Jurnal CyberTech

Vol.4. No.4, April 2021, pp. xx~xx
P-ISSN : 9800-3456
E-ISSN : 2675-9802

Implementasi Algoritma Schnorr Untuk Tanda Tangan Digital Pada Surat Pendaftaran Online PKBM Hanuba Medan

Indriyani Silaban*, Puji Sari Ramadhan, Deski Helsa Pane****

* Sistem Informasi, STMIK Triguna Dharma Medan
** Sistem Informasi, STMIK Triguna Dharma Medan

Article Info

Article history:
Received Apr 12th, 2021
Revised Apr 20th, 2021
Accepted Apr 29th, 2021

Kata Kunci:
Tanda tangan digital
Schnorr
Sistem Pendaftaran Online
Otentikasi
SHA

ABSTRAK

Sistem Pendaftaran *Online* merupakan penerimaan peserta didik baru secara *online* yang bertujuan memberikan kesempatan yang seluas-luasnya kepada setiap warga negara agar memperoleh kemudahan dalam melakukan pendaftaran dimasa pandemi saat ini. Dengan adanya kemudahan tersebut, maka otentikasi dan integritas data merupakan hal yang sangat penting untuk menjaga kerahasiaan dan keamanan data pada file pendaftaran *online* dari pihak tidak bertanggung jawab guna memanfaatkan data untuk kepentingan pribadi. Pada permasalahan tersebut adapun cara untuk melakukan tindakan pencegahan yaitu dengan mengubah pesan menjadi sebuah kode dan kode tersebut diubah menjadi *QRCode*. Ilmu pengetahuan yang dapat diterapkan untuk menjaga otentikasi dan integritas data tetap dalam keadaan aman yaitu kriptografi pada tanda tangan digital. Hasil penelitian ini adalah sistem tanda tangan digital untuk memvalidasi keabsahan *file* pendaftaran *online* dengan penerapan metode Schnorr dan SHA-1. Pemanfaatan algoritma Schnorr dapat memberikan jaminan otentikasi pengirim dan SHA-1 akan melindungi pesan saat proses distribusi yaitu dengan menghitung nilai hash sehingga tanda tangan digital tidak mudah diretas.

Corresponding Author: *First Author
Indriyani Silaban
Sistem Informasi
STMIK Triguna Dharma
Email: Indrislbn@gmail.com

1. PENDAHULUAN

Saat ini berbagai negara tengah dilanda wabah suatu penyakit yang disebabkan oleh virus corona atau *Corona Virus Diseases* (COVID-19). Melihat kasus COVID-19 yang terus meningkat maka pemerintah Indonesia menerapkan kebijakan *social distancing* (jarak sosial) dan *physical distancing* (jarak fisik) untuk mengurangi risiko penularan virus COVID-19[1]. Sehingga berimbas pada kegiatan belajar mengajar yang dilakukan secara *online* untuk semua jenjang pendidikan baik sekolah formal maupun non formal (Kemdikbud RI, 2020). Termasuk sekolah non formal Pusat Kegiatan Belajar Mengajar Hati Nurani Baru Medan.

Pusat Kegiatan Belajar Mengajar Hati Nurani Baru (PKBM Hanuba) Medan merupakan salah satu lembaga pendidikan non-formal atau yang biasa dikenal dengan sekolah kesetaraan yang menerapkan *physical distancing* dan *social distancing*. PKBM Hanuba sendiri sudah memiliki sistem registrasi *online* yang terintegrasi dengan media pembelajaran *online* dan memudahkan sekolah dalam penyampaian informasi

