Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 1; Januari 2025 ; Page 73-82
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

Pengamanan Data Pengiriman Barang Di J&T Cargo Menggunakan Metode Rivest Shamir Adleman (RSA)

Desmi Natalia Simbolon[1], Nurcahyo Budi Nugroho[2], Rina Mahyuni[3]

[1,2] Sistem Informasi, STMIK Triguna Dharma
[3]Sistem Komputer, STMIK Triguna Dharma
Email: [1] desminatalia72@gmail.com, [2]nurcahyobn@gmail.com, [3]rinamahyuni14@gmail.com
Email Penulis Korespondensi: desminatalia72@gmail.com

Article History:
Received Dec 31th, 2025
Revised Jan 15th, 2025
Accepted Jan 31th, 2025

Abstrak

Keamanan dan kerahasiaan data merupakan hal yang penting dalam pengiriman barang, Salah satu masalah yang dihadapi oleh J&T Cargo Padang Bulan Medan dalam pengamanan data pengiriman barang adalah pemalsuan data. Pihak karyawan dengan sengaja mengubah jumlah total ongkos pengiriman barang dalam perhari hanya untuk mendapatkan keuntungan pribadi, tentu hal ini sangat merugikan pihak J&T Cargo Padang Bulan Medan. Selain itu, risiko penyadapan dan pencurian informasi juga menjadi ancaman yang harus ditangani. Dalam menyelesaikan masalah tersebut, J&T Cargo Padang Bulan Medan menerapkan tindakan dengan mengimplementasikan kriptografi algoritma Rivest Shamir Adleman (RSA), algoritma ini menggunakan dua kunci yaitu kunci public dan kunci private yang unik setiap entitas yang terlibat. Dengan menggunakan kunci public untuk mengenkripsi data pengiriman barang, informasi tersebut tidak dapat dibaca oleh pihak yang tidak memiliki kunci private yang tidak sesuai. Dengan demikian hasil dari sistem yang telah dirancang, maka akan membantu pihak J&T Cargo Padang Bulan Medan dalam menentukan pengamanan data pengiriman barang yang lebih tepat, baik, dan akurat.
Kata Kunci: Kriptografi RSA, Pengamanan Data, Pengiriman Barang

Abstract

Data security and confidentiality is important in shipping goods. One of the problems faced by J&T Cargo Padang Bulan Medan in securing data on shipping goods is data falsification. The employees deliberately changed the total amount of goods delivery costs per day just to gain personal profit, of course this was very detrimental to J&T Cargo Padang Bulan Medan. Apart from that, the risk of eavesdropping and theft of information is also a threat that must be addressed. In solving this problem, J&T Cargo Padang Bulan Medan implemented actions by implementing the Rivest Shamir Adleman (RSA) cryptographic algorithm. This algorithm uses two keys, namely a public key and a private key that is unique for each entity involved. By using a public key to encrypt goods delivery data, the information cannot be read by parties who do not have an inappropriate private key. Thus, the results of the system that has been designed will help J&T Cargo Padang Bulan Medan in determining the security of goods delivery data that is more precise, good and accurate.
***Keywords**: RSA Cryptography, Data Security, Goods Delivery*

1. PENDAHULUAN

Masalah keamanan dan kerahasiaan data merupakan hal yang penting dalam pengiriman barang, data yang bersifat rahasia tersebut penting dibuat sistem penyimpanan dan pengirimannya agar tidak terbaca atau diubah oleh orang-orang yang tidak bertanggung jawab, baik saat data barang tersebut tersimpan di dalam komputer maupun saat barang tersebut di kirim melalui jalur darat dan laut[1].

Kasus manipulasi data pengiriman ini pernah terjadi di J&T Cargo Padang Bulan Medan. Pihak karyawan dengan sengaja mengubah jumlah total ongkos pengiriman dalam perhari hanya untuk mendapatkan keuntungan pribadi. Tentu hal ini sangat merugikan pihak perusahaan dan juga merugikan Manajer Departemen selaku pihak yang bertanggung jawab atas data pengiriman, data tersebut tersimpan dalam bentuk file XLSX (Microsoft Excel Spreadsheet), file ini bisa dibuka diberbagai text editor, seperti Excel dan Notepad. Namun demikian, tujuan dari kriptografi adalah untuk memastikan penggunaan kriptografi mennggunakan metode RSA yang tepat dan efektif demi melindungi kerahasiaan, keaslian dan integritas informasi.

