PENERAPAN ALGORITMA RSA DALAM PENGAMANAN DATA TUNGGAKAN TAGIHAN AIR PELANGGAN DI PDAM TIRTANADI SUNGGAL

Disusun Sebagai Salah Satu Syarat Untuk Menempuh Ujian Akhir Memperoleh
Gelar Sarjana Komputer Pada Fakultas Sains & Teknologi
Universitas Pembangunan Panca Budi
Medan

SKRIPSI

OLEH :

NAMA	: PANDI PURNOMO
N.P.M	: 1514370003
PROGRAM STUDI	: SISTEM KOMPUTER

FAKULTAS SAINS & TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2019

ABSTRAK

PANDI PURNOMO

PENERAPAN ALGORITMA RSA DALAM PENGAMANAN DATA TUNGGAKAN TAGIHAN AIR PELANGGAN DI PDAM TIRTANADI SUNGGAL

2019

Bagi perusahaan data merupakan suatu informasi yang sangat penting, Hal ini sangat bergantung dari tipe usaha yang dijalakannya. Seperti halnya PDAM Tirtandi, Perusahaan Badan Usaha Milik Daerah tersebut tidak terlalu mementingkan masalah kerahasiaan data, contohnya mengenai data tunggakan pelanggan. Padahal dalam praktiknya data tunggakan pelanggan merupakan data yang sangat penting, karena di dalam data tersebut memuat informasi penting tentang identitas pelanggan. Jika data tersebut bocor ke pihak yang tidak bertanggung jawab, tentunya akan merugikan pihak PDAM dan pelanggan itu sendiri. Dengan alasan itulah maka penelitian ini dibuat bertujuan untuk menciptakan suatu sistem komputer berbasis *dekstop Programming*, kemudian dengan diterapkannya sistem tersebut maka data pelanggan yang bersifat rahasia dapat diamanakan.

Kata Kunci ***: Data, Kriptografi, PDAM Tirtanadi, RSA***

DAFTAR ISI

Halaman

BAB I

PENDAHULUAN

1.1 Latar Belakang

Informasi merupakan suatu data yang berguna karena bisa mendapatkan manfaat ekonomi atau manfaat lainnya. Setiap perusahaan pasti memiliki data yang nilainya sangat berharga. Hal ini sangat bergantung dari tipe usaha yang dijalakannya. Seperti halnya PDAM Tirtandi, Perusahaan Badan Usaha Milik Daerah tersebut tidak terlalu mementingkan masalah kerahasiaan data, seperti salah satu contohnya mengenai data tunggakan pelanggan. Padahal dalam praktiknya data tunggakan pelanggan PDAM Tirnadi merupakan data yang sangat penting, karena di dalam data tersebut memuat informasi penting tentang identitas pelanggan. Jika data tersebut bocor ke pihak yang tidak bertanggung jawab, tentunya akan merugikan pihak PDAM dan pelanggan itu sendiri.

Padahal banyak hal yang dapat dilakukan perusahaan dalam mengamankan data tunggakan pelanggan. Salah satunya dengan menggunakan kriptografi, kriptografi merupakan sebuah ilmu yang mempelajari bagaimana cara merahasiakan data dengan mengubah data asli (*plaintext*) menjadi kode-kode yang tidak dapat dimengerti (*Cipherteks*). Banyak sekali penelitian yang membahas masalah ini, baik dalam bentuk jurnal atau karya ilmiah lainya. salah satu kriptografi yang banyak digunakan dalam mengamankan data yaitu dengan menggunakan algoritma RSA. Seharusnya dengan banyak nya penelitian yang ada

pihak perusahaan dapat menjadikan penelitian - penelitian tersebut sebagai referensi mereka dalam mengamankan data tunggakan pelanggan mereka.

Namun sampai saat ini belum ada upaya dari isntansi terkait dalam hal ini adalah PDAM Tirtanadi sunggal dalam mengatasi masalah pengamanan data tunggakan tagihan air pelanggan mereka. Berdasarkan masalah diatas, penulis mencoba membarikan solusi yang dituangkan dalam sebuah penelitian dalam bentuk skripsi dengan judul **"Penerapan Algoritma RSA Dalam Pengaman Data Tunggakan Tagihan Air Pelanggan di PDAM Tirtanadi Sunggal"** Sehingga diharapkan penelitian ini dapat membantu PDAM Tirtanadi Sunggal dalam mengamankan data tunggakan tagihan air pelanggan mereka.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan di atas rumusan masalah yang harus dipecahkan yaitu :

1. Bagaimana menerapkan algoritma RSA dalam pengamanan data tunggakan tagihan air pelanggan di PDAM Tirtanadi Sunggal?
2. Bagaimana hasil dan penerapan algoritma RSA terhadap pengamanan data tunggakan tagihan air pelanggan di PDAM Tirtanadi Sunggal?

1.3 Batasan Masalah

Adapun batasan masalah yang akan dibahas dalam penelitian ini adalah sebagai berikut :

1. Penelitian ini hanya membahas pengamanan data tunggakan air pelanggan. Data yang akan di enkripsi adalah Nama, Alamat, Status, Tarif, Dan Jumlah Tunggakan.

2. Metode yang digunakan untuk pengamanan data tunggakan air pelanggan hanya dengan algoritma Rivest Shamir Adleman (RSA).
3. Bahasa yang digunakan dalam pembuatan aplikasi berbasis *Dekstop Programming* yaitu menggunakan VB.Net 10 (Visual Studio 2010).
4. Pada pencarian kunci RSA nilai p dan q hanya akan menggunakan bilangan prima antara 0 - 100.

1.4 Tujuan Penulisan

Adapun tujuan penelitian untuk pengamanan data tunggakan tagihan air pelanggan menggunakan algoritma Rivest Shamir Adleman (RSA) yaitu :

1. Untuk merancang aplikasi berbasis *Dekstop Programming* yang dapat digunakan untuk pengamanan data tunggakan tagihan air pelanggan di PDAM Tirtanadi Sunggal.
2. Untuk Mengetahui sistem yang telah di rancang sejauh mana kinerjanya dalam pengamanan data tunggakan tagihan air pelanggan di PDAM Tirtanadi Sunggal.

1.5 Manfaat Penulisan

Berdasarkan dari uraian diatas memberikan manfaat bagi perusahaan dan peneliti, adapun manfaat dari penelitian ini adalah :

1. Dapat membantu PDAM Tirtanadi Sunggal dalam pengamanan data tunggakan tagihan air pelanggan.
2. Dari penelitian tersebut diharapkan dapat memberikan solusi dalam menjaga data tunggakan air PDAM Tirtanadi Sunggal dari pihak-pihak yang tidak bertanggung jawab.

3. Dapat menjadi referensi bagaimana cara mengamankan data, dalam hal ini adalah data tunggakan tagihan air di PDAM Tirtanadi Sunggal menggunakan algoritma Rivest Shamir Adleman (RSA).

BAB II

LANDASAN TEORI

2.1 Keamanan Data

Pada umumnya data dikategorikan menjadi dua, yaitu data yang bersifat rahasia dan data yang tidak bersifat rahasia. Data yang sifatnya tidak rahasia biasanya tidak akan terlalu diperhatikan. Namun yang perlu diperhatikan adalah data yang bersifat rahasia, dimana setiap informasi yang ada didalamnya akan sangat berharga bagi pihak yang membutuhkan karena data tersebut dapat dengan mudah digandakan. Untuk mendapatkan informasi didalamnya biasanya dilakukan berbagai cara yang tidak sah (Permana Angga A dan Nurnaningsih Desi, 2018).

Informasi merupakan aset yang harus dilindungi keamanannya. Keamanan informasi dapat melindungi informasi dari berbagai ancaman untuk menjamin kelangsungan usaha, meminimalisasi kerusakan akibat terjadinya ancaman, serta mempercepat kembalinya investasi dan peluang usaha. Setiap individu dalam organisasi memiliki peran yang berbeda - beda terhadap informasi. Merupakan hal yang penting bagi seluruh anggota organisasi untuk memahami bagaimana peran dan tanggung jawab mereka terhadap informasi. Unsur utama yang menjadi subjek dari informasi adalah peran pengguna, pemilik, atau kustodian terhadap informasi (Islami Dian C, *et.al*, 2016).

2.1.1 Aspek Keamanan Data

Ada empat aspek utama dalam keamanan data dan dua aspek lain yang saling berkaitan yaitu (Putra Satria D dan Rifqi Muhammad, 2017) :

1. *Privacy/Confidentiality*, Usaha menjaga data informasi dari orang yang tidak berhak mengakses (memastikan bahwa data informasi pribadi kita tetap pribadi).
2. *Integrity*, Usaha untuk menjaga data atau informasi agar tidak diubah oleh orang yang tidak berhak.
3. *Authentication*, Usaha atau metode untuk mengetahui keaslian dari informasi. Misalnya, apakah informasi yang dikirim dibuka oleh orang yang benar (asli) atau layanan dari *server* yang diberikan benar berasal dari *server* yang dimaksud.
4. *Availability*, berhubungan dengan ketersedian informasi ketika dibutuhkan, Data yang diserang atau dijebol dapat mengubah atau meniadakan data yang sudah tersedia.
5. *Access Control*, berhubungan dengan cara pengaturan akses informasi dan pastinya berhubungan dengan klasifikasi data.
6. *Non-repudiation*, Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan perubahan data sehingga data yang diberikan valid.

2.2 Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu *kripto* dan *graphia*. *Kripto* artinya menyembunyikan, sedangkan *graphia* artinya tulisan. Sehingga kriptografi dapat diartikan sebagai ilmu yang

mempelajari tentang penyembunyian huruf atau tulisan sehingga membuat tulisan tersebut tidak dapat dibaca oleh orang yang tidak berkepentingan. Kriptografi mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi. Seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Algoritma kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang - orang yang tidak berhak atas pesan tersebut. Algoritma kriptografi terdiri dari tiga fungsi dasar, yaitu (Ginting Natalia F dan Ginting Misalina, 2017) :

1. Enkripsi

   Merupakan hal yang sangat penting dalam kriptografi, merupakan pengamanan data yang dikirimkan agar terjaga kerahasiaannya. Pesan asli disebut *plaintext*, yang diubah menjadi kode - kode yang tidak dimengerti. Enkripsi bisa diartikan dengan *cipher* (kode). Sama halnya dengan kita tidak mengerti akan sebuah kata maka kita akan melihatnya di dalam kamus atau daftar istilah. Beda halnya dengan enkripsi, untuk mengubah teks-asli ke bentuk teks-kode kita menggunakan algoritma yang dapat mengkodekan data yang kita inginkan.

2. Dekripsi

   Merupakan kebalikan dari enkripsi, pesan yang telah dienkripsi dikembalikan ke bentuk asalnya (teks-asli) disebut dengan dekripsi pesan. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan algoritma yang digunakan untuk enkripsi.

3. Kunci

   Untuk melakukan enkripsi dan dekripsi, kunci terbagi menjadi dua bagian. kunci privat (*private key*) yaitu kunci yang digunakan untuk mendekripsikan data. Kunci publik (*public key*) yaitu kunci yang digunakan untuk mengenkripsikan data.

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Dalam ilmu kriptografi, terdapat dua buah proses yaitu melakukan enkripsi dan dekripsi. Pesan yang akan dienkripsi disebut sebagai *plaintext* (teks biasa). Disebut demikian karena informasi ini dengan mudah dapat dibaca dan dipahami oleh siapa saja. Algoritma yang dipakai untuk mengenkripsi dan mendekripsi sebuah *plaintext* melibatkan penggunaan suatu bentuk kunci. Pesan *plaintext* yang telah dienkripsi (dikodekan) dikenal sebagai *ciphertext* (teks sandi) (Pabokory Fresly N, *et.al*, 2015).

Di dalam kriptografi kita akan sering menemukan berbagai istilah atau *terminology*. Beberapa istilah yang harus diketahui yaitu :

1. Pesan, *Plainteks*, dan *Cipherteks*

   Pesan (*message*) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah (*plaintext*) atau teks jelas (*cleartext*).

2. Pengirim dan Penerima

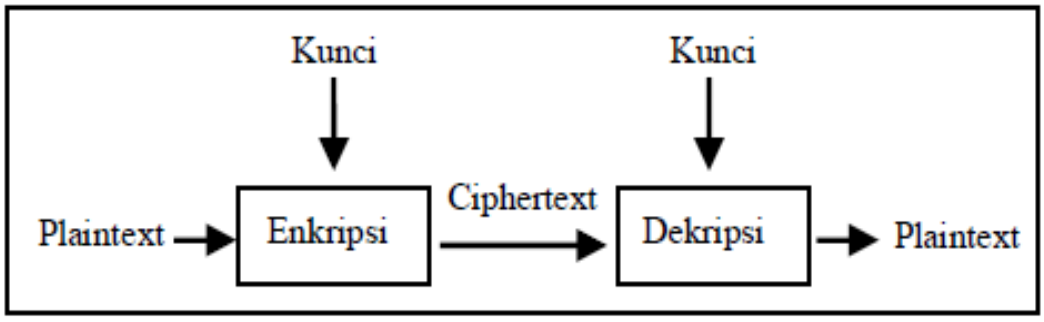
   Komunikasi data melibatkan pertukaran pesan antara dua entitas. Pengirim (*sender*) adalah entitas yang mengirim pesan kepada entitas lainnya. Penerima (*receiver*) adalah entitas yang menerima pesan.

3. Enkripsi dan dekripsi

   Proses menyandikan *plainteks* menjadi *cipherteks* disebut enkripsi (*encryption*). Sedangkan proses mengembalikan *cipherteks* menjadi *plainteks* semula disebut dekripsi (*decryption*).

4. *Cipher* dan kunci

   Algoritma kriptogarfi disebut juga *cipher*, yaitu aturan untuk enkripsi dan dekripsi, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Beberapa *cipher* memerlukan algoritma yang berbeda untuk enkripsi dan dekripsi. Konsep matematis yang mendasari algoritma kriptografi adalah relasi antara dua buah himpunan yang berisi elemen- elemen *plainteks* dan himpunan yang berisi *cipherteks*. Enkripsi dan dekripsi merupakan fungsi yang memetakan elemen-elemen antara dua himpunan tersebut.



Gambar 2.1 Skema Enkripsi dan Deskripsi Dengan Menggunakan Kunci

(Pabokory Fresly N, *et.al*, 2015)

Kriptografi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan. Ketika suatu pesan dikirim dari suatu tempat ke tempat lain, isi pesan tersebut mungkin dapat disadap oleh pihak lain yang tidak berhak untuk mengetahui isi pesan tersebut. Untuk menjaga pesan, maka pesan tersebut dapat diubah menjadi sebuah kode yang tidak dapat dimengerti pihak lain (Amin Miftakul, 2016).

2.3 Algoritma RSA

Dari banyak algoritma kriptografi yang ada, algotirma yang paling populer adalah RSA. Algoritma RSA merupakan algoritma kriptografi asimetris dimana kunci enkripsi tidak sama dengan kunci dekripsinya. Algortima RSA dibuat oleh tiga orang peneliti dari MIT (Massachussets Institute of Technology) pada tahun 1976. Nama RSA merupakan singkatan dari nama tiga orang penemunya, yaitu Ron Rivest, Adi Shamir, dan Len Adleman (Ginting Natalia F dan Ginting Misalina, 2017).

Algoritma RSA ini mengambil dua bilangan prima secara acak yang akan dijadikan kunci sehingga didapat dua kunci yaitu kunci publik (*public key*) dan kunci privat(*private key*) (Adianson Niko, *et.al*, 2015).

Diketahui bahwasanya :

1. *p* dan *q* adalah bilangan prima sembarang
2. n = modulus
3. e = *public key*
4. d = *private key*
5. c = *chipertext*

6. m = *plaintext*

2.3.1 Pembangkit Kunci RSA

Dalam membuat suatu sandi, RSA mempunyai cara kerja dalam membuat kunci publik dan kunci privat adalah sebagai berikut (Muchlis Budi S, *et.al*, 2017) :

1. Pilih dua bilangan prima sembarang p dan q.
2. Hitung $n = p \,.\, q$
3. Hitung $\varphi(n) = (p - 1)(q - 1)$.
4. Pilih kunci publik e, dengan syarat e > 1 dan gcd $\varphi(n)$ kemudian gcd $(e, \varphi(n)) = 1$.
5. Bangkitkan kunci privat dengan menggunakan persamaan :

   $d.e \; mod \; \varphi(n) = 1$ .....(1)

Sehingga hasil dari algoritma di atas adalah :

1. Kunci publik adalah pasangan (e, n).
2. Kunci privat adalah pasangan (d, n).

Contoh: Misalkan A akan membangkitkan kunci publik dan kunci privat miliknya. A memilih p = 47 dan q = 71 (keduanya bilangan prima). Selanjutnya A menghitung :

$$n = p \,.\, q$$

$$n = 47 \,.\, 71 = 3337$$

$$\varphi(n) = (p - 1)\,(q - 1)$$

$$\varphi(n = (47 - 1)\,(71 - 1) = 3220$$

A memilih kunci publik e = 79 karena relatif prima dengan 3320. A mengumumkan nilai e dan n. Selanjutnya A menghitung kunci privat (d), sehingga dituliskan berdasarkan persamaan (1) :

$d.79\ mod\ 3220 = 1$

Dengan mencoba nilai-nilai d = 1, 2, 3, …, diperoleh nilai d yaitu 1019.

1.79 *mod* 3220 = 79

2.79 *mod* 3220 = 158

3.79 *mod* 3220 = 237

.

.

.

1019.79 *mod* 3220 = 1

Kunci privat digunakan untuk mendekripsi pesan dan harus dirahasiakan A. Jadi, perhitungan kunci ini menghasilkan pasangan kunci:

a. Kunci publik (e = 79, n = 3337)

b. Kunci privat (d = 1019, n = 3337)

Pada RSA hanya diberikan kunci publik yaitu e dan n. Sedangkan kunci privat d dirahasiakan. Selanjutnya, karena kunci enkripsi e diumumkan (tidak rahasia), maka kunci dekripsi d dapat dihitung dari persamaan (1). Kemudian dilakukan dekripsi *ciphertext* c menjadi *plaintext* m menggunakan persamaan (2).

