Implementasi Digital Signature Bilyet Deposito Nasabah Dengan RSA Algorithm di Bank Perkreditan Rakyat Perbaungan Hombar Makmur

Diky Pratama[*] , Kamil Erwansyah[**], Hafizah[**]
[*]Program Studi Sistem Informasi, STMIK Triguna Dharma
[**]Program Studi Sistem Komputer Dan Sistem Informasi Dosen Pembimbing, STMIK Triguna Dharma

Article Info
Article history:
-

Keyword:
Digital Signature

Bilyet Deposito Nasabah

Rivest Shamir Adleman.

ABSTRACT

Di zaman yang semakin maju ini, perkembangan simpan uang sudah sangat mudah hanya dengan memanfaatkan telepon genggam transaksi keuangan dapat dilakukan. Salah satu Lembaga penyimpanan uang adalah Bank, Bank merupakan suatu badan keuangan dibawah Peraturan Undang-Undang dalam suatu Negara yang didasari oleh hukum, membuat Bank harus taat terhadap prosedur yang ditetapkan.[1]

Deposito merupakan produk simpan uang Bank yang menghasilkan keuntungan bunga dan penarikannya hanya dapat dilakukan pada jangka waktu tertentu sesuai perjanjian Nasabah dengan pihak Bank.[2] Pihak Bank akan memberi Nasabah buku tabungan jika menggunakan layanan Tabungan, lain halnya Deposito, Deposan akan diberikan Sertifikat Deposito yang biasa disebut dengan Bilyet Deposito. Selama ini terjadi beberapa masalah dalam pendistribusian Bilyet Deposito kepada nasabah, seperti pemalsuan yang menyebabkan kerugian dan nasabah yang tertipu dengan penerbitan Bilyet tidak terdaftar di Bank Perkreditan Rakyat Perbaungan Hombar Makmur (BPR PHM)

Digital Signature atau Tanda Tangan Digital adalah suatu teknik Kriptografi yang dapat digunakan untuk menandatangani Informasi Digital, Tanda Tangan Digital Sendiri merupakan hasil dari penggabungan teknik Kriptografi dengan Pesan atau dokumen asli.[3].

Algoritma Rivest Shamir Adleman (RSA) dipilih dalam penelitian ini karena dirasa sangat cocok untuk membantu proses enkripsi Tanda Tangan Digital, RSA sering digunakan untuk proses enkripsi satu arah dan tidak membutuhkan proses deskripsi, karena digunakan untuk validasi suatu dokumen asli.

First Author
Nama : Diky Pratama
Kampus : STMIK Triguna Dharma
Program Studi : Sistem Informasi
E-Mail : dickyp71.dp@gmail.com

1. PENDAHULUAN

Di zaman yang semakin maju ini, perkembangan simpan uang sudah sangat mudah hanya dengan memanfaatkan telepon genggam transaksi keuangan dapat dilakukan. Salah satu Lembaga penyimpanan uang adalah Bank, Bank merupakan suatu badan keuangan dibawah Peraturan Undang-Undang dalam suatu Negara yang didasari oleh hukum, membuat Bank harus taat terhadap prosedur yang ditetapkan.[1]

Deposito hampir sama dengan Tabungan, hanya saja Deposito menawarkan bunga yang relatif lebih tinggi dari Tabungan pada biasanya. Deposito merupakan produk simpan uang Bank yang menghasilkan keuntungan bunga dan penarikannya hanya dapat dilakukan pada jangka waktu tertentu sesuai perjanjian Nasabah dengan pihak Bank.[2]

Pihak Bank akan memberi Nasabah buku tabungan jika menggunakan layanan Tabungan, lain halnya Deposito, Deposan akan diberikan Sertifikat Deposito yang biasa disebut dengan Bilyet Deposito. Bilyet hanya diterbitkan oleh Bank dengan satu kali terbit saja oleh pihak Bank. Jadi ketika deposito telah dicairkan oleh Nasabah, maka Bilyet Deposito akan otomatis tidak berlaku lagi. Menurut Undang-Undang Republik Indonesia Nomor 10 Tahun 1998 Sertifikat Deposito adalah simpanan dalam bentuk deposito yang sertifikat bukti penyimpannya dapat dipindahtangankan.

Selama ini terjadi beberapa masalah dalam pendistribusian Bilyet Deposito kepada nasabah, seperti pemalsuan yang menyebabkan kerugian dan nasabah yang tertipu dengan penerbitan Bilyet tidak terdaftar di Bank Perkreditan Rakyat Perbaungan Hombar Makmur (BPR PHM). Oleh karena itu, dibutuhkan suatu sistem yang mengamankan Bilyet sehingga tidak mudah dipalsukan, serta Nasabah dapat melihat keaslian distribusinya. Maka dibuatlah tanda tangan digital dengan QR *code* yang dapat mempermudah nasabah dalam melihat keaslian Bilyet.

