanda Tangan Digital Pada Surat Pendaftaran Online PKBM Hanuba Medan," *J-SISKO TECH (Jurnal Teknol. Sist. Inf. dan Sist. Komput. TGD)*, vol. 5, no. 1, p. 25, 2022, doi: 10.53513/jsk.v5i1.3827.

[14] H. F. Isnaini, K. Karyati, and J. P. Matematika, "Penerapan Skema Tanda Tangan Schnorr pada Pembuatan Tanda Tangan Digital Implementation of Schnorr Signature Scheme in The Form of Digital Signature," *Pythagoras J. Pendidik. Mat*, vol. 12, no. 1, pp. 57–64, 2017.

[15] E. Cahyo Prabowo and I. Afrianto, "Penerapan Digital Signature Dan Kriptografi PadaOtentikasi Sertifikat Tanah Digital - Teknik Informatika Universitas Komputer Indonesia," *J. Ilm. Komput. dan Inform.*, vol. 6, no. 2, 2017.

[16] T. Wang, L. Song, "An Improved Digital Signature Algorithm and Authentication Protocols in Cloud Platform. PROTOCOL," *IEEE Int. Conf. Smart Cloud, New York, NY, USA*, 2016.

[17] M. Mesran, M. Syahrizal, and R. Rahim, "Enhanced security for data transaction with public key Schnorr authentication and digital signature protocol," *ARPN J. Eng. Appl. Sci.*, vol. 13, no. 11, pp. 3839–3846, 2018.

[18] E. Wahyudi, M. M. Efendi, M. Subli, A. Subki, and M. R. Alfian, "Penerapan Digital Signature Scheme Dengan Metode Schnorr Authentication," *Explore*, vol. 10, no. 1, p. 23, 2020, doi: 10.35200/explore.v10i1.360.

[19] R. A. Saputra and A. S. Purnomo, "Implementasi Algoritma Schnorr Untuk Tanda Tangan Digital," *JMAI (Jurnal Multimed. Artif. Intell.*, vol. 2, no. 1, pp. 21–26, 2018, doi: 10.26486/jmai.v2i1.69.

[20] R. Pavuluru, "Miller-Rabin," 2015.

[21] Z. WANG, "Methods of Primality Testing," *MIT Undergrad. J. Math.*, vol. 1, no. January, pp. 133–142, 2021, [Online]. Available: https://www.researchgate.net/profile/Zixing-Wang-5