JURNAL SISTEM INFORMASI TGD
Volume 1, Nomor 6, November 2022, Hal 906-914
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

Penerapan Digital Signature Metode SHA dan DSA Pada Slip Gaji Pegawai

Afnita Eritza[1], Mukhlis Ramadhan[2], Hafizah[3]
[1,2,3] Sistem Informasi, STMIK Triguna Dharma
Email: [1]afnita3@gmail.com, [2]mukhlis_ramadhan@trigunadharma.ac.id, [3]hafizah22isnartiilyas@gmail.com
Email Penulis Korespondensi: afnita3@gmail.com

Abstrak
Proses pengolahan data dan penggajian Mis Al-Hasanah masih menggunakan cara yang manual. Pengolahan data gaji sehingga menimbulkan beberapa permasalahan diantaranya kesalahan dalam menghitung data, hilangnya data, dan membutuhkan banyak waktu. Penggunaan Kriptografi dan sistem Digital Signature adalah langkah yang tepat dalam mengelola keamanan dan memperbaiki metode manual menjadi metode digital. Penggunaan algoritma tanda tangan digital dapat digunakan untuk menandatangani dokumen digital. SHA (Secure Hash Algorithm) dan DSA (Digital Signature Algorithm) merupakan salah satu jenis kriptografi yang dapat diterapkan. Penerapan algoritma SHA akan melindungi pesan dengan melakukan proses hash dari rangkuman dokumen data gaji sehingga menghasilkan nilai hash yang berbeda-beda dalam setiap slip gaji. Sedangkan algoritma DSA memaksimalkan nilai hash untuk dilakukan pembentukan Digital Signature. Slip gaji yang dihasilkan merupakan kode Digital Signature dalam bentuk QR Code sehingga mencegah data dimanipulasi pihak yang tidak bertanggung jawab. Sistem kode Digital Signature menghasilkan angka yang berbeda-beda dalam setiap slip gaji.
Kata Kunci: Kriptografi, *Digital Signature*, SHA, DSA, *QR Code*

1. PENDAHULUAN

Proses pengolahan data untuk penggajian pada Mis Al-Hasanah masih menggunakan metode manual sehingga pada saat pengolahan data gaji sering kali menemukan beberapa permasalahan antara lain dokumen rusak atau dokumen hilang dan kesalahan perhitungan data, belum lagi permasalahan dalam melakukan pengolahan data untuk menghasilkan slip gaji serta laporan penggajian[1]. Masalah gaji atau imbalan kerja bagi karyawan ialah hal yang sensitif serta berpengaruh langsung pada produktivitas kerja. Penerapan sistem penggajian yang tepat dapat memberikan kepuasan bagi pekerja dan instansi, sehingga siklus penggajian di instansi sangat penting[2].

Dalam hal ini Mis Al-Hasanah sendiri membutuhkan sistem yang akan mempermudah pengelolaan gaji, dan dalam sistem tersebut mempunyai data yang hanya boleh diketahui pihak tertentu saja. Keamanan data merupakan salah satu hal yang paling perlu diperhatikan dalam menjaga kerahasiaan data penting. Diperlukan suatu teknik pengaman tambahan untuk menjaga keamanan informasi penting tersebut. Tanpa adanya teknik tambahan untuk menjaga kerahasiaan data, maka banyak pihak yang tak berhak dapat melakukan serangan, salah satunya merupakan pencurian data[3].

Algoritma kriptografi merupakan satu solusi yang bisa digunakan untuk menjaga kerahasiaan informasi data[4]. Algoritma ini digunakan untuk melindungi blok data, seperti melindungi suatu dokumen dari perubahan. *Digital signature* ialah salah satu algoritma untuk menjaga integritas suatu dokumen. Teknologi tanda tangan *digital* memanfaatkan sepasang kunci privat-publik yang didesain untuk keperluan seseorang.

Digital signature adalah salah satu teknik yang dapat digunakan untuk menjaga keaslian data, sehingga penerima dapat mengetahui bahwa data yang diterima asli atau data palsu[5].

Penelitian ini diharapkan dapat menentukan keabsahan tanda tangan digital. Untuk memberikan metode perlindungan maksimum terhadap keabsahan *Digital signature*, pada penelitian ini metode kriptografi menggunakan algoritma SHA-1 dan DSA. Dengan dibangunnya aplikasi ini bisa memudahkan Mis Al-Hasanah dalam mengelola data gaji serta mempercepat proses penggajian.

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Tahapan penelitian merupakan proses dimana sebuah penelitian dapat terstuktur secara logis dan sistematis sehingga mendapatkan hasil yang optimal dan sesuai dengan yang diharapkan. Adapun dalam tahapan penelitian dilakukan beberapa teknik pengumpulan data sebagai berikut:

a. Observasi
b. Wawancara
c. Penerapan metode SHA dan DSA dalam pengolahan data menjadi hasil *Digital signature*

Pengumpulan data dilakukan di Mis Al-Hasanah Tanjung Morawa. Dalam pengumpulan data dilakukan observasi langsung ke lokasi penelitian dengan melakukan proses wawancara langsung dengan kepala sekolah di yayasan tersebut.

JURNAL SISTEM INFORMASI TGD
Volume 1, Nomor 6, November 2022, Hal 906-914
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

Data yang dikumpulkan merupakan data primer yaitu merupakan slip gaji pegawai yang akan digunakan dalam proses penelitian.

2.2 Kriptografi

Kriptografi (*Cryptography*) dari bahasa Yunani, terdiri dari 2 suku kata yaitu kripto dan graphia. Kripto artinya menyembunyikan, sedangkan *graphia* ialah tulisan. Kriptografi ialah ilmu yang mempelajari teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasian data, integritas data, keabsahan data , serta autentikasi data[6]. Kriptografi ialah ilmu dan seni untuk menjaga kerahasiaan dan keamanan pesan dengan cara menyandikannya ke dalam bentuk yang tak dapat dimengerti lagi maknanya[7]-[8].

2.3 Digital Signature

Digital signature merupakan sebuah skema matematis yang membentuk tanda tangan secara unik untuk mengidentifikasikan seorang pengirim, sekaligus untuk membuktikan keaslian dari pemilik sebuah dokumen digital atau pesan. Sebuah *Digital signature* yang autentik (sah), sudah cukup menjadi alasan bagi penerima untuk percaya bahwa sebuah pesan atau dokumen yang diterima adalah dari berasal pengirim yang sudah diketahui. Teknologi *Digital signature* memanfaatkan sebuah teknologi kunci publik. Sepasang kunci publik dan privat dibuat untuk keperluan seseorang. Kunci privat ada pada pemiliknya untuk membentuk tanda tangan *digital*. Serta kunci publik diserahkan pada siapa saja yang ingin memeriksa tanda tangan digital pada suatu dokumen. Proses pembuatan dan pemeriksaan tanda tangan menggunakan teknik kriptografi seperti hashing (membentuk "sidik jari" dokumen)[8].

2.4 Algoritma SHA-1

Secure Hash Algorithm (SHA) dikembangkan sang NIST (National Institue of Standars and Technology) yang digunakan bersama DSS (Digital Signature Standart). SHA-1 merupakan revisi terhadap SHA yang dipublikasikan pada tahun SHA disebut aman karena dibuat secara komputasi sehingga tidak mungkin menemukan pesan yang berkoresponden dengan message digest yang diberikan. SHA1 mempunyai panjang 20 bytes atau 40 karakter, contohnya : 356a192b7913b04c54574d18c28d46e6395428ab[10].

2.5 DSA (*Digital Signature Algorithm*)

Digital Signature Algorithm adalah algoritma kriptografi yang difokuskan untuk menjamin *integrity* dan *autentication*, bukan *confidentiality*[11]. DSA memiliki dua fungsi utama yaitu pembentukan tanda tangan (*Signature generation*) serta pemeriksaan keabsahan tanda tangan (*Signature verification*)[12]. Adapun beberapa prosedur dalam pembentukan *Digital Signature Algorithm*, yaitu:

1. Membuat sepasang kunci:
   Pilih bilangan prima $p\ dan\ q$, dengan persamaan $(p-1)\ mod\ q = 0$ (1)
   $g = h^{(p-1)/q}\ mod\ p$, dalam persamaan $1 < h < p-1$ dan $h^{(p-1)/q}\ mod\ p > 1$
   $x < q$ = merupakan kunci privat
   $y = g^x\ mod\ p$ = kunci publik
2. Proses pembuatan tanda tangan
   $k < q$ = bilangan acak (2)
   $r = (g^k\ mod\ p)\ mod\ q$
   $s = (k^{-1}(H(m) + x * r))mod\ q$. k^{-1} yaitu invers $k\ mod\ q$
   (r, s): tanda tangan digital
3. Proses pembuktian tanda tangan (verifikasi)
   $w = s^{-1}\ mod\ q$ (3)
   $u1 = (H(m) * w)\ mod\ q$
   $u2 = (r * w)\ mod\ q$
   $v = ((g^{u1} * y^{u2})\ mod\ p)\ mod\ q$
   Jika $v = r$, maka tanda tangan terbukti asli.

3. HASIL DAN PEMBAHASAN

3.1 Penerapan Metode SHA dan DSA

Algoritma yang digunakan pada penelitian ini dalam proses pembentukan *Digital Signature* adalah SHA-1 dan DSA. Hal ini dilakukan untuk mencegah terjadinya kepalsuan dan modifikasi data oleh pihak tidak bertanggung jawab. Pesan akan di *enkripsi* dengan fungsi *hash* SHA-1 dan menghasilkan *message digest* lalu akan di *dekripsi* dengan kunci publik dari algoritma DSA. Berikut ini merupakan pesan yang akan diolah menjadi tanda tangan digital:

JURNAL SISTEM INFORMASI TGD
Volume 1, Nomor 6, November 2022, Hal 906-914
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

Tabel 1. Pesan

Data slip gaji					
W	A	D	7	8	7

a. Mengubah pesan dalam bentuk ASCII lalu ke binner
W = 87 : 01010111
A = 65 : 01000001
D = 68 : 01000100
7 = 55 : 00110110
8 = 56 : 00111000
7 = 55 : 00110110
Maka panjang pesan (l) = 6 x 8 = 48 bit = 00110000 (binner).

b. Menambahkan bit *Padding* pesan
$k = l + 1 = 448 \; mod \; 512$
$k = 48 + 1 = 448 \; mod \; 512$
$k = 49 = 448 \; mod \; 512$
$k = 448 - 49 = 399$
Ditemukan nilai k = 399, maka bit "0" yang ditambahkan sejumlah 399 bit pada akhiran pesan tambahkan 8 bit (l), yaitu 00110000. Berikut adalah hasil pesan yang di *padding*.