Digital Signature atau Tanda Tangan Digital adalah suatu teknik Kriptografi yang dapat digunakan untuk menandatangani Informasi Digital, Tanda Tangan Digital Sendiri merupakan hasil dari penggabungan teknik Kriptografi dengan Pesan atau dokumen asli.[3]. Kriptografi digunakan untuk menunjukan setiap metode enkripsi atau penyembunyian informasi seperti Tanda Tangan Digital agar mempermudah proses Validasi. Kriptografi merupakan ilmu yang mempelajari cara pengamanan kirim Data atau Informasi dengan merubahnya menjadi kode-kode tertentu dimaksudkan agar Data atau Informasi hanya bisa kembali diubah oleh penerima yang memiliki kunci.[4]

Algoritma Rivest Shamir Adleman (RSA) dipilih dalam penelitian ini karena dirasa sangat cocok untuk membantu proses enkripsi Tanda Tangan Digital, proses perumusan Algoritma RSA mengginakan dua kunci yaitu kunci pribadi dan kunci publik dengan begitu proses enkripsi akan membantu data atau informasi tidak mudah dimanipulasi. RSA sering digunakan untuk proses enkripsi satu arah dan tidak membutuhkan proses deskripsi, karena digunakan untuk validasi suatu dokumen asli.

Pengimplementasian algoritma RSA dirasa perlu untuk menjamin keamanan data dan juga memvalidasi Bilyet deposito agar lebih mudah. Dengan penjelasan tersebut maka diangkat judul "Implementasi Digital Signature pada Bilyet Deposito Nasabah dengan RSA Algorithm di Bank Perkreditan Rakyat Perbaungan Hombar Makmur".

2. KAJIAN PUSTAKA

2.1 Bilyet Deposito

Bilyet deposito atau Sertifikat Deposito merupakan instrumen yang diterbitkan oleh Bank yang dinyatakan dalam jumlah, jangka waktu, dan tingkat bunga. Deposito biasanya memiliki jangka waktu tertentu 1,3,6 atau 12 bulan, dimana uang yang didepositkan tidak boleh di tarik nasabah jika belum tanggal jatuh temponya. Apabila nasabah mencairkannya sebelum tanggal jatuh tempo maka nasabah akan dikenai pinalti sesuai dengan kebijakan bank. Deposito dapat diperpanjang otomatis dengan sistem *automatic roll over* (ARO) jika nasabah tidak mencairkannya setelah tanggal jatuh tempo sesuai dengan persetujuan nasabah.[5]

2.2 Kriptografi

Tulisan dan suara merupakan salah satu sarana komunikasi yang sering digunakan oleh manusia bertujuan untuk menyampaikan informasi kepada penerima informasi. Seiring berkembangnya teknologi, pengiriman dan penerimaan suatu informasi juga berkembang dari cara menyembunyikan informasi agar orang lain yang bukan dimaksud untuk penerima pesan tidak mengetahui isi informasi yang ada pada pesan, meskipun pesan ditemukan, di situlah lahir ilmu baru yang disebut kriptografi.[6]

2.3 *Digital Signature*

Digital signature adalah kombinasi dari fungsi *hash* dan proses enkripsi dengan kunci asimetrik. Untuk membuat suatu *digital signature*, informasi tentu disebut sebagai *input* dalam *hash* dan menjadi nilai unik. Karena itu jika terjadi perubahan satu *bit* saja pada *input* maka nilai *hash* akan jauh berbeda hasilnya. Setelah itu nilai *hash* di enkripsi dengan *private key* yang selanjutnya hasil dari enkripsi adalah sebuah *signature* dari sebuah dokumen, *signature* kemudian ditambahkan pada dokumen atau informasi tersebut. Proses verifikasi dapat dilakukan dengan cara melakukan dekripsi *signature* dokumen. Hasil dekripsi tersebut nantinya akan menghasilkan nilai *hash* yang selanjutnya akan dibandingkan dengan nilai *hash* dari dokumen yang dibangkitkan oleh penerima dokumen. Jika nilai *hash* sesuai atau sama, maka dokumen yang diterima adalah valid atau asli. Dan sebaliknya jika nilai *hash* yang dibandingkan tidak sesuai atau sama, maka bisa dipastikan bahwa dokumen telah mengalami modifikasi oleh pihak yang tidak berhak [7].

2.4 Algoritma RSA

Rivest, Shamir dan Adleman atau disingkat RSA adalah sebuah *public key cipher* yang dibuat oleh tiga orang peneliti dari MIT (*Massachusetts Institute of Technology*) pada tahun 1978. Peneliti tersebut antara lain Ron Rivest, Adi Shamir dan Leonard Adleman. *Cipher* ini memiliki 2 kunci, yaitu kunci publik dan kunci rahasia. Keamanan *cipher* RSA ini terletak pada sulitnya menfaktorkan bilangan yang besar menjadi faktor-faktor prima [8].

Di dalam kriptografi, RSA adalah algoritma yang digunakan untuk enkripsi kunci publik, RSA merupakan algoritma pertama yang diketahui sangat cocok untuk menandai atau *signing* dan enkripsi. RSA juga masih digunakan secara luas dalam aturan perdagangan elektronik karena kunci kunci yang diterbitkan cukup panjang membuat RSA sangat aman. [9].