seputar sekolah. Ketika calon warga belajar yang ingin mendaftar mereka akan mengisi *form* pendaftaran *online* dan akan mendapat dokumen yang akan mereka simpan guna untuk mendaftar ulang kembali. Namun, dokumen yang diberikan belum memiliki sistem keamanan yang di mana sistem keamanan ini berguna bagi pihak sekolah agar tidak terjadi penyadapan atau pemberian dokumen palsu. Dalam Perkembangan teknologi yang begitu cepat, pemanfaatan jaringan internet meningkat pesat juga. Sehingga kejahatan dalam pemalsuan maupun penyadapan data tidak dapat di pungkiri. Oleh sebab itu, PKBM Hanuba Medan membutuhkan aplikasi yang dapat menjamin keaslian surat pendaftaran online ini yang di tanda tangani secara digital. Sehingga dapat memberikan keamanan terhadap tindakan modifikasi maupun pemalsuan surat pendaftaran *online*. Salah satu seni pengamanan yang dapat dilakukan dalam mengamankan surat pendaftaran *online* tersebut adalah dengan kriptografi.

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikan pesan ke dalam bentuk yang tidak dapat dipahami lagi maknanya. Salah satu seni kriptografi yang dapat digunakan dalam mengidentifikasi keabsahan sebuah dokumen adalah penerapan tanda tangan digital. Tanda tangan digital dapat menggunakan *cryptosystem* kunci publik, yaitu sebuah metode kriptografi yang menggunakan kunci algoritma asimetris, yaitu kunci publik dan kunci privat[2]. Salah satu metode asimetris yang dapat membentuk tanda tangan digital tersebut adalah metode Schnorr.

Metode Schnorr merupakan pengembangan dari metode El-Gamal sehingga sistem keamanan El-Gamal terdapat pada Schnorr. Pembuatan Tanda Tangan Schnorr dimulai dari pembentukan kunci, pembuatan tanda tangan dengan menambahkan nilai hash, serta proses verifikasinya[3]. Dengan penerapan tanda tangan digital menggunakan metode Schnorr diharapkan penelitian ini mampu membantu keamanan dalam proses pendaftaran online di sekolah non formal PKBM Hanuba Medan.

Berdasarkan latar belakang tersebut maka diangkatlah sebuah judul yaitu "IMPLEMENTASI ALGORITMA SCHNORR UNTUK TANDA TANGAN DIGITAL PADA SURAT PENDAFTARAN ONLINE PKBM HANUBA MEDAN".

2. METODE PENELITIAN

Metode yang digunakan adalah model *waterfall*. Metode *waterfall* merupakan suatu proses pengembangan perangkat lunak berurutan, yang kemajuannya dipandang sebagai terus mengalir ke bawah (seperti air terjun). Berikut ini adalah tahapan model *waterfall* untuk pendekatan alur sistem yang tersusun yaitu:

1. *Requirement* (Analisis Kebutuhan)
   Requirement (analisis kebutuhan) adalah proses awal dalam perancangan sebuah sistem. Langkah ini merupakan analisa kebutuhan sistem yang dilakukan dengan cara pengumpulan data sehingga menemukan masalah sebenarnya dan sistem apa yang dibutuhkan untuk menyelesaikan masalah tersebut.
2. *Design*
   Tahap selanjutnya adalah mendesain sistem yang dibagi beberapa elemen yaitu pemodelan menggunakan *flowchart system*, pemodelan menggunakan UML (*Unified Modelling Language*), desain *input*, dan desain *output*. Semua tahap desain dilakukan untuk dapat di implementasikan menjadi program dalam pemecahan masalah.
3. *Implementation* (Pengembangan Sistem)
   Proses ini melakukan pembangunan sistem dengan pengkodingan yang sesuai dengan desain sistem yang telah dirancang baik dari sistem *input*, proses dan *output* menggunakan bahasa pemrograman berbasis *web*.
4. *Verification* (Pengujian Sistem)
   Pengujian sistem merupakan tahap dalam menguji sistem secara fungsional serta memastikan semua bagian dalam sistem sudah diuji. Tujuan dilakukannya pengujian ini adalah untuk mengurangi

kemungkinan terjadinya kesalahan (*error*) dan memastikan bahwa hasil sistem sesuai dengan apa yang diinginkan.