2.3.2 Enkripsi RSA

Proses enkripsi pesan sebagai berikut (Muchlis Budi S, *et.al,* 2017) :

1. Ambil kunci publik penerima pesan e dan n.
2. Nyatakan plaintext m menjadi blok-blok m_1, m_2, dst.
3. Setiap blok m_i dienkripsi menjadi blok c_i dengan rumus :

$c_i = m_i^e \ mod \ n$.....(2)

Contoh: Misalkan B mengirim pesan kepada A. Pesan (*plaintext*) yang akan dikirim ke A adalah :

m = BUDI

B mengubah m ke dalam desimal pengkodean ASCII dan sistem akan memecah m menjadi blok – blok yang lebih keci.

m_1= 66

m_2 = 85

m_3 = 68

m_4= 73

B mengetahui kunci publik A adalah e = 79 dan n = 3337. B dapat mengenkripsi setiap blok *plaintext* sebagai berikut:

$c_1 = 66^{79} \ mod$ 3337 = 795

$c_2 = 85^{79} \ mod$ 3337 = 3048

$c_3 = 68^{79} \ mod$ 3337 = 2753

$c_4 = 73^{79} \ mod$ 3337 = 725

Maka, *ciphertext* yang dihasilkan adalah c = 795,3048,2753,725

2.3.3 Dekripsi RSA

Berikut adalah proses Dekripsi pesan yaitu : (Muchlis Budi S, *et.al*, 2017) :

1. Ambil kunci privat penerima pesan d dan n. Nyatakan *plaintext c* menjadi blok-blok c_1, c_2, dst.
2. Setiap blok c_i didekripsi menjadi blok m_i dengan rumus :

$$m_i = c_i{}^d \ mod \ n \quad \text{.....(3)}$$

Contoh: Dengan kunci privat d = 1019, *chiperteks* yang telah dibagi menjadi blok-blok *cipher*, *c* = 795,3048,2753,725. Kembali diubah ke dalam *plaintext* : BUDI

$m_1 = 795^{1019} \ mod \ 3337 = 66$

$m_2 = 3048^{1019} \ mod \ 3337 = 85$

$m_3 = 2753^{1019} \ mod \ 3337 = 68$

$m_4 = 735^{1019} \ mod \ 3337 = 73$

Sehingga *plaintext* yang dihasilkan m = BUDI

2.3.4 ASCII

ASCII (American Standard Code of Information Interchange) merupakan standar internasional dalam kode huruf dan simbol seperti HEX dan UNICODE yang memetakan kode numerik seperti a~z atau karekter simbol seperti '@'. Kode ASCII mempunyai komposisi bilangan biner sebesar 7 bit, namun ASCII disimpan sebagai 8 bit dengan menambahkan nilai 0 sebagai nilai signifikan paling tinggi. *Encoding* pada ASCII menggunakan 3 tipe bilangan bulat yaitu decimal (2^2), oktadesimal (2^8) dan hexadecimal (2^{16}) (Zainuddin Muhammad A dan Mulyana Dadang I, 2016).

Tabel 2.1 Tabel ASCII

Des	Chr	Des	Chr	Des	Chr	Des	Chr
0	NULL	32	(Space)	64	@	96	`
1	SOH	33	!	65	A	97	a
2	STX	34	“	66	B	98	b
3	ETX	35	#	67	C	99	c
4	EOT	36	$	68	D	100	d
5	ENQ	37	%	69	E	101	e
6	ACK	38	&	70	F	102	f
7	BEL	39	‘	71	G	103	g
8	BS	40	(	72	H	104	h
9	HT	41	)	73	I	105	i
10	LF	42	*	74	J	106	j
11	VT	43	+	75	K	107	k
12	FF	44	,	76	L	108	l
13	CR	45	-	77	M	109	m
14	SO	46	.	78	N	110	n
15	SI	47	/	79	O	111	o
16	DLE	48	0	80	P	112	p
17	DC1	49	1	81	Q	113	q
18	DC2	50	2	82	R	114	r
19	DC3	51	3	83	S	115	s
20	DC4	52	4	84	T	116	t
21	NAK	53	5	85	U	117	u
22	SYN	54	6	86	V	118	v
23	ETB	55	7	87	W	119	w
24	CAN	56	8	88	X	120	x
25	EM	57	9	89	Y	121	y
26	SUB	58	:	90	Z	122	z
27	ESC	59	;	91	[	123	{
28	FS	60	<	92	\	124	|
29	GS	61	=	93	]	125	}
30	RS	62	>	94	^	126	~
31	US	63	?	95	_	127	Del

Sumber : Zainuddin Muhammad A dan Mulyana Dadang I, 2016

2.4 Pengenalan UML

UML *(Unified Modeling Language)* adalah bahasa spesifikasi standar untuk mendokumentasikan, menspesifikasikan dan membangun sistem *software*. Pada perkembangan teknologi perangkat lunak, diperlukan adanya bahasa yang

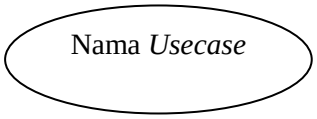
digunakan untuk memodelkan perangkat lunak yang akan dibuat dan perlu adanya standarisasi agar orang diberbagai negara dapat mengerti pemodelan perangkat lunak (Munawar, 2018).

2.4.1 Use Case Diagram

Use case adalah deskripsi fungsi dari sebuah sistem dari perspektif pengguna. *Use case* bekerja dengan cara mendeskripsikan tipikal interaksi antar *user* (pengguna) sebuah sistem dengan sistemnya sendiri melalui sebuah cerita bagaimana sebuah sistem dipakai. Urutan langkah-langkah yang menerangkan antara pengguna dan sistem disebut skenario. Setiap skenario mendeskripsikan urutan kejadian. Setiap urutan diinisialisasi oleh orang, sistem yang lain, perangkat keras atau urutan waktu (Munawar, 2018).

Berikut adalah simbol-simbol yang ada pada *Use Case Diagram* :

Tabel 2.2 Simbol-Simbol *Use Case*

No	Simbol	Deskripsi
1	*Use Case* 	Fungsionalitas yang disediakan sistem sebagai unit-unit yang saling bertukar pesan antar unit atau aktor, biasanya dinyatakan dengan menggunakan kata kerja di awal frasa nama *use case*.

Tabel 2.2 Simbol-Simbol *Use Case* (Lanjutan)

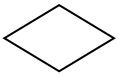
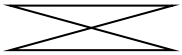
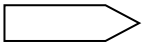
No	Simbol	Deskripsi
2	Aktor */Actor*  Nama *Actor*	Orang, proses, atau sistem lain yang berinteraksi dengan sistem informasi yang akan dibuat di luar sistem informasi yang akan dibuat itu sendiri, jadi walaupun simbol dari aktor adalah gambar orang, tapi aktor belum tentu merupakan orang, biasanya dinyatakan menggunakan kata benda di awal frase nama aktor.
3	Asosiasi/*Association* ————	Komunikasi antara aktor dan *use case* yang berpartisipasi pada *use case* atau *use case* memilikiinteraksi dengan aktor.
4	Ekstensi/*Extend* <<extend>> ·····▶	Relasi *use case* tambahan ke sebuah *use case* dimana *use case* yang ditambahkan dapat berdiri sendiri walau tanpa *use case* tambahan itu, mirip dengan prinsip *inheritance* pada pemrograman berorientasi objek, biasanya *use case* tambahan memiliki nama depan yang sama dengan *use case* yang ditambahkan, arah panah menuntuk pada *use case* yang dituju.
5	Menggunakan/*Include/Uses* <<*include*>> ·····▶	Relasi *use case* tambahan ke sebuah *use case* dimana *use case* yang ditambahkan memerlukan *use case* ini untuk menjalankan fungsinya.

Sumber: *Rekayasa Perangkat Lunak (Rosa, 2014)*

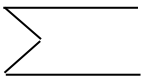
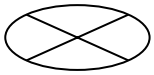
2.4.2 *Activity Diagram*

Activity diagram adalah bagian penting dari UML yang menggambarkan aspek dinamis dari sistem. Logika prosedural, proses bisnis dan aliran kerja suatu bisnis bisa dengan mudah dideskripsikan dalam *activity diagram. Activity diagram* mempunya peran seperti halnya *flowchart*, akan tetapi perbedaannya dengan *flowchart* adalah *activity diagram* bisa mendukung perilaku paralel sedangkan *flowchart* tidak bisa (Munawar, 2018).

Tabel 2.3 Simbol-Simbol *Activity Diagram*

No	Simbol	Keterangan
1		Titik awal
2		Titik Akhir
3		*Activity*
4		Pilihan untuk mengembalikan keputusan
5		*Fork* : digunakan untuk menunjukkan kegiatan yang dilakukan secara paralel atau untuk menggabungkan dua kegiatan paralel menjadi satu
6		Rake : menunjukkan adanya dekomposisi
7		Tanda waktu
8		Tanda pengiriman

Tabel 2.3 Simbol-Simbol *Activity Diagram* (Lanjutan)

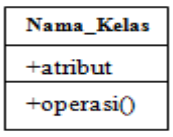
No	Simbol	Keterangan
9		Tanda penerimaan
10		Aliran akhir (*Flow Final*)

Sumber : Munawar, 2018

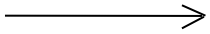
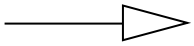
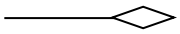
2.4.3 *Class diagram*

Class diagram adalah *diagram* statis. Ini mewakili pandangan statis dari suatu aplikasi. *Class diagram* tidak hanya digunakan untuk memvisualisasika, menggambarkan, dan mendokumentasikan berbagai aspek sistem tetapi juga untuk menbangun kode eksekusi (*executable code*) dari aplikasi perangkat lunak (Munawar, 2018).

Tabel 2.4 Simbol-Simbol *Class Diagram*

No	Gambar	Keterangan
1	Kelas 	Kelas pada struktur sistem
2	Antarmuka/*Interface*  nama_interface	Sama dengan konsep *interface* dalam pemrograman beroirentasi objek
3	Asosiasi/*Association*	Relasi antarkelas dengan makna umum, asosiasi biasanya juga disertai dengan *multiplicity*

Tabel 2.4 Simbol-Simbol *Class Diagram* (Lanjutan)

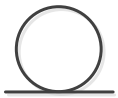
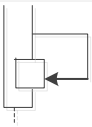
No	Gambar	Keterangan
4	Asosiasi Berarah/*Directed Association* 	Relasi antarkelas dengan makna kelas yang satu digunakan oleh kelas yang lain, asosiasi biasanya juga disertai dengan *multiplicity*
5	*Generalisasi* 	Relasi antarkelas dengan makna generalisasi-spesialisasi (umum - khusus)
6	Agregasi/*Aggregation* 	Relasi antarkelas dengan makna semua-bagian (*whole-part*)

Sumber : Rosa, 2014

2.4.4 *Squence Diagram*

Sequence Diagram adalah *tool* yang sangat populer dalam pengembangan sistem informasi secara *object-oriented* untuk menampilkan interaksi antar *object*. Atau dapat disimpulkan bahwa *sequence diagram* adalah sebuah *tool* yang digunakan dalam pengembangan sistem(Heriyanto Yunahar, 2018).

Table 2.5 Simbol – Simbol *Squence Diagram*

Keterangan	Simbol
Entity Class, merupakan bagian dari sistem yang berisi kumpulan kelas berupa entitas-entitas yang membentuk gambaran awal sistem dan menjadi landasan untuk menyusun basis data	
Boundary Class, berisi kumpulan kelas yang menjadi *interfaces* atau interaksi antara satu atau lebih aktor dengan sistem, seperti tampilan *form entry* dan *form* cetak	
Control class, suatu objek yang berisi logika aplikasi yang tidak memiliki tanggung jawab kepada entitas, contohnya adalah kalkulasi dan aturan bisnis yang melibatkan berbagai objek	
Message, simbol mengirim pesan antar *class*	
Recursive, menggambarkan pengiriman pesan yang dikirim untuk dirinya sendiri	
Activation,mewa kili sebuah eksekusi operasi dari objek, panjang kotak ini berbanding lurus dengan durasi aktivasi sebuah operasi	
Lifeline, garis titik-titik yang terhubung dengan objek, sepanjang *lifeline* terdapat *activation*	

Sumber : Hendini, 2016

2.5 Aplikasi Pemrograman Visual

Visual Studio 2010 merupakan suatu perangkat lunak yang dapat digunakan untuk pengembangan berbagai macam aplikasi yang memiliki berbagai macam tipe antara lain aplikasi *desktop* (*Windows Form, CommandLine* (*Console*)), Aplikasi *Web*, *Windows Mobile* (*Poket PC*).

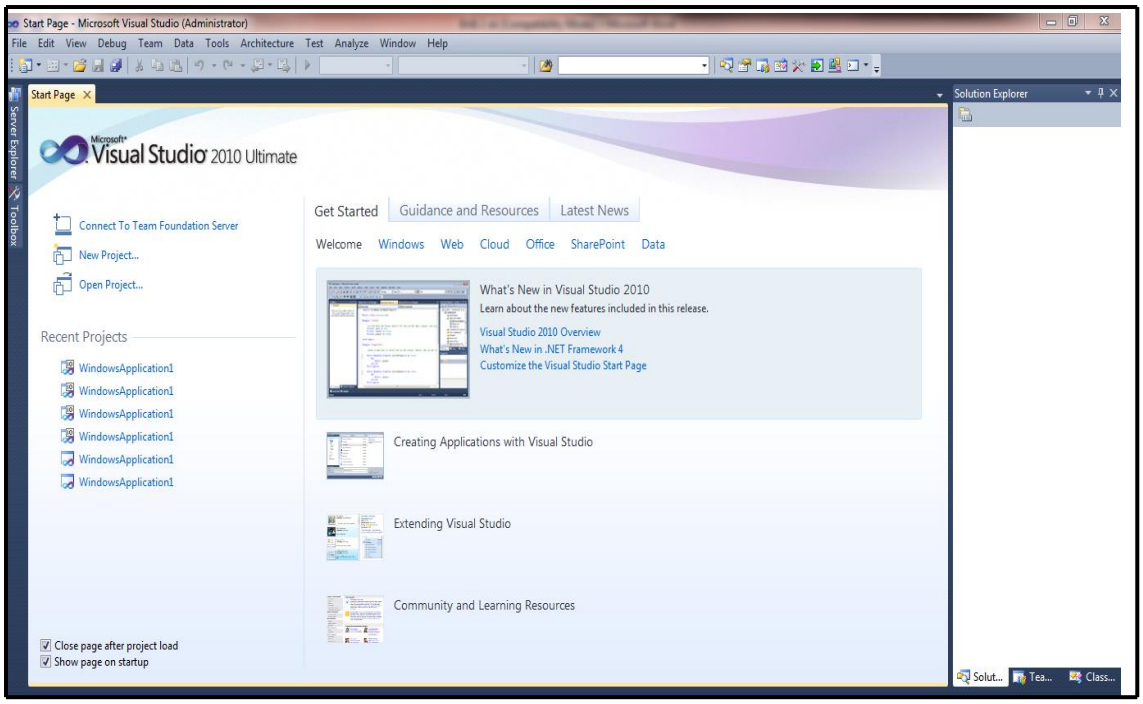
Visual Studio 2010 memiliki lebih dari satu kompiler, SDK (*Software Development Kid*), dan Dokumentasi Tutorial (*MSDN Library*). Kompiler yang

dimasukkan kedalam Visual Studio 2010 antara lain *Visual Basic, Visual C#, Visual C++, Visual InterDev, Visual J++,Visual F#, dan Visual Source Safe*, dan banyak yang lainnya. Dan semua itu sudah terpaket dan diperuntukkan kedalam *platform .Net Framework* 4.0 atau versi yang lebih tinggi.

Visual studio ini dapat digunakan untuk membuat aplikasi yang berbasis *desktop* yang merupakan *platform windows*, namun juga dapat dijalankan dalam bentuk *Microsoft Intermediate Language* diatas *.Net Framework*. Selain itu *Visual Studio* juga dapat digunakan untuk membuat aplikasi yang dapat dijalankan diatas *windows mobile* yang berjalan diatas *.Net Compact Framework* (Yesputra, 2017).

Visual Studio 2010 terbagi menjadi beberapa tipe diantaranya :

1. *Visual Studio* 2010 *Express Edition* yang bisa digunakan secara gratis tanpa memberikan royalti kepada *Microsoft Inc*.
2. *Visual Studio Standard Edition*
3. *Visual Studio* 2010 *Professional Edition*
4. *Visual Studio* 2010 *Ultimate Edition*

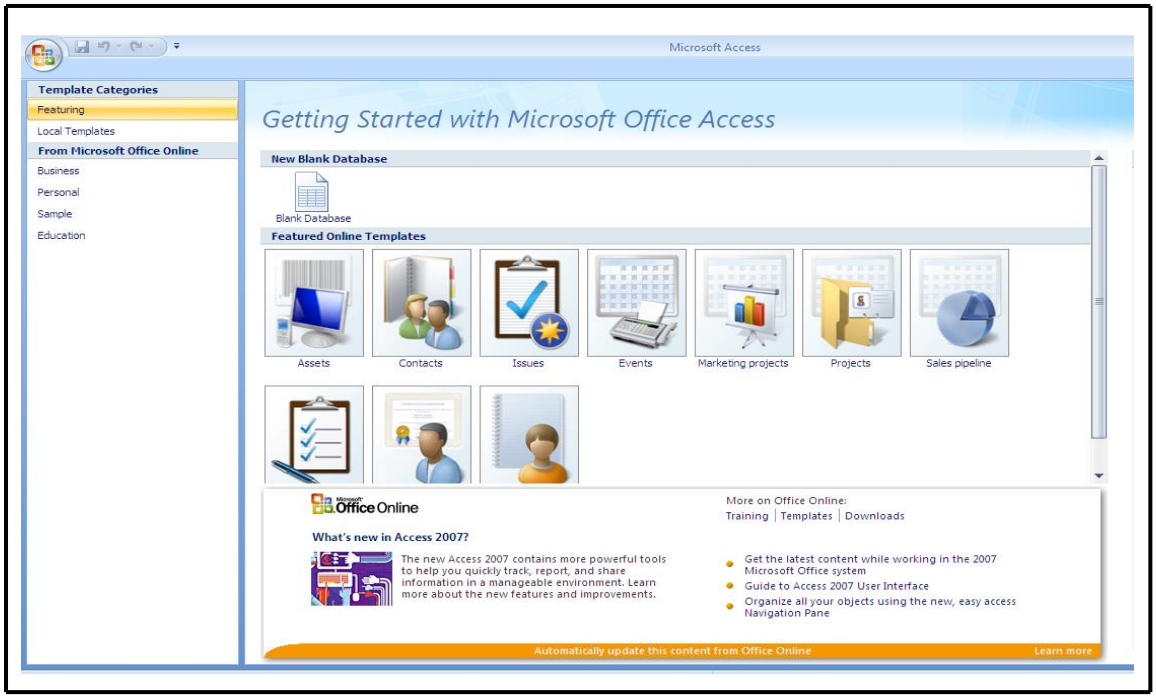


Gambar 2.2 *IDE Visual Studio* 2010

2.6 *Database Access*

Database adalah kumpulan fakta-fakta sebagai representasi dari dunia nyata yang saling berhubungan dan mempunyai arti tertentu. *Database* adalah kumpulan data yang terdiri atas satu atau lebih tabel yang terintegrasi satu sama lain, di mana setiap pemakai *(user)* diberi wewenang (*otorisasi*) untuk dapat mengakses (mengubah, menghapus, menganalisis, menambah, dan memperbaiki) data dalam tabel-tabel tersebut (Elizabeth dan Darmawan H, 2015).

Microsoft Access dikenal sebagai program basis data komputer relasional yang biasanya digunakan untuk mendesain, membuat serta mengelolah berbagai jenis data dengan kapasitas yang cukup besar (Agency Beranda, 2015).



Gambar 2.3 Tampilan awal *Microsoft Access*

2.7 Aplikasi Pembuatan Laporan

Crystal Report merupakan peranti standar untuk pembuatan laporan pada sistem operasi *Windows*, dimana cetakan (*template*) laporan yang dihasilkan dapat disertakan pada banyak bahasa pemrograman (Elizabeth dan Darmawan H, 2015).