2.4.1 Membangkitkan Kunci Algoritma RSA

Untuk *p* dan *q* bilangan prima bersifat rahasia, *n = p, q* tidak bersifat rahasia, *φ* (n) = (*p* - 1) (*q* - 1) bersifat rahasia, *e* (kunci enkripsi) bersifat tidak rahasia, *d* (kunci dekripsi) bersifat rahasia, *m* (*plainteks*) bersifat rahasia, dan *chiperteks* bersifat tidak rahasia. Algoritma membangkitkan kunci RSA sebagai berikut:

1. Menentukan dua bilangan prima, dengan nama:
   p dan q
2. Menghitung nilai modulus (*n*):
   $n = p \times q$
3. Menghitung nilai *totient* (φ) *n*:
   $\varphi(n) = (p-1) \times (q-1)$
4. Menentukan nilai *e* dengan syarat (*greater common divisor) gcd* (*e*, φ (*n*)) =1
   Dimana *e* = bilangan prima, dan $1 < e < \varphi(n)$.
5. Mencari nilai *deciphering exponent* (*d*), maka:
   $d = (1 + (k \times \varphi(n)) / e)$
   Nilai *k* merupakan sembarang angka untuk pencarian hingga dihasilkan suatu nilai *integer* atau bulat. Dengan mencoba nilai *k* = 1,2,3 dan seterusnya hingga diperoleh nilai *d* yang bulat.
6. Dari langkah-langkah yang sudah diuraikan sebelumnya, maka nilai *n*, *e*, dan *d* telah didapatkan sehingga pasangan kunci telah terbentuk.[10]

2.4.2 Proses Enkripsi

Enkripsi adalah proses mengamankan data atau informasi, dengan kata lain mengacak data atau informasi agar tidak dapat dibaca oleh pihak lain[11]. Rumus enkripsi algoritma RSA sebagai berikut: $C = M^e \bmod n$

3. ANALISA DAN HASIL

3.1 Algoritma Sistem

Algoritma sistem merupakan penjelasan langkah-langkah penyelesaian masalah dalam perancangan sistem penerapan kriptografi berbasis *digital signature* menggunakan algoritma RSA pada Bilyet Deposito Nasabah.

3.3.1 Membangkitkan Kunci Algoritma RSA

Untuk *p* dan *q* bilangan prima bersifat rahasia, *n = p, q* tidak bersifat rahasia, *φ* (n) = (*p* - 1) (*q* - 1) bersifat rahasia, *e* (kunci enkripsi) bersifat tidak rahasia, *d* (kunci dekripsi) bersifat rahasia, *m* (*plaintext*) bersifat rahasia, dan *ciphertext* bersifat tidak rahasia. Berikut ini merupakan tahapan-tahapan dalam menyelesaikan masalah dengan menggunakan algoritma RSA:

1. Membangkitkan kunci algoritma RSA dengan menentukan dua bilangan prima *p* dan *q*:
   $p = 19$
   $q = 41$
2. Menghitung nilai modulus (*n*):
   $n = p \times q$
   $n = 19 \times 41$
   $n = 779$
3. Menghitung nilai *totient* (φ) *n*:
   $\varphi(n) = (p - 1) \times (q - 1)$
   $\varphi(n) = (19 - 1) \times (41 - 1)$
   $\varphi(n) = 18 \times 40$
   $\varphi(n) = 720$
4. Menentukan nilai *e*, dimana *e* bilangan prima dengan syarat *gcd*:
   $gcd(e, \varphi(n)) = 1$
   $\gcd(7, 720) = 1$
   $e = 7$

5. Mencari nilai *deciphering exponent* (*d)* dimana *(d)* bilangan bulat:
   $d = (1 + (k \times \varphi (n)) / e)$
   $d = (1 + (1x\ 720) / 7)$
   $d = 721 / 7$
   $d = 103$
6. Dalam bilyet deposito ini yang dijadikan *plaintext* dalam enkripsi ini adalah tanggal, no rekening nasabah dan tipe jangka waktu deposito.

3.3.2 Proses Enkripsi

Berikut merupakan proses megenkripsi *plaintext* yaitu sebagai berikut:

Tabel 3.1 Kode ASCII

Karakter	Hex	Desimal	Karakter	Hex	Desimal	Karakter	Hex	Desimal	Karakter	Hex	Desimal
NUL (null)	0	0	Space	20	32	@	40	64	`	60	96
Start Heading	1	1	!	21	33	A	41	65	a	61	97
Start Text	2	2	"	22	34	B	42	66	b	62	98
End Text	3	3	#	23	35	C	43	67	c	63	99
End Transmit.	4	4	$	24	36	D	44	68	d	64	100
Enquiry	5	5	%	25	37	E	45	69	e	65	101
Acknowlege	6	6	&	26	38	F	46	70	f	66	102
Bell	7	7	`	27	39	G	47	71	g	67	103
Backspace	8	8	(	28	40	H	48	72	h	68	104
Horiz. Tab	9	9	)	29	41	I	49	73	i	69	105
Line Feed	A	10	*	2A	42	J	4A	74	j	6A	106
Vert. Tab	B	11	+	2B	43	K	4B	75	k	6B	107
Form Feed	C	12	,	2C	44	L	4C	76	l	6C	108
Carriage Return	D	13	-	2D	45	M	4D	77	m	6D	109
Shift Out	E	14	.	2E	46	N	4E	78	n	6E	110
Shift In	F	15	/	2F	47	O	4F	79	o	6F	111
Data Link Esc	10	16	0	30	48	P	50	80	p	70	112
Direct Control 1	11	17	1	31	49	Q	51	81	q	71	113
Direct Control 2	12	18	2	32	50	R	52	82	r	72	114
Direct Control 3	13	19	3	33	51	S	53	83	s	73	115
Direct Control 4	14	20	4	34	52	T	54	84	t	74	116
Negative ACK	15	21	5	35	53	U	55	85	u	75	117
Synch Idle	16	22	6	36	54	V	56	86	v	76	118
End Trans Block	17	23	7	37	55	W	57	87	w	77	119
Cancel	18	24	8	38	56	X	58	88	x	78	120
End of Medium	19	25	9	39	57	Y	59	89	y	79	121
Substitue	1A	26	:	3A	58	Z	5A	90	z	7A	122
Escape	1B	27	;	3B	59	[	5B	91	{	7B	123
Form separator	1C	28	<	3C	60	\	5C	92	l	7C	124
Group separator	1D	29	=	3D	61	]	5D	93	}	7D	125
Record Separator	1E	30	>	3E	62	^	5E	94	~	7E	126
Unit Separator	1F	31	?	3F	63	_	5F	95	Delete	7F	127

Tabel 3.2 *Plaintext* dan Kode Desimal ASCII

Plaintext	**Kode Desimal ASCII**
2	50
7	57
1	49
2	50
2	50
0	48
1	49
9	57
1	49
0	48
6	54
0	48
0	48
2	50
1	49
.	46
6	54
.	46

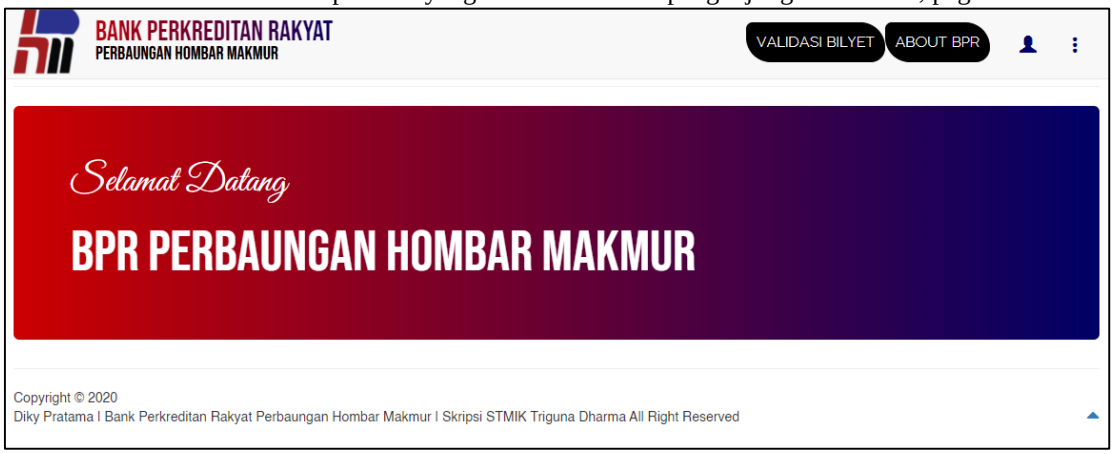
Setelah *plaintext* diubah ke kode ASCII desimal selanjutnya proses enkripsi dengan rumus $C = M^e \bmod n$ yaitu sebagai berikut:

$C_1 = M^e \bmod n = 50^7 \bmod 779 = 278$
$C_2 = M^e \bmod n = 57^7 \bmod 779 = 133$
$C_3 = M^e \bmod n = 49^7 \bmod 779 = 125$
$C_4 = M^e \bmod n = 50^7 \bmod 779 = 379$
$C_5 = M^e \bmod n = 50^7 \bmod 779 = 278$
$C_6 = M^e \bmod n = 48^7 \bmod 779 = 509$
$C_7 = M^e \bmod n = 49^7 \bmod 779 = 125$
$C_8 = M^e \bmod n = 57^7 \bmod 779 = 133$
$C_9 = M^e \bmod n = 49^7 \bmod 779 = 125$
$C_{10} = M^e \bmod n = 48^7 \bmod 779 = 509$
$C_{11} = M^e \bmod n = 54^7 \bmod 779 = 682$
$C_{12} = M^e \bmod n = 48^7 \bmod 779 = 509$
$C_{13} = M^e \bmod n = 48^7 \bmod 779 = 509$
$C_{14} = M^e \bmod n = 50^7 \bmod 779 = 278$
$C_{15} = M^e \bmod n = 49^7 \bmod 779 = 125$
$C_{16} = M^e \bmod n = 46^7 \bmod 779 = 635$
$C_{17} = M^e \bmod n = 54^7 \bmod 779 = 682$
$C_{18} = M^e \bmod n = 46^7 \bmod 779 = 635$