Data adalah komponen utama dari sistem informasi perusahaan karena proses pengambilan keputusan berasal dari data. Oleh karena itu pengolahan data sudah seharusnya dianggap sebagai kebutuhan primer oleh perusahaan. Pengolahan

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 1; Januari 2025 ; Page 73-82
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

data yang buruk dapat menyebabkan tidak tersedianya data penting yang digunakan untuk menghasilkan informasi yang diharapkan dalam pengambilan keputusan. Data mempunyai fungsi yang sangat penting bagi kinerja perusahaan[2].

Penelitian ini menjelaskan bagaimana pemanfaatan kriptografi dalam mengamankan data pengiriman barang. Kriptografi adalah metode untuk mencegah kebocoran data rahasia. Kriptografi memiliki dua proses utama yang terdiri dari proses enkripsi dan dekripsi. Proses enkripsi adalah proses pengkodean yang mengubah plaintext menjadi ciphertext menjadi teks-kode sehingga pesan sulit dimengerti. Dalam mengamankan data, kriptografi memiliki beberapa metode, salah satunya ialah metode Rivest Shamir Adleman (RSA).

Rivest Shamir Adleman (RSA) merupakan salah satu metode yang terdapat dalam cabang ilmu kriptografi, algoritma RSA mendasarkan proses enkripsi dan dekripsi pada konsep bilangan prima dan aritmatika modulo, baik kunci enkripsi maupun dekripsi keduanya merupakan bilangan bulat. Melalui penelitian ini diharapkan algoritma RSA dapat diterapkan untuk mengenkripsi file ataupun teks yang berekstensi .xlsx[3].

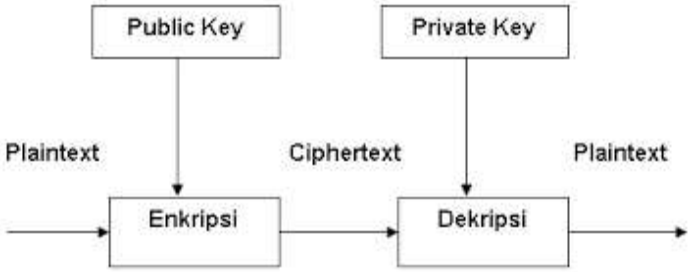
Dari pembahasan penelitian tersebut diharapkan sistem pengiriman barang berbasis web ini, dapat membantu dan dapat dikelola dengan aman tanpa adanya kekhawatiran penyalahgunaan data oleh orang yang tidak bertanggung jawab .

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kriptografi merupakan bahasa Yunani kuno yang terdiri dari dua kata yaitu : *cripto* dan *graphia*. *crypto* yang berarti *scret* (rahasia) dan *graphia* yang berarti *writing* (tulisan). Pengertian kriptografi yaitu ilmu serta seni yang menjaga keamanan pesan saat pesan dikirimkan dari suatu tempat ke tempat lain. Kriptografi memiliki beberapa tujuan yang mendasar dalam konteks keamanan informasi antara lain yaitu : kerahasiaan *(confidentiality)*, autentikasi *(authentication)*, integritas data atau keutuhan data *(*data *integrity)* dan tidak terbantahkan *(non-repudiation)*[4].

Dengan kata lain, kriptografi adalah seni dan ilmu mengamankan pesan. Pada dunia enkripsi, pesan dianggap plaintext atau cleartext. Enkripsi adalah proses mengamankan pesan dengan cara mengubah isi aslinya menjadi bentuk yang tidak dapat dibaca, kecuali oleh pihak yang memiliki kunci atau metode dekripsi yang benar. Pesan terenkripsi disebut ciphertext. Proses pengembalian teks terenkripsi menjadi teks biasa disebut dekripsi.