Crystal Report terdiri dari tiga bagian utama, yaitu (Elizabeth dan Darmawan H, 2015):

1. *Toolbox*, yang berfungsi untuk menambahkan objek-objek ke dalam *report designer*
2. *Field Explorer*, yang berfungsi untuk menampilkan daftar *field*, formula, dan pernyataanpernyataan SQL serta yang lainnya.
3. *Report Designer*, yang berfungsi untuk meletakkan objek-objek yang digunakan pada laporan.

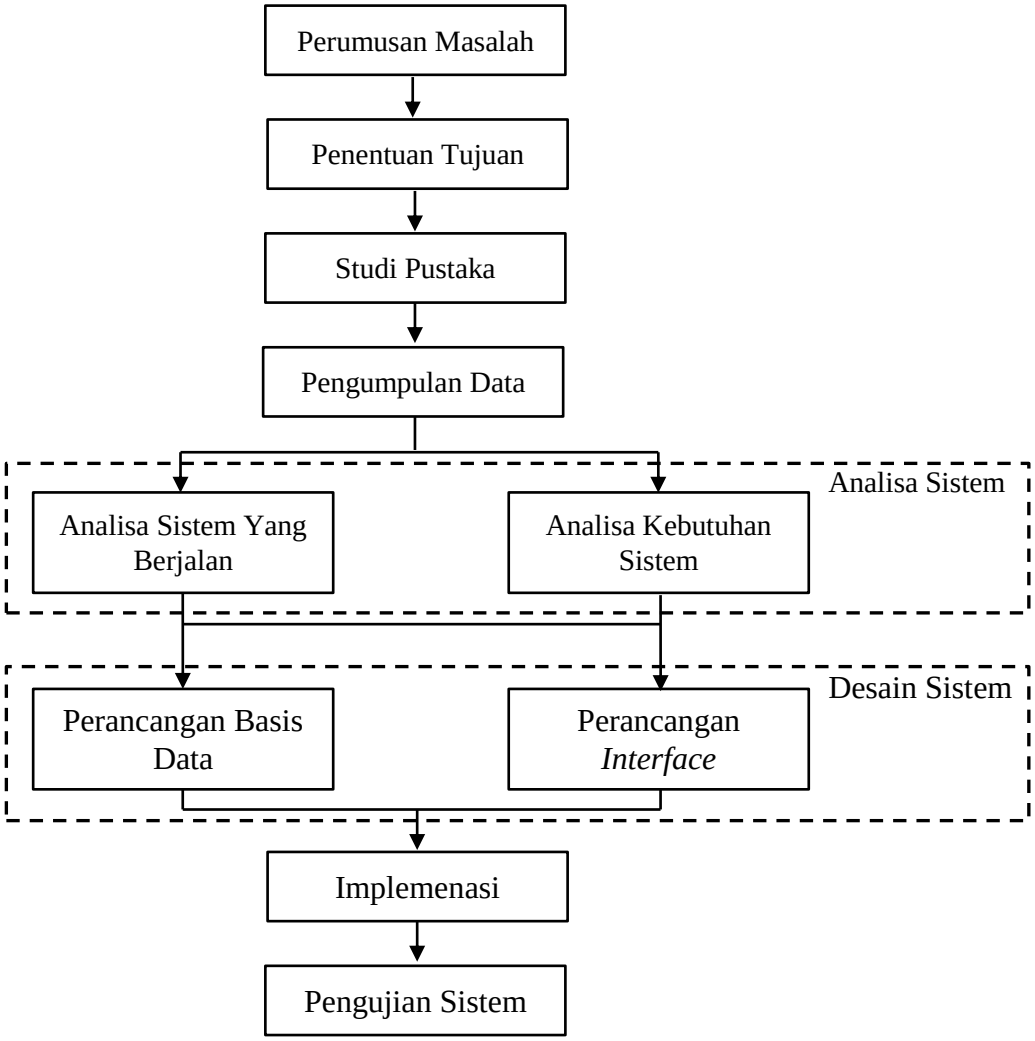
Gambar 2.4 Tampilan awal *Crystal Report*

BAB III

METODE PENELITIAN

3.1 Tahapan Penelitian

Adapun tahapan penelitian dalam memperoleh data yang digunakan dalam penelitian ini adalah :



Gambar 3.1 Tahapan Penelitian

Berdasarkan gambar di atas, berikut merupakan keterangan mengenai tahapan penelitian yaitu :

1. Perumusan masalah

   Merupakan bentuk pernyataan atau pertanyaan yang jelas mengenai penelitian

2. Penentuan tujuan

   Penentuan tujuan ini memperkuat tentang perlunya dilaksanakan suatu penelitian sehingga pemecahan masalah yang diuraikan pada perumusan masalah dapat dicapai setelah penelitian selesai dilakukan.

3. Studi pustaka

   Studi pustaka merupakan hal yang mendukung sebagai landasan teori penelitian dalam membahas penelitian yang sedang dilakukan.

4. Pengumpulan data

   Merupakan kegiatan mengumpulkan data yang diambil langsung dari objek penelitian untuk menjawab permasalahan.

5. Analisa sistem

   Sebelum merancang sebuah sistem, tahapan yang terlebih dahulu harus dilakukan adalah dengan menganasisa sistem yang ingin dibuat. Sistem yang harus dianalisa yaitu :

   a. Analisa sistem yang berjalan
   b. Analisa kebutuhan sistem

6. Desain sistem

   Desain sistem adalah tahap dari kebutuhan yang dianalisa dalam bentuk yang lebih mudah dimengerti. Yaitu dengan cara menampilkan kedalam *Use*

Case Diagram, *Activity Diagram*, *Class Diagram*, dan mengoneksikan aplikasi berbasis *Dekstop Programming*. Berikut ini adalah yang merupakan desain sistem, yaitu:

a. Perancangan Basis Data

b. Perancangan *Interface*

7. Implementasi,

   Merupakan penerapan sistem yang telah di rancang berdasarkan penelitian yang dilakukan.

8. Pengujian sistem,

   Pengujian terhadap sistem yang telah dirancang apakah semua berjalan sesuai dengan yang di inginkan.

3.2 Metode Pengumpulan Data

Dalam penelitia ini terdapat metode yang digunakan dalam pengumpulan data yaitu :

1. Penelitian Lapangan (*field research*)

   Pada Metode ini, dilakukan penelitian dengan cara mengumpulkan data secera langsung dari perusahaan dengan cara :

   a. Observasi

      Melakukan pengamatan secara langsung dengan cara mencari data – data secara langsung yang terdapat pada arsip perusahaan.

   b. Dokumentasi

      Melakukan pengumpulan data yang dibutuhkan dalam penelitian yang diambil langsung dari arsip perusahaan.

c. Wawancara

Melakukan komunikasi secara langsung kepada karyawan perusahaan mengenai data yang dibutuhkan dalam penelitian ini.

3.3 Analisa Sistem Sedang Berjalan

Sistem ini dibangun untuk mengamankan data tunggakan tagihan air di PDAM Tirtanadi Sunggal. Dalam hal ini proses tersebut menggunakan metode RSA. Melalui proses perhitungan metode RSA (*Rivest, Shamir,* dan *Adleman*) dilakukan dengan membangkitkan kunci RSA, melakukan enkripsi dan dekripsi yang menjadi penilaian dalam pengaman data tunggakan tagihan air yaitu data apa saja yang harus diamankan.

Kebijakan atau keputusan yang dilakukan oleh Pimpinan PDAM Tirtanadi Sunggal untuk mengamankan setiap data tunggakan tagihan air yang dikerjakan perusahaan adalah bentuk pelayanan kepada pelanggan untuk memberikan keamanan dan kenyamanan karena ada beberapa data-data tunggakan tagihan air yang bersifat rahasia. Maka dari itu untuk mengatasi permasalahan dalam mengamankan data tunggakan tagihan air di PDAM Tirtanadi Sunggal, diperlukan suatu analisis untuk mengatasi masalah tersebut.

Analisa tersebut berupa kriptografi berbasis komputer yang mengimplemtasikan metode RSA. Dengan ketersediaan data tunggakan tagihan air yang lengkap, maka data yang bersifat rahasi tersebut dapat diamankan dengan membangkitkan kunci RSA, melakukan enkripsi dan dekripsi.

3.4 Rancangan Sistem

Pada penelitian ini akan dibangun sebuah sistem yang dapat mengamankan data tunggakan tagihan air pelanggan menggunakan metode RSA, Berikut ini adalah rancangan sistem tersebut:

3.4.1 Algoritma Sistem

Algoritma sistem merupakan suatu tahapan yang dilakukan sebelum proses mengamankan data tunggakan tagihan air di PDAM Tirtanadi Sunggal. Adapun algoritma sistem penyelesaian dengan metode RSA adalah sebagai berikut:

1. Membangkitkan Kunci RSA.
    1. Pilih dua bilangan prima sembarang, p dan q.
    2. Hitung $n = p \,.\, q$
    3. Hitung $\varphi(n) = (p - 1)(q - 1)$.
    4. Pilih kunci publik e, dengan syarat e > 1 dan gcd $\varphi(n)$ kemudian gcd $(e, \varphi(n)) = 1$.
    5. Bangkitkan kunci privat dengan menggunakan rumus

       $d.e \; mod \; \varphi(n) = 1$
2. Melakukan Enkripsi Data
    1. Ambil kunci publik penerima pesan e dan n (modulus).
    2. Nyatakan *plaintext* m menjadi blok-blok m_1, m_2, dst.
    3. Setiap blok m_i dienkripsi menjadi blok c_i dengan rumus :

       $c_i = m_i^e \; mod \; n$

3. Melakukan Dekripsi Data

1. Ambil kunci privat penerima pesan d, dan n (modulus). Nyatakan *plaintext* c menjadi blok-blok c_1, c_2, dst.
2. Setiap blok c_i didekripsi menjadi blok m_i dengan rumus :

   $m_i = c_i{}^d \bmod n$

Berikut ini adalah data tunggakan tagihan air yang di dapat dari PDAM Tirtanadi Sunggal, yang akan diamankan. Dalam pengujiannya, sebagai contoh data yang akan diamankan adalah data nama pelanggan. Berikut ini adalah algoritma penyelesaiannya:.

Tabel 3.1. Data Tunggakan Tagihan Air Pelanggan PDAM Tirtanadi Sunggal

NPA	719140014
Nama	Hawani
Alamat	Jl. Pinang Baris Gg. Wakaf Pondok Indah No. A9
Tarif	RT-4
Status	Aktif
Jumlah Tunggakan	Rp. 535.606,12

Sumber : PDAM Tirtanadi Sunggal (2019)

3.4.2 Pembangkit Kunci RSA

Untuk menggunakan RSA terlebih dahulu pendeskripsi membangkitkan sepasang kunci yaitu kunci publik dan kunci privat. Hal pertama yang dilakukan algoritma pembangkit kunci adalah membangkitkan 2 bilangan prima besar. Berikut ini algoritma penyelesaiannya:

1. Pilihlah bilangan prima dengan sembarang, dalam pemilihan ini, di pilih nilai prima (p) = 73 dan nilai (q) = 83.

2. Untuk mencari nilai dari kedua bilangan tersebut, maka dilakukan perkalian

   *n= p * q*

   *n= 73 * 83 = 6059*

3. Hitung (*phi*) *n*= (*p-1*) (q-1)

   *n= 72 * 82 = 5904*

4. Pilih nilai *e* dengan syarat *e* > 1 dan *greatest comman divisior* (*e, 5904*) = 1

   Nilai *e* yang diambil adalah 79.

   Bukti:

   (79, 5904)

   5904 mod 79 = 58

   79 mod 58 = 21

   58 mod 21 = 16

   21 mod 16 = 5

   16 mod 5 = 1

5. Sehingga *d.e* mod n =1

   *d * 79 mod 5904 =1*

   d = 4783

   Bukti:

   4783 * 79 mod *5904* = 1

   Sehingga pasangan kunci yang didapat adalah :

   Kunci enkripsi (*public key*)(*e,n*) = (79, 6059) dan

   Kunci dekripsi (*private key*)(*d,n*) = (4783, 6059)

3.4.3 Proses Enkripsi Data

Setelah didapat nilai dari kunci enkripsi (*public key*), maka selanjutnya adalah melakukan enkripsi data *plaintext* M = Hawani

Pertama yang harus dilakukan adalah merubah *plaintext* menjadi format ASCII, berikut ini adalah penyelesaiannya:

Plaintext : H a w a n i

ASCII : 72 97 119 97 110 105

Kemudian m dipecah menjadi tiap karakter *plaintext*. Berikut ini adalah tebel m_i:

Tabel 3.2. Karakter m_i dan Kode ASCII untuk *Plaintext* Hawani

m_i	**Keterangan**	**Kode ASCII**
m_1	H	72
m_2	a	97
m_3	w	119
m_4	a	97
m_5	n	110
m_6	i	105

Setelah dibagi perkarakater, selanjutnya dienkripsi dengan rumus $c_i = m_i^e \ mod \ n$, yaitu sebagai berikut:

C_1 = 72^{79} mod 6059 = 802

C_2 = 97^{79} mod 6059 = 4283

C_3 = 119^{79} mod 6059 = 3677

C_4 = 97^{79} mod 6059 = 4283

C_5 = 110^{79} mod 6059 = 588

C_6 = 105^{79} mod 6059 = 3614

Tabel 3.3. Karakter *Ci* dan Kode ASCII untuk *Plaintext* Hawani

C_i	**Kode**
C_1	802
C_2	4283
C_3	3677
C_4	4283
C_5	588
C_6	3614

Maka, setelah di enkripsi hasilnya yaitu, 802,4283,3677,4283,588,3614.

3.4.4 Proses Dekripsi Data

Proses dekripsi adalah proses untuk mengembalikan ke bentuk semula (*plaintext*), setelah *chipertext* dari kata Hawani didapatkan. Untuk merubah kembali menjadi *plaintext* yaitu melakukan dekripsi dengan rumus $m_i = c_i{}^d \ mod \ n$. Berikut ini adalah penyelesaiannya:

m_1 = 802^{4783} mod 6059 = 72

m_2 = 4283^{4783} mod 6059 = 97

m_3 = 3677^{4783} mod 6059 = 119

m_4 = 4283^{4783} mod 6059 = 97

m_5 = 588^{4783} mod 6059 = 110

m_6 = 3614^{4783} mod 6059 = 105

Maka, setelah didekripsikan hasilnya yaitu, 72 97 119 97 110 105 dalam karakter ASCII adalah:

ASCII : 72 97 119 97 110 105

Karakter : H a w a n i

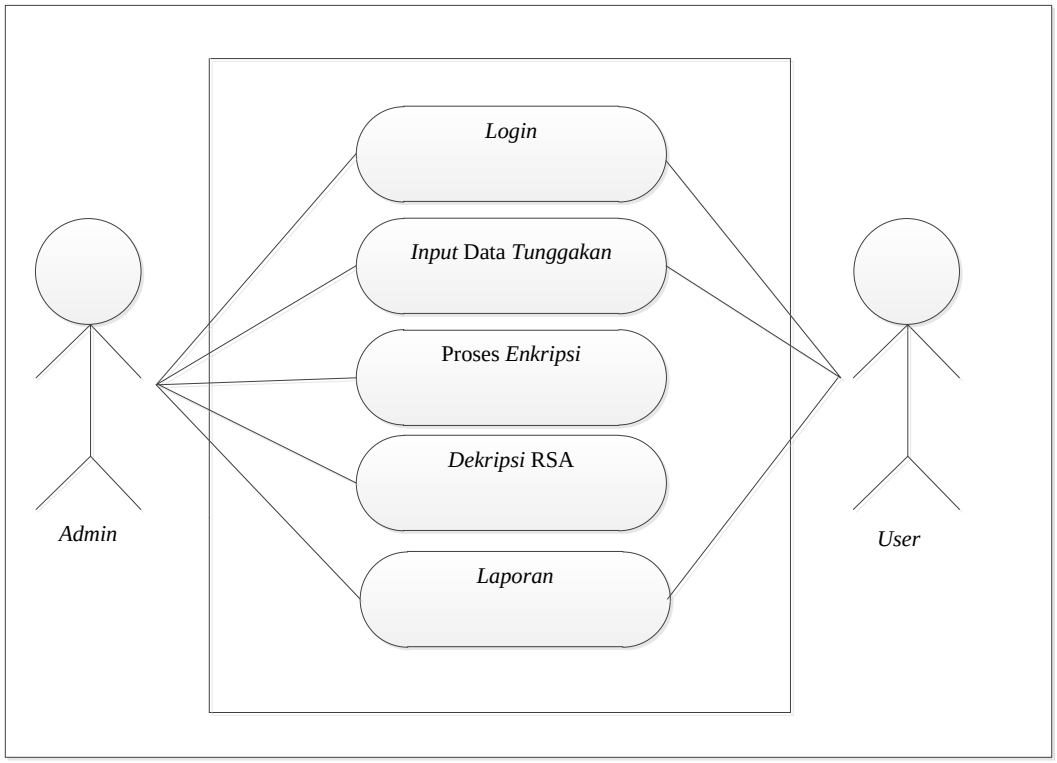
3.5 Pemodelan Sistem

Adapun pemodelan sistem yang diusulkan akan dijelaskan dengan metode UML (*Unified Modelling Language*) yang akan dijelaskan melalui *Use Case*, *Activity Diagram*, dan *Class Diagram*.

3.5.1 *Use Case Diagram*

Use Case menunjukan hubungan interaksi antar aktor dengan *use case* didalam suatu sistem yang bertujuan untuk menentukan bagaimana aktor berinteraksi dengan sebuah sistem.