4 PENGUJIAN DAN IMPLEMENTASI

4.1 Halaman Utama

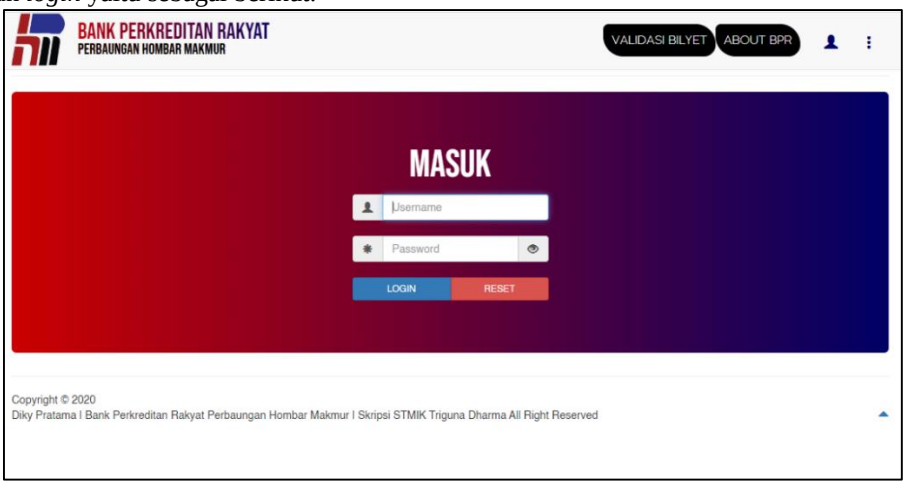
Halaman ini berisi antarmuka pertama yang akan dilihat oleh pengunjung baik admin, pegawai serta nasabah.



Gambar 4.1 Halaman Utama

4.2 Halaman *Login*

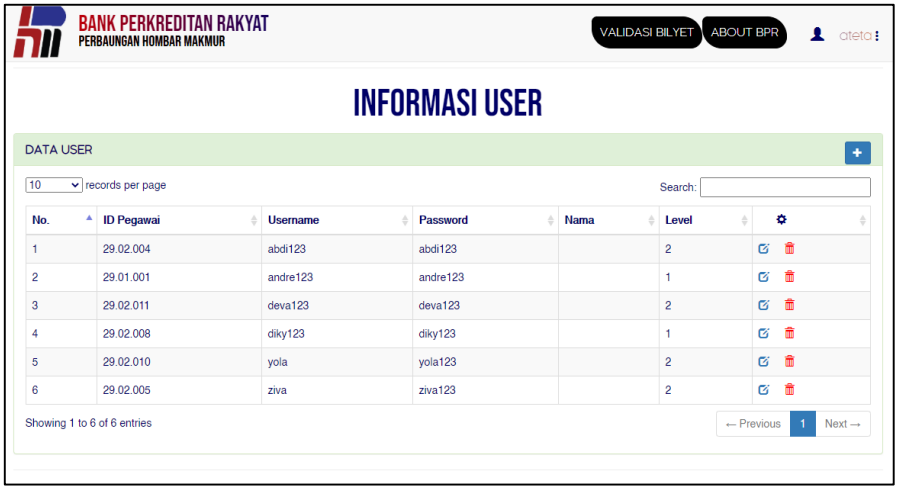
Halaman ini berfungsi sebagai proses masuk bagi setiap *user* untuk dapat mengkases halaman BPR PHM sesuai *level* yang dimana *level* satu untuk halaman admin dan *level* dua untuk halaman pegawai. Berikut ini adalah tampilan halaman *login* yaitu sebagai berikut:



Gambar 4.2 Halaman *Login*

4.2 Halaman *User*

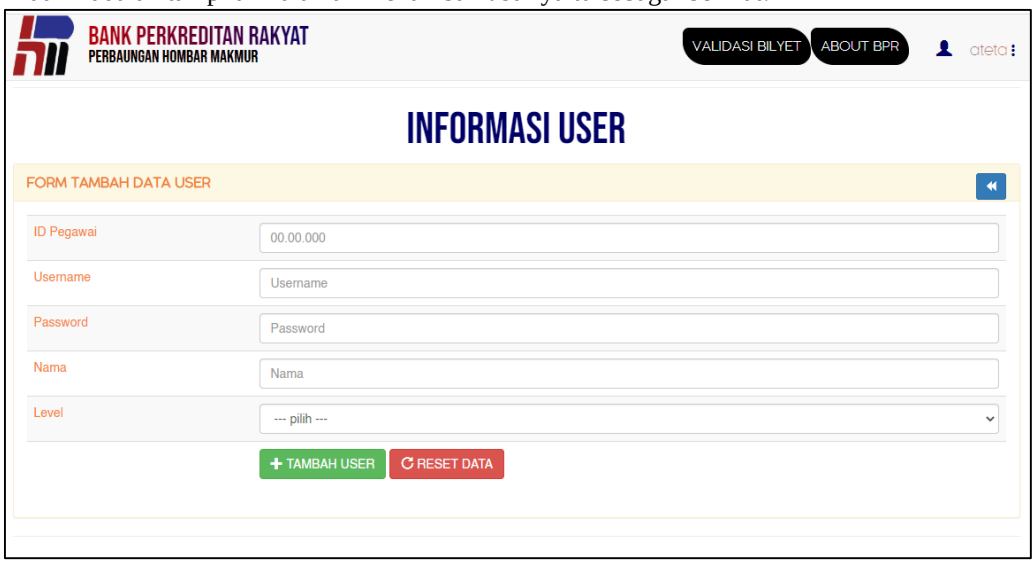
Berikut ini adalah tampilan halaman *user* yang berfungsi untuk melihat informasi masing-masing *user* yaitu sebagai berikut:



Gambar 4.3 Halaman *User*

4.3 Halaman Menambah User

Berikut ini adalah tampilan halaman menambah *user* yaitu sebagai berikut:



Gambar 4.4 Halaman Menambah *User*

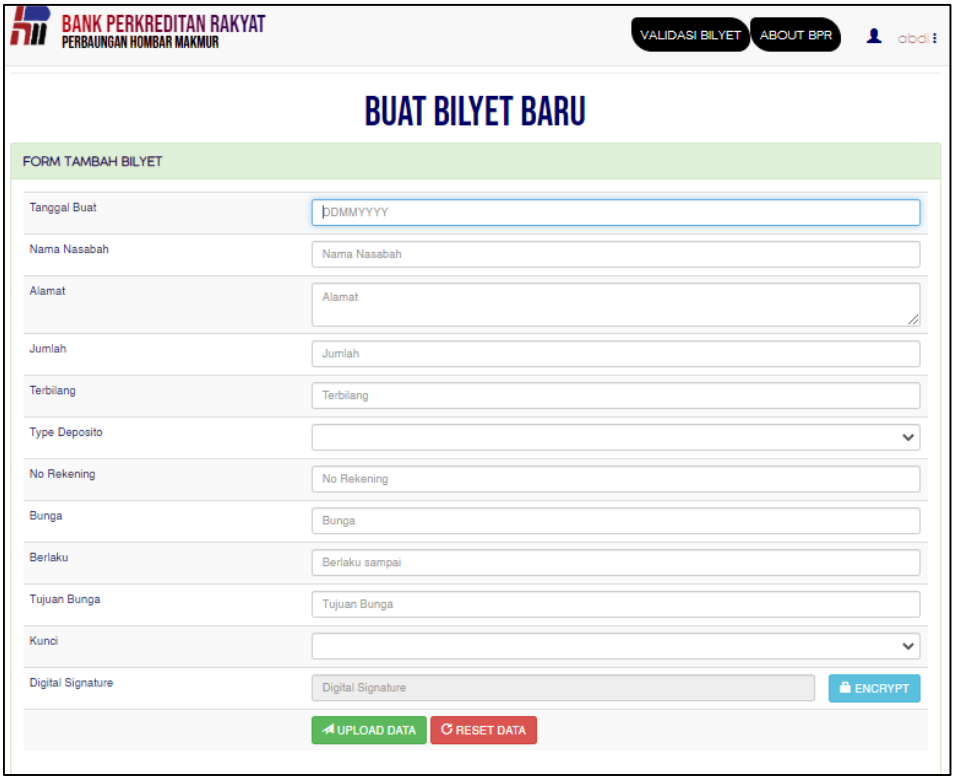
4.4 Halaman Kunci

Berikut ini adalah tampilan halaman kunci yang berfungsi untuk membangkitkan kunci RSA yaitu sebagai berikut:

Gambar 4.5 Halaman Kunci

4.5 Halaman Enkripsi

Berikut ini adalah tampilan halaman enkripsi yaitu sebagai berikut:



Gambar 4.6 Tampilan Halaman *Enkripsi Bilyet*

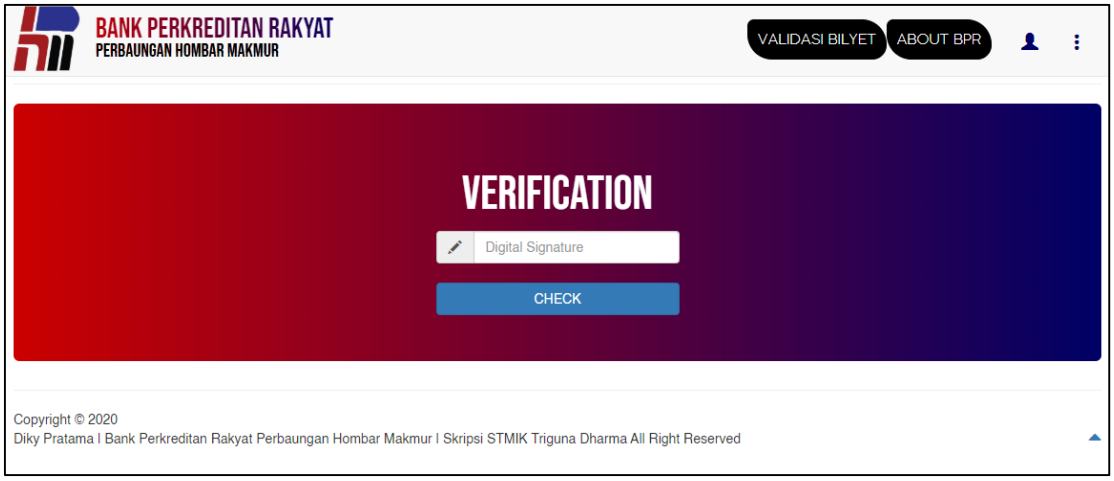
4.6 asda

Berikut ini adalah tampilan halaman Data Deposito yaitu sebagai berikut:

Gambar 4.7 Tampilan Halaman Data Deposito

5.2 Tampilan Halaman *Form* Verifikasi

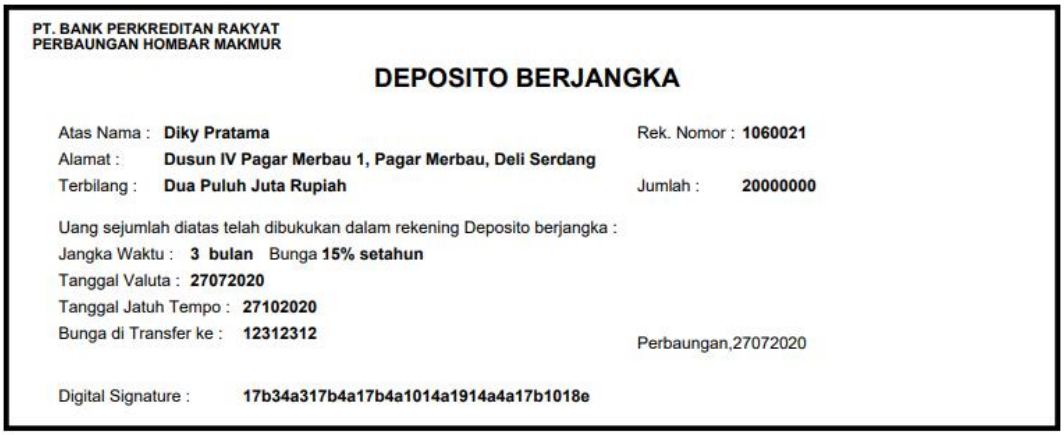
Berikut ini adalah tampilan halaman *form* verifikasi yaitu sebagai berikut:



Gambar 4.8 Tampilan Halaman *Form* Verifikasi

5.3 Tampilan Bilyet Deposito

Pada halaman ini terdapat Bilyet Deposito beserta *digital signature*. Berikut ini adalah Bilyet Deposito yaitu sebagai berikut:



Gambar 4.9 Tampilan Bilyet Deposito

5. KESIMPULAN

Berdasarkan perumusan dan pembahasan bab-bab sebelumnya dapat diambil kesimpulan sebagai berikut

1. Perancangan tanda tangan digital dengan RSA pada bilyet menggunakan penggabungan tgl, no rekening, dan tipe deposito nasabah dengan akhirnya di enkripsi menjadi sebuah kunci.
2. Dalam merancang program menggunakan algoritma Rivest Shamir Adleman yang dapat digunakan terkait memverifikasi keaslian Bilyet pada BPR PHM yaitu dengan membuat pemodelan sistem yang terdiri dari skenario, *use case* diagram, *activity* diagram dan *class* diagram selanjutnya membangun *database* sebagai pusat untuk menyimpan *data* dan dalam pembuatan program ini berbasis *web*.
3. Bilyet di amankan menggunakan RSA dengan enkripsi kunci public dan private.
4. Program yang dirancang selanjutnya diuji dan diimplementasikan dengan menginput identitas pegawai sesuai pada bab sebelumnya, jika hasil *output*nya sesuai maka pengujian program ini berjalan dengan baik, lalu untuk proses

input data untuk menambahkan dan menyimpan Bilyet ke *database*, proses ubah untuk merubah identitas pegawai di *database*, dan perintah hapus untuk menghapus identitas pegawai di *database*.

5. Tanda tangan digital di cetak dengan menggunakan lampiran, sehingga tidak mengganggu sistem yang telah berjalan pada BPR PHM.