Gambar 1. Proses *Enkripsi* dan *Dekripsi* Data

Dalam kriptografi klasik, salah satu teknik *enkripsi* yang digunakan adalah *enkripsi simetris* dimana kunci *dekripsi* sama dengan kunci *enkripsi*. Untuk kriptografi kunci *public* merupakan kunci yang dapat diakses oleh semua orang. Dalam teknik *Enkripsi*, diperlukan teknik *enkripsi asimetris* dimana kunci *dekripsi* tidak sama dengan kunci *enkripsi*. Karena *enkripsi asimetris* menggunakan bilangan yang sangat besar, *enkripsi*, *dekripsi*, dan pembuatan kunci membutuhkan komputasi yang lebih besar dibandingkan dengan *enkripsi simetris.*

2.2 Keamanan Data

Dunia semakin berkembang dengan cepat seiring majunya teknologi informasi. Dan komunikasi sekarang menjadi tidak terbatas. Dengan banyaknya kemudahan untuk melakukan pengaksesan informasi, adakalanya diperlukan pengamanan data informasi tersebut. Pengamanan data ini berfungsi menangani pencegahan atas sampainya informasi ke tangan yang tidak berhak yang dapat mengakibatkan kerugian bagi pemilik informasi.

Keamanan informasi dapat diimplementasikan menggunakan berbagai teknologi dan teknik, termasuk kontrol administratif, keamanan fisik, kontrol logis, standar organisasi, dan teknik keamanan lainnya yang membatasi akses ke pengguna atau proses yang tidak sah atau berbahaya (Rao dan Selvamani, 2015).

Keamanan data adalah konsep yang mengacu pada praktik dan tindakan perlindungan yang diambil untuk menjaga kerahasiaan, integritas, ketersediaan data, dan dapat diterapkan untuk mencegah akses yang tidak sah ke komputer, *database*, dan situs *web*. Keamanan data juga melindungi data dari korupsi. Keamanan data dapat melibatkan sejumlah tindakan dan teknologi yang bertujuan melindungi data dari ancaman seperti kehancuran, modifikasi, atau pengungkapan yang tidak sah. Ini melibatkan perlindungan terhadap data baik saat data tersebut disimpan maupun saat data tersebut berpindah atau dipertukarkan. Keamanan data ini juga dikenal sebagai keamanan informasi atau keamanan komputer. Keamanan data tentu tidak dapat lepas dari masalah kriptografi (ilmu penyandian). *Cryptography* adalah penopang utama sekaligus merupakan metode teraman dan paling efektif dalam dunia keamanan data, selanjutnya perkembangan

keamanan data saat ini umumnya banyak berlomba-lomba untuk membentuk metode *encryption* (penyandian) yang terkuat[5].

2.2.1 Komponen-Komponen Pada Kriptografi

Kriptografi terdiri dari berbagai komponen-komponen pendukung antara lain sebagai berikut:[6]

1. *Enkripsi* sangat penting pada kriptografi, yaitu metode untuk melindungi data yang dikirim supaya tetap rahasia. Teks biasa, sebuah istilah untuk pesan aslinya, diubah menjadi kode yang sulit dipahami.
2. *Dekripsi* adalah kebalikan dari *enkripsi*. Pesan terenkripsi dipulihkan dalam bentuk aslinya. Algoritma yang dipergunakan untuk *dekripsi* pasti berbeda dengan algoritma yang digunakan untuk *enkripsi*.
3. Kunci adalah informasi rahasia atau data yang digunakan dalam proses *enkripsi* dan *dekripsi*. Kunci terbagi menjadi dua bagian, yaitu *public key* dan *private key*.
4. *Ciphertext* merupakan suatu pesan yang telah melalui proses *enkripsi*. Pesan yang terdapat pada teks kode ini tidak bisa dibaca karena berupa karakter-karakter yang tidak memiliki makna.
5. *Plaintext* Sering disebut dengan teks asli atau teks biasa ini merupakan pesan yang diketik yang memiliki makna dan dapat dibaca oleh manusia. Teks asli *(plaintext)* adalah informasi yang ingin di *enkripsi* atau diubah ke dalam bentuk terenkripsi *chipertext* (teks-kode).

2.2.2 Tujuan Kriptografi

Kriptografi bertujuan untuk menyampaikan layanan keamanan informasi (yang dinamakan juga seperti aspek-aspek keamanan informasi), yaitu :

1. Kerahasiaan *(confidentiality)* adalah layanan yang bertujuan untuk menjaga kerahasiaan data sehingga pihak yang tidak berhak tidak dapat membaca pesan.
2. Integritas Data *(integrity)* adalah layanan yang dapat mengklaim bahwa pesan masih asli dan utuh dan belum pernah dimanipulasi selama pengiriman.
3. Autentikasi *(authentication)* adalah proses memveferifikasi identitas pihak yang berkomunikasi atau mengidentifikasi keaslian sumber pesan.
4. Nir penyangkalan *(non repudiation)* salah satu layanan keamanan data yang mencegah pihak yang berkomunikasi, baik pengirim pesan maupun penerima pesan, untuk menyangkal bahwa mereka terlibat dalam proses komunikasi atau transaksi.

