Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 22 ; Nomor 2 ; Agustus 2023 ; Page 528-538
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index

Implementasi Algoritma Kriptografi RSA (*Rivest Shamir Adleman*) Dalam Pengamanan Data Gaji Karyawan Di Kantor BSPJI

Siti Julianita Siregar[1], Nurcahyo Budi Nugroho[2], Hendrik Sigalingging[3]

[1,2,3]Sistem Informasi, STMIK Triguna Dharma, Medan, Indonesia
Email: [1]siti.julianita18@gmail.com, [2]nurcahyobn@gmail.com, [3,*]Hendrik.sigalik123@gmail.com
Email Penulis Korespondensi: siti.julianita18@gmail.com

Article History:
Received Jun 12th, 2023
Revised Aug 20th, 2023
Accepted Aug 26th, 2023

Abstrak

Keamanan informasi atau data menjadi suatu hal yang sangat penting dalam pertukaran data, namun banyak juga ancaman pada proses pertukaran data dilakukan, terutaman dokumen maupun data yang diasumsikan bersifat rahasia (*private and confidential*). Kantor BSPJI 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 suatu pengamanan data dengan menggunakan algortima 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 Kantor BSPJI dalam menentukan keamanan data gaji karyawan yang lebih tepat, baik, dan akurat.

Kata Kunci : Gaji, Keamanan, Kriptografi, RSA

Abstract

Information or data security is very important in data exchange, but there are also many threats to the data exchange process, especially documents and data that are assumed to be private and confidential. The BSPJI office often has problems with employee salary data in changing and misusing salary data which causes losses to several parties concerned. Therefore, the problem of data security is an important aspect of a system, for that it is necessary to apply a data security method. Data security is carried out to maintain the confidentiality of information and to keep it safe from irresponsible people, so data security is carried out using cryptographic algorithms. In cryptography there are several algorithms that can be used, including RSA. RSA is an asymmetric algorithm. RSA has two keys, a public key and a private key. The public key may be known by anyone, and is used for the encryption process. Whereas the private key is only certain parties who are allowed to know it, and is used for the decryption process. Thus the results of the system that has been designed will assist the BSPJI Office in determining the security of employee salary data that is more precise, good, and accurate.

Keyword : *Salary, Security, Cryptography, RSA*

1. PENDAHULUAN

Data gaji merupakan salah satu data yang bersifat rahasia dan hanya dapat dilihat oleh pihak-pihak tertentu, seperti bendahara dan kepala kantor. Gaji merupakan suatu hal yang sudah sangat pokok pada kegiatan finansial pada sebuah instansi perusahaan, karena hal tersebut berpengaruh terhadap kinerja para karyawan. Kantor BSPJI (Balai

Standardisasi Pelayanan jasa Industri) Medan adalah salah satu unit pelaksana teknis kementerian perindustrian republik Indonesia yang bertanggung jawab kepada badan standardisasi dan kebijakan jasa industri (BSKJI). Didalam perusahaan ini data gaji karyawannya dijaga agar tidak disalah gunakan atau dimanipulasi oleh orang-orang yang tidak berhak dan akan menimbulkan kerugian bagi perusahaan. Dalam hal ini diperlukan sebuah sistem dalam pengamanan data yang dapat melakukan penyandian dan pengacakan sebuah informasi yang berbasis komputer [1].

Keamanan data merupakan hal yang sangat penting di era digital pada saat ini, berbagai permasalah keamanan data yang sering muncul diantari lain seperti pencurian data, perusakan data, dan penyadapan informasi. Jika data informasi ini jatuh ke tangan orang yang tidak bertanggung jawab, maka data informasi ini akan dapat disalahgunakan atau dijadikan sumber pencarian uang secara ilegal, oleh karena itu dibutuhkan suatu mekanisme pengamanan data untuk memastikan suatu data tetap aman terhadap pihak-pihak yang tidak berwenang [2].

Kriptografi adalah seni dan ilmu untuk mengamankan data yang akan dikirim, dengan menjadikanya kode tertentu dan hanya ditunjukan kepada orang yang memiliki sebuah kunci untuk mengubah struktur kode itu kembali, yang berfungsi dalam menjaga kerahasiaan data atau pesan [3].

Setiap algoritma kriptografi memiliki tingkat keamanan yang berbeda-beda, begitu juga dengan tingkat enkripsi dan dekripsi yang berbeda dengan algoritma lainnya. Salah satu algoritma dengan metode perlindungan data yang paling banyak digunakan adalah metode *RSA* (*Rivest Shamir Adleman*), yang merupakan salah satu algoritma *public key* yang paling populer dipakai hingga pada saat ini. Algoritma *RSA* masih dianggap aman dikaranakan perluasan dari *caesar cipher*, yang menggalikan *plainteks* dengan sebuah nilai dan menambahkannya dengan sebuah pergeseran [4].

Algoritma RSA dipilih dalam penelitian ini karena dirasa sangat cocok untuk membantu proses enkripsi dokumen simpan p injam uang, proses perumusan algoritma RSA menggunakan du a kunci yaitu kunci pribadi dan kunci publik dengan begitu membantu proses enkripsi dokumen agar tidak mudah diketahui oleh pihak ketiga yang tidak beertanggung jawab.

Pada tahun 1977, *Rivest, Shamir, dan Adleman* merumuskan algoritma praktis yang mengimplementasikan sistem kriptografi kunci publik yang disebut dengan sistem kriptografi *RSA*. Meskipun pada tahun 1997 badan sandi Inggris membulikasikan bahwa *Clifford Cock* telah merumuskan sistem kriptografi *RSA* 3 tahun lebih dahulu daripada *Rivest, Shamir, dan Adleman.* Keamanan algoritma *RSA* terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Dengan demekian jika terjadi kebocoran data informasi tersebut maka data tersebut tidak dapat digunakan atau tidak dapat dibaca dengan baik. Pengimplementasian algoritma *RSA* dirasa perlu untuk menjamin keamanan data informasi tersebut.

Pada penelitian ini, akan dibangun sistem keamanan data gaji karyawan di kantor BSPJI (Balai Standardisasi Pelayanan Jasa Industri) menggunakan metode RSA. Sistem ini bertujuan untuk menjaga keamanan data – data para karyan BSPJI secara optimal. Sistem ini akan membantu para karyawab BSPJI dalam menjaga keamanan data gaji karyawan.

Dengan penjelsan tersebut maka dalam penelitian ini diangkat judul "Implementasi Algoritma Kriptografi RSA (Rivest Shamir Adleman) Dalam Pengamanan Data Gaji karyawan Di Kantor BSPJI (Balai Standardisasi Pelayanan jasa Industri)".

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Metode penelitian adalah cara-cara ilmiah untuk mendapatkan data yang *valid*, dengan tujuan dapat ditemukan,dikembangkan dan dibuktikan, suatu pengetahuan tertentu sehingga pada gilirannya dapat digunakan untuk memahami, memecahkan dan mengantisipasi masalah.

1. Observasi
   Dalam penelitian ini dilakukan observasi pra-riset terlebih dahulu untuk mencari masalah yang terjadi di kantor BSPJI dalam pengamanan data gaji karyawan, dari masalah tersebut masalah akan dirumusakan 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 perusahan kantor BSPJI Medan yang mempunyai hak dalam pengelolaan data karyawan. Serta mencari solusi untuk kendala yang dihadapi oleh bagian pengamanan data itu sendiri selama ini.

2.2 Data

Data merupakan komponen utama dari sistem informasi perusahaan karena proses pengambilan keputusan berasal dari data. Oleh karena itu sudah sewajarnya jika pengolahan data dipandang sebagai kebutuhan primer oleh perusahaan.

Pengolahan data yang buruk dapat mengakibatkan tidak tersedianya data penting yang digunakan untuk menghasilkan informasi yang diperlukan dalam pengambilan keputusan. Data memiliki fungsi yang sangat penting bagi kinerja perusahaan [5].

2.3 Kriptografi

Kriptografi terdiri dari dua kata yang merupakan bahasa yunani yaitu *"cripto"* dan *"graphia"*. *"crypto"* yang mempunyai arti yaitu *"scret* (rahasia)*"* dan *"graphia"* yang mempunayai arti yaitu *"writing* (tulisan)*"*. Pengertian kriptografi itu sendiri yaitu ilmu dan seni yang menjaga keamanan pesan ketika pesan dikirimkan dari suatu tempat ke tempat lain. Tujuan dari kriptografi yang juga merupakan aspek keamanan yang mendasar antara lain kerahasiaan *(confidentiality)*, autentikasi *(authentication)*, integritas data atau keutuhan data *(data integrity)* dan tak terbantahkan *(non-repudiation)*" [6].

Dengan kata lain, kriptografi adalah seni dan ilmu mengamankan suatu informasi agar informasi tersebut menjadi tidak dapat dipahami oleh pihak ketiga yang tidak mempunyai wewenang [13]. Dalam dunia enkripsi, pesan disebut *plaintext* atau *cleartext.* Proses menyembunyikan pesan sehingga menyembunyikan isi aslinya disebut enkripsi. Pesan terenkripsi disebut *ciphertext*. Proses mengembalikan teks terenkripsi menjadi teks biasa disebut dekripsi.

2.4 Komponen-Komponen Pada Kriptografi

Krpotografi terdiri dari berbagai komponen pendukung, seperti berikut [7] :

1. Enkripsi
   Enkripsi sangat penting dalam kriptografi, yaitu metode untuk melindungi data yang dikirim agar tetap rahasia. Pesan aslinya disebut Teks biasa, diubah menjadi kode-kode yang sulit dipahami.
2. Dekripsi
   Dekripsi adalah kebalikan dari enkripsi. Pesan terenkripsi dipulihkan dalam bentuk aslinya. Algoritma yang digunakan untuk dekripsi pasti berbeda dengan algoritma yang digunakan untuk *enkripsi*.
3. Kunci
   Adalah kunci yang dipakai untuk melakukan *enkripsi* dan dekripsi. Kunci terbagi menjadi dua bagian, yaitu *private key* dan *public key*.
4. *Chipertext*
   Merupakan suatu pesan yang telah melalui proses *enkripsi.* Pesan yang ada pada teks kode ini tidak bisa dibaca karena berupa karakter-karakter yang tidak mempunyai makna.
5. *Plaintext*
   Sering disebut dengan teks asli atau teks biasa ini merupakan pesan yang diketik yang memiliki makna. Teks asli inilah yang diproses menggunakan algoritma kriptografi untuk menjadi *chipertext* (teks-kode).

2.5 Tujuan Kriptografi

Kriptografi bertujuan untuk memberikan layanan keamanan informasi (yang dinamakan juga sebagai aspek-aspek keamanan informasi), yaitu [8] :

1. Kerahasiaan *(confidentiality)*
   Merupakan layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak- pihak yang tidak berhak.
2. Integritas Data *(integrity)*
   Merupakan layanan yang menjamin bahwa pesan masih utuh/asli atau belum pernah dimanipulasi selama pengiriman.
3. Otentikasi *(authentication)*
   Merupakan layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi *(user authentication atau entity authentication)* maupun mengidentifikasi kebenaran sumber pesan (data *origin authentication*).
4. Nir penyangkalan *(non repudiation)*
   Merupakan layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

2.6 Algoritma Kriptografi Asimetris

Kriptografi kunci asimetris memiliki kunci yang berbeda dalam proses enkripsi dan dekripsi, dikenal dengan *enkripsi* kunci publik. Salah satu kunci disebarkan (kunci publik) dan yang lainnya dirahasiakan (kunci *privat*). Apabila kunci *enkripsi* bersifat publik maka sistem membuka koneksi *privat* dari publik untuk membuka kunci pengguna. Apabila kunci dekripsi bersifat publik maka sistem berperan sebagai verifikasi data yang dikunci oleh pemilik kunci privat [9].

Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 22 ; Nomor 2 ; Agustus 2023 ; Page 528-538
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index

2.7 RSA (*Rivest Shamir Adleman*)

Algoritma *RSA* merupakan algoritma yang sering digunakan didalam dunia kriptografi dalam pengamanan data dan salah satu algoritma yang paling maju didalam dunia kriptografi. Algoritma *RSA* dikemukakan oleh *Ron Rivest*, *Adi Shamir*, dan *Leonard Adleman* dari *MIT* tahun 1977. Salah satu teknik pengamanan file dokumen menggunakan algoritma *RSA* adalah dengan cara mencocokkan kunci publik yang dimiliki oleh sipengirim file dokumen dan sipenerima file dokumen lalu untuk langkah selanjutnya dilakukan proses penguraian atau pengembalian kebentuk semula dengan menggunakan kunci *privat* [10].

2.8 Perhitungan RSA

Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci pribadi. Selama pemfaktoran bilangan besar menjadi faktor-faktor prima belum ditemukan algoritma yang mangkus, maka selama itu pula keamanan algoritma *RSA* tetap terjamin.
Langkah-langkah algoritma mendapatkan kunci publik dan kunci private adalah sebagai berikut [11] :

1. Pilih dua buah bilangan prima acak a,b (sangat rahasia).
2. Hitung n = p*q.
3. Hitung m = (p-1) * (q-1)
4. Pilih bilangan bulat yang memenuhi persyaratan pada rumus *gcd* (e,m) = 1
5. Hitung kunci untuk dekripsi (d) dengan rumus e.d mod m = 1.

Proses *Enkripsi* : $\mathbf{Pi = C^d \bmod n}$

Proses *Deskripsi* : $\mathbf{Ci = Pi^e \bmod n}$

Algoritma Kriptografi *RSA* memerlukan sepasang kunci yang dibangkitkan dengan memilih bilangan prima p dan q, beberapa besaran yang digunakan dalam mengenerate kunci *RSA* yaitu :

Tabel 1. *Generate* Kunci *RSA*

Besaran	Sifat
P dan q (bilangan prima)	Rahasia
N = p x q	Tidak Rahasia
Totient(n) = (p - 1)(q – 1)	Rahasia
e (Kunci *Enkripsi*)	Tidak Rahasia
d (Kunci *Dekripsi*)	Rahasia
m (*Plaintext*)	Rahasia
c (*Ciphertext*)	Tidak Rahasia

2.9 Kode ASCII

Kode ASCII merupakan sebuah kode atau huruf yang berstandar internasional dan bersifat universal, dan kepanjangan dari ASCII adalah *American Standar Code for Information Interchange*. Kode ASCII ini biasa digunakan untuk mewakili karakter-karakter angka maupun huruf didalam komputer. Pada gambar dibawah ini merupakan gambar tabel kode ASCII 8 bit standar internasional *(Nurul, 2017)* [12].

Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 22 ; Nomor 2 ; Agustus 2023 ; Page 528-538
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index

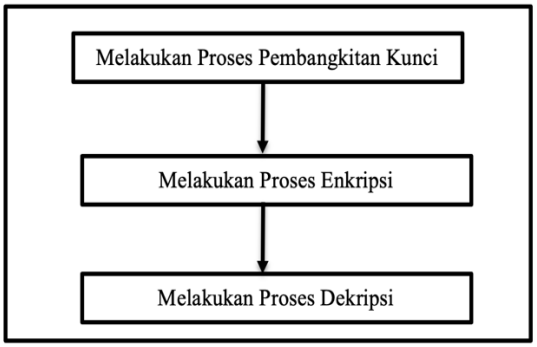
Tabel 2. Kode ASCII 8 Bit

Char	ASCII Code	Binary	Char	ASCII Code	Binary
a	097	01100001	**A**	065	01000001
b	098	01100010	**B**	066	01000010
c	099	01100011	**C**	067	01000011
d	100	01100100	**D**	068	01000100
e	101	01100101	**E**	069	01000101
f	102	01100110	**F**	070	01000110
g	103	01100111	**G**	071	01000111
h	104	01101000	**H**	072	01001000
i	105	01101001	**I**	073	01001001
j	106	01101010	**J**	074	01001010
k	107	01100011	**K**	075	01001011
l	108	01101100	**L**	076	01001100
m	109	01101101	**M**	077	01001101
n	110	01101110	**N**	078	01001110
o	111	01101111	**O**	079	01001111
p	112	01110000	**P**	080	01010000
q	113	01110001	**Q**	081	01010001
r	114	01110010	**R**	082	01010010
s	115	01110011	**S**	083	01010011
t	116	01110100	**T**	084	01010100
u	117	01110101	**U**	085	01010101
v	118	01110110	**V**	086	01010110
w	119	01110111	**W**	087	01010111
x	120	01111000	**X**	088	01011000
y	121	01111001	**Y**	089	01011001
z	122	01111010	**Z**	090	01011010

3. HASIL DAN PEMBAHASAN

3.1 Penerapan Metode RSA

Sistem keamanan dokumen simpan pinjam uang di badan usaha milik desa adalah dengan menggunakan metode RSA. Berikut kerangka kerja dari metode RSA.



Gambar 1. Kerangka Kerja Metode RSA

Kerangka kerja yang telah disusun dapat dijadikan pedoman dalam penerapan metode *RSA* untuk menyelesaikan permasalahan tentang keamanan data gaji karyawan BSPJI, berikut tahapan-tahapan dari kerangka kerja yang telah disusun:

1. Melakukan Proses Pembangkitan Kunci
   Pada tahap ini akan dilakukan proses pembangkitan kunci algoritma *RSA*, yaitu sebagai berikut :
   a. Menentukan dua bilangan prima antara 1-1000 yang nantinya akan diacak dan diinisialkan dengan p dan q. Kedua nilai tersebut harus dirahasiakan. Dipilih nilai prima p = 53 dan prima q = 73.

   b. Untuk memberi niali n dari kedua bilangan prima tersebut, maka harus melakukan perkalian.
      n = p * q
      n = 53 * 73
      n = 3869
   c. Hitung nilai *totien* (Ø) dengan cara
      Ø(n) = (p-1) (q-1)
      Ø(n) = (53-1) (73-1)
      Ø(n) = (52) (72)
      Ø(n) = 3744
   d. Secara sistematis *gcd*(e, Ø(n)) = 1.
      untuk mencarinya dapat menggunakan algoritma *Euclid*. Dengan rumus *GCD*(e, Ø(n)) = 1
      $e^{Ø(n)} = 1 \bmod n$ atau $e^{Ø(n)} \bmod n = 1$
      e = 71 sehingga *gcd*(71, 3744) = 1
   e. Membangkitkan kunci rahasia d, sehingga e*d = 1 mod(Ø(n)) atau d = (1+k. Ø(n))/e. untuk bilangan besar, dapat menggunakan algoritma *extended eculid*. Pada bagian ini nilai *k* merupakan sembarangan angka yang digunakan untuk menghasilkan suatu nilai interger atau bilangan bulat. Kita misalkan dengan d = (1+k. Ø(n))/e, nilai k = 15. Maka d = (1+k. Ø(n))/e. d = (1+15,3744)/71 = 791
      sehingga diperoleh pasangan kunci sebagai berikut:
      kunci public *(e, n)* = (71, 3869)
      kunci private *(d, n)* = (791, 3869)
2. Melakukan Proses Enkripsi
   Pada proses enkripsi ini menggunakan kunci *public* yaitu K = *(e, n)* = (71, 3869) dan dengan menggunakan rumus $C = P^e \bmod n$. Sebelum melakukan pengenkripsian data, hal yang harus dilakukan adalah merubah kata kunci tersebut menjadi pengkodean ASCII, berikut penyelesaiannya:

m =	1	9	6	0	1	0	0	3	1
	049	057	054	048	049	048	048	051	049
	9	9	1	0	3	1	0	0	2
	057	057	049	048	051	049	048	048	050

   m akan dibagi menjadi 18 blok yang berukuran 3 digit.
   m1 : 049
   m2 : 057
   m3 : 054
   m4 : 048
   m5 : 049
   m6 : 048
   m7 : 048
   m8 : 051
   m9 : 049
   m10: 057
   m11: 057
   m12: 049
   m13: 048
   m14: 051
   m15: 049
   m16: 048
   m17: 048
   m18: 050
   nilai-nilai m ini masih terletak di dalam selang [0, 3869-1]
   K = (71, 3869)
   $C = p^e \bmod n$

Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 22 ; Nomor 2 ; Agustus 2023 ; Page 528-538
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index

Maka :
C1 = 049^{71} mod 3869 = 3142
C2 = 057^{71} mod 3869 = 2158
C3 = 054^{71} mod 3869 = 2651
C4 = 048^{71} mod 3869 = 1714
C5 = 049^{71} mod 3869 = 3142
C6 = 048^{71} mod 3869 = 1714
C7 = 048^{71} mod 3869 = 1714
C8 = 051^{71} mod 3869 = 2691
C9 = 049^{71} mod 3869 = 3142
C10 = 057^{71} mod 3869 = 2158
C11 = 057^{71} mod 3869 = 2158
C12 = 049^{71} mod 3869 = 3142
C13 = 048^{71} mod 3869 = 1714
C14 = 051^{71} mod 3869 = 2691
C15 = 049^{71} mod 3869 = 3142
C16 = 048^{71} mod 3869 = 1714
C17 = 048^{71} mod 3869 = 1714
C18 = 050^{71} mod 3869 = 19
Maka *ciphertext* yang dihasilkan adalah :

C = 3142 2158 2651 1714 3142 1714 1714 2691 3142 2158 2158 2158 3142 1714 2691 3142 1714 1714 19

3. Melakukan Proses Dekripsi
Pada proses dekripsi ini menggunakan kunci *private* yaitu K = *(d,n)* = (791, 3869) dan dengan rumus P = C^d mod n. Dimana pada proses dekripsi ini merupakan proses untuk mengembalikan *ciphertext* ke bentuk *plaintext* dan berikut penyelesaiannya :
K = (791, 3869)
P = C^d mod n
Maka :
m1 = 3142^{791} mod 3869 = 049
m2 = 2158^{791} mod 3869 = 057
m3 = 2651^{791} mod 3869 = 054
m4 = 1714^{791} mod 3869 = 048
m5 = 3142^{791} mod 3869 = 049
m6 = 1714^{791} mod 3869 = 048
m7 = 1714^{791} mod 3869 = 048
m8 = 2691^{791} mod 3869 = 051
m9 = 3142^{791} mod 3869 = 049
m10 = 2158^{791} mod 3869 = 057
m11 = 2158^{791} mod 3869 = 057
m12 = 3142^{791} mod 3869 = 049
m13 = 1714^{791} mod 3869 = 048
m14 = 2691^{791} mod 3869 = 051
m15 = 3142^{791} mod 3869 = 049
m16 = 1714^{791} mod 3869 = 048
m17 = 1714^{791} mod 3869 = 048
m18 = 19^{791} mod 3869 = 050
Maka hasil *ciphertext* yang telah didekripsi kedalam bentuk *plaintext*, yaitu sebagai berikut:

m = 049 057 054 048 049 048 048 051 049 057 057 049 048 051 049 048 048 050
1 9 6 0 1 0 0 3 1 9 9 1 0 3 1 0 0 2

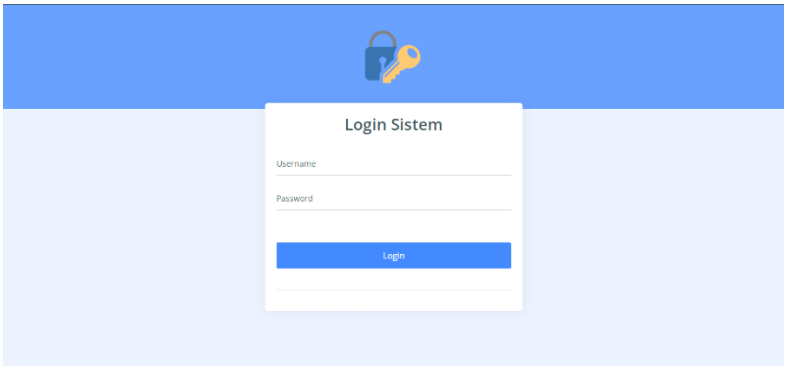
3.2 Implementasi Sistem

Berikut ini merupakan tampilan dari program Sistem "Imp lementasi Kriptografi Menggunakan Metode RSA Untuk Keamanan Dokumen Simpan Pinjam Uang di Badan Usaha Milik Desa Pematang Kuala.

1. Tampilan *Form Login*

Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 22 ; Nomor 2 ; Agustus 2023 ; Page 528-538
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index

Halaman ini digunakan untuk *administrator* ketika membatasi hak akses kedalam halaman tertentu dimana hanya dapat diakses oleh admin yang memiliki *username* dan *password* yang benar, berikut ini adalah tampilan antarmuka dari *form login* yang telah dibangun.



Gambar 2. Tampilan Halaman *Login*

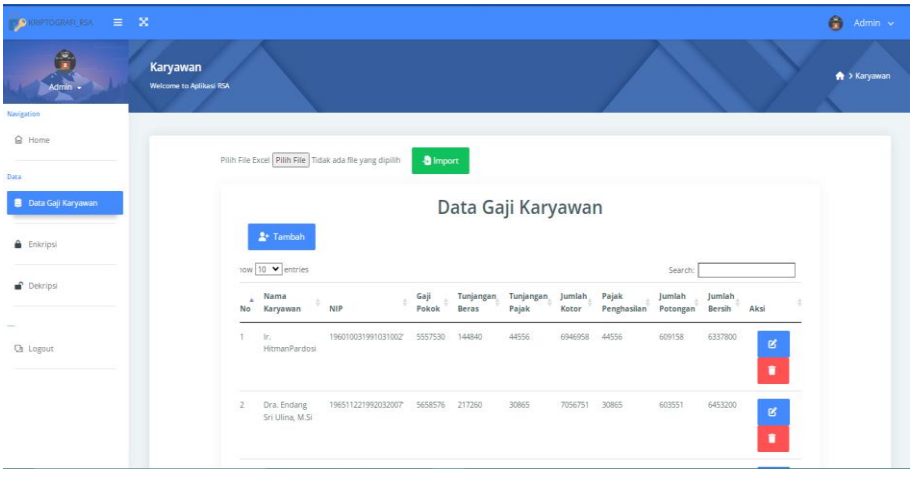
2. Tampilan *Form* Menu Utama

Form utama *admin* merupakan halaman yang hanya dapat diakses oleh seorang *admin* yang telah memiliki hak akses ke aplikasi, yang digunakan untuk menampilkan halaman utama dari aplikasi kriptografi *RSA*. berikut ini adalah tampilan antarmuka *(interface)* yang telah dibangun:

Gambar 3. Tampilan *Form* Menu Utama

3. Tampilan *Form* Data Gaji Karyawan

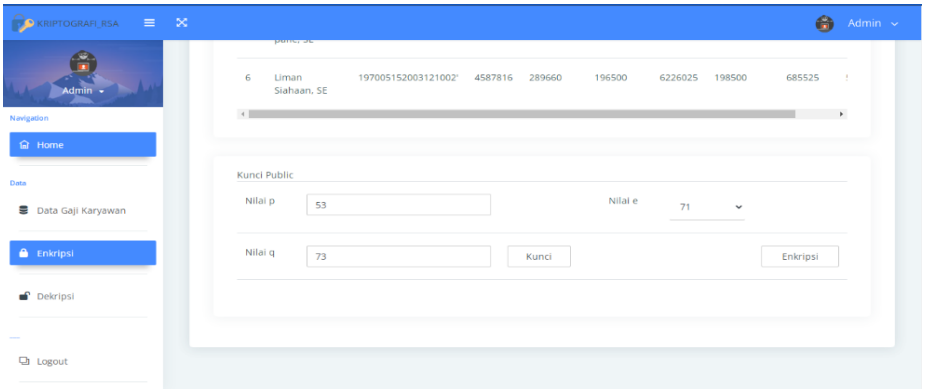
Form data gaji karyawan adalah halaman yang berfungsi untuk mengelola data gaji karyawan dari aplikasi kriptografi *RSA*. Berikut ini adalah tampilan antarmuka dari form data gaji karyawan yang telah dibangun:



Gambar 4. Tampilan *Form* Data Gaji Karyawan

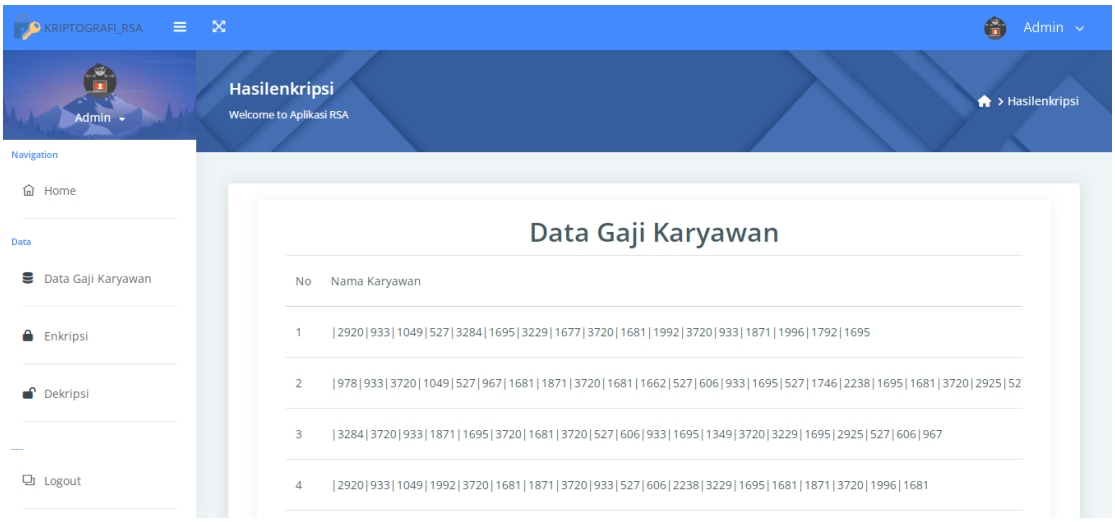
Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 22 ; Nomor 2 ; Agustus 2023 ; Page 528-538
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index

4. Tampilan *Form* Enkripsi
Form enkripsi adalah untuk melakukan proses *enkripsi* terhadap seluruh data gaji karyawan. Berikut ini adalah tampilan antar muka dari *form enkripsi* yang telah dibangun:



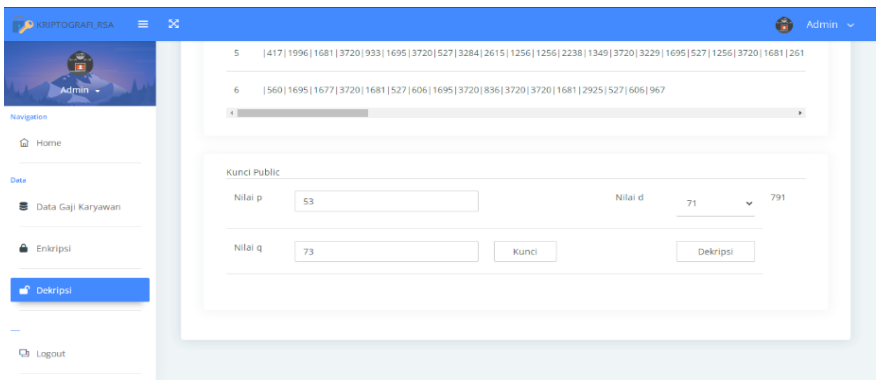
Gambar 5. Tampilan *Form* Enkripsi

5. Tampilan *Form* Hasil Enkripsi
Form hasil *enkripsi* adalah *form* yang tampil apa bila seluruh data gaji karyawan sudah di enkripsi. Berikut ini adalah tampilan antar muka dari *form* hasil enkripsi yang telah dibangun:



Gambar 6. Tampilan *Form* Hasil Enkripsi

6. Tampilan *Form* Dekripsi
Form dekripsi adalah untuk melakukan proses dekripsi terhadap seluruh data gaji karyawan yang telah di *enkripsi*. Berikut ini adalah tampilan antar muka dari *form* dekripsi yang telah dibangun :



Gambar 7. Tampilan *Form* Dekripsi

7. Tampilan Form Hasil Dekripsi
   Form hasil dekripsi adalah form yang tampil apa bila seluruh data gaji karyawan sudah di dekripsi. Berikut ini adalah tampilan antar muka dari *form* hasil dekripsi yang telah dibangun:

Gambar 8. Tampilan *Form* Hasil Dekripsi

4. KESIMPULAN

Algoritma RSA ini sangat membantu mengurangi resiko penyalagunaan pada data laporan gaji karyawan sehingga dapat memudahkan admin dalam mengisi hasil pengujian. Dari segi teknis penghitungan, sistem *RSA* mempunyai cara enkripsi yang mudah, tetapi jika sudah dienkripsi, data yang sudah terenkripsi sulit untuk dibobol. Aplikasi yang dibangun hanya berfungsi untuk melakukan proses enkripsi dan dekripsi dan tidak dapat mencegah pihak luar untuk menghapus data. Aplikasi yang dibuat mampu melakukan proses enkripsi dan dekripsi terhadap sebuah file berextention **.xls* dan **.doc* dengan menerapkan algoritma *RSA*.

UCAPAN TERIMA KASIH

Terima kasih disampaikan kepada Bapak Nurcahyo Budi Nugroho dan Hendrik Sigalingging serta pihak-pihak yang telah mendukung terlaksananya penelitian ini.

DAFTAR PUSTAKA

[1] B. Anwar, R. Kustini, and I. Zulkarnain, "Penerapan Algoritma RSA (Rivest Shamir Adelman) Untuk Mengamankan Nilai Siswa SMP HKBP P. Bulan," *J-SISKO TECH (Jurnal Teknol. Sist. Inf. dan Sist. Komput. TGD)*, vol. 4, no. 1, p. 88, 2021, doi: 10.53513/jsk.v4i1.2623.

[2] J. Prayudha, _ S., and _ I., "Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode Advanced Encryption Standard (AES)," *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 18, no. 2, p. 119, 2019, doi: 10.53513/jis.v18i2.150.

[3] M. Haris Hrp, N. B. Nugroho, S. Kom, M. Kom, and R. I. Ginting, "Implementasi Keamanan Data Gaji Pada Dinas Komunikasi Dan Persandian Kabupaten Aceh Tamiang Menggunakan Algoritma RC4," *J. CyberTech*, vol. x. No.x, no. x, pp. 1–10, 2020, [Online]. Available: https://ojs.trigunadharma.ac.id/

[4] M. A. F. MANIK, "Penerapan Algoritma Rsa Dan Affine Cipher Dalam Keamanan File Ms Word," vol. 01, no. 02, pp. 95–100, 2021, [Online]. Available: http://repository.potensi-utama.ac.id/jspui/handle/123456789/5074

[5] Y. H. Syahputra, A. Azlan, and L. A. Girsang, "Pengamanan Data Penggajian Menggunakan Vigenere Cipher Pada Mom's Kitchen Medan," *J-SISKO TECH (Jurnal Teknol. Sist. Inf. dan Sist. Komput. TGD)*, vol. 5, no. 1, p. 1, 2022, doi: 10.53513/jsk.v5i1.4766.

[6] H. S. Djong and S. Siswanto, "Implementasi Kriptografi Dengan Menggunakan Metode Rc4 Dan Aes-256 Untuk Mengamankan File Implementation of Cryptography Using Rc4 and Aes-256 Methods To Secure Document Files At Pt Varnion," no. September, pp. 149–158, 2022.

[7] D. Febriyanto, "Sistem Keamanan Data Pada IoT Berbasis MQTT Dan Database MySQL Menggunakan Metode RSA," vol. 8, no. 6, pp. 3932–3943, 2022. [8] A. C. N. Ria Agustina, "Rancang Bangun Pencarian Rute Terpendek Tempat Wisata Berbasis Web Menggunakan Algoritma Djikstra," *J. Technol.*, vol. 1, no. 1, pp. 1–12, 2021.

[8] M. Aria, A. Widodo, M. Thasandra, S. O. Sutra, and A. B. Nasution, "Pemanfaatan Kriptografi dalam Mewujudkan Keamanan Informasi pada E-Voting di Kota Medan dengan Menggunakan Algoritma AES," vol. 05, no. 03, pp. 6780–6787, 2023.

[9] S. Suhandinata, R. A. Rizal, D. O. Wijaya, P. Warren, and S. Srinjiwi, "Analisis Performa Kriptografi Hybrid Algoritma Blowfish Dan Algoritma Rsa," *JURTEKSI (Jurnal Teknol. dan Sist. Informasi)*, vol. 6, no. 1, pp. 1–10, 2019, doi: 10.33330/jurteksi.v6i1.395.

[10] A. Marpaung, P. S. Ramadhan, and A. Pranata, "Implementasi RSA Untuk Enkripsi Dan Dekripsi File Dokumen," *J. Sist. Inf. TGD*, vol. 2, no. 1, pp. 39–48, 2023.

[11] S. Rahmadhiyanti, "Implementasi Kriptografi Rsa Untuk Peningkatan Keamanan Database E-Commerce," *Pelita Inform.*, vol. 8, p. 4, 2019.

[12] T. Hidayatullah, "… Base-64 Dalam Mengamankan Url (Uniform Resource Locator) Website Layanan Pengaduan Masyarakat Desa Bojongraharja," *J. Media Infotama*, vol. 18, no. 2, pp. 337–343, 2022, [Online]. Available: https://jurnal.unived.ac.id/index.php/jmi/article/view/2937%0Ahttps://jurnal.unived.ac.id/index.php/jmi/article/download/2937/2606.

[13] S. J. Siregar, M. Zarlis and Z. Situmorang, "*Application and Manual Encryption Process With The Combination Algorithm of One Time Pad and Vigenere Cipher*", Journal of Physics:Conference Series, 1641 01210, 2020, [Online]. Available: https://iopscience.iop.org/article/10.1088/1742-6596/1641/1/012106/pdf.