Tabel 2. Padding Pesan

01010111	01000001	01000100	00110110	00111000	00110110	10000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00110000

c. Melakukan *Parsing* Pesan
Dengan memecahkan 512 bit blok, setiap blik menjadi 16 potongan, setiap potongan berukuran 32 bit dan diberi simbol W_0 sampai W_{15}

Tabel 3. Hasil *Parsing* Pesan

Parsing Pesan			
W_0	01010111010000010100010000110110	W_8	00000000000000000000000000000000
W_1	00111000001101101000000000000000	W_9	00000000000000000000000000000000
W_2	00000000000000000000000000000000	W_{10}	00000000000000000000000000000000
W_3	00000000000000000000000000000000	W_{11}	00000000000000000000000000000000
W_4	00000000000000000000000000000000	W_{12}	00000000000000000000000000000000
W_5	00000000000000000000000000000000	W_{13}	00000000000000000000000000000000
W_6	00000000000000000000000000000000	W_{14}	00000000000000000000000000000000
W_7	00000000000000000000000000000000	W_{15}	00000000000000000000000000110000

d. Melakukan Penjadwalan Pesan
Penjadwalan pesan dilakukan dengan menambahkan potongan blok menjadi 80 potongan hasilnya akan menjadi W_{16} sampai W_{79} lalu pesan diubah ke bentuk hexadesimal, dengan persamaan berikut:
$W_t = ROTL^1 \, (W_{t-16} \oplus W_{t-14} \oplus W_{t-8} \oplus W_{t-3})$

Tabel 4. Penjadwalan Pesan (W_t)

Penjadwalan Pesan (Hexadesimal)							
W_{16}	AE82886C	W_{32}	EAAF317B	W_{48}	D78B0E68	W_{64}	EF0F23C7
W_{17}	706D0000	W_{33}	216E0809	W_{49}	B4CF6D99	W_{65}	DB1D53B7
W_{18}	00000060	W_{34}	A0E21AAB	W_{50}	284423FC	W_{66}	107B0A0D
W_{19}	5D0510D9	W_{35}	6F5444C5	W_{51}	97C75DB8	W_{67}	609629EB
W_{20}	E0DA0000	W_{36}	272D5EE3	W_{52}	831E8F93	W_{68}	CFB58728
W_{21}	000000C0	W_{37}	CF0C37DA	W_{53}	64E96C2D	W_{69}	1C831430
W_{22}	BA0A21B2	W_{38}	42944725	W_{54}	B1F5A3F2	W_{70}	37EEF78A

JURNAL SISTEM INFORMASI TGD
Volume 1, Nomor 6, November 2022, Hal 906-914
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

W_{23}	C1B40061	W_{39}	83282123	W_{55}	D94D3E2F	W_{71}	D5227EDE
W_{24}	5D051159	W_{40}	F79C2FF7	W_{56}	ABD66E61	W_{72}	7123E061
W_{25}	94CE4365	W_{41}	EE681E93	W_{57}	AEC406A7	W_{73}	DCBB487B
W_{26}	83680003	W_{42}	91157A82	W_{58}	E1CAA9A6	W_{74}	557EC06F
W_{26}	00000300	W_{43}	3C30D3AB	W_{59}	AC6AC6C3	W_{75}	3E823A76
W_{27}	E82886CA	W_{44}	10F93386	W_{60}	8E2CBC42	W_{76}	FAC1D899
W_{29}	06D001E7	W_{45}	D6148313	W_{61}	A39ED216	W_{77}	519D0D0C
W_{30}	291157BC	W_{46}	7A35E493	W_{62}	60429F5D	W_{78}	0C42E2CD
W_{31}	B3C30D36	W_{47}	02F82F34	W_{63}	C2AD80CF	W_{79}	6CA6EA6E

e. Inisialisasi Penyangga (*Buffer*) MD
A = h0 = 67452301 (01100111010001010010001100000001)
B = h1 = efcdab89 (11101111110011011010101110001001)
C = h2 = 98badcfe (10011000101110101101110011111110)
D = h3 = 10325476 (00010000001100100101010001110110)
E = h4 = c3d2e1f0 (11000011110100101110000111110000)

f. Operasi Logika *Bitwise*
Pesan yang sudah ditambahkan nilai *buffer* dengan panjang pesan selanjutnya diuraikan dengan pesan setiap blok 512 bit sebanyak 80 bit putaran. Setiap putaran menggunakan bilangan penambah. Adapun hasil dari setiap putaran yaitu:

Tabel 5. Hasil Setiap Putaran

	A	B	C	D	E
Init	67452301	EFCDAB89	98BADCFE	10325476	C3D2E1F0
t=0	F6F5DCE9	67452301	7BF36AE2	98BADCFE	10325476
t=1	5AECB525	F6F5DCE9	59D148C0	7BF36AE2	98BADCFE
t=2	9AA76604	5AECB525	7DBD773A	59D148C0	7BF36AE2
t=3	85201AEE	9AA76604	56BB2D49	7DBD773A	59D148C0
t=4	D0125563	85201AEE	26A9D981	56BB2D49	7DBD773A
t=5	3145DACE	D0125563	A14806BB	26A9D981	56BB2D49
t=6	80A28DBB	3145DACE	F4049558	A14806BB	26A9D981
t=7	458A9103	80A28DBB	8C5176B3	F4049558	A14806BB
t=8	A120B4CF	458A9103	E028A352	8C5176B3	F4049558
t=9	3AF79097	A120B4CF	D162A440	E028A352	8C5176B3
t=10	06EEAA83	3AF79097	E8482D33	D162A440	E028A352
t=11	01C0919E	06EEAA83	CEBDE425	E8482D33	D162A440
t=12	62A3F6CA	01C0919E	C1BBAAA0	CEBDE425	E8482D33
t=13	670764B9	62A3F6CA	80702467	C1BBAAA0	CEBDE425
t=14	8B652144	670764B9	98A8FDB2	80702467	C1BBAAA0
t=15	0952B1F0	8B652144	59C1D92E	98A8FDB2	80702467
t=16	D7954223	0952B1F0	22D94851	59C1D92E	98A8FDB2
t=17	A7120423	D7954223	0254AC7C	22D94851	59C1D92E
t=18	B8E0E00B	A7120423	F5E55088	0254AC7C	22D94851
t=19	9BC17C96	B8E0E00B	E9C48108	F5E55088	0254AC7C
t=20	6EF95C7B	9BC17C96	EE383802	E9C48108	F5E55088
t=21	E02891F2	6EF95C7B	A6F05F25	EE383802	E9C48108
t=22	3DEC0813	E02891F2	DBBE571E	A6F05F25	EE383802
t=23	79ADC034	3DEC0813	B80A247C	DBBE571E	A6F05F25
t=24	6B8ECD27	79ADC034	CF7B0204	B80A247C	DBBE571E
t=25	601D115D	6B8ECD27	1E6B700D	CF7B0204	B80A247C
t=26	688CFAFA	601D115D	DAE3B349	1E6B700D	CF7B0204
t=27	F48A220B	688CFAFA	58074457	DAE3B349	1E6B700D
t=28	F11A31DA	F48A220B	9A233EBF	58074457	DAE3B349
t=29	AA823512	F11A31DA	FD228882	9A233EBF	58074457
t=30	D654B1F0	AA823512	BC468C76	FD228882	9A233EBF

JURNAL SISTEM INFORMASI TGD
Volume 1, Nomor 6, November 2022, Hal 906-914
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