UCAPAN TERIMA KASIH

Puji syukur kehadirat Allah SWT atas izin-Nya yang telah melimpahkan rahmat dan karunia-Nya sehingga dapat menyelesaikan jurnal ilmiah ini. Pada kesempatan ini diucapkan terima kasih yang sebesar-besarnya kepada kedua Orang Tua tercinta yang selama ini memberikan do'a dan dorongan baik secara moril maupun materi sehingga dapat terselesaikan pendidikan dari tingkat dasar sampai bangku perkuliahan dan terselesaikannya jurnal ini. Di dalam penyusunan jurnal ini, banyak sekali bimbingan yang didapatkan serta arahan dan bantuan dari pihak yang sangat mendukung. Oleh karena itu dengan segala kerendahan hati, diucapkan terima kasih yang sebesar-besarnya kepada Bapak Rudi Gunawan, SE., M.Si., selaku Ketua Sekolah Tinggi Manajemen Informatika Dan Komputer (STMIK) Triguna Dharma Medan. Bapak Dr. Zulfian Azmi, ST., M.Kom., selaku Wakil Ketua I Bidang Akademik STMIK Triguna Dharma Medan. Bapak Marsono, S.Kom., M.Kom., selaku Ketua Program Studi Sistem Informasi STMIK Triguna Dharma Medan. Bapak Kamil Erwansyah, S.Kom., M.Kom., selaku Dosen Pembimbing I yang telah memberikan saran, arahan dan dukungannya serta motivasi, sehingga penelitian ini dapat terselesaikan dengan baik dan tepat waktu. Ibu Hafizah, S.Kom., M.Kom., selaku Dosen Pembimbing II yang telah memberikan saran, arahan dan dukungannya serta motivasi, sehingga penelitian ini dapat terselesaikan dengan baik dan tepat waktu. Seluruh Dosen, Staff dan Pegawai di STMIK Triguna Dharma Medan.

REFERENSI

[1] A. Pengaruh, R. Car, L. D. R. Dan, B. Yang, and T. Di, "Analisis Pengaruh Rasio Car, Bopo, Ldr Dan Ukuran Perusahaan Terhadap Profitabilitas Bank Yang Terdaftar Di Bei," *E-Jurnal Akunt.*, vol. 4, no. 1, pp. 230–245, 2013.

[2] Y. Efni, "Pengaruh Suku Bunga Deposito, SBI, Kurs dan Inflasi terhadap Harga Saham Perusahaan Real Estate dan Property di Bei," *J. Ekon.*, vol. 17, no. 01, 2009.

[3] R. A. Azdy, "Tanda tangan Digital Menggunakan Algoritme Keccak dan RSA," *J. Nas. Tek. Elektro dan Teknol. Inf.*, vol. 5, no. 3, pp. 184–191, 2016, doi: 10.22146/jnteti.v5i3.255.

[4] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," *Inform. Mulawarman J. Ilm. Ilmu Komput.*, vol. 10, no. 1, p. 20, 2016, doi: 10.30872/jim.v10i1.23.

[5] B. Prishardoyo, "Analisis Faktor-Faktor Yang Mempengaruhi Volume Transaksi Pasar Uang Antar Bank Di Indonesia Tahun 1983–2007," vol. 3, no. 2, pp. 123–131, 2010, doi: 10.15294/jejak.v3i2.4655.

[6] R. Kurniawan, P. Studi, I. Komputer, U. Islam, N. Sumatera, and U. Medan, "Rancang Bangun Aplikasi Pengaman Isi File Dokumen Dengan RSA," *J. Ilmu Komput. dan Inform.*, vol. 01, no. November, pp. 46–52, 2017.

[7] L. S. Negara, J. Harsono, R. M. No, and J. Selatan, "Elektronik Pemerintahan Guna Mendukung E-Government," 2016.

[8] J. B. Sanger, "DESAIN DAN IMPLEMENTASI MEKANISME TANDA TANGAN DIJITAL DALAM PERTUKARAN DATA DENGAN HASH MD5 DAN ENKRIPSI / DEKRIPSI MENGGUNAKAN ALGORITMA RSA," vol. 12, no. 2, 2015.

[9] Z. Arifin, K. kunci, A. Rsa, K. Privat, and K. Publik, "Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman," *J. Inform. Mulawarman Progr. Stud. Ilmu Komput. Univ. Mulawarman*, vol. 4, no. 3, pp. 7–14, 2009.

[10] A. N. Agustina, Aryanti, and Nasron, "Pengamanan Dokumen Menggunakan Metode Rsa (Rivest Shamir Adleman) Berbasis Web," *Proceeding SENDI_U*, vol. 3, no. 3, pp. 14–19, 2017.

[11] E. R. Sardju, R. Magdalena, and R. D. Atmaja, "Implementasi Algoritma Rsa Untuk Enkripsi Dan Dekripsi Sms (short Message Service) Pada Ponsel Berbasis Android," *eProceedings Eng.*, vol. 2, no. 2, pp. 2435–2442, 2015.

Jurnal CyberTech
Vol., No., Agustus 2020, pp.
P-ISSN :
E-ISSN : ❒

BIOGRAFI PENULIS

	**Diky Pratama**, Pria kelahiran Kisaran, 31 Mei 1999, anak pertama dari dua bersaudara ini merupakan seorang mahasiswa STMIK Triguna Dharma yang sedang dalam proses menyelesaikan skripsi.
	**Kamil Erwansyah, S.Kom., M.Kom**, Beliau merupakan dosen tetap STMIK Triguna Dharma Medan dan aktif sebagai pengajar pada bidang ilmu Sistem Informasi.
	**Hafizah, S.Kom., M.Kom**, Beliau merupakan dosen tetap STMIK Triguna Dharma Medan dan aktif sebagai pengajar pada bidang ilmu Sistem Informasi.