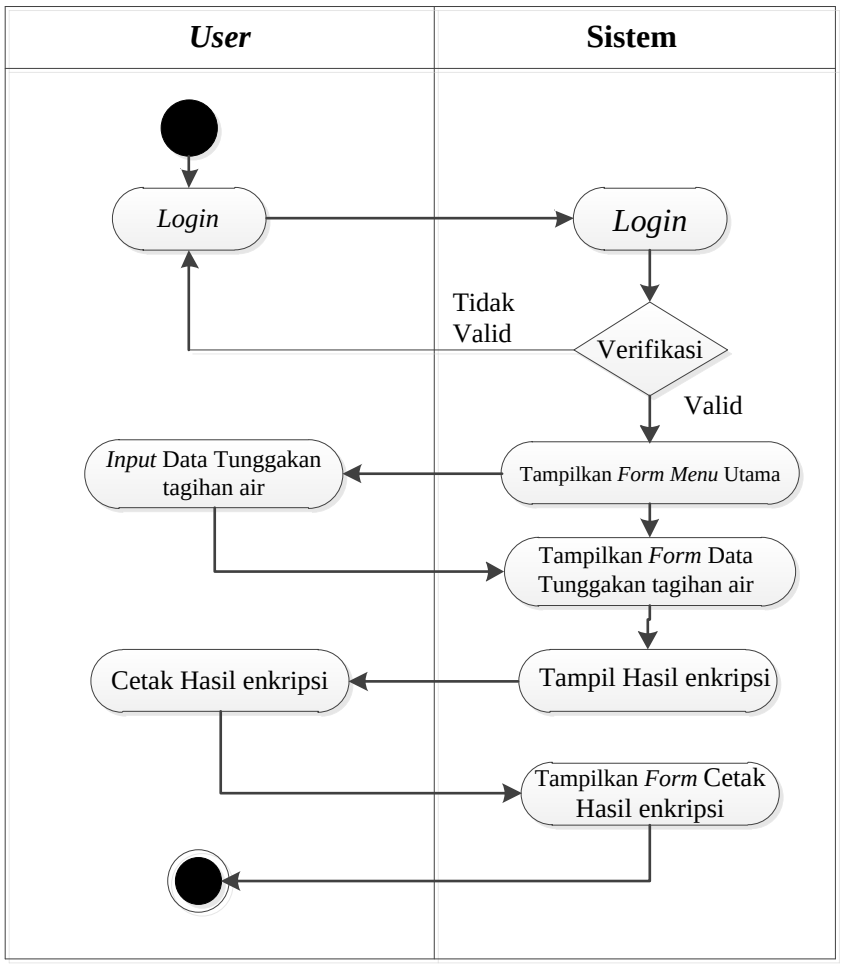
Berikut ini merupakan *Use Case Diagram* pada sistem keamanan data tunggakan tagihan air di PDAM Tirtanadi Sunggal yaitu :



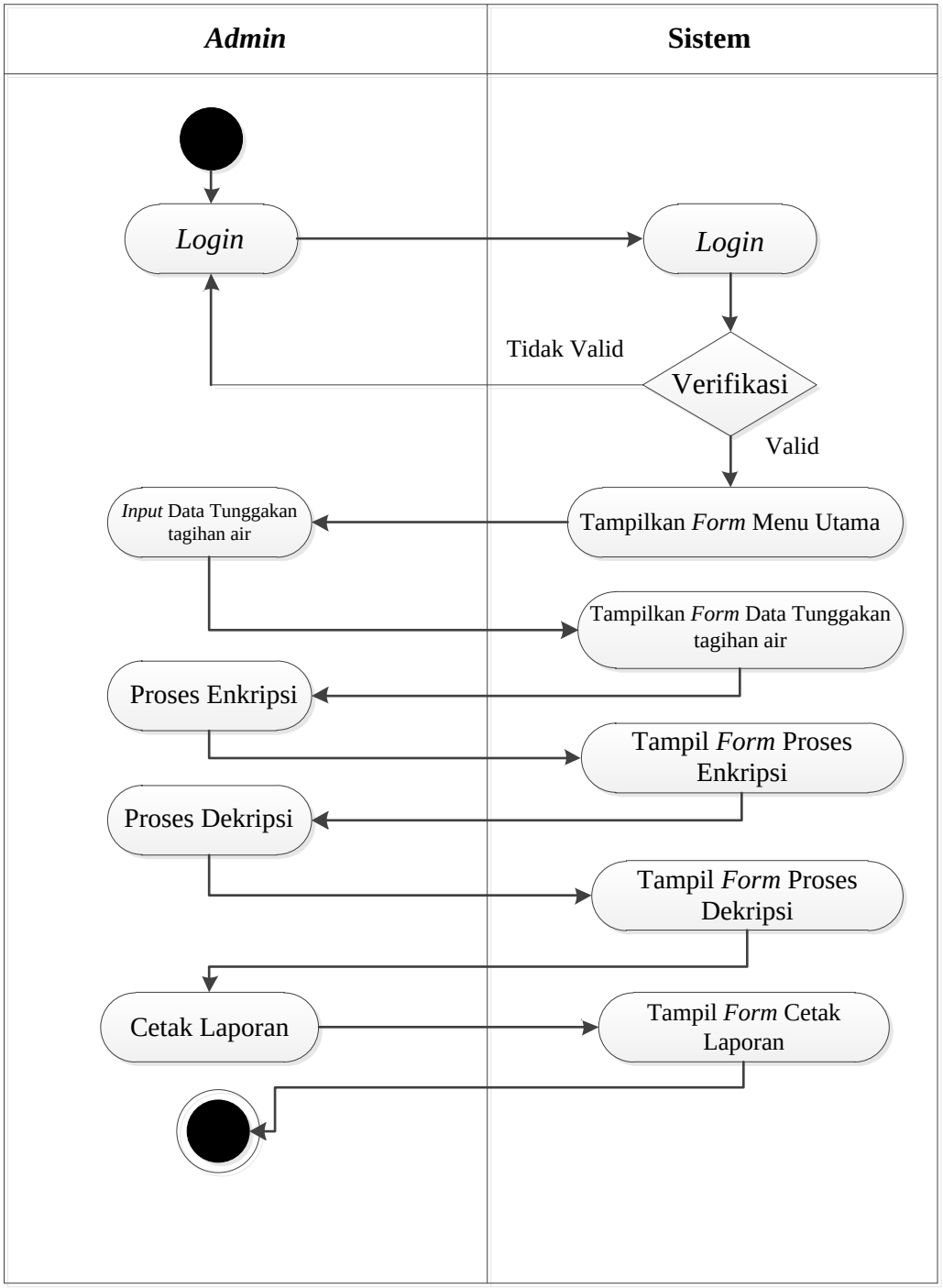
Gambar 3.3 *Use Case* Diagram

3.5.2 *Activity Diagram*

Berikut ini merupakan *Activity Diagram* pada sistem keamanan data tunggakan tagihan air di PDAM Tirtanadi Sunggal, yaitu :



Gambar 3.4 *Activity Diagram User*



Gambar 3.5 *Activity Diagram Admin*

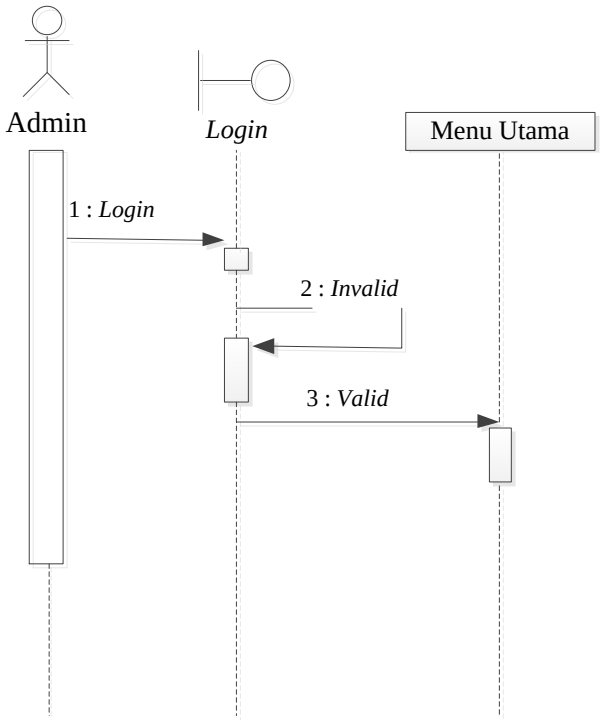
3.5.3 *Sequence Diagram*

Sequence diagram digunakan untuk menggambarkan prilaku pada sebuah *scenario*. *Diagram* ini menunjukkan sejumlah contoh objek dan *message* (pesan) yang diletakkan diantara objek-objek ini di dalam *use case*.

Berikut ini merupakan *Sequence Diagram* pada penerapan algoritma RSA dalam mengamankan data tunggakan tagihan air di PDAM Tirtanadi Sunggal, yaitu :

1. *Sequence Diagram Login*

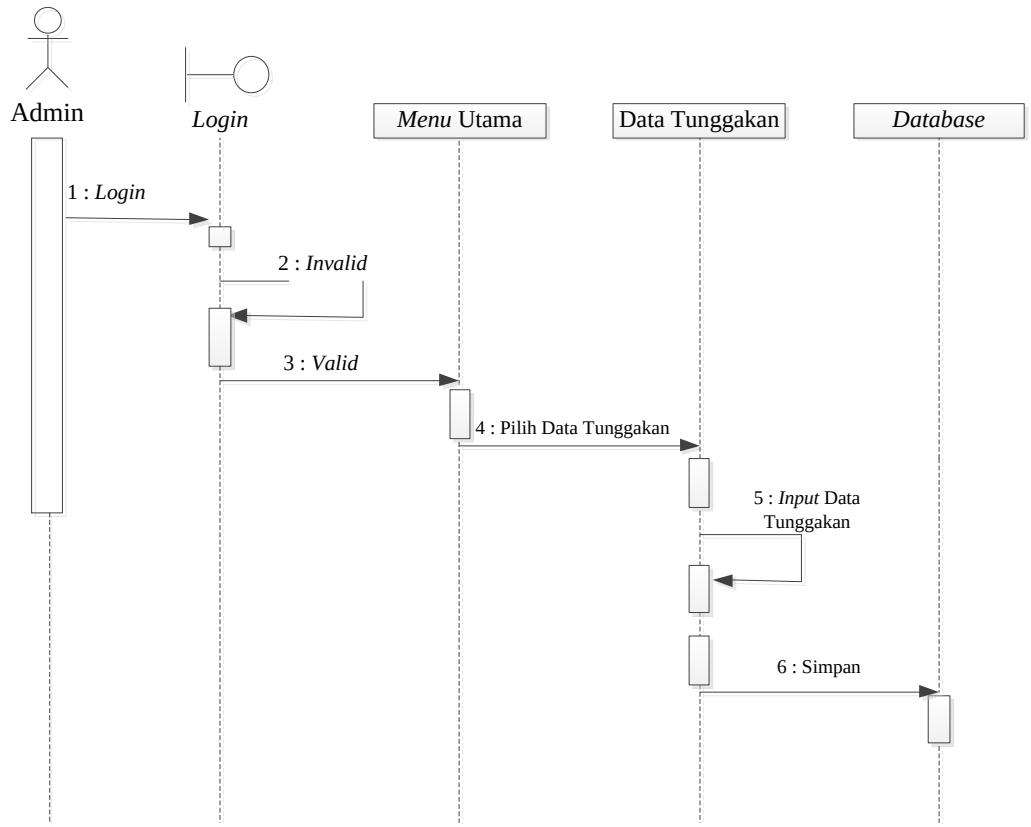
   Berikut ini merupakan *Sequence diagram login* pada aplikasi pengamanan data tunggakan tagihan air.



Gambar 3.6 *Sequence Diagram Login*

2. *Sequence Diagram* Proses *Input* Data Tunggakan

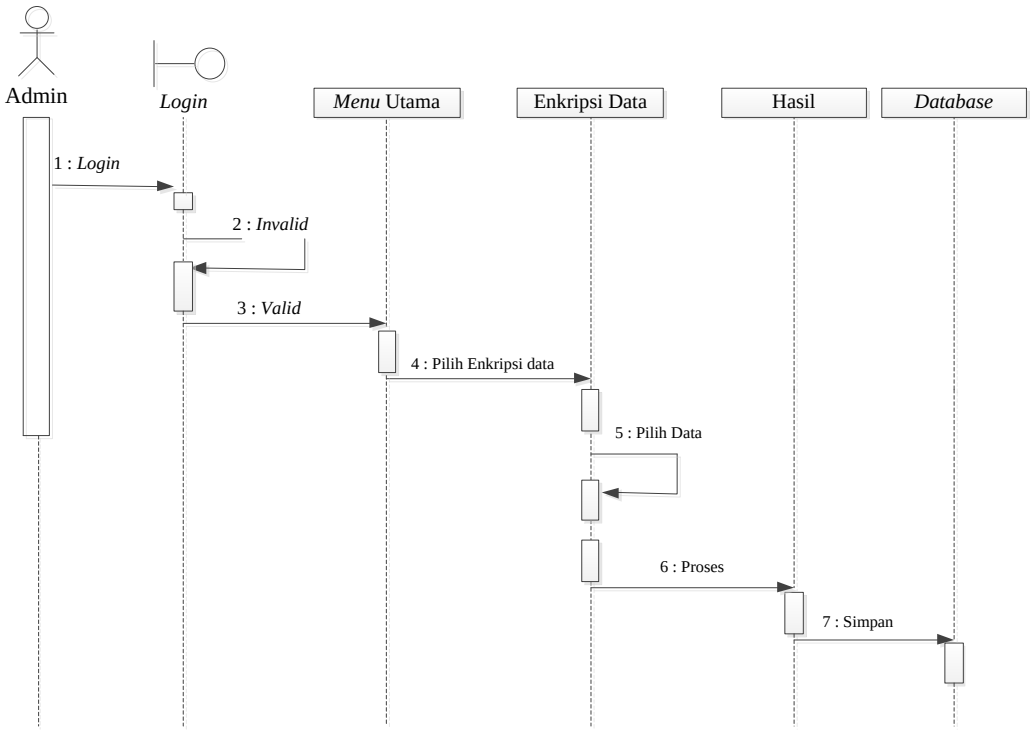
Berikut ini merupakan *Sequence Diagram* Proses *Input* Data Tunggakan dimana nantinya stiap data yang di dapat dari PDAM Tirtanadi Sunggal Akan di *input*.



Gambar 3.7 *Sequence Diagram* Proses *Input* Data Tunggakan

3. *Sequence Diagram* Proses Enkripsi Data

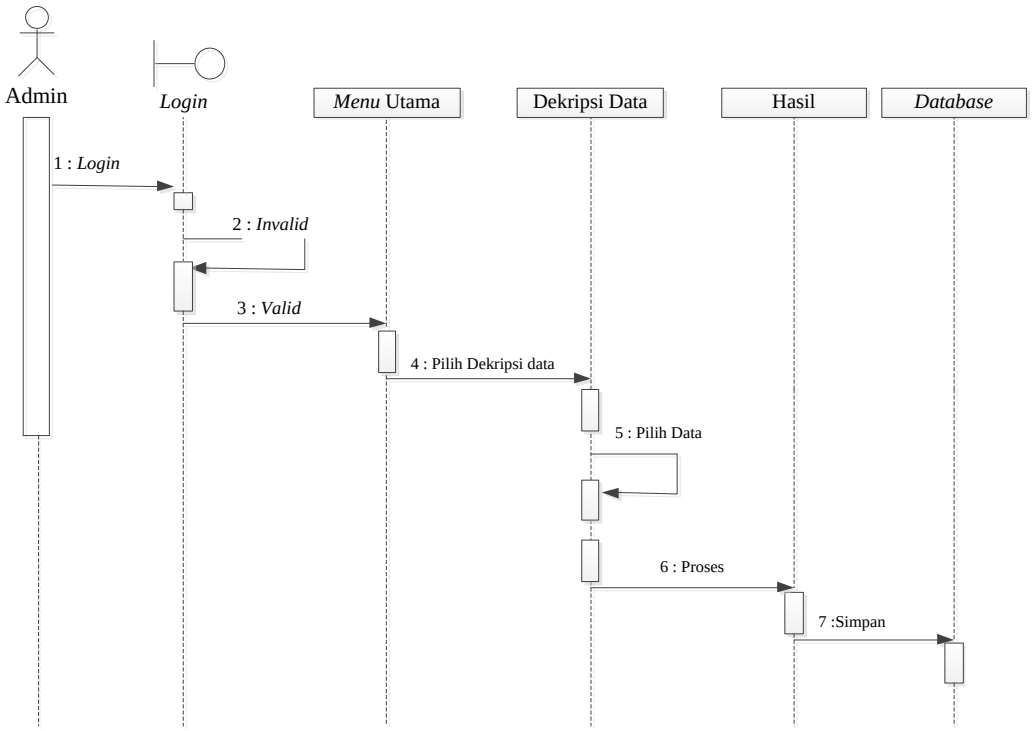
Berikut ini merupakan *Sequence diagram* proses enkripsi data tunggakan tagihan air. Dimana setiap data asli (*plaintext*) akan diubah menjadi kode – kode yang tidak dapat dimengerti, :



Gambar 3.8 *Sequence Diagram* Proses Enkripsi Data

4. *Sequence Diagram* Proses Dekripsi Data

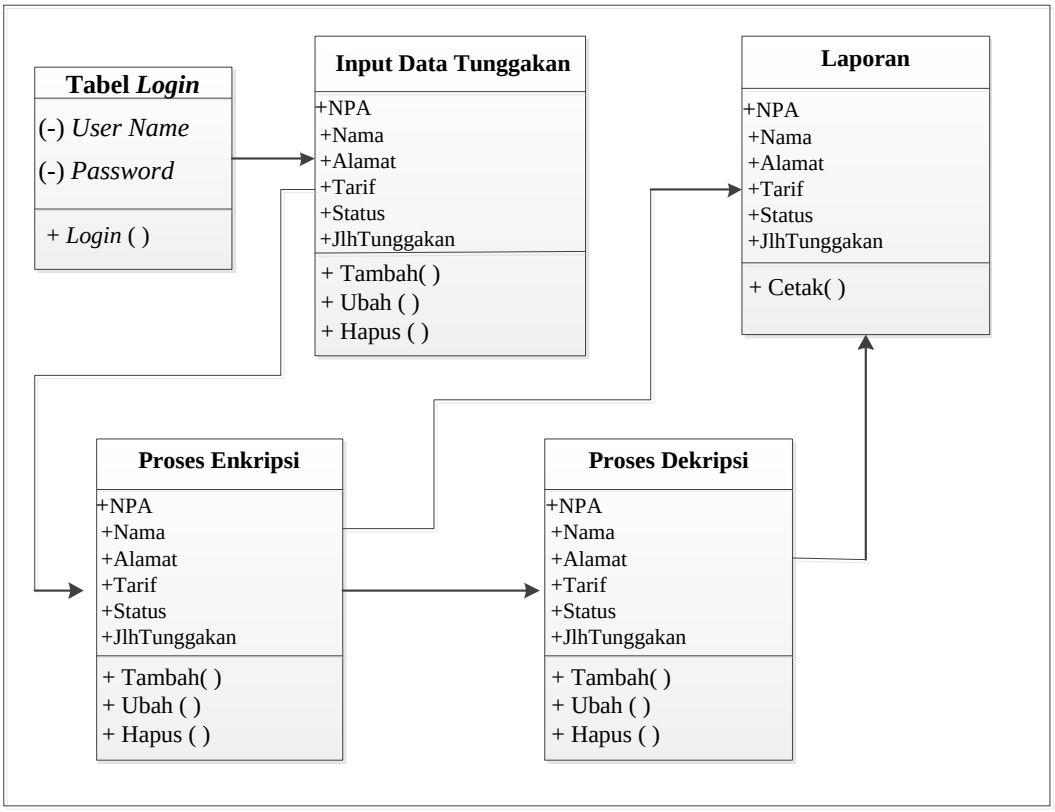
   Berikut ini merupakan *Sequence diagram* proses Dekripsi data tunggakan tagihan air. Dimana setiap data yang telah di enkripsi akan diubah kembali ke data asli.



Gambar 3.9 *Sequence Diagram* Proses Dekripsi Data

3.5.4 *Class Diagram*

Berikut ini merupakan rancangan hubungan relasi antar *Class* pada sistem keamanan data tunggakan tagihan air di PDAM Tirtanadi Sunggal adalah sebagai berikut:



Gambar 3.10 *Class Diagram* Kriptografi RSA

3.5.5 Rancangan *Database*

Rancangan *database* marupakan sebuah perancangan pada sistem yang digunakan sebagai tempat penyimpanan data-data. Adapun bentuk rancangan *database* pada sistem keamanan data tunggakan tagihan air di PDAM Tirtanadi Sunggal, yaitu :

1. Nama Tabel: Tabel *Login*

   Adapun struktur tabel dari *login*, yaitu:

Tabel 3.4 Tabel *Login*

No.	***Field Name***	**Tipe Data**	***Size***	***Description***
1.	*Username*	*Text*	25	Nama Pengguna
2.	*Password*	*Text*	15	Kata Sandi Pengguna

2. Nama Tabel: Tabel Pembangkitan Kunci

   Adapun struktur tabel dari pembangkitan kunci, yaitu:

Tabel 3.5 Tabel Pembangkitan Kunci

No.	***Field Name***	**Tipe Data**	**Size**	***Description***
1.	*Public Key*	*Number*		*Public Key*
2.	*Private Key*	*Number*		*Private Key*

3. Nama Tabel: Tabel Data Tunggakan tagihan air

   Adapun struktur tabel dari tabel tunggakan tagihan air, yaitu:

Tabel 3.6 Tabel Tunggakan tagihan air

No.	***Field Name***	**Tipe Data**	***Size***	***Description***
1.	NPA	*Text*	10	Nomor Pokok Anggota
2.	Nama	*Text*	35	Nama Pelanggan
3.	Alamat	*Text*	225	Alamat
4.	Tarif	*Text*	15	Tarif Pengguna
5.	Status	*Text*	55	Status Pelanggan
6.	JlhTunggakan	*Number*		Jumlah Tunggakan

4. Nama Tabel: Tabel Proses Enkripsi

Adapun struktur tabel dari tabel proses enkripsi, yaitu:

Tabel 3.7 Tabel Proses Enkripsi

No.	***Field Name***	**Tipe Data**	***Size***	***Description***
1.	NPA	*Text*	10	Nomor Pokok Anggota
2.	Nama	*Text*	35	Nama Pelanggan
3.	Alamat	*Text*	225	Alamat
4.	Tarif	*Text*	15	Tarif Pengguna
5.	Status	*Text*	55	Status Pelanggan
6.	JlhTunggakan	*Number*		Jumlah Tunggakan

5. Nama Tabel: Tabel Proses Dekripsi

Adapun struktur tabel dari tabel proses dekripsi, yaitu:

Tabel 3.8 Tabel Proses Dekripsi

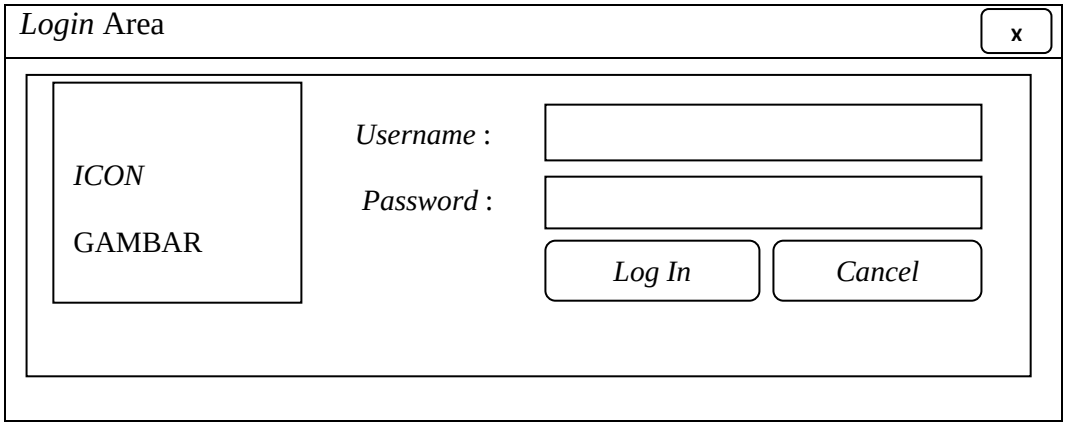
No.	***Field Name***	**Tipe Data**	***Size***	***Description***
1.	NPA	*Text*	10	Nomor Pokok Anggota
2.	Nama	*Text*	35	Nama Pelanggan
3.	Alamat	*Text*	225	Alamat
4.	Tarif	*Text*	15	Tarif Pengguna
5.	Status	*Text*	55	Status Pelanggan
6.	JlhTunggakan	*Number*		Jumlah Tunggakan

3.5.6 Rancangan Masukan

Berikut ini merupakan bentuk rancangan *input* atau data masukan pada sistem keamanan data tunggakan tagihan air di PDAM Tirtanadi Sunggal, yaitu sebagai berikut:

1. Rancangan *Login*

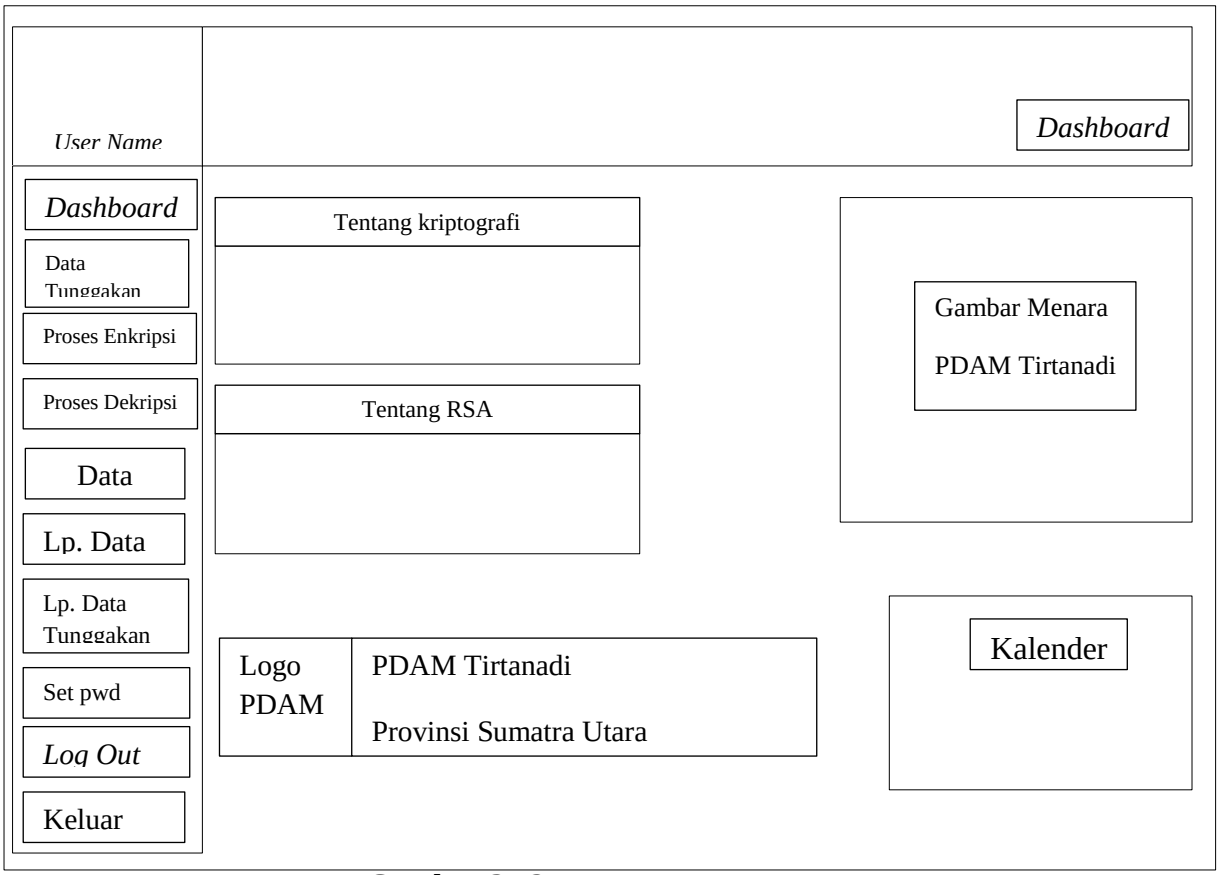
   Berikut ini adalah rancangan dari *form* login pada sistem keamanan data tunggakan tagihan air di PDAM Tirtanadi Sunggal.



Gambar 3.11 Rancangan *Login*

2. Rancangan *Menu* Utama

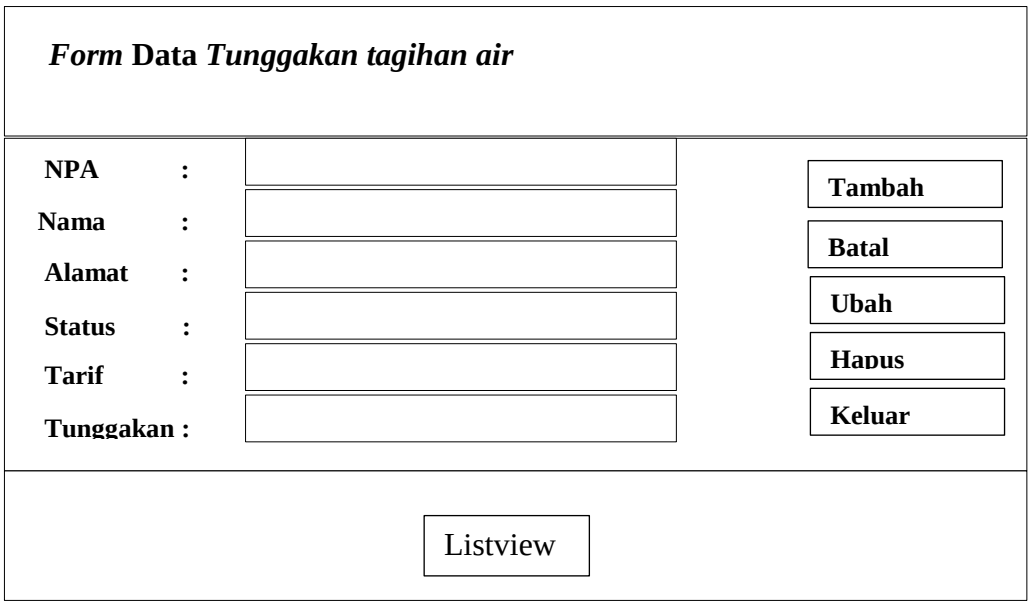
   Berikut ini adalah rancangan dari *form menu* utama pada sistem keamanan data tunggakan tagihan air di PDAM Tirtanadi Sunggal.



Gambar 3.12 Rancangan *Menu* Utama

3. Rancangan *Form* Data *Tunggakan tagihan air*

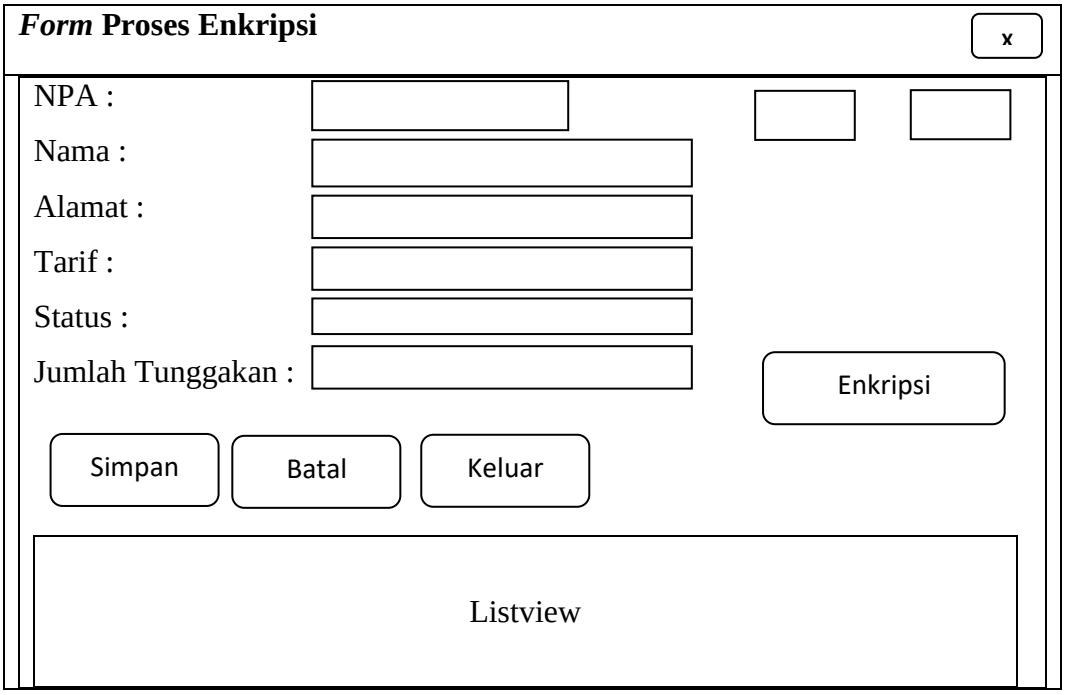
Berikut ini adalah rancangan dari *form* data barang pada sistem keamanan data tunggakan tagihan air di PDAM Tirtanadi Sunggal.



Gambar 3.13 Rancangan *Form* Data Tunggakan tagihan air

4. Rancangan *Form* Proses Enkripsi

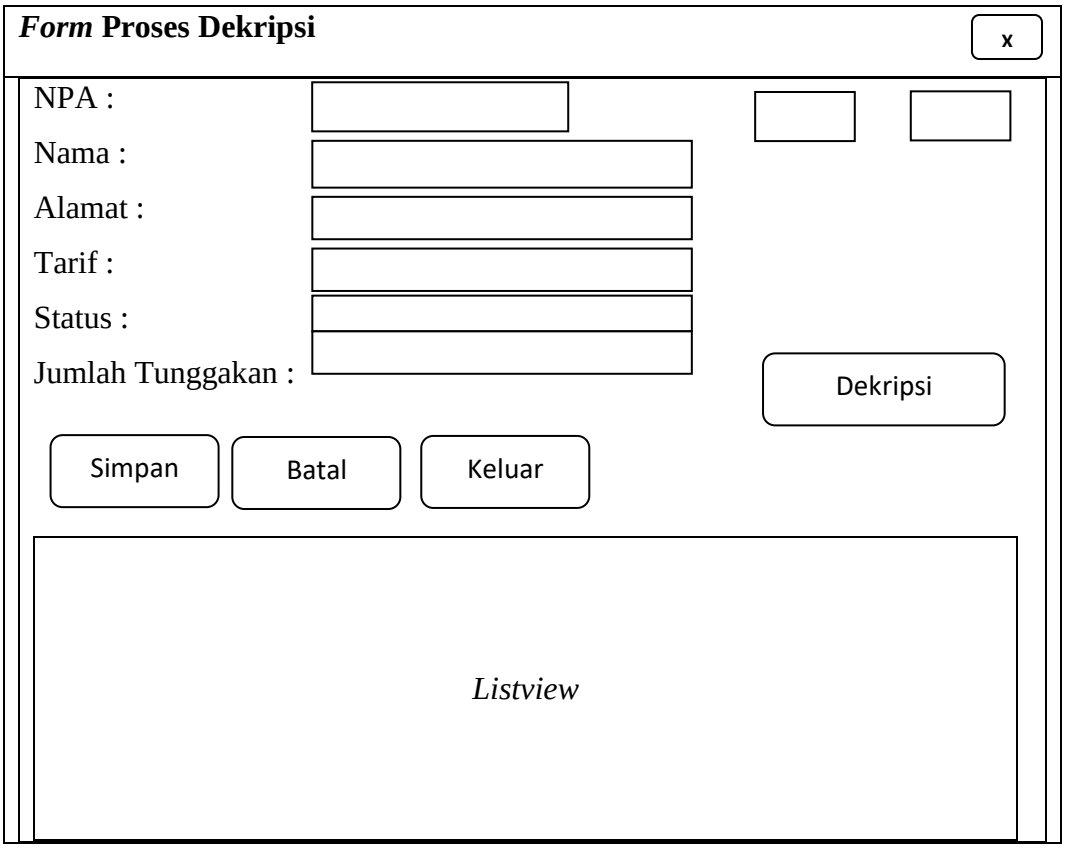
   Berikut ini adalah rancangan dari *form* proses enkripsi pada sistem keamanan data tunggakan tagihan air di PDAM Tirtanadi Sunggal.



Gambar 3.14 Rancangan *Form* Proses Enkripsi

5. Rancangan *Form* Proses Dekripsi

   Berikut ini adalah rancangan dari *form* proses dekripsi pada sistem keamanan data tunggakan tagihan air di PDAM Tirtanadi Sunggal.



Gambar 3.15 Rancangan *Form* Proses Dekripsi

3.5.7 Rancangan Keluaran

Berikut ini merupakan bentuk rancangan hasil keluaran dalam sistem keamanan data tunggakan tagihan air di PDAM Tirtanadi Sunggal adalah sebagai berikut :

1. Laporan Hasil

Logo

PDAM TIRTANADI SUNGGAL
Medan Sunggal
Telp. (xxx) xxxxxxx

LAPORAN DATA TUNGGAKAN TAGIHAN AIR

NPA	**Nama**	**Alamat**	**Tarif**	**Status**	**Jumlah Tunggakan**
xxx	Xxx	Xxx	Xxx	Xxx	xxx
xxx	Xxx	Xxx	Xxx	Xxx	xxx

Gambar 3.16 Hasil *Chipertext*

BAB IV

HASIL DAN PEMBAHASAN

4.1 Kebutuhan Sistem

Pada penerapan algoritma RSA dalam pengamanan data tunggakan tagihan air pelanggan di PDAM Tirtanadi Sunggal dibutuhkan beberapa fasilitas pendukung. Berikut ini merupakan bahan pendukung yang dibutuhkan oleh sistem baik perangkat keras maupun perangkat lunak.

4.1.1 Perangkat Keras *(Hardware)*

Spesifikasi *hardware* yang dibutuhkan untuk menerapkan sistem agar berjalan dengan baik adalah sebagai berikut :

1. Komputer atau laptop dengan *processor* mulai dari Intel *dual Core*
2. *Memory* dengan kapasitas minimal 2 GB
3. *Harddisk* dengan kapasitaas minimal 320 GB
4. *Monitor*
5. *Printer*
6. *Mouse* dan *Keyboard*

4.1.2 Perangkat Lunak (*Software*)

Sistem aplikasi penerapan algoritma RSA dalam pengamanan data tunggakan tagihan air pelanggan di PDAM Tirtanadi Sunggal tidak terlalu banyak memerlukan perangkat lunak sebagai pendukung aplikasinya. Untuk membuat suatu Aplikasi dibutuhkan beberapa *software* pendukung, yaitu:

1. *Visual Basic.Net 2010*

   Perangkat *Visual Basic.Net 2010* dipergunakan dalam pembuatan aplikasi penerapan algoritma RSA dalam pengamanan data tunggakan tagihan air pelanggan di PDAM Tirtanadi Sunggal karena sarana akses data yang lebih cepat dan akurat.

2. *Microsoft Access*

   Software ini digunakan sebagai aplikasi sistem basis data (*database*) yang berfungsi sebagai tempat penyimpanan data yang di*input*kan ke dalam sistem.

3. *Crystal Report 8.5*

   Crystal report berguna untuk membuat laporan yang diperlukan oleh suatu program aplikasi *database* atau aplikasi lain yang membutuhkan tampilan suatu laporan dari suatu data.

4.1.3 Pengendali *(Brainware)*

Brainware adalah seseorang yang mengoperasikan perangkat komputer. Dalam hal ini diperlukan seorang yang bertugas untuk mengentri data maupun mencetak laporan dari hasil analisa aplikasi tersebut. Aplikasi yang dibuat membutuhkan tiga pengendali yaitu :

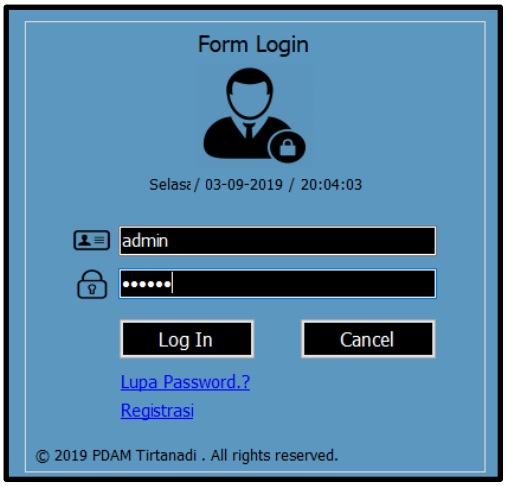
1. Seorang analis, yakni bertugas untuk merancang dan membentuk sebuah aplikasi.
2. *Operator*, adalah orang yang menggunakan dan menjalankan aplikasi yang bertugas untuk mengentri dan mencetak data serta mengoperasikan peralatan yang digunakan pada saat proses pengolahan data.

3. *Programmer*, adalah orang yang memahami bahasa pemrograman dan membuat program pada aplikasi yang diusulkan.

4.2 Aplikasi dan Pembahasan

1. Tampilan *Form Login*

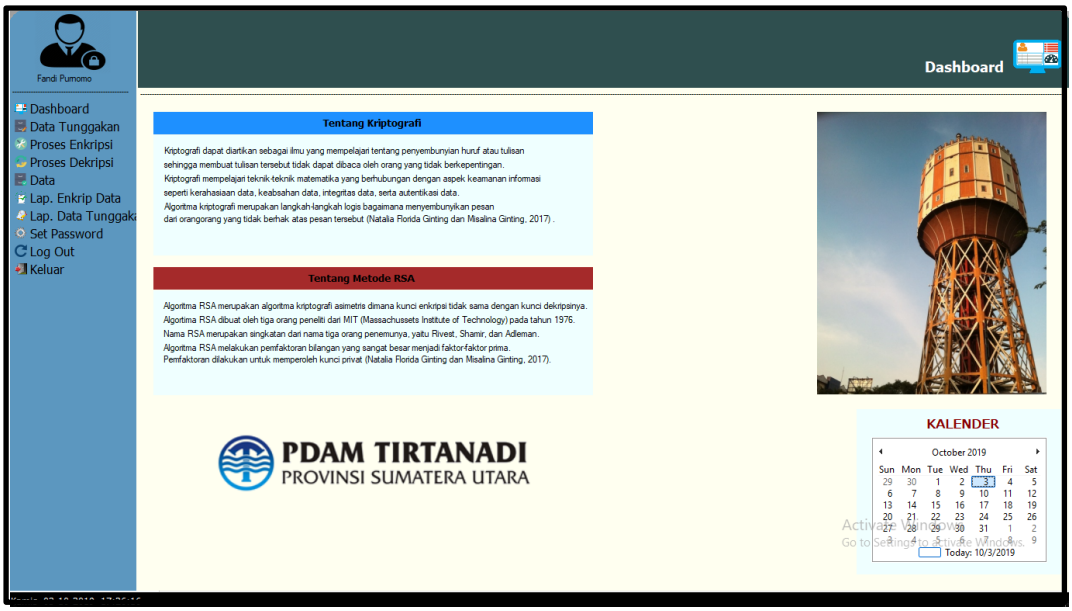
   Berikut ini merupakan tampilan dari *form login* yang berfungsi untuk melakukan proses validasi *username* dan *password* pengguna. Pada *menu* ini terdapat 2 buah akun yang memiliki tugas yang berbeda yaitu *admin* yg memiliki tugas meng*input* data, mengenkripsi dan dekripsi data, serta mencetak sebuah laporan. Kemudian *user* yang hanya memiliki tugas meng*input* data dan mencetak laporan data yang telah dienkripsi.



Gambar 4.1 *Form Login*

2. Tampilan *Menu* Utama

   Berikut ini merupakan tampilan *menu* utama dari aplikasi penerapan algoritma RSA dalam pengamanan data tunggakan tagihan air pelanggan di PDAM Tirtanadi Sunggal :



Gambar 4.2 *Form Menu* Utama

Pada *menu* ini terdapat beberapa *menu* yang memiliki fungsi yang berbeda, yaitu :

a. *Dashboard* adalah tampilan awal dimana terdapat *menu* – *menu* seperti data tunggakan, proses enkripsi data, proses dekripsi data, data, lap. data, lap data tunggakan, *set password*, *log out*, dan keluar.

b. Data Tunggakan, yaitu *menu* yang berfungsi sebagai tempat untuk meng*input* data tunggakan tagihan air.

c. Proses Enkripsi Data, *menu* ini berfungsi sebagai tempat dimana data yang telah di*input*kan akan dienkripsi. Dimana data asli (*plaintext*) akan diubah kedalam kode – kode yang tidak dapat dimengerti (*ciphertext*).

d. Proses Dekripsi Data, *menu* ini berufungsi untuk merubah kembali data yang telah dienkripsi (*ciphertext*) ke data asli (*plaintext*)

e. Data, pada *menu* ini berfungsi sebagai tempat untuk meng*input*kan data. Tetapi data yang telah di*input* tidak dapat lagi terlihat sebagai data asli (plaintext) melaikan data yang telah dienkripsi (*ciphertext*).

f. Lap. Enkrip Data, pada *menu* ini berfungsi untuk mencetak data yang telah dienkripsi.

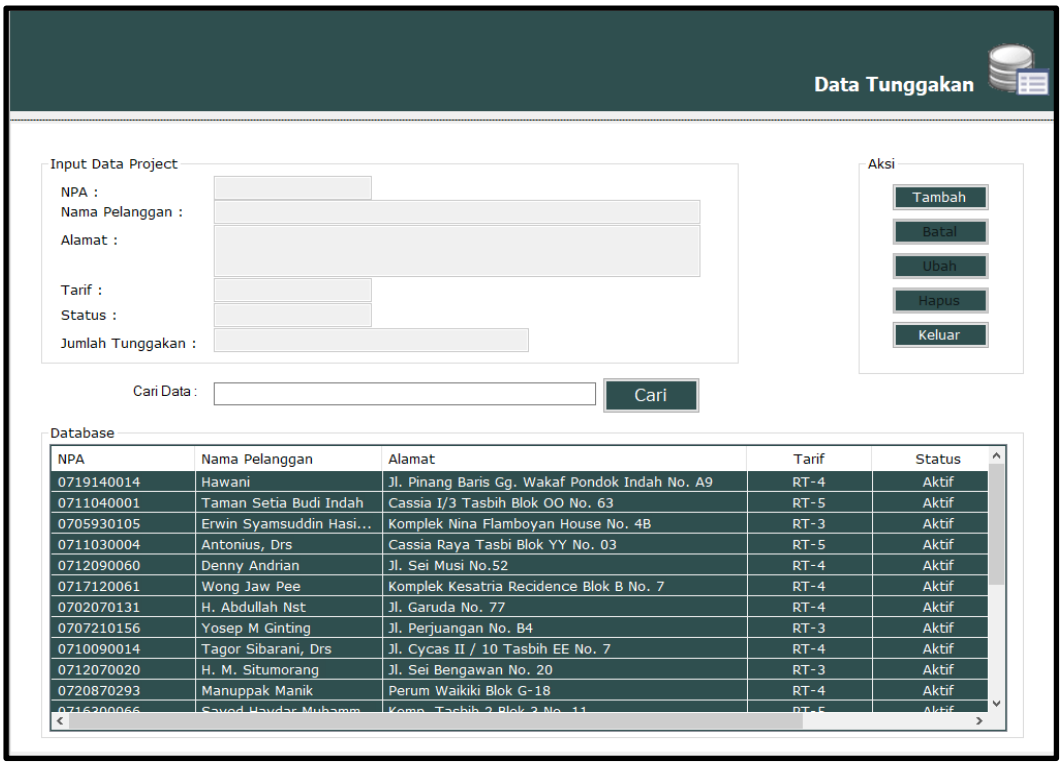
g. Lap. Data Tunggakan, pada *menu* ini berfungsi untuk mencetak data tunggakan tagihan air pelanggan

h. *Set Password*, yaitu *menu* yang berfungsi sebagai tempat untuk merubah *password.*

i. Log out, adalah *menu* ini berfungsi untuk kembali ke *menu login*

j. Keluar, adalah *menu* yang berfungsi untuk keluar dari apliksi.

3. *Form input* data tunggakan



Gambar 4.3 *Form input* data tunggakan

Form input data tunggakan ini berfungsi untuk menginput data pelanggan yang memiliki tunggakan air pada PDAM Tirtanadi yang nantinya data tersebut akan disimpan dan akan dienkripsi. Pada *form* ini terdapat beberapa *menu*, yaitu :

a. Tambah, berfungsi untuk menambah data.

b. Simpan, berfungsi untuk menyimpan data.

c. Batal, berfungsi untuk membatalkan data yang ingin di simpan.

d. Ubah, berfungsi untuk mengubah data.

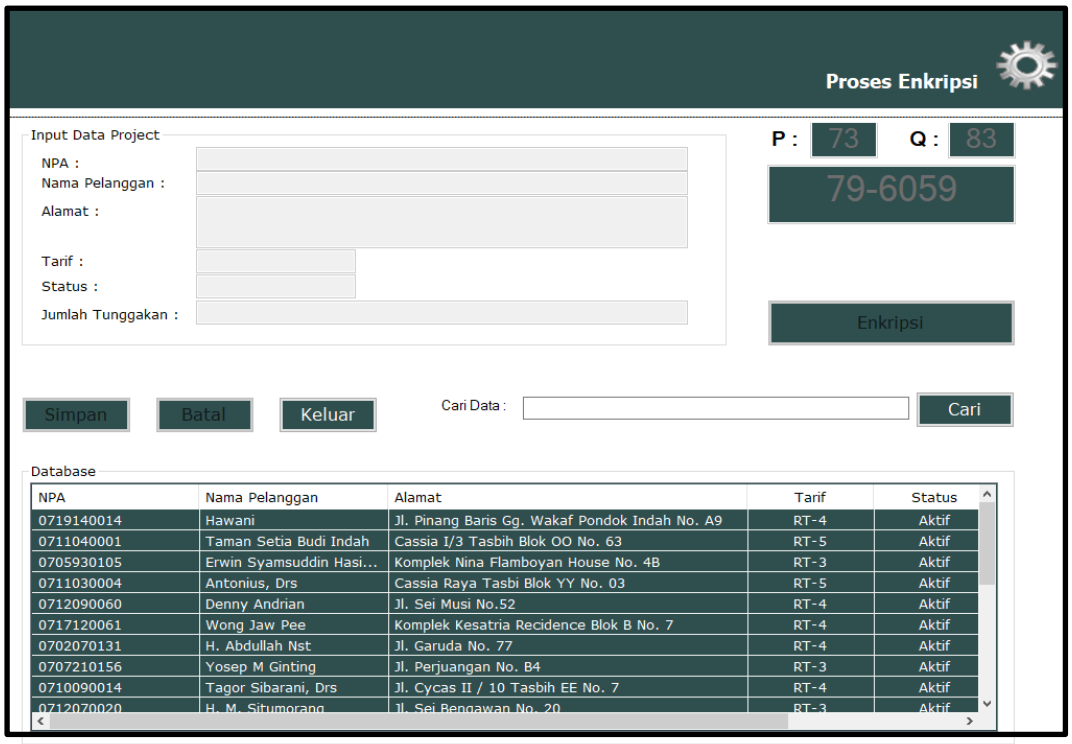
e. Hapus, berfungsi untuk menghapus data.

f. Keluar, berfungsi untuk keluar dari *form input* data dan kembali ke *dashboard*,

g. Cari, berfungsi untuk mencari data yang telah di*input*.

4. *Form* Enkripsi Data

Berikut ini merupakan tampilan dari *form* enkripsi data yang berfungsi untuk merubah data asli (*plaintext*) menjadi pengkodean yang tidak dapat di mengerti (*ciphertext*) :



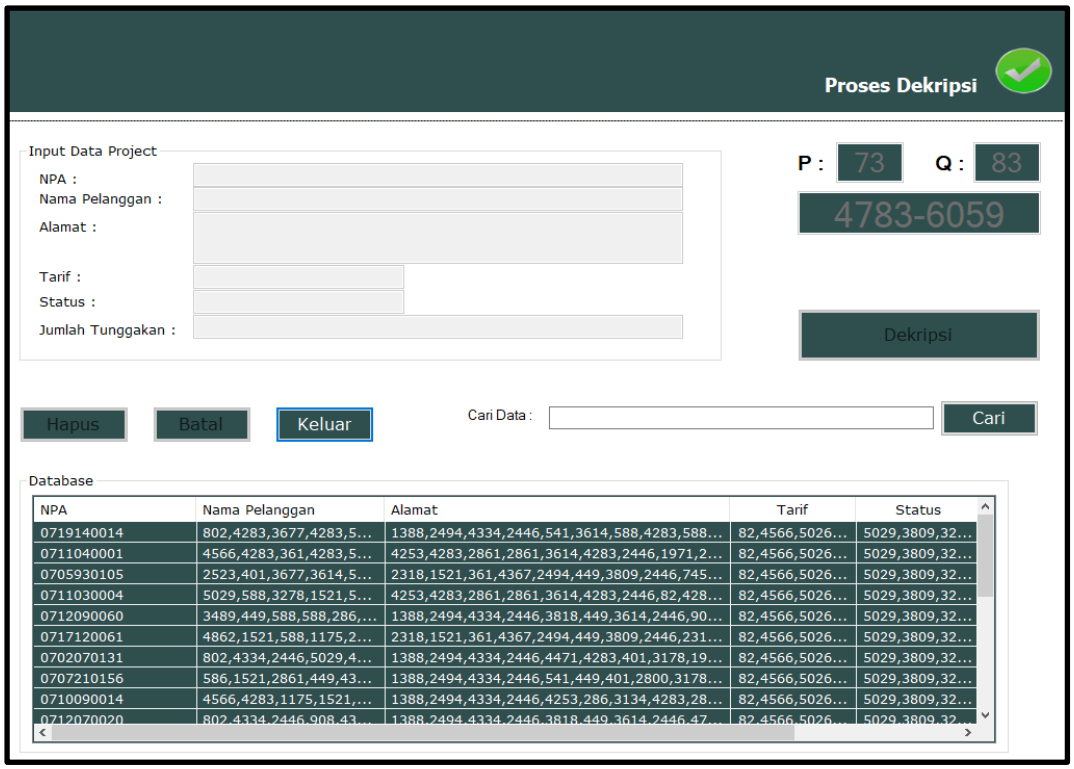
Gambar 4.4 *Form* Enkripsi Data

Pada *menu* ini terdapat beberapa menu yang memiliki fungsi yaitu :

a) Enkripsi, berfungsi untuk merubah data asli kedalam kode – kode yang tidak dapat dimengerti.
b) Simpan, berfungsi untuk menyimpan data yang telah dirubah menjadi kode-kode yang tidak dapat dimengerti.
c) Batal, berfungsi untuk membatalkan data yang ingin disimpan setelah di enkripsi.
d) Keluar, berfungsi untuk keluar dari *form* enkripsi data dan kembali ke *dashboard*.
e) Cari, berfungsi untuk mencari data yang telah dienkripsi.

5. *Form* Dekripsi Data

Berikut ini merupakan tampilan dari *form* dekripsi data, kebalikan dari enkripsi. Dekripsi data berfungsi untuk menterjemahkan pengkodean yang telah dilakukan dalam proses enkripsi kedalam data asli.



Gambar 4.5 *Form* Dekripsi Data

Pada *menu* ini terdapat beberapa menu yang memiliki fungsi yaitu :

a) dekripsi, berfungsi untuk merubah data yang telah dienkripsi ke dalam data asli.

b) Simpan, berfungsi untuk menyimpan data yang telah dirubah dari data enkripsi ke data asli.

c) Batal, berfungsi untuk membatalkan data yang ingin disimpan setelah mendekripsi data yang telah dienkripsi.

d) Keluar, berfungsi untuk keluar dari *form* dekripsi data dan kembali ke *dashboard*.

e) Cari, berfungsi untuk mencari data yang telah didekripsi.

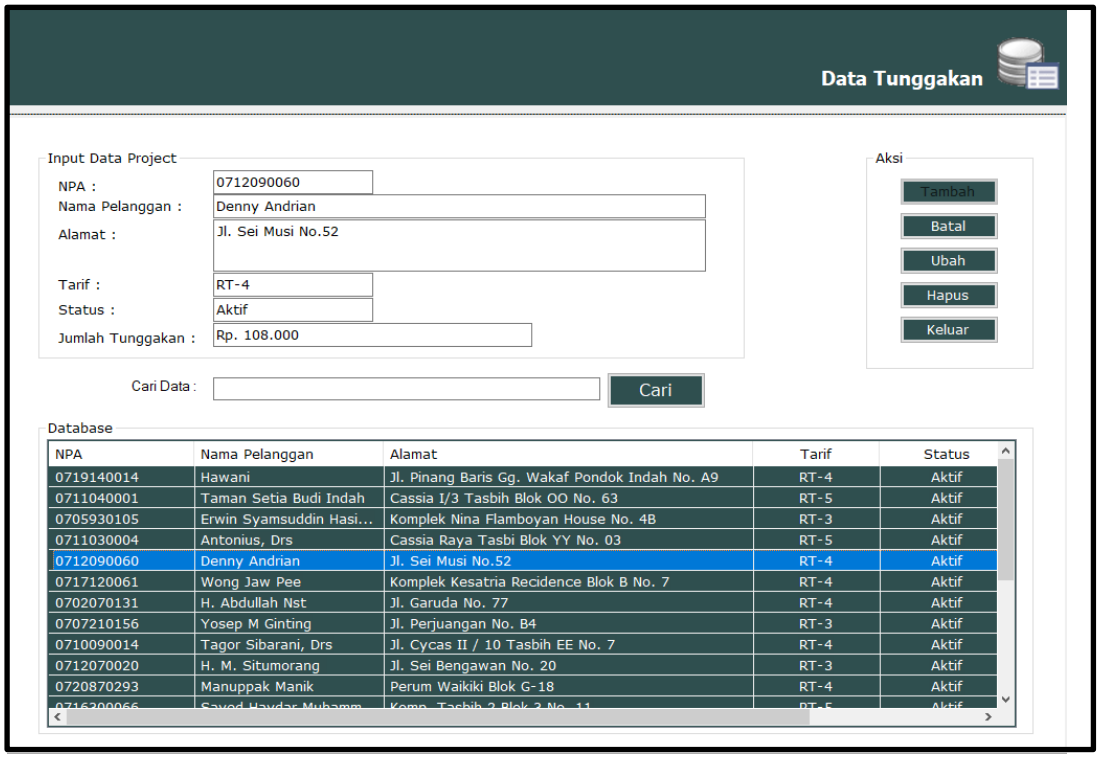
4.2.1 Pengujian Aplikasi

Uji coba aplikasi bertujuan untuk membuktikan apakah aplikasi yang dirancang dapat berjalan sebagaimana mestinya. Bahwa *input*, *process*, *output* yang dihasilkan oleh aplikasi yang dirancang telah benar dan sesuai dengan yang diinginkan.

Pengujian sistem dengan cara memasukkan data ke dalam sistem dan memperhatikan *output* yang dihasilkan. Jika *input*, *process* dan *output* telah sesuai, maka aplikasi telah benar. Berikut merupakan tahapan untuk pengujian sistem yaitu:

1. Melakukan *input* data

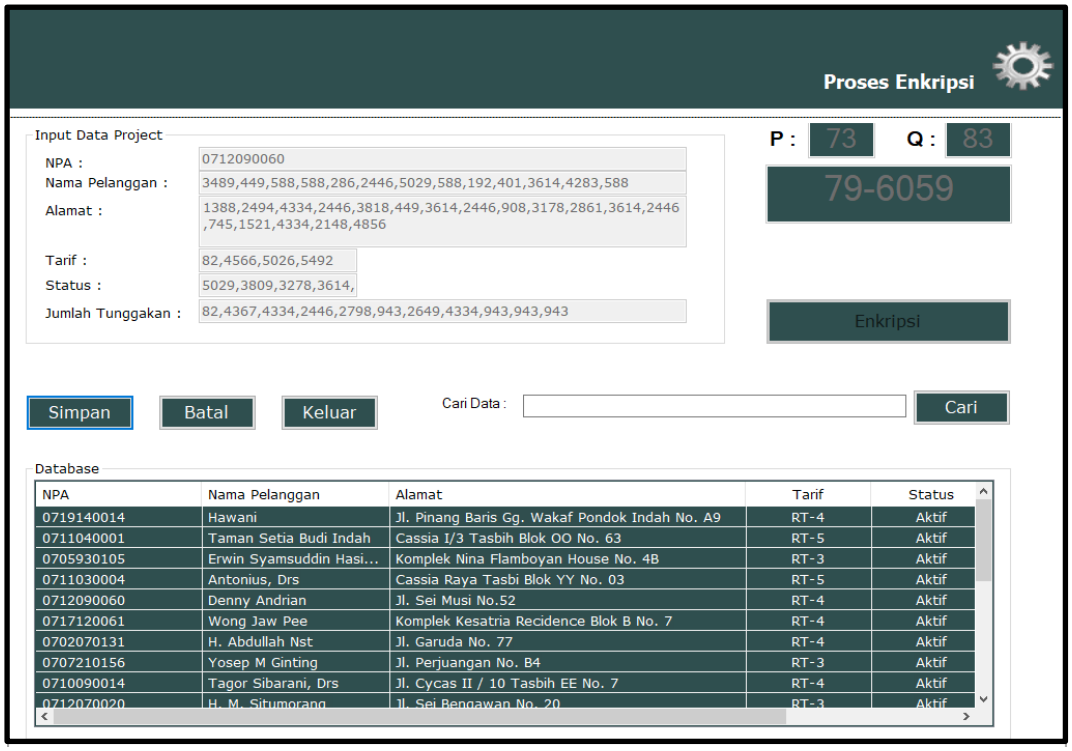
   Pada *menu* ini, *input*kan data pelanggan yang akan dienkripsi. Kemudian simpan



Gambar 4.6 Proses *Input* Data Pelanggan

2. Melakukan proses enkripsi

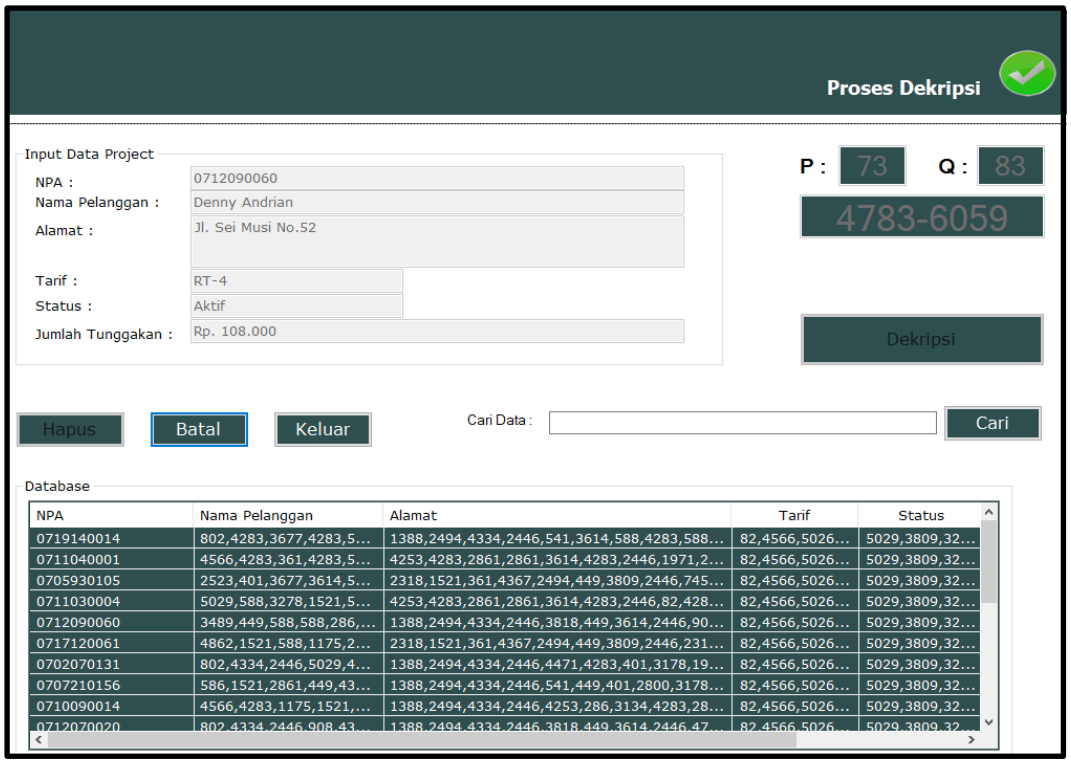
   Enkripsi adalah proses merubah data asli ke dalam data yang telah dirubah menjadi kode-kode yang tidak dapat dimengerti. Sebelumnya pilih sebuah data yang ingin dienkripsi, dalam hal ini diambil sebuah contoh data dengan NPA : 0712090060 yang akan dienkripsi. Berikut hasil enkripsi data.



Gambar 4.7 Hasil Enkripsi Data

3. Melakukan proses dekripsi

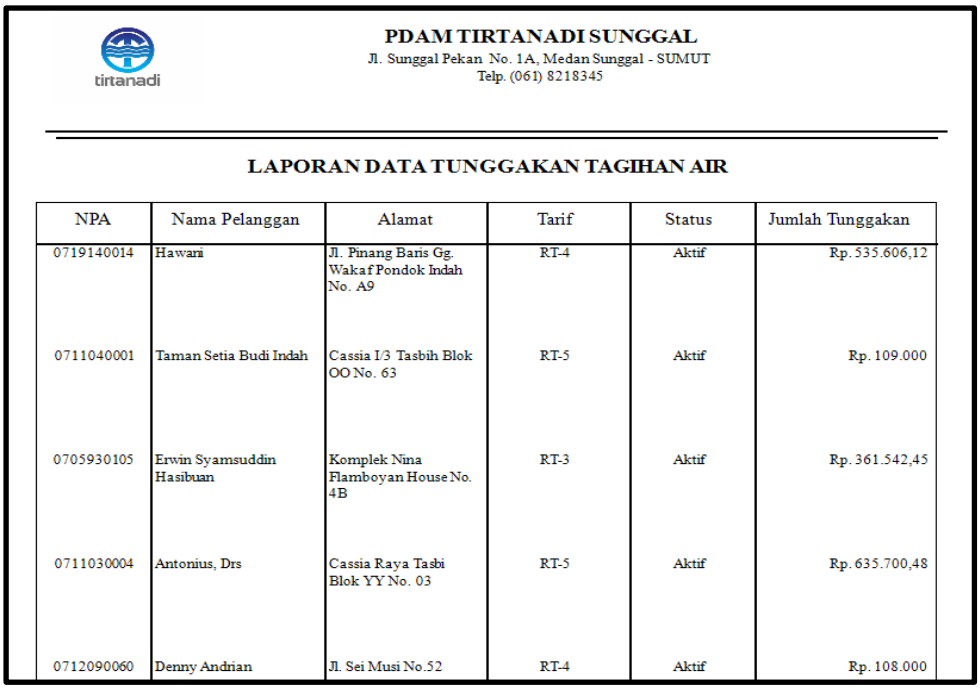
   Pada menu ini, data yang telah dienkripsi akan diubah kembali kedalam data asli. Dalam artian bahwa data yang telah dirubah menjadi kode-kode (*ciphertext*) akan di ubah kembali kedalam data aslinya (*plaintext*).



Gambar 4.8 Hasil Deskripsi Data

4. Laporan Data Tunggakan

Pada *menu* ini, setiap data yang telah di *input* akan di cetak dalam bentuk sebuah laporan.



PDAM TIRTANADI SUNGGAL
Jl. Sunggal Pekan No. 1A, Medan Sunggal - SUMUT
Telp. (061) 8218345

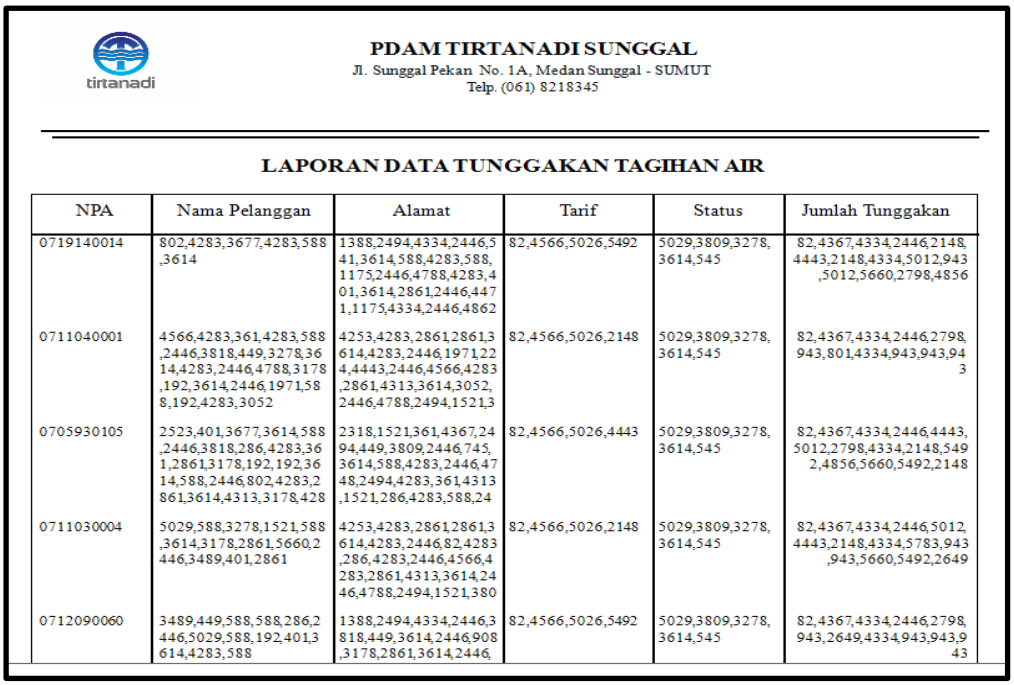
LAPORAN DATA TUNGGAKAN TAGIHAN AIR

NPA	Nama Pelanggan	Alamat	Tarif	Status	Jumlah Tunggakan
0719140014	Hawani	Jl. Pinang Baris Gg. Wakaf Pondok Indah No. A9	RT-4	Aktif	Rp. 535.606,12
0711040001	Taman Setia Budi Indah	Cassia I/3 Tasbih Blok OO No. 63	RT-5	Aktif	Rp. 109.000
0705930105	Erwin Syamsuddin Hasibuan	Komplek Nina Flamboyan House No. 4B	RT-3	Aktif	Rp. 361.542,45
0711030004	Antonius, Drs	Cassia Raya Tasbi Blok YY No. 03	RT-5	Aktif	Rp. 635.700,48
0712090060	Denny Andrian	Jl. Sei Musi No.52	RT-4	Aktif	Rp. 108.000

Gambar 4.9 Laporan Data Tunggakan

5. Laporan Enkripsi Data Tunggakan

Pada menu ini, setiap data yg telah di input dan di enkripsi akan di cetak dalam bentuk laporan.



PDAM TIRTANADI SUNGGAL
Jl. Sunggal Pekan No. 1A, Medan Sunggal - SUMUT
Telp. (061) 8218345

LAPORAN DATA TUNGGAKAN TAGIHAN AIR

NPA	Nama Pelanggan	Alamat	Tarif	Status	Jumlah Tunggakan
0719140014	802,4283,3677,4283,588,3614	1388,2494,4334,2446,541,3614,588,4283,588,1175,2446,4788,4283,401,3614,2861,2446,4471,1175,4334,2446,4862	82,4566,5026,5492	5029,3809,3278,3614,545	82,4367,4334,2446,2148,4443,2148,4334,5012,943,5012,5660,2798,4856
0711040001	4566,4283,361,4283,588,2446,3818,449,3278,3614,4283,2446,4788,3178,192,3614,2446,1971,588,192,4283,3052	4253,4283,2861,2861,3614,4283,2446,1971,224,4443,2446,4566,4283,2861,4313,3614,3052,2446,4788,2494,1521,3	82,4566,5026,2148	5029,3809,3278,3614,545	82,4367,4334,2446,2798,943,801,4334,943,943,943
0705930105	2523,401,3677,3614,588,2446,3818,286,4283,361,2861,3178,192,192,3614,588,2446,802,4283,2861,3614,4313,3178,428	2318,1521,361,4367,2494,449,3809,2446,745,3614,588,4283,2446,4748,2494,4283,3614313,1521,286,4283,588,24	82,4566,5026,4443	5029,3809,3278,3614,545	82,4367,4334,2446,4443,5012,2798,4334,2148,5492,4856,5660,5492,2148
0711030004	5029,588,3278,1521,588,3614,3178,2861,5660,2446,3489,401,2861	4253,4283,2861,2861,3614,4283,2446,82,4283,286,4283,2446,4566,4283,2861,4313,3614,2446,4788,2494,1521,380	82,4566,5026,2148	5029,3809,3278,3614,545	82,4367,4334,2446,5012,4443,2148,4334,5783,943,943,5660,5492,2649
0712090060	3489,449,588,588,286,2446,5029,588,192,401,3614,4283,588	1388,2494,4334,2446,3818,449,3614,2446,908,3178,2861,3614,2446,	82,4566,5026,5492	5029,3809,3278,3614,545	82,4367,4334,2446,2798,943,2649,4334,943,943,943

Gambar 4.10 Laporan Enkripsi Data Tunggakan

4.3 Perhitungan RSA Pada Program

Untuk menggunakan RSA terlebih dahulu pendeskripsi membangkitkan sepasang kunci yaitu kunci publik dan kunci privat. Hal pertama yang dilakukan algoritma pembangkit kunci adalah membangkitkan 2 bilangan prima besar. Berikut ini algoritma penyelesaiannya:

1. Pilihlah bilangan prima dengan sembarang, dalam pemilihan ini, dipilih nilai prima (p) = 73 dan nilai (q) = 83.
2. Untuk mencari nilai dari kedua bilangan tersebut, maka dilakukan perkalian

   n= p * q

   n= 73 * 83 = 6059
3. Hitung $\varphi(n)$= (p-1) (q-1)

   $\varphi(n) = 72 * 82 = 5904$
4. Pilih nilai *e* dengan syarat bilangan prima *e* > 1 dan *greatest comman divisior* (*e, 5904*) = 1

   Nilai *e* yang diambil adalah 79.

   Bukti:

   (79, 5904)

   5904 mod 79 = 58

   79 mod 58 = 21

   58 mod 21 = 16

   21 mod 16 = 5

   16 mod 5 = 1

   Kemudian cari nilai *d* dengan rumus :

d*e mod φ(n) = 1

d * 79 mod 5904=1

d = 4783

Bukti:

4783 * 79 mod 5904 = 1

Sehingga pasangan kunci yang didapat adalah :

Kunci enkripsi (public key) (e,n) = (79, 6059) dan

Kunci dekripsi (private key) (d,n) = (4783, 6059)

4.3.1 Perhitungan Enkripsi Data

Setelah didapat nilai dari kunci enkripsi (*public key*), maka selanjutnya adalah melakukan enkripsi data. Data yang akan dienkripsi adalah data Nama, Alamat, Status, Tarif, dan Jumlah Tunggakan.

Pertama yang harus dilakukan adalam merubah data asli (*plaintext*) menjadi format ASCII sebagai Berikut :

1. Proses Enkripsi Nama

   Plaintext : Denny Andrian

   Kemudian *Plaintext* akan dipecah menjadi tiap-tiap karakter sebagai berikut :

Tabel 4.1 Karakter m_i dan Kode ASCII untuk Data Nama

m_i	Keterangan	Kode ASCII
m_1	D	68
m_2	e	101
m_3	n	110
m_4	n	110
m_5	y	121
m_6	(spasi)	32
m_7	A	65
m_8	n	110
m_9	d	100
m_{10}	r	114
m_{11}	i	105
m_{12}	a	97
m_{13}	n	110

Setelah dibagi perkarakter, selanjutnya dienkripsi dengan rumus :

$c_i = m_{i^e} \ mod \ n$

$c_1 = 68^{79} \ mod \ 6059 \quad = 3489$

$c_2 = 101^{79} \ mod \ 6059 \quad = 449$

$c_3 = 110^{79} \ mod \ 6059 \quad = 588$

$c_4 = 110^{79} \ mod \ 6059 \quad = 588$

$c_5 = 121^{79} \ mod \ 6059 \quad = 286$

$c_6 = 32^{79} \ mod \ 6059 \quad = 2446$

$c_7 = 65^{79} \ mod \ 6059 \quad = 5029$

$c_8 = 110^{79} \ mod \ 6059 \quad = 588$

$c_9 = 100^{79} \ mod \ 6059 \quad = 192$

$c_{10} = 114^{79} \ mod \ 6059 \quad = 401$

$c_{11} = 105^{79} \ mod \ 6059 \quad = 3614$

c_{12} = 97^{79} *mod* 6059 = 4283

c_{13} = 110^{79} *mod* 6059 = 588

Maka, setelah dienkripsi hasilnya yaitu : 3489, 449, 588, 588, 286, 2446, 5029, 588, 192, 401, 3614, 4283, 588.

2. Proses Enkripsi Alamat

Plaintext : Jl. Sei Musi No.52

Kemudian *Plaintext* akan dipecah menjadi tiap-tiap karakter sebagai berikut :

Tabel 4.2 Karakter m_i dan Kode ASCII untuk Data Alamat

m_i	**Keterangan**	**Kode ASCII**
m_1	J	74
m_2	l	108
m_3	. (titik)	46
m_4	(Spasi)	32
m_5	S	83
m_6	e	101
m_7	i	105
m_8	(spasi)	32
m_9	M	77
m_{10}	u	117
m_{11}	s	115
m_{12}	i	105
m_{13}	(spasi)	32
m_{14}	N	78
m_{15}	o	111
m_{16}	. (titik)	46
m_{17}	5	53
m_{18}	2	50

Setelah dibagi perkarakter, selanjutnya dienkripsi dengan rumus :

$c_i = m_{i^e}$ *mod n*

c_1 = 74^{79} *mod* 6059 = 1388

c_2 = 108^{79} *mod* 6059 = 2494

c_3 = 46^{79} *mod* 6059 = 4334

c_4 = 32^{79} *mod* 6059 = 2446

c_5 = 83^{79} *mod* 6059 = 3818

c_6 = 101^{79} *mod* 6059 = 449

c_7 = 105^{79} *mod* 6059 = 3614

c_8 = 32^{79} *mod* 6059 = 2446

c_9 = 77^{79} *mod* 6059 = 908

c_{10} = 117^{79} *mod* 6059 = 3178

c_{11} = 115^{79} *mod* 6059 = 2861

c_{12} = 105^{79} *mod* 6059 = 3614

c_{13} = 32^{79} *mod* 6059 = 2446

c_{14} = 78^{79} *mod* 6059 = 745

c_{15} = 111^{79} *mod* 6059 = 1521

c_{16} = 46^{79} *mod* 6059 = 4334

c_{17} = 53^{79} *mod* 6059 = 2148

c_{18} = 50^{79} *mod* 6059 = 4856

Maka, setelah dienkripsi hasilnya yaitu :1388, 2494, 4334, 2446, 3818, 449, 3614, 2446, 908, 3178, 2861, 3614, 2446, 745, 1521, 4334, 2148, 4856.

3. Proses Enkripsi Status

Plaintext : Aktif

Kemudian *Plaintext* akan dipecah menjadi tiap-tiap karakter sebagai berikut :

Tabel 4.3 Karakter m_i dan Kode ASCII untuk Data Status

m_i	Keterangan	Kode ASCII
m_1	A	65
m_2	k	107
m_3	t	116
m_4	i	105
m_5	f	102

Setelah dibagi perkarakter, selanjutnya dienkripsi dengan rumus :

$c_i = m_{i^e} \ mod \ n$

$c_1 = 65^{79} \ mod \ 6059 \quad = 5029$

$c_2 = 107^{79} \ mod \ 6059 \quad = 3809$

$c_3 = 116^{79} \ mod \ 6059 \quad = 3278$

$c_4 = 105^{79} \ mod \ 6059 \quad = 3614$

$c_5 = 102^{79} \ mod \ 6059 \quad = 545$

Maka, setelah dienkripsi hasilnya yaitu : 5029, 3809, 3278, 3614, 545.

4. Proses Enkripsi Tarif

Plaintext : RT-4

Kemudian *Plaintext* akan dipecah menjadi tiap-tiap karakter sebagai berikut :

Tabel 4.4 Karakter m_i dan Kode ASCII untuk Data Tarif

m_i	Keterangan	Kode ASCII
m_1	R	82
m_2	T	84
m_3	-	45
m_4	4	52

Setelah dibagi perkarakter, selanjutnya dienkripsi dengan rumus :

$c_i = m_{i^e} \ mod \ n$

$c_1 = 82^{79} \ mod \ 6059 \quad = 82$

$c_2 = 84^{79} \ mod \ 6059 \quad = 4566$

$c_3 = 45^{79} \ mod \ 6059 \quad = 5026$

$c_4 = 52^{79} \ mod \ 6059 \quad = 5492$

Maka, setelah dienkripsi hasilnya yaitu : 82, 4566, 5026, 5492.

5. Proses Enkripsi Jumlah Tunggakan

Plaintext : Rp. 108.000

Kemudian *Plaintext* akan dipecah menjadi tiap-tiap karakter sebagai berikut :

Tabel 4.5 Karakter m_i dan Kode ASCII untuk Data Jumlah Tunggakan

m_i	Keterangan	Kode ASCII
m_1	R	82
m_2	P	112
m_3	. (titik)	46
m_4	(Spasi)	32
m_5	1	49
m_6	0	48
m_7	8	56
m_8	. (titik)	46
m_9	0	48
m_{10}	0	48
m_{11}	0	48

Setelah dibagi perkarakter, selanjutnya dienkripsi dengan rumus :

$c_i = m_{i^e} \ mod \ n$

$c_1 = 82^{79} \ mod \ 6059 \quad = 82$

$c_2 = 112^{79} \ mod \ 6059 \quad = 4367$

$c_3 = 46^{79} \ mod \ 6059 \quad = 4334$

c_4 = 32^{79} *mod* 6059 = 2446

c_5 = 49^{79} *mod* 6059 = 2798

c_6 = 48^{79} *mod* 6059 = 943

c_7 = 56^{79} *mod* 6059 = 2649

c_8 = 46^{79} *mod* 6059 = 4334

c_9 = 48^{79} *mod* 6059 = 943

c_{10} = 48^{79} *mod* 6059 = 943

c_{11} = 48^{79} *mod* 6059 = 943

Maka, setelah dienkripsi hasilnya yaitu : 82, 4367, 4334, 2446, 2798, 943, 2649, 4334, 943, 943, 943.

4.3.2 Perhitungan Dekripsi Data

Dekripsi data merupakan sebuah proses mengembalikan data yang telah dienkripsi kembali ke data asli.

1. Dekripsi Data Nama

   Ciphertext : 3489, 449, 588, 588, 286, 2446, 5029, 588, 192, 401, 3614, 4283, 588.

   Untuk merubah kembali data yang telah dienkripsi menjadi data asli (*Plaintext*) dapat menggunakan rumus :

   $m_i = c_i{}^d \ mod \ n$. Berikut Penyelesaiyannya:

   m_1= 3489^{4783} *mod* 6059 = 68

   m_2= 449^{4783} *mod* 6059 = 101

   m_3= 588^{4783} *mod* 6059 = 110

   m_4= 588^{4783} *mod* 6059 = 110

m_5= 286^{4783} *mod* 6059 = 121

m_6= 2446^{4783} *mod* 6059 = 32

m_7= 5029^{4783} *mod* 6059 = 65

m_8= 588^{4783} *mod* 6059 =110

m_9= 192^{4783} *mod* 6059 =100

m_{10}= 401^{4783} *mod* 6059 =114

m_{11}= 3614^{4783} *mod* 6059 =105

m_{12}= 4283^{4783} *mod* 6059 = 97

m_{13}= 588^{4783} *mod* 6059 =110

Maka hasil dekripsi yaitu, 68 101 110 110 121 32 65 110 100 114 105 97 110.

Dalam karakter ASCII adalah :

ASCII : 68 101 110 110 121 32 65 110 100 114 105 97 110

Karakter : Denny Andrian

2. Dekripsi Data Alamat

Ciphertext : 1388, 2494, 4334, 2446, 3818, 449, 3614, 2446, 908, 3178, 2861, 3614, 2446, 745, 1521, 4334, 2148, 4856.

Untuk merubah kembali data yang telah dienkripsi menjadi data asli (*Plaintext*) dapat menggunakan rumus :

m_i= $c_i{}^a$ *mod* n. Berikut Penyelesaiyannya:

m_1= 1388^{4783} *mod* 6059 = 74

m_2= 2494^{4783} *mod* 6059 = 108

m_3= 4334^{4783} *mod* 6059 = 46

m_4= 2446^{4783} *mod* 6059 = 32

$m_5 = 3818^{4783} \ mod \ 6059 \quad = 83$

$m_6 = 449^{4783} \ mod \ 6059 \quad = 101$

$m_7 = 3614^{4783} \ mod \ 6059 \quad = 105$

$m_8 = 2446^{4783} \ mod \ 6059 \quad = 32$

$m_9 = 908^{4783} \ mod \ 6059 \quad = 77$

$m_{10} = 3178^{4783} \ mod \ 6059 \quad = 117$

$m_{11} = 2861^{4783} \ mod \ 6059 \quad = 115$

$m_{12} = 3614^{4783} \ mod \ 6059 \quad = 105$

$m_{13} = 2446^{4783} \ mod \ 6059 \quad = 32$

$m_{14} = 745^{4783} \ mod \ 6059 \quad = 78$

$m_{15} = 1521^{4783} \ mod \ 6059 \quad = 111$

$m_{16} = 4334^{4783} \ mod \ 6059 \quad = 46$

$m_{17} = 2148^{4783} \ mod \ 6059 \quad = 53$

$m_{18} = 4856^{4783} \ mod \ 6059 \quad = 50$

Maka hasil dekripsi yaitu, 74 108 46 32 83 101 105 32 77 117 115 105 32 78 111 46 53 50. Dalam karakter ASCII adalah :

ASCII : 74 108 46 32 83 101 105 32 77 117 115 105 32 78 111 46 53 50

Karakter : Jl. Sei Musi No.52

3. Dekripsi Data Status

Ciphertext : 5029, 3809, 3278, 3614, 545

Untuk merubah kembali data yang telah dienkripsi menjadi data asli (*Plaintext*) dapat menggunakan rumus :

$m_i = c_i^d \ mod \ n$. Berikut Penyelesaiyannya:

$m_1 = 5029^{4783} \ mod \ 6059$ = 65

$m_2 = 3809^{4783} \ mod \ 6059$ = 107

$m_3 = 3614^{4783} \ mod \ 6059$ = 116

$m_4 = 545^{4783} \ mod \ 6059$ = 105

$m_5 = 3818^{4783} \ mod \ 6059$ = 102

Maka hasil dekripsi yaitu,. Dalam karakter ASCII adalah :

ASCII : 65 107 116 105 102

Karakter : Aktif

4. Dekripsi Data Tarif

Ciphertext : 82, 4566, 5026, 5492.

Untuk merubah kembali data yang telah dienkripsi menjadi data asli (*Plaintext*) dapat menggunakan rumus :

$m_i = c_i^d \ mod \ n$. Berikut Penyelesaiyannya:

$m_1 = 82^{4783} \ mod \ 6059$ = 82

$m_2 = 4566^{4783} \ mod \ 6059$ = 84

$m_3 = 5026^{4783} \ mod \ 6059$ = 45

$m_4 = 5492^{4783} \ mod \ 6059$ = 52

Maka hasil dekripsi yaitu,. Dalam karakter ASCII adalah :

ASCII : 82 84 45 52

Karakter : RT-4

5. Dekripsi Data Jumlah Tunggakan

   Ciphertext : 82, 4367, 4334, 2446, 2798, 943, 2649, 4334, 943, 943, 943.

   Untuk merubah kembali data yang telah dienkripsi menjadi data asli (*Plaintext*) dapat menggunakan rumus :

   $m_i = c_i{}^d \ mod\ n$. Berikut Penyelesaiyannya:

   $m_1 = 82^{4783} \ mod\ 6059 = 82$

   $m_2 = 4367^{4783} \ mod\ 6059 = 112$

   $m_3 = 4334^{4783} \ mod\ 6059 = 46$

   $m_4 = 2446^{4783} \ mod\ 6059 = 32$

   $m_5 = 2798^{4783} \ mod\ 6059 = 49$

   $m_6 = 943^{4783} \ mod\ 6059 = 48$

   $m_7 = 2649^{4783} \ mod\ 6059 = 56$

   $m_8 = 4334^{4783} \ mod\ 6059 = 46$

   $m_9 = 943^{4783} \ mod\ 6059 = 48$

   $m_{10} = 943^{4783} \ mod\ 6059 = 48$

   $m_{11} = 943^{4783} \ mod\ 6059 = 48$

   Maka hasil dekripsi yaitu, Dalam karakter ASCII adalah :

   ASCII : 82 112 46 32 49 48 46 48 48 48

   Karakter : Rp. 108.000

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarakan perumusan masalah, analisa, perancangan,implemantasi dan pengujian aplikasi yang dilakukan. Maka, kesimpulan yang didapat yaitu :

1. Aplikasi ini mampu untuk mengamankan data tunggakan tagihan air pelanggan di PDAM Tirtanadi Sunggal sehingga keamanan data pelanggan tersebut dapat terjamin kerahasiaanya.
2. Hasil enkripsi data berupa pengkodean yang didapat dari bilangan ASCII yang sulit diterjemahkan.
3. Dalam aplikasi penerapan algoritma RSA dalam pengamanan data tunggakan tagihan air di PDAM Tirtanadi Sunggal ini kunci publik dan kunci privat telah dimasukan kedalam aplikasi secara otomatis. Sehingga memudahkan pengguna dalam menjalankan proses enkripsi dan dekripsi.

5.2 Saran

Untuk lebih mengembangkan dan meningkatkan aplikasi penerapan algoritma RSA dalam pengamanan data tunggakan tagihan air di PDAM Tirtanadi Sunggal. Pada penelitian ini menggunakan metode RSA, diharapkan pada penelitian selanjutnya dapat dikembangkan dengan menggunakan algoritma kriptografi lainnya atau dengan mengkombinasikan metode RSA dengan algoritma kriptografi lain agar data semakin kuat keamananya.

DAFTAR PUSTAKA

Adianson Niko., Yupianti., & Kurniawan Adhadi. (2015). Analisa Perbandingan Performansi RSA (Rivest Shamir Adleman) Dan ECC (Elliptic Curve) Pada Protokol Secure Socket Layer (SSL). *Jurnal Media Infotama*, 11(1), 72-80.

Agency Beranda. 2015. MS Access untuk Database Bisnis Perkantoran. Jakarta : PT Elex Media Komputindo.

Amin Miftakul. (2016). Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks. *Jurnal Pseudocode*, 3(2), 129-136.

Azmi, Fadhillah, And Winda Erika. "Analisis Keamanan Data Pada Block Cipher Algoritma Kriptografi Rsa." Cess (Journal Of Computer Engineering, System And Science) 2.1: 27-29.

Bandung : Informatika.

Dian Islami C., Bunga Khodijah., & Candiwan. 2016. Kesadaran Keamanan Informasi Pada Pegawai Bank X di Bandung Indonesia. Jurnal INKOM, 10

Elizabeth Triana., & H Darmawan S. (2015). Sistem Informasi Pemakaian Sparepart Mesin Packing pada PT. XYZ. *Jastisi*, 1(2), 164-174.

Erika, Winda, Heni Rachmawati, and Ibnu Surya. "Enkripsi Teks Surat Elektronik (E-Mail) Berbasis Algoritma Rivest Shamir Adleman (RSA)." Jurnal Aksara Komputer Terapan 1.2 (2012).

Ginting Natalia F., & Ginting Misalina. (2017). Perbandingan Kriptografi RSA dengan Base64. *Jurnal Teknik Informatika*, 2(2), 47-52.

Hartanto, S. (2017). Implementasi fuzzy rule based system untuk klasifikasi buah mangga. TECHSI-Jurnal Teknik Informatika, 9(2), 103-122.

Harumy, T. H. F., & Sulistianingsih, I. (2016). Sistem penunjang keputusan penentuan jabatan manager menggunakan metode mfep pada cv. Sapo durin. In Seminar Nasional Teknologi Informasi dan Multimedia (pp. 6-7).

Havena, M., & Marlina, L. (2018). The Technology of Corn Processing as an Effort to Increase The Income of Kelambir V Village. Journal of Saintech Transfer, 1(1), 27-32.

Hendini Ade. (2016). Pemodelan Uml Sistem Informasi Monitoring Penjualan Dan Stok Barang (Studi Kasus: Distro Zhezha Pontianak). *Jurnal Khatulistiwa Informatika*, 4(2), 107-116.

Herdianto, H. (2018). Perancangan Smart Home dengan Konsep Internet of Things (IoT) Berbasis Smartphone. Jurnal Ilmiah Core IT: Community Research Information Technology, 6(2).

Heriyanto Yunahar. (2018). Perancangan Sistem Informasi Rental Mobil Berbasis Web Pada Pt.Apm Rent Car. *Jurnal Intra-Tech*. 2(2), 64-77.

Khairul, K., Haryati, S., & Yusman, Y. (2018). Aplikasi Kamus Bahasa Jawa Indonesia dengan Algoritma Raita Berbasis Android. Jurnal Teknologi Informasi dan Pendidikan, 11(1), 1-6.

Kisaran : Royal Asahan Press.

Marlina, L., Muslim, M., Siahaan, A. U., & Utama, P. (2016). Data Mining Classification Comparison (Naïve Bayes and C4. 5 Algorithms). Int. J. Eng. Trends Technol, 38(7), 380-383.

Marlina, L., Putera, A., Siahaan, U., Kurniawan, H., & Sulistianingsih, I. (2017). Data Compression Using Elias Delta Code. Int. J. Recent Trends Eng. Res, 3(8), 210-217.

Muchli Budi S., Budiman M A., & Rachmawati Dian. (2017). Teknik Pemecahan Kunci Algoritma Rivest Shamir Adleman (RSA) dengan Metode Kraitchi. *Jurnal & Penelitian Teknik Informatika*, 2(2), 49-64.

Munawar. (2018). Analisa Perancangan Sistem Berorientasi Objek Dengan UML.

Muttaqin, Muhammad. "Analisa Pemanfaatan Sistem Informasi E-Office Pada Universitas Pembangunan Panca Budi Medan Dengan Menggunakan Metode Utaut." Jurnal Teknik Dan Informatika 5.1 (2018): 40-43.

Muttaqin, Muhammad. "Portal Academic Portal Innovation Based On Website In The Era Of Digital 4.0 Technology Now."

Pabokory Fresly N., Astuti Indah F., & Kridalaksana Awang H. (2015). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File

Dokumen Menggunakan Algoritma Advanced Encryption Standard. *Jurnal Informatika Mulawarman*, 10 (1), 20-31.

Permana Aditya A., & Nurnaningsih Desi. (2018). Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (AES). *Jurnal Teknik Informatika*, 11(2), 177-186.

Perwitasari, I. D. (2018). Teknik Marker Based Tracking Augmented Reality untuk Visualisasi Anatomi Organ Tubuh Manusia Berbasis Android. INTECOMS: Journal of Information Technology and Computer Science, 1(1), 8-18.

Putra Satria D., & Rifqi Muhammad. (2017). Rancangan Implementasi Manajemen Database pada Background Process Menggunakan CrondManager Sebagai Upaya Peningkatan Performance dan Keamanan Data Secara Online: Studi Kasus PT. YZI. *Jurnal Format*, 6(2), 25-32.

Putri, R. E., & Siahaan, A. (2017). Examination of document similarity using Rabin-Karp algorithm. International Journal of Recent Trends in Engineering & Research, 3(8), 196-201.

Ramadhani, S., Suherman, S., Melvasari, M., & Herdianto, H. (2018). Perancangan Teks Berjalan Online Sebagai Media Informasi Nelayan. Jurnal Ilmiah Core IT: Community Research Information Technology, 6(2).

Rizal, Chairul. "Pengaruh Varietas dan Pupuk Petroganik Terhadap Pertumbuhan, Produksi dan Viabilitas Benih Jagung (Zea mays L.)." ETD Unsyiah (2013).

Sukamto Ariani R., & Shalahuddin M. (2014). Rekayasa Perangkat Lunak Struktur dan Berorientasi Objek. Bandung : Informatika.

Yesputra Rolly. (2017). Belajar Visual Basic. Net Dengan Visual Studio 2010.

Zainuddin Muhammad A., & Mulyana Dadang I. (2016). Penerapan Algoritma RSA Untuk Keamanan Pesan Instan Pada Perangkat Android. *Jurnal CKI On SPO*, 9 (2), 105-114.