t=31	733CA796	D654B1F0	AAA08D44	BC468C76	FD228882
t=32	7EF3492E	733CA796	35952C7C	AAA08D44	BC468C76
t=33	1700AC9D	7EF3492E	9CCF29E5	35952C7C	AAA08D44
t=34	721B73E9	1700AC9D	9FBCD24B	9CCF29E5	35952C7C
t=35	6BA53143	721B73E9	45C02B27	9FBCD24B	9CCF29E5
t=36	4FE4275B	6BA53143	5C86DCFA	45C02B27	9FBCD24B
t=37	4D0BA7CD	4FE4275B	DAE94C50	5C86DCFA	45C02B27
t=38	622F0F87	4D0BA7CD	D3F909D6	DAE94C50	5C86DCFA
t=39	D886BCF5	622F0F87	5342E9F3	D3F909D6	DAE94C50
t=40	C5E3E1B5	D886BCF5	D88BC3E1	5342E9F3	D3F909D6
t=41	E67C05EE	C5E3E1B5	7621AF3D	D88BC3E1	5342E9F3
t=42	1798C2E2	E67C05EE	7178F86D	7621AF3D	D88BC3E1
t=43	0D695E17	1798C2E2	B99F017B	7178F86D	7621AF3D
t=44	F4FB22EB	0D695E17	85E630B8	B99F017B	7178F86D
t=45	0BAB96D4	F4FB22EB	85E630B8	85E630B8	B99F017B
t=46	BE49AE23	0BAB96D4	FD3EC8BA	85E630B8	85E630B8
t=47	6EDE71F7	BE49AE23	02EAE6B5	FD3EC8BA	85E630B8
t=48	86C6299C	6EDE71F7	EF926B88	02EAE6B5	FD3EC8BA
t=49	88C98A74	86C6299C	DBB79C7E	EF926B88	02EAE6B5
t=50	A3123F4A	88C98A74	21B18A67	DBB79C7E	EF926B88
t=51	826EF9E6	A3123F4A	2232629D	21B18A67	DBB79C7E
t=52	5F03500C	826EF9E6	A8C48FD2	2232629D	21B18A67
t=53	9887A0D1	5F03500C	A09BBE79	A8C48FD2	2232629D
t=54	9CBB7BF6	9887A0D1	17C0D403	A09BBE79	A8C48FD2
t=55	3920BE01	9CBB7BF6	6621E834	17C0D403	A09BBE79
t=56	1647A213	3920BE01	A72EDEFD	6621E834	17C0D403
t=57	45B5D81D	1647A213	4E482F80	A72EDEFD	6621E834
t=58	141200EF	45B5D81D	C591E884	4E482F80	A72EDEFD
t=59	2A876902	141200EF	516D7607	C591E884	4E482F80
t=60	78B36C49	2A876902	C504803B	516D7607	C591E884
t=61	08EFA4DD	78B36C49	8AA1DA40	C504803B	516D7607
t=62	D11DA90D	08EFA4DD	5E2CDB12	8AA1DA40	C504803B
t=63	1FB15249	D11DA90D	5E2CDB12	5E2CDB12	8AA1DA40
t=64	0B5BB20D	1FB15249	74476A43	5E2CDB12	5E2CDB12
t=65	A4FE1558	0B5BB20D	47EC5492	74476A43	5E2CDB12
t=66	11BDDEE5	A4FE1558	42D6EC83	47EC5492	74476A43
t=67	F8C0DFEF	11BDDEE5	293F8556	42D6EC83	47EC5492
t=68	F47552BF	F8C0DFEF	446F77B9	293F8556	42D6EC83
t=69	4DF74787	F47552BF	FE3037FB	446F77B9	293F8556
t=70	38A4429C	4DF74787	FD1D54AF	FE3037FB	446F77B9
t=71	475730C7	38A4429C	D37DD1E1	FD1D54AF	FE3037FB
t=72	3B61BAEC	475730C7	0E2910A7	D37DD1E1	FD1D54AF
t=73	AA76AE08	3B61BAEC	D1D5CC31	0E2910A7	D37DD1E1
t=74	26D27BB5	AA76AE08	0ED86EBB	D1D5CC31	0E2910A7
t=75	66D89019	26D27BB5	2A9DAB82	0ED86EBB	D1D5CC31
t=76	74A42858	66D89019	49B49EED	2A9DAB82	0ED86EBB
t=77	C54EEE21	74A42858	59B62406	49B49EED	2A9DAB82
t=78	0FC7A710	C54EEE21	1D290A16	59B62406	49B49EED
t=79	FB84ED63	0FC7A710	7153AB88	1D290A16	59B62406

Melakukan penjumlahan hasil putaran dengan *buffer* yaitu sebagai berikut:

H_0 = 67452301 + fb84ed63 = f6d634e0

JURNAL SISTEM INFORMASI TGD
Volume 1, Nomor 6, November 2022, Hal 906-914
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

H_1 = efcdab89 + 0fc7a710 = a11a7788
H_2 = 98badcfe + 7153ab88 = c71c6d53
H_3 = 10325476 + 1d290a16 = de76400d
H_4 = c3d2e1f0 + 59b62406 = 61d65252

Maka menhasilkan nilai massage digest (MD) dari pesan "WAD787" sebanyak 40 dikit karakter yaitu:
f6d634e0a11a7788c71c6d53de76400d61d65252

g. 1. $p = 35533$ dan $q = 2538$ memenuhi (2538*14 = 35533-1) $Mod\ 2538 = 0$. (1)
h = 100
$g = 100^{(35533-1)/2538}\ Mod\ 35533$ = 3260
x = 303 (Private Key)
$y = 3260^{303}\ Mod\ 35533 = 1131$ (*Public Key*)

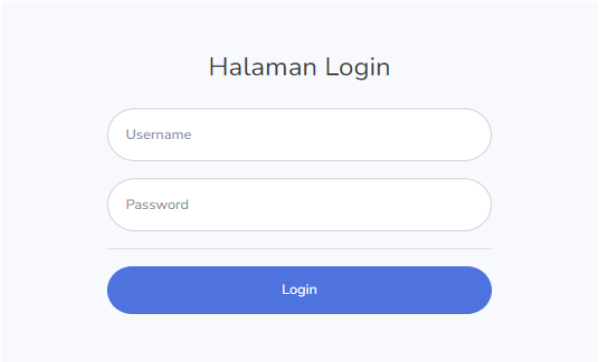
2. k = 427 (2)
$r = (3260^{427}\ mod\ 35533)\ mod\ 2538$ = 511
k^{-1} yaitu invers k mod q.
k^{-1} = 529
s = (511(140918869537141184961977165859437459158422456379 4 + 303 * 511)) mod 2538 = 407
didapatkan *Digital Signature* 511407.

3. w = 1877 mod 2538 = 1877 (3)
$u1$ = (140918869537141184961977165859437459158422456379 4 * 1877) mod 2538 = 190
$u2$ = (511 * 1877) mod 2538 = 2321
v = $((3260^{190} * 11391^{2321})$ mod 35533) mod 2538) = 511
karena v = r, maka tanda tangan asli.

3.2 Implementasi Program

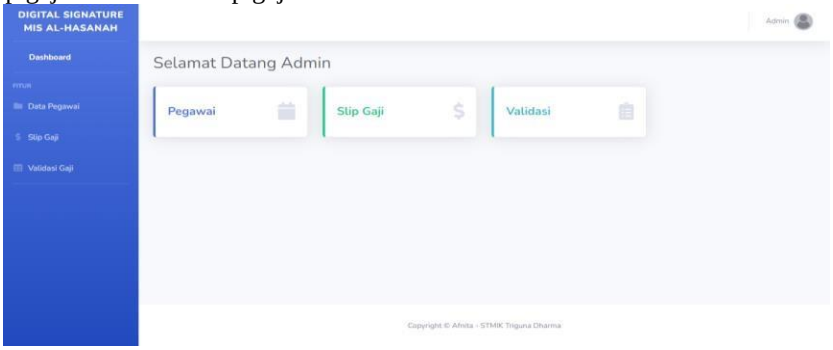
Berikut ini merupakan hasil tampilan antarmuka (*interface*) dari sistem yang telah dibangun :

1. Tampilan Halaman Login
Halaman *login* merupakan halaman yang hanya dapat diakses oleh pengguna yang telah memiliki hak akses.



Gambar 1. Tampilan Form Login

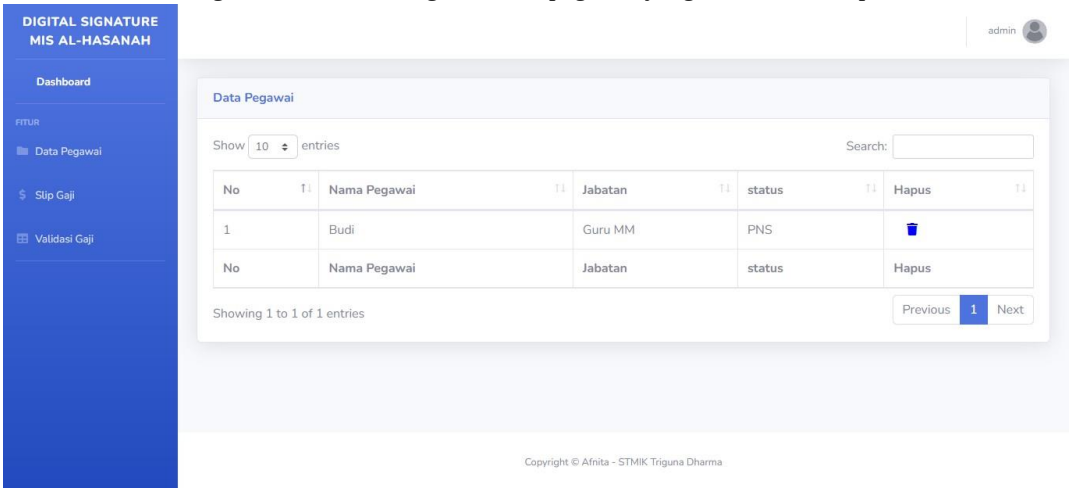
2. Tampilan Halaman Utama
Setelah admin *login*, sistem akan menampilkan halaman utama. Halaman ini menampilkan beberapa akses, seperti menu pegawai, slip gaji dan validasi slip gaji.



Gambar 2. Tampilan Halaman Utama

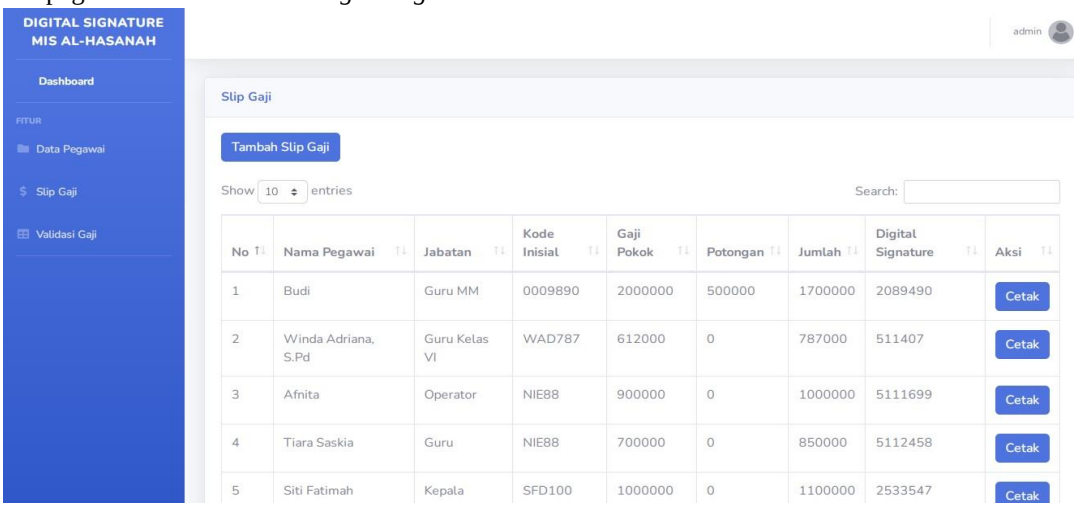
JURNAL SISTEM INFORMASI TGD
Volume 1, Nomor 6, November 2022, Hal 906-914
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

3. Tampilan Halaman Data Pegawai
   Halaman ini disediakan bagi admin untuk mengelola data pegawai yang telah terdaftar pada Mis Al-hasanah.



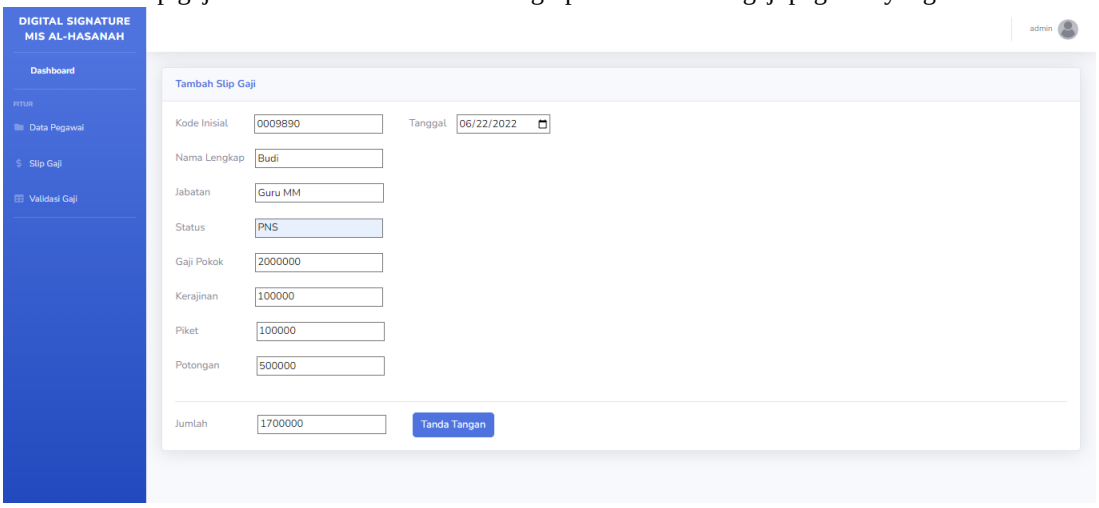
Gambar 3. Tampilan Halaman Data Pegawai

4. Tampilan Halaman Slip Gaji
   Halaman slip gaji disediakan bagi admin untuk mengelola data gaji pada sistem untuk mencetak slip gaji yang telah berisi data pegawai dan telah diberi *Digital signature*.



Gambar 4. Tampilan Halaman Slip Gaji

5. Tampilan Halaman Tambah Slip Gaji
   Halaman tambah slip gaji disediakan untuk admin menginput seluruh data gaji pegawai yang akan di tanda tangani.



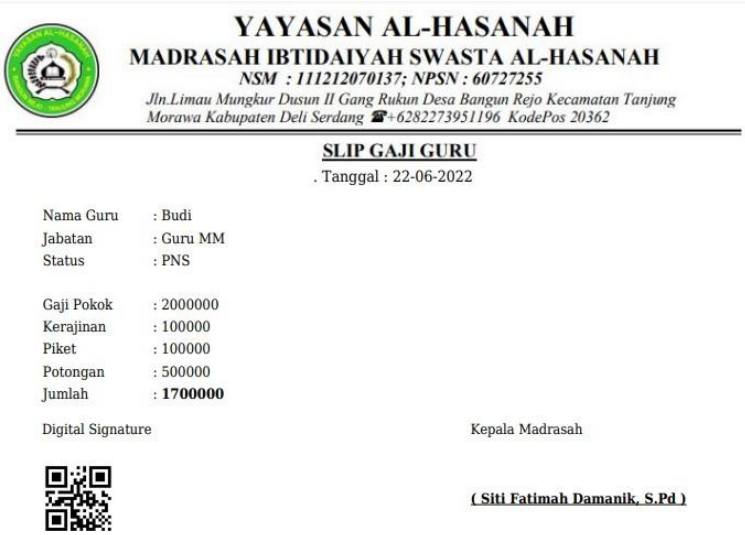
Gambar 5. Tampilan Halaman Tambah Slip Gaji

JURNAL SISTEM INFORMASI TGD
Volume 1, Nomor 6, November 2022, Hal 906-914
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

6. Tampilan Halaman Validasi
   Halaman ini digunakan untuk memberikan informasi terkait keaslian data slip gaji pegawai.

Gambar 6. Tampilan Halaman Validasi

7. Tampilan Hasil Slip Gaji
   Setelah data gaji diinput, sistem akan mencetak hasil slip gaji yang telah di tanda tangani dalam bentuk *QR Code*.