5. *Maintenance* (Pemeliharaan Sistem)
   Dalam pembuatan sebuah sistem, tidak menutup kemungkinan sistem mengalami perubahan ketika diberikan kepada user maupun karena adanya kesalahan sistem yang tidak terdeteksi saat dilakukan pengujian

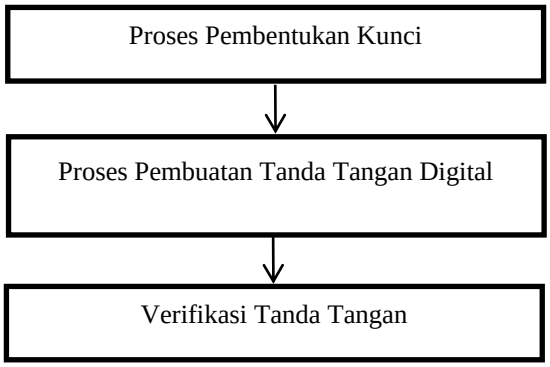
3. ANALISA DAN HASIL

Adapun dalam analisa ini menggunakan kombinasi dari dua metode diantaranya yaitu Skema Tanda Tangan Schnorr dan SHA-1. Pemanfaatan algoritma Schnorr dapat memberikan jaminan otentikasi pengirim dan SHA-1 akan melindungi pesan saat proses distribusi yaitu dengan menghitung nilai hash sehingga tanda tangan digital tidak mudah diretas.

3.1. Skema Tanda Tangan Schnorr

Skema tanda tangan Schnorr (*Schnorr Signature Scheme*) pertama kali diperkenalkan oleh Claus Schnorr pada tahun 1989[3]. Skema tanda tangan ini merupakan variasi dari skema tanda tangan ElGamal dengan ukuran tanda tangan yang lebih kecil dibandingkan dengan skema tanda tangan ElGamal itu sendiri[4]. Skema tanda tangan Schnorr mengambil sekuritas dari permasalahan menghitung logaritma diskrit. Skema ini juga menggunakan bilangan prima dan perpangkatan modulo dalam proses pembentukan kuncinya. Keamanan skema tanda tangan ini berdasarkan pada keyakinan bahwa menemukan logaritma diskret pada yang diberikan itu sulit, sehingga terjamin keamanannya.

Algoritma pada skema tanda tangan Schnorr terdiri dari tiga proses yaitu, proses pembentukan kunci, proses pembuatan tanda tangan digital dengan menambahkan nilai hash, serta proses verifikasi. Secara umum, urutan proses pada skema tanda tangan Schnorr dapat digambarkan dengan bagan sebagaimana ditunjukkan pada gambar 1 berikut :



Gambar 1. Urutan Proses Skema Tanda Tangan Schnorr

3.2. Fungsi One-Way Hash SHA-1

Fungsi *hash* (*hash function* atau *hash algorithm*) adalah suatu cara untuk menghasilkan sebuah digital *"fingerprint"* kecil dari sembarang data. Fungsi ini mencampurkan data untuk menghasilkan *fingerprint* yang sering disebut sebagai nilai *hash* (*hash value*)[2]. *Secure Hash Algorithm* (SHA-1) ini dikembangkan oleh NIST (*National Institute of Standard and Technology*). SHA-1 dapat diterapkan dalam penggunaan Algoritma Tanda Tangan Digital (*Digital Signature Algorithm*). SHA-1 dikatakan aman karena proses SHA-1 dihitung secara infisibel untuk mencari pesan yang sesuai untuk menghasilkan pencerna pesan atau dapat juga digunakan untuk mencari dua pesan yang berbeda yang akan menghasilkan pencerna pesan yang sama. Menurut jenisnya SHA dapat dispesifikasikan menjadi 4 bagian. Berikut ini merupakan daftar-daftar properti dari keempat SHA yang ditunjukan pada Tabel 1 Berikut :