2.3 *Rivest Shamir Adleman*

RSA adalah salah satu algoritma yang sering digunakan didalam dunia kriptografi pada pengamanan data dan salah satu algoritma yang paling maju didalam dunia kriptografi. Algoritma *Rivest Shamir Adleman (RSA*) dikemukakan oleh Ron Rivest, Adi Shamir, serta Leonard Adleman dari *Massachussetts Institute of Technology* (*MIT)* pada tahun 1977. Salah satu teknik pengamanan file dokumen menggunakan algoritma *RSA* adalah dengan cara mencocokkan kunci publik yang dimiliki oleh sipengirim file dokumen serta sipenerima file dokumen kemudian untuk langkah selanjutnya dilakukan proses penguraian atau pemulihan kebentuk semula menggunakan kunci privat[7].

Algoritma Kriptografi *RSA* memerlukan sepasang kunci yang dibangkitkan dengan memilih bilangan prima p dan q, beberapa besaran yang digunakan dalam menghasilkan kunci *RSA* meliputi : [8]

Tabel 1. Mengenerate Kunci *RSA*

Besaran	Sifat
P dan q (bilangan prima)	Rahasia
N = p x q	Tidak Rahasia
Totien(n) = (p-1) (q-1)	Rahasia
E *(*Kunci *Enkripsi)*	Tidak Rahasia
D (Kunci *Dekripsi*)	Rahasia
M (*Plaintext*)	Rahasia
C (*Ciphertext)*	Tidak Rahasia

2.3.1 Kelebihan dan Kekurangan Metode *RSA*

Adapun kelebihan dan kekurangan dari metode *RSA* dibandingkan metode lainnya adalah sebagai berikut :

1. Kelebihan metode *RSA*
   a. Tingkat keamanan berlapis karena memakai dua kunci yang berbeda pada proses *enkripsi* dan *dekripsi* nya.
   b. Dapat digunakan sebagai tanda tangan digital, sehingga pembantahan terhadap sesuatu aksi dapat dicegah.
   c. Distribusi kunci jadi lebih simpel karena jalur aman untuk distribusi kunci tidak lagi dibutuhkan.
   d. Manajemen kunci menjadi lebih mudah karena setiap pelaku sistem informasi memiliki sepasang kunci, maka untuk n pelaku diperlukan total 2n kunci saja.

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 1; Januari 2025 ; Page 73-82
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

e. Sulitnya memfaktorkan bilangan non prima menjadi faktor prima adalah tugas yang sulit dan memerlukan waktu yang cukup lama, terutama jika bilangan tersebut besar.

2. Kekurangan metode *RSA*
   a. Kecepatan operasi yang jauh lebih lambat dari pada kriptografi simetrik.
   b. Ukuran *cipher* menjadi sekitar 2 lipat ukuran semula.
   c. Ukuran kunci *private* yang terlalu besar akan mengakibatkan proses *dekripsi* yang cukup lama.
   d. *RSA* biasanya digunakan untuk mengenkripsi pesan yang berukuran kecil.

2.4 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 di dalam komputer. Pada Gambar 1 dibawah ini merupakan gambar *ASCII* 8 bit standar internasional [9].

Tabel 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	01101011	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

Gambar 2. Kode *ASCII* 8 bit

2.5 *Unified Modeling Languange*

Unified Modeling Language adalah salah satu standar bahasa yang paling populer untuk analisis dan desain, mengidentifikasikan *requeriment* (tata syarat), dan mendefenisikan arsitektur untuk program berorientasi objek. *Unified Modeling Language (UML)* merupakan sebuah standarisasi bahasa pemodelan dalam pemograman berorientasi objek untuk membangun perangkat lunak. Dalam membangun sistem perangkat lunak dibutuhkan pemodelan visual untuk penggambaran agar mudah dalam dokumentasi diri secara detail dan spesifikasi. membangun dan dokument asi diri sistem perangkat lunak. *UML* adalah *visual* untuk pemodelan serta komunikasi tentang sebuah sistem dengan menggunakan diagram dan teks-teks pendukung[10].

2.5.1 *Activity Diagram*

Activity Diagram menggambarkan aliran kerja dari sistem yang sedang dirancang, bagaimana masing-masing alur berawal dