

Perancangan Aplikasi Keamanan Data Gaji Karyawan Pada Prima Printing Dengan Menggunakan Metode Kriptografi RSA (Rivest, Shamir, Adleman)

Lidya Novita Sari Dalimunthe¹, Widiarti Rista Maya², Hafizah³

^{1,3}Program Studi Sistem Informasi, STMIK Triguna Dharma

²Program Studi Teknik Komputer, STMIK Triguna Dharma

Article Info

Article history:

Received Jan 12th, 2019

Revised Jan 20th, 2019

Accepted Jan 30th, 2019

Keyword:

Keamanan, Data Gaji
Karyawan, Perancangan
Aplikasi, Kriptografi RSA

ABSTRAK

Keamanan informasi atau data menjadi suatu hal yang sangat penting dalam pertukaran data, namun banyak juga ancaman pada proses pertukaran data dilakukan, terutama dokumen maupun data yang diasumsikan bersifat rahasia (private and confidential). Toko Prima Printing sering terjadi masalah pada data gaji karyawan dalam pengubahan dan penyalahgunaan data gaji yang menyebabkan kerugian beberapa pihak yang bersangkutan. Oleh karena itu, masalah keamanan data merupakan suatu aspek yang penting dari suatu sistem, untuk itu perlu diterapkan suatu metode pengamanan data. Pengamanan pada data dilakukan untuk menjaga kerahasiaan informasi dan agar aman dari orang-orang yang tidak bertanggung jawab, maka dilakukanlah pengamanan data dengan menggunakan algoritma kriptografi. Dalam kriptografi terdapat beberapa algoritma yang dapat digunakan, diantaranya RSA. RSA merupakan algoritma asimetris. RSA mempunyai dua kunci, yaitu kunci publik dan kunci pribadi. Kunci publik boleh diketahui oleh siapa saja, dan digunakan untuk proses enkripsi. Sedangkan kunci pribadi hanya pihak-pihak tertentu saja yang boleh mengetahuinya, dan digunakan untuk proses dekripsi. Dengan demikian hasil dari sistem yang telah dirancang, maka akan membantu pihak Prima Printing dalam menentukan keamanan data gaji karyawan yang lebih tepat, baik, dan akurat.

Copyright © 2019 STMIK Triguna Dharma.

All rights reserved.

Corresponding Author

Nama : Lidya Novita Sari Dalimunthe

Program Studi : Sistem Informasi

STMIK Triguna Dharma

Email: lidyanovitadlt226@gmail.com

1. PENDAHULUAN

Seperti yang kita ketahui bahwa pertukaran informasi atau data memang sangat menguntungkan bahkan krusial kepada beberapa organisasi, tak terkecuali pada prima printing. Keamanan informasi atau data menjadi suatu hal yang sangat penting dalam pertukaran data, namun banyak juga ancaman pada proses pertukaran data dilakukan, terutama dokumen maupun data yang diasumsikan bersifat rahasia (private and confidential). Dalam beberapa kasus, informasi data sangat rentan membuat kerugian pada organisasi maupun individual.

Pada Toko Prima Printing terjadi masalah data gaji karyawan yang sering terjadinya pengubahan dan penyalahgunaan data gaji yang menyebabkan kerugian beberapa pihak yang bersangkutan. Oleh karena itu, masalah keamanan data merupakan suatu aspek yang penting dari suatu sistem, untuk itu perlu diterapkan

suatu metode pengamanan data, dengan teknik kriptografi. Data gaji pada perusahaan ini berupa file text dari Microsoft Excel, lalu file tersebut akan di input pada aplikasi yang akan digunakan, dan hal ini rawan terjadinya manipulasi data yang menyebabkan kerugian pihak perusahaan [1].

Kriptografi merupakan ilmu untuk menjaga keamanan pesan yang dikirim dari suatu tempat ketempat yang lain . Pengamanan data ini dilakukan untuk menjaga kerahasiaan informasi dari orang-orang yang tidak bertanggung jawab, Maka dari itu pengamanan data dilakukan dengan menggunakan algoritma kriptografi [2].

Dalam kriptografi terdapat beberapa algoritma yang dapat digunakan, diantaranya RSA. RSA merupakan algoritma asimetris. Yang ditemukan pertama kali dia tahun 1977 oleh Ron Rivest, Adi Shamir, dan Leonard Adleman. Nama RSA diambil dari nama depan ketiga penemunya . RSA mempunyai dua kunci, yaitu kunci publik dan kunci pribadi. Kunci publik digunakan untuk proses enkripsi dan boleh diketahui oleh siapa saja . Sedangkan kunci pribadi hanya boleh diketahui pihak tertentu, dan digunakan untuk proses dekripsi [3].

Dalam beberapa referensi , RSA adalah algoritma yang digunakan untuk enkripsi kunci publik (public-key encryption). Algoritma adalah yang pertama diketahui paling cocok untuk menandai (signing) dan enkripsi (encryption) ini adalah salah satu penemuan pertama yang besar dalam kriptografi kunci publik. RSA sendiripun masih banyak digunakan secara luas dalam perdagangan elektronik, dan dipercayai sangat aman karena memberikan kunci-kunci yang sangat up-to-date (mutakhir) [4].

Berdasarkan permasalahan diatas maka dapat diangkat judul skripsi yaitu “Perancangan Aplikasi Keamanan Data Gaji Karyawan Pada Prima Printing Menggunakan Metode Kriptografi RSA (Rivest, Shamir, Adleman)”.

2. METODE PENELITIAN

2.1 Metode Penelitian

Pengumpulan data dilakukan untuk memperoleh informasi yang dibutuhkan apabila pengumpulan data dilakukan dengan tidak benar maka hasil dan kesimpulan bisa menjadi rancu [20].

1. Observasi

Dalam penelitian ini dilakukan observasi pra-riset terlebih dahulu untuk mencari masalah yang terjadi di prima printing Medan dalam pengamanan data gaji karyawan, dari masalah tersebut masalah akan dirumuskan dalam penelitian ini sehingga dapat menemukan rumusan apa saja yang perlu dipersiapkan untuk bagaimana cara menyelesaikan masalah tersebut.

2. Wawancara

Setelah itu dilakukan wawancara kepada pemilik bisnis printing atau prima printing Medan yang mempunyai andil dalam pengelolaan data pelanggan. Serta mencari solusi untuk kendala yang dihadapi oleh bagian pengamanan data itu sendiri selama ini. Berikut adalah data gaji karyawan yang didapatkan dari prima printing :

Tabel 2.1 Data Penggajian

No.	Nama Lengkap	Alamat	No Handphone	Posisi	Rate Gaji	Kehadiran
1	Lidya Novita	Medan, Jl.Sidodadi	081262241942	Desainer	70.000	24
2	Cici Syahara	Deli Tua, Jl.Cempaka	083197384650	Kasir	80.000	19
3	Shandy Suswanto	Medan, Jl.Johor	085296866840	Desainer	80.000	23
4	Dinda Widya	Patumbak, Jl.Langgar	081256458976	Desainer	70.000	15
5	Tita Chaniago	Medan, Jl.Cempaka	081260435006	Kasir	90.000	23

6	Febria Rusely	Johor, Jl.Eka Surya	081930392998	Desainer	65.000	18
7	Aryansyah Putra	Sunggal, Jl.Mawar	081361762267	Owner	150.000	24
8	Rizky syahputra	Marendal, Jl.Sejati	085624897536	Pencetak stiker	120.000	20
9	Marini Oktavia	Polonia, Jl.Cuka	082199546784	Desainer	65.000	18
10	Zaki Azizi	Kampung Baru, Jl.Tanjung	082369849922	Pencetak stiker	110.000	21
11	Fikri Haikal	Titi Kuning, Jl.Sedia	081967543289	Pemasang Stiker	75.000	17
12	Ahmad Bahary	Marendal, Jl.Roso	083100552287	Pemasang Stiker	70.000	15

2.2 Proses Enkripsi Algoritma Rivest Shamir Adleman (RSA)

Proses enkripsi algoritma Rivest Shamir Adleman (RSA), yaitu sebagai berikut:

1. Pilihlah bilangan prima dengan sembarang, dalam pemilihan ini, di pilih nilai prima (p) = 13 dan nilai (q) = 31.
2. Untuk mencari nilai dari kedua bilangan tersebut, maka dilakukan perkalian
 $n = p * q$
 $n = 13 * 31 = 403$
3. Hitung (ϕ) $n = (p-1) (q-1)$
 $n = 12 * 30 = 360$
4. Pilih nilai e dengan syarat $e > 1$ dan $greatest\ common\ divisor(e, 360) = 1$ Nilai e yang di ambil adalah 7.
5. Sehingga $de = 1 \pmod{360}$ dan $d < 360$
 $d * 7 = 1 \pmod{360}$
 $d * 7 \pmod{360} = 1$
 $d = 103$

Bukti:

$$103 * 7 \pmod{360} = 1$$

Sehingga pasangan kunci yang didapat adalah :

Kunci enkripsi (*public key*) (e, n) = (7, 403) dan Kunci dekripsi (*private key*) (d, n) = (103, 403)

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

Plaintext : M e d a n , J l . S i d o d a d i
 ASCII : 77 101 100 97 110 44 32 106 108 46 83 105 100 111 100 97 100 105

Kemudian p dipecah menjadi tiap karakter *plaintext*. Berikut ini adalah tabel P_i :

Tabel 2.2 Karakter P_i dan Kode ASCII untuk *Plaintext* Medan, jl.Sidodadi

P_i	Keterangan	Kode ASCII
P_1	M	77
P_2	e	101
P_3	d	100

<i>P4</i>	a	97
<i>P5</i>	n	110
<i>P6</i>	,	44
<i>P7</i>	Spasi	32
<i>P8</i>	J	106
<i>P9</i>	l	108
<i>P10</i>	.	46
<i>P11</i>	S	83

Lanjutan Tabel 2.2 Karakter *Pi* dan Kode ASCII untuk *Plaintext* Medan, Jl.Sidodadi

<i>Pi</i>	Keterangan	Kode ASCII
<i>P12</i>	i	105
<i>P13</i>	d	100
<i>P14</i>	o	111
<i>P15</i>	d	100
<i>P16</i>	a	97
<i>P17</i>	d	100
<i>P18</i>	i	105

Setelah dibagi perkarakter, selanjutnya dienkripsi dengan rumus $C_i = P_i^e \text{ mod } n$, yaitu sebagai berikut:

$$\begin{aligned}
 C_1 &= 77^7 \text{ mod } 403 = 116 \\
 C_2 &= 101^7 \text{ mod } 403 = 374 \\
 C_3 &= 100^7 \text{ mod } 403 = 152 \\
 C_4 &= 97^7 \text{ mod } 403 = 202 \\
 C_5 &= 110^7 \text{ mod } 403 = 384 \\
 C_6 &= 44^7 \text{ mod } 403 = 177 \\
 C_7 &= 32^7 \text{ mod } 403 = 280 \\
 C_8 &= 106^7 \text{ mod } 403 = 115 \\
 C_9 &= 108^7 \text{ mod } 403 = 147 \\
 C_{10} &= 46^7 \text{ mod } 403 = 240 \\
 C_{11} &= 83^7 \text{ mod } 403 = 73 \\
 C_{12} &= 105^7 \text{ mod } 403 = 365 \\
 C_{13} &= 100^7 \text{ mod } 403 = 152 \\
 C_{14} &= 111^7 \text{ mod } 403 = 71 \\
 C_{15} &= 100^7 \text{ mod } 403 = 152 \\
 C_{16} &= 97^7 \text{ mod } 403 = 202 \\
 C_{17} &= 100^7 \text{ mod } 403 = 152 \\
 C_{18} &= 105^7 \text{ mod } 403 = 365
 \end{aligned}$$

Tabel 2.3 Karakter C_i dan Kode untuk *Plaintext* Medan, jl.Sidodadi yang telah dienkripsi dengan algoritma Rivest Shamir Adleman (RSA)

C_i	Kode
C_1	116
C_2	374
C_3	152
C_4	202
C_5	384
C_6	177
C_7	280
C_8	115
C_9	147
C_{10}	240
C_{11}	73
C_{12}	365
C_{13}	152
C_{14}	71

Lanjutan Tabel 2.3 Karakter C_i dan Kode untuk *Plaintext* Medan, jl.Sidodadi yang telah dienkripsi dengan algoritma Rivest Shamir Adleman (RSA)

C_i	Kode
C_{15}	152
C_{16}	202
C_{17}	152
C_{18}	365

Maka, setelah dienkripsi hasilnya yaitu, 116, 374, 152, 202, 384, 177, 280, 115, 147, 240, 73, 365, 152, 71, 152, 202, 152, 365.

2.3 Proses Deskripsi Algoritma Rivest Shamir Adleman (RSA)

Selanjutnya didekripsi kembali menggunakan algoritma Rivest Shamir Adleman (RSA) dengan rumus $P_i = C_i^d \text{ mod } n$, yaitu sebagai berikut:

$P_1 = 116^{103} \text{ mod } 403 = 77$
 $P_2 = 374^{103} \text{ mod } 403 = 101$
 $P_3 = 152^{103} \text{ mod } 403 = 100$
 $P_4 = 202^{103} \text{ mod } 403 = 97$
 $P_5 = 384^{103} \text{ mod } 403 = 110$
 $P_6 = 177^{103} \text{ mod } 403 = 44$
 $P_7 = 280^{103} \text{ mod } 403 = 32$
 $P_8 = 115^{103} \text{ mod } 403 = 106$
 $P_9 = 147^{103} \text{ mod } 403 = 108$
 $P_{10} = 240^{103} \text{ mod } 403 = 46$
 $P_{11} = 73^{103} \text{ mod } 403 = 83$
 $P_{12} = 365^{103} \text{ mod } 403 = 105$
 $P_{13} = 152^{103} \text{ mod } 403 = 100$
 $P_{14} = 71^{103} \text{ mod } 403 = 111$
 $P_{15} = 152^{103} \text{ mod } 403 = 100$
 $P_{16} = 202^{103} \text{ mod } 403 = 97$
 $P_{17} = 152^{103} \text{ mod } 403 = 100$
 $P_{18} = 365^{103} \text{ mod } 403 = 105$

Maka, setelah didekripsi hasilnya yaitu, 77, 101, 100, 97, 110, 44, 32, 106, 108, 46, 83, 105, 100, 111, 100, 97, 100, 105 dalam karakter ASCII adalah:

ASCII : 77 101 100 97 110 44 32 106 108 46 83 105 100 111 100 97 100 105

Karakter : M e d a n , J l . S i d o d a d i

3. ANALISA DAN HASIL

Hasil tampilan antarmuka adalah tahapan dimana sistem atau aplikasi siap untuk dioperasikan pada keadaan yang sebenarnya sesuai hasil analisis dan perancangan yang dilakukan.

3.1 Tampilan *Form Login*

Halaman ini berfungsi sebagai tampilan awal sebelum *login* dari aplikasi yang dibuat sebagai berikut :

Gambar 3.1 Form Login

3.2 Tampilan *Form Menu Utama*

Halaman ini berfungsi sebagai tampilan awal setelah login dari aplikasi yang dibuat sebagai berikut :

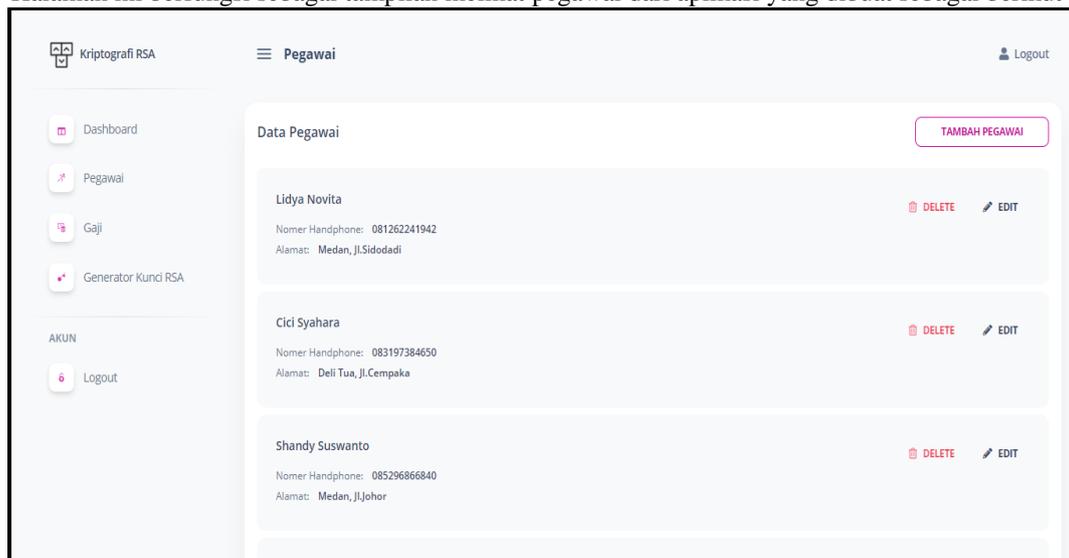


Gambar 3.2 From Utama Tampilan Form Alternatif

3.3 Halaman Administrator

1. From Data Pegawai

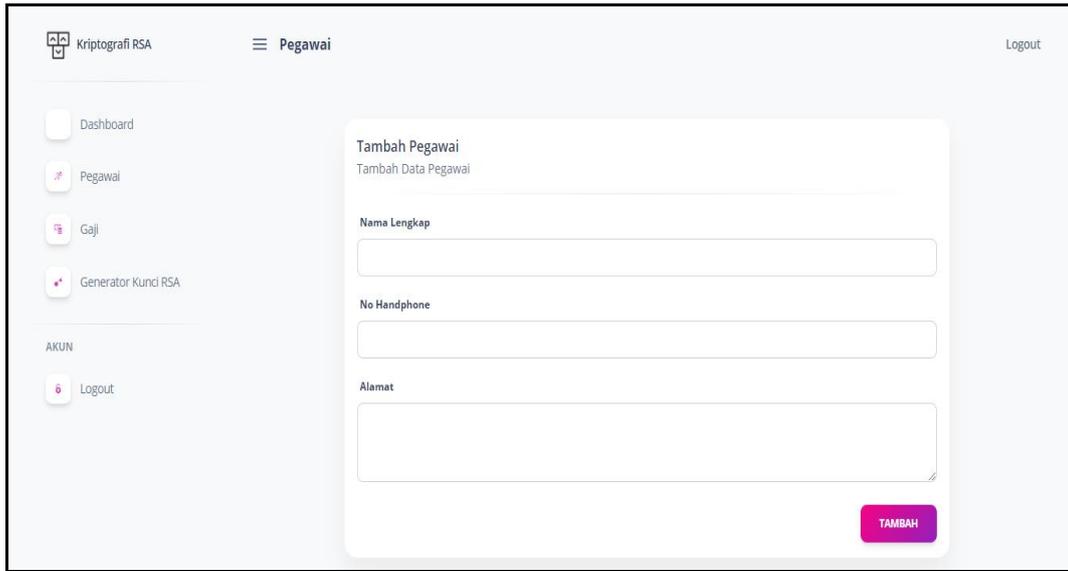
Halaman ini berfungsi sebagai tampilan melihat pegawai dari aplikasi yang dibuat sebagai berikut :



Gambar 3.3 From Data Pegawai

2. From Tambah Data Pegawai

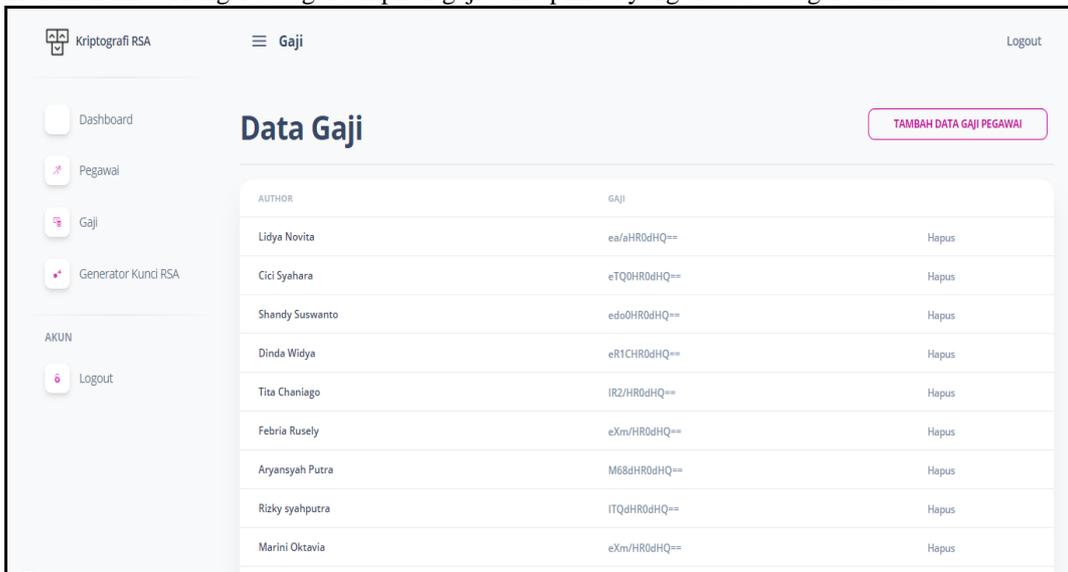
Halaman ini berfungsi sebagai tampilan tambah pegawai dari aplikasi yang dibuat sebagai berikut :



Gambar 3.4 From Tambah Data Pegawai

3. From Data Gaji

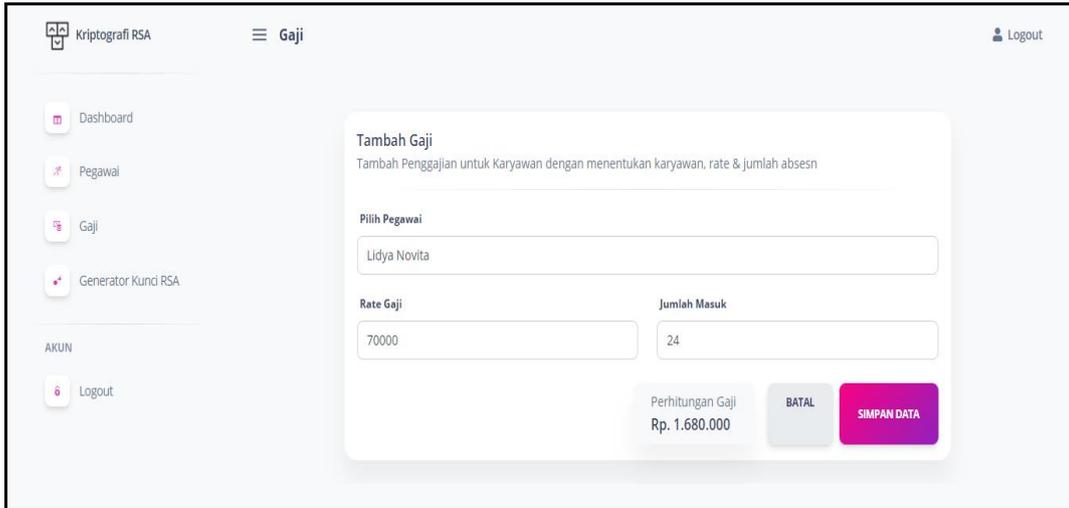
Halaman ini berfungsi sebagai tampilan gaji dari aplikasi yang dibuat sebagai berikut :



Gambar 3.5 From Data Gaji

4. From Tambah Gaji

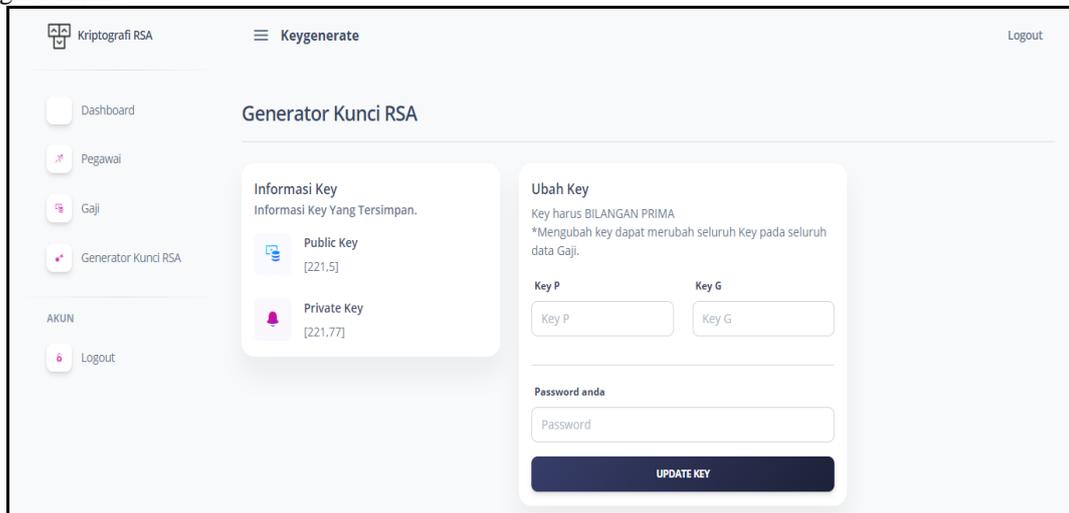
Halaman ini berfungsi sebagai tampilan penilaian dari aplikasi yang dibuat sebagai berikut :



Gambar 3.6 From Data Tambah Gaji

5. Form Generator Kunci RSA

Halaman ini berfungsi sebagai tampilan pengujian Generator Kunci RSA dari aplikasi yang dibuat sebagai berikut :



Gambar 3.7 From Generator Kunci RSA

4. KESIMPULAN

Berdasarkan penelitian yang telah dilalui dalam setiap tahapan perancangan keamanan data gaji karyawan dengan menggunakan metode RSA maka dapat disimpulkan bahwa :

1. Untuk mengamankan data gaji karyawan pada Prima Printing menggunakan metode RSA sebab data laporan hasil pengujian ini bersifat rahasia.
2. Algoritma RSA ini sangat membantu mengurangi resiko penyalahgunaan pada data laporan gaji karyawan sehingga dapat memudahkan admin dalam menginput hasil pengujian.
3. Perancangan keamanan data gaji karyawan dengan menggunakan metode RSA dalam aplikasi berbasis *website* sesuai dengan kebutuhan Prima Ptinting.

UCAPAN TERIMA KASIH

Puji syukur dipanjatkan kehadirat Allah Subhanu wa ta'ala karena berkat rahmat dan hidayah-Nya, yang masih memberikan kesehatan dan kesempatan sehingga dapat diselesaikan jurnal ilmiah ini dengan baik. ucapan terima kasih ditujukan kepada kedua Orang tua, atas kesabaran, ketabahan serta ketulusan hati memberikan dorongan moril maupun material serta do'a yang tiada henti-hentinya. Ucapan terimakasih juga ditujukan untuk pihak-pihak yang telah mengambil bagian dalam penyusunan jurnal ilmiah ini.

REFERENSI

- [1] Jaka Prayudha, Saniman, Ishak, "Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode *Advanced Encryption Standard* (AES)," Vol.18, No.2, Agustus 2019.
- [2] Kori Carda Puspita, "Implementasi Kriptografi Dengan Metode RSA Menggunakan Java," 2016.
- [3] Ivan Wibowo, Budi Susanto, Junius Karel T, "Penerapan Algoritma Kriptografi Asimetris RSA Untuk Keamanan Data Di Oracle," *J. Inform.* 2008.
- [4] Zainal Arifin, "Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman," Vol 4 No. 3 September 2009.
- [5] Muhammadiyah Pacitan Reny Utami, Informasi, S., Pada, P., Menengah, S., Pacitan, M., & Utami, R. (2014). "Sistem Informasi Penggajian Pada Sekolah Menengah Atas (SMA)" 6(3), 32–35.

BIBLIOGRAFI PENULIS

	<p>Lidya Novita Sari Dalimunthe Perempuan kelahiran Medan, 02 November 1998 anak ke 1 dari 3 bersaudara pasangan Bapak Ali Aman Dalimunthe dan Ibu Fitri Armaya Sari, Mempunyai pendidikan Sekolah Dasar SD Swasta Muhajirin Medan tamat tahun 2010, kemudian melanjutkan pendidikan Sekolah Menengah Pertama SMP Negeri 34 Medan tamat tahun 2013, kemudian melanjutkan pendidikan Sekolah Menengah Atas SMA Swasta Angkasa Medan tamat tahun 2016. Saat ini menempuh pendidikan Strata Satu (S-1) di STMIK Triguna Dharma Medan serta aktif sebagai mahasiswa.</p> <p>Program Studi : Sistem Informasi E-Mail : lidyanovitadlt226@gmail.com</p>
	<p>Widiarti Rista Maya, St., M.Kom NIDN : 0102128603 Program Studi : Teknik Komputer Deskripsi : Dosen Tetap STMIK Triguna Dharma yang aktif mengajar dan fokus pada bidang Ilmu Komputer dengan bidang keilmuan yaitu Simulasi, Kriptografi, Pemrograman Berbasis Visual Dan Pemrograman Berbasis Web E-Mail : widiartirm87@gmail.com</p>
	<p>Hafizah, S.Kom., M.Kom NIDN : 0122059001 Program Studi : Sistem Informasi Deskripsi : Dosen Tetap STMIK Triguna Dharma yang aktif mengajar dan fokus pada bidang Keilmuan Ilmu Komputer, Sistem Informasi = JST, SPK, Basis Data E-Mail : hafizah22isnartiilyas@gmail.com</p>