Tabel 1. Jenis-jenis SHA

Algorithm	Message Size (Bits)	Block Size (Bits)	Word Size (Bits)	Message Digest Size (Bits)	Security2 (Bits)
SHA-1	$< 2^{64}$	512	32	160	80
SHA-256	$< 2^{64}$	512	32	256	128
SHA-384	$< 2^{128}$	1024	64	384	192
SHA-512	$< 2^{128}$	1024	64	512	256

Algoritma SHA-1 Dapat diringkas sebagai berikut[3] :

1. Penghitungan menggunakan dua penyangga dimana masing-masing penyangga terdiri dari lima sebesar 32 bit kata dan urutan 80 juga sebesar 32 bit kata. Lima kata pertama pada penyangga kata diberi nama A, B, C, D, E sedangkan lima kata kedua diberi nama H_0, H_1, H_2, H_3, dan H_4. Kemudian pada 80 kata yang berurutan diberi nama W_0, W_1, …, W_{79} dan pada penghitungan ini juga memakai sebuah variabel sementara.
2. Lakukan pengisian pesan, M dan kemudian parsingkan pesan tersebut ke dalam N 512 bit blok pesan, $M_{(1)}$, $M_{(2)}$, …, $M_{(n)}$. Caranya : 32 bit pertama dari blok pesan ditunjukkan ke $M_0^{(i)}$, lalu 32 bit berikutnya adalah $M_1^{(i)}$ dan selanjutnya berlaku hingga $M_{15}^{(i)}$
3. Inisialisasi Nilai Hash (dalam bentuk hex) :
4. H0 = 67452301
   H3 = 10325476
   H1 = EFCDAB89
   H4 = C3D2E1F0
   H2 = 98BADCFE
5. Lakukan proses M_1, M_2, …, Mn dengan cara membagi Mi ke dalam 16 kata W_0, W_1, …, W_{15} dimana W_0 merupakan *left most*.
6. Hitung : *For* t = 16 to 79
   $Wt = S^1 (W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16})$
7. Inisialisasi 5 variabel A, B, C, D, dan E dengan nilai *Hash* :
   $A = H_0$; $B = H_1$; $C = H_2$; $D = H_3$; $E = H_4$
8. Hitung : For t = 0 to 79
   $TEMP = S^5 (A) + f_t(B,C,D) + E + Wt + Kt$
   $E = D$; $D = C$; $C = S^{30}(B)$; $B = A$; $A = TEMP$
9. Hitung Nilai *Hash* :
10. $H_0 = H_0 + A$; $H_1 = H_1 + B$;

Hasil dari pencerna pesan sebesar 160 bit dari pesan, M adalah : $H_0\ H_1\ H_2\ H_3\ H_4$

3.3 Penerapan Dengan Metode

Berikut data yang digunakan sebagai sampel dalam penelitian yaitu :

Tabel 2. Data Awal

Nomor Pendaftaran	001

Berikut ini adalah langkah-langkah penyelesaian berdasarkan data awal yang diperoleh, yaitu :

1. Pembentukan Kunci

Langkah yang harus dilakukan pada saat pembentukan kunci yaitu :

a. Memilih nilai p, q dan a.

P = 1292603
q = 571
a = 87367

b. Memilih nilai s (s < q).
s = 366 (s adalah kunci privat)

c. Menghitung nilai v dengan rumus :
v = a^(-s) mod p
v = 87367^(-366) mod 1291603
v = ((87367^(-1) mod 1291603)^366) mod 1291603
v = (1253269^366) mod 1291603
v = 1122071

2. Proses Tanda Tangan Digital

a. Memilih nilai t dan menghitung nilai x
t = 562
x = a^t mod p
x = 87367^562 mod 1291603
x = 470752

b. Menggabungkan M dan x lalu menghitung nilai *Hash* : e = H(M, x)

Hasil perhitungan nilai *Hash* terlihat pada Tabel 3 di bawah ini :

Tabel 3. Perhitungan Nilai Hash

M_i	ASCII	(M_i, x_i)	$e_i = H(M_i, x_i)$
0	48	48470752	56489951
0	48	48470752	56489951
1	49	49470752	50555469

c. Proses enkripsi dengan menghitung nilai y = (t + (s . e(1)) mod q

Hasil proses enkripsi terlihat pada Tabel 4. di bawah ini :

Tabel 4. Proses Enkripsi

$e_i = H(M_i, x_i)$	$y_i = (t + (s \cdot e_i(1)) \bmod q$
56489951	187
56489951	187
50555469	394

Sehingga tanda tangan digital yang dihasilkan adalah :
56489951,187 | 56489951,187 | 50555469,394

3. Proses Verifikasi

a. Menghitung nilai x' = ((a^y) . (v^e)) mod p

Hasil perhitungan nilai x' terlihat pada Tabel 5. di bawah :

Tabel 5. Proses Perhitungan nilai x'

$e_i = H(M_i, x_i)$	$y_i = (t + (s \cdot e_i(1)) \bmod q$	$x'_i = ((a^y) \cdot (v^e)) \bmod p$
56489951	187	470752
56489951	187	470752
50555469	394	470752

b. Menggabungkan M dengan x' dan melalukan verifikasi e = H(M, x')

Hasil proses verifikasi terlihat pada Tabel 6. dibawah ini :

Tabel 6. Proses Verifikasi

M_i	ASCII	(M, x')	H(M, x')	e = H(M, x')
0	48	48470752	56489951	True
0	48	48470752	56489951	True
1	49	49470752	50555469	True

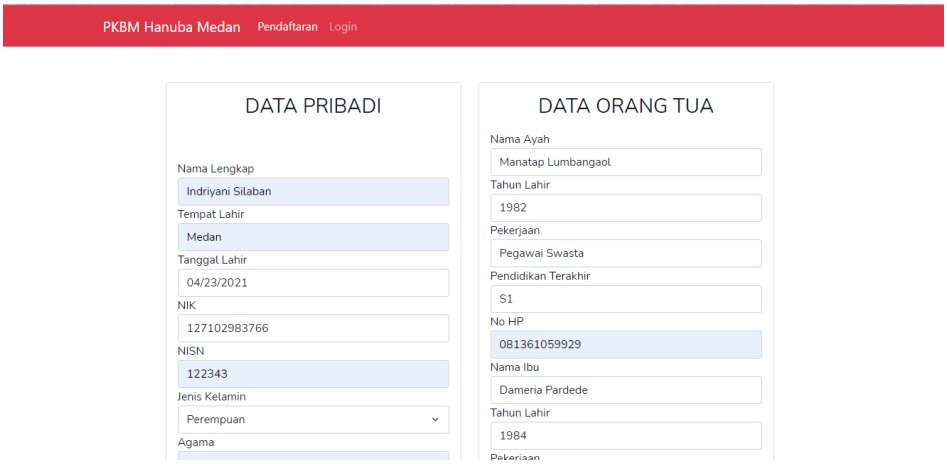
Hasil perhitungan H(M, x') sama dengan nilai e sehingga proses verifikasi tanda tangan berhasil.

3.4 Pengujian

Pada kasus ini akan dilihat bagaimana sistem dapat dijalankan sebagai mana fungsinya yaitu mengakses halaman menu utama, mengklik menu pendaftaran, melakukan pendaftaran dan sistem melakukan tanda tangan dokumen (enkripsi) serta admin memverifikasi dokumen (dekripsi). Pada tahap awal implementasi, pendaftar mengakses menu utama, selanjutnya mengakses menu pendaftaran dan melakukan pendaftaran pada halaman pendaftaran. Adapun tahap ini dapat dilihat pada gambar 2. berikut :

Gambar 2. Akses Halaman Utama

Selanjutnya, pendaftar mengakses halaman pendaftaran untuk mengisi *form* pendaftaran serta melakukan pendaftaran. Adapun tahap ini dapat dilihat pada gambar 3. berikut :



Gambar 3. Akses Pendaftaran

Jika selesai mengisi *form* pendaftaran maka pendaftar akan mendapatkan *file* pendaftaran berupa PDF yang memiliki tanda tangan digital berupa *QRcode.* Berikut *file* pendaftaran yang berisi *QRcode* :

Pusat Kegiatan Belajar Masyarakat
Hati Nurani Baru
P K B M H A N U B A
Pusat Pemberdayaan Masyarakat Putus Sekolah untuk dapat mengikuti Paket belajar A, B & C
Badan Hukum: No. 80, Tanggal 29 Juli 2013, Dana Barus, SH. SpN
Kantor Pusat : Jl. A.H. Nasution Gg.Jadi I No.18B Simp.Pos - Medan (061) 8363308 e-mail: pkbmhanuba@yanur.net

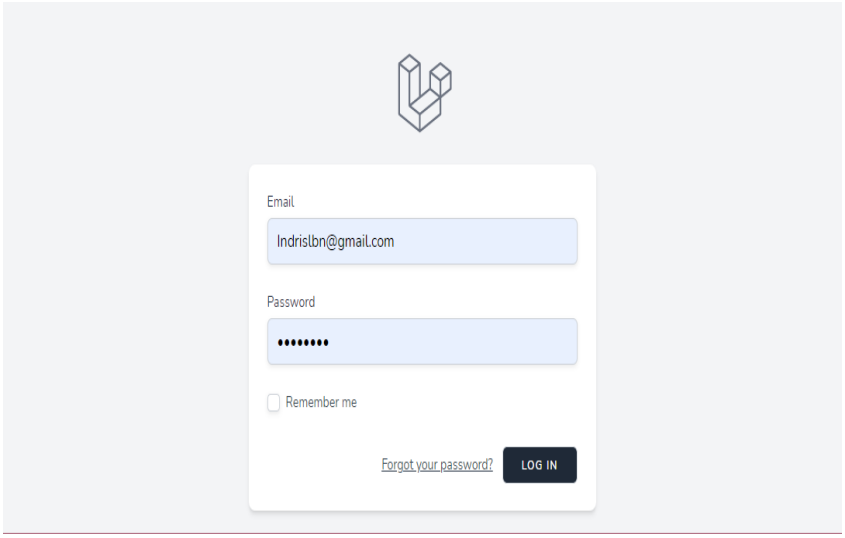
Bukti Pendaftaran Siswa Baru PKBM Hanuba Medan

Nama : Indriyani Silaban

Program : B

Gambar 4. *File* Pendaftaran

Langkah selanjutnya, pendaftar melakukan daftar ulang dengan membawa *file* pendaftaran dan menyerahkannya kepada admin. Sebelum admin melakukan verifikasi, admin harus terlebih dahulu melakukan *login*. Adapun tampilan halaman *login* dilihat pada gambar 5. berikut :



Gambar 5. Halaman *Login*

Selanjutnya untuk melakukan pemeriksaan keabsahan *file* pendaftaran *online* maka dilakukan proses verifikasi yang dilakukan oleh admin dengan cara mengscan *QRCode* yang ada pada *file* pendaftaran. Proses verifikasi ini dilakukan untuk mengetahui bahwa dokumen masih terjaga integritas nya atau tidak. Ketika dilakukan proses validasi *file* pendaftaran *online* maka sistem akan memvalidasi keabsahan dokumen dengan memberikan informasi "Formulir Pendaftaran Valid" dan admin dapat mengklik tombol validasi agar datanya sudah tervalidasi pada *database*. Adapun hasilnya sebagai berikut :

Gambar 6. Halaman Validasi *File* Pendaftaran

4. KESIMPULAN

Adapun kesimpulan dari penelitian ini yaitu sebagai berikut :

1. Berdasarkan pengujian proses pembangkitan sepasang kunci dilakukan secara sistematis dan dinamis tanpa dilakukan penginputan secara manual.
2. Berdasarkan pengujian sistem dapat melakukan proses membuat tanda tangan pada file pendaftaran online.
3. Berdasarkan pengujian sistem dapat melakukan verifikasi sehingga mampu mendeteksi keabsahan pada dokumen file pendaftaran online.
4. Berdasarkan pengujian sistem dapat diimplementasikan dengan menerapkan skema tanda tangan schnorr dan SHA-1.
5. Berdasarkan hasil penelitian sistem tanda tangan digital dapat membantu untuk mengatasi masalah yang terjadi pada PKBM Hanuba Medan.

UCAPAN TERIMA KASIH

Penulis mengucapkan terimakasih kepada program studi S1 Sistem Informasi STMIK Triguna Dharma yang telah memberikan dukungan dalam penyelesaian tulisan ini.

REFERENSI

[1] W. A. F. Dewi, “Dampak COVID-19 terhadap Implementasi Pembelajaran Daring di Sekolah Dasar,” Edukatif J. Ilmu Pendidik., vol. 2, no. 1, pp. 55–61, 2020, doi: 10.31004/edukatif.v2i1.89.

[2] U. A. Dony Ariyus, Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi. Penerbit Andi, 2008.

[3] 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,” vol. 12, no. 1, pp. 57–64, 2017.

[4] F. Arie Pratama, “Sistem Informasi Akuntansi Persediaan Bahan Baku menggunakan Metode First Expired First Out,” KOPERTIP J. Ilm. Manaj. Inform. dan Komput., vol. 2, no. 2, pp. 38–49, 2018, doi: 10.32485/kopertip.v2i2.37.

[5] 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.

[6] A. Shamir, “New directions in croptography,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 2162, p. 159, 2001, doi: 10.1007/3-540-44709-1_14.

BIBLIOGRAFI PENULIS

	**Indriyani Silaban** Lahir pada tahun 1998 di Medan, Sumatera Utara. Saat ini sedang menempuh studi Sistem Informasi di STMIK Triguna Dharma. Bekerja sebagai Academic Support di Sekolah Highscope Indonesia Medan. Tahun 2014 pernah menjabat sebagai pengurus di organisasi sekolah yaitu PA Nazareth SMA Negeri 2 Medan. Tahun 2017 pada organisasi kampus yaitu Ikatan Mahasiswa Kristen (IMK) dan saat ini aktif di organisasi PND (Pengurus Naposo Distrik X Medan Aceh dan sedang menjalankan kegiatan kreativitas untuk pemuda-pemudi HKBP Distrik X Medan menjabat sebagai sekretaris serta telah menyelesaikan Program Kreativitas Mahasiswa (PKM-T) bersama rekan lainya pada tahun 2020.
	**Puji Sari Ramadhan., S.Kom., M.Kom** Merupakan dosen Tetap STMIK Triguna Dharma yang aktif mengajar dan fokus pada bidang keilmuan kecerdasan buatan dan data sains. Telah menulis 1 buku dibidang Ilmu komputer. Memiliki sebanyak 2 Hak Kekayaan Intelektual (HKI). Menjabat sebagai Ketua Program studi Sistem Informasi. Dosen Terbaik Tahun 2018 serta pemenang PDP 2018 dan 2019.
	**Deski Helsa Pane., S.Kom., M.Kom** Lahir pada tahun 1993 di Bagansiapiapi. Menyelesaikan pendidikan Strata 1 di STMIK Triguna Dharma, Strata 2 di Universitas Putra Indonesia "YPTK" Padang. Saat ini merupakan Dosen tetap di STMIK Triguna Dharma Medan. Pada tahun 2011 berhasil memenangkan juara II Lomba Debat pada bulan Bahasa di Universitas Riau. Pada tahun 2013 mendapat penghargaan sebagai Inovator Teknologi Multimedia pada MTq XIII Kab.Rokan Hilir. Pada tahun 2017 mendapatkan penghargaan Best Network Engineer dari PT CCSI. Pemenang PDP tahun 2020 dan 2021.