YAYASAN AL-HASANAH
MADRASAH IBTIDAIYAH SWASTA AL-HASANAH
NSM : 111212070137; NPSN : 60727255
Jln.Limau Mungkur Dusun II Gang Rukun Desa Bangun Rejo Kecamatan Tanjung Morawa Kabupaten Deli Serdang ☎+6282273951196 KodePos 20362

SLIP GAJI GURU
. Tanggal : 22-06-2022

Nama Guru	: Budi
Jabatan	: Guru MM
Status	: PNS
Gaji Pokok	: 2000000
Kerajinan	: 100000
Piket	: 100000
Potongan	: 500000
Jumlah	: **1700000**

Digital Signature

Kepala Madrasah

(Siti Fatimah Damanik, S.Pd)

Gambar 7. Tampilan Hasil Slip Gaji

4. KESIMPULAN

Berdasarkan hasil analisa metode SHA dan DSA yang diterapkan kedalam sistem aplikasi *digital signature* dapat mempermudah proses pengolahan dokumen slip gaji. Algoritma SHA-1 dan DSA dapat melakukan proses pembuatan tanda tangan digital yang menghasilkan kode acak. Aplikasi yang dibangun dapat membuktikan bahwa algoritma DSA dapat berjalan dengan baik, Aplikasi ini dapat digunakan untuk pemberian *digital signature* terhadap dokumen slip gaji di Mis Al-Hasanah dengan file berupa .pdf, tanda tangan berupa *QR code* sehingga mudah di aplikasikan dan di cek keabsahannya.

UCAPAN TERIMAKASIH

Terima kasih diucapkan kepada Bapak Mukhlis Ramadhan dan Ibu Hafizah atas segala waktu dan ilmunya yang telah memberikan bimbingan selama masa pengerjaan hingga menyelesaikan jurnal ini dan kepada seluruh dosen serta staff pegawai kampus STMIK Triguna Dharma yang telah banyak membantu baik dalam bentuk informasi ataupun dukungan lainnya.

JURNAL SISTEM INFORMASI TGD
Volume 1, Nomor 6, November 2022, Hal 906-914
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

DAFTAR PUSTAKA

[1] Y. Malau and T. A. Somadiningrat D.W.K, "Implementasi Slip Gaji Elektronik Pada Cv Mediaku Kreatif (Motion Production)," *Swabumi*, vol. 6, no. 1, pp. 8–17, 2018, doi: 10.31294/swabumi.v6i1.3311.

[2] N. Raras Setyoningrum and D. Syah Arihardjo, "Analisis Dan Perancangan Sistem Informasi Penggajian Karyawan Berbasis Web Pada Pt. Batam Bintan Telekomunikasi Lagoi," *J. Inform. Teknol. dan Sains*, vol. 3, no. 1, pp. 272–277, 2021, doi: 10.51401/jinteks.v3i1.978.

[3] B. Anwar, N. B. Nugroho, J. Prayudha, and A. Azanuddin, "Implementasi Algoritma RSA Terhadap Keamanan Data Simpan Pinjam," *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 18, no. 1, p. 30, 2019, doi: 10.53513/jis.v18i1.100.

[4] M. Syaifuddin *et al.*, "Project-based learning on cryptographic using lms," *JURTEKSI (Jurnal Teknol. dan Sist. Informasi)*, vol. VIII, no. 2, pp. 147–152, 2022, doi: : https://doi.org/10.33330/jurteksi.v8i2.1381.

[5] B. K. Hutasuhut, S. Efendi, and Z. Situmorang, "Digital Signature untuk Menjaga Keaslian Data dengan Algoritma MD5 dan Algoritma RSA," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 3, no. 2, pp. 164–169, 2019, doi: 10.30743/infotekjar.v3i2.1019.

[6] M. M. Amin, "Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks," *Pseudocode*, vol. 3, no. 2, pp. 129–136, 2017, doi: 10.33369/pseudocode.3.2.129-136.

[7] L. A. Fitriani, "Analisa Keamanan Data Teks Dengan Menerapkan Kriptografi RSA Dan Steganografi LSB," *J. Comput. Syst. Informatics …*, vol. 1, no. 2, pp. 32–38, 2020.

[8] M. Syaifuddin, J. Hutagalung, and G. Ganefri, "E-Learning Dalam Pengembangan Pembelajaran Kriptografi," *JURTEKSI (Jurnal Teknol. dan Sist. Informasi)*, vol. 7, no. 2, pp. 117–126, 2021, doi: 10.33330/jurteksi.v7i2.914.

[9] Sugiyatno and D. A. Prima, "Digital Signature dengan Algoritma SHA-1 dan RSA Sebagai Autentikasi," *J. Cendikia Vol. XVI Cendikia 2018*, vol. XVI, no. 021, p. 88955882, 2018.

[10] L. Silalahi and A. Sindar, "Penerapan Kriptografi Keamanan Data Administrasi Kependudukan Desa Pagar Jati Menggunakan SHA-1," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 3, no. 2, pp. 182–186, 2020.

[11] H. R. Tampubolon, A. Kusyanti, and F. A. Bakhtiar, "Implementasi Digital Signature pada Secure Electronic Prescription menggunakan Digital Signature Algorithm berbasis Android," *Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 8, pp. 7834–7843, 2019.

[12] D. Arisandi, M. B. Yusuf, and S. Sukri, "Pemeriksaan Integritas Dokumen Dengan Digital Signature Algorithm," *JOISIE (Journal Inf. Syst. Informatics Eng.*, vol. 4, no. 1, p. 1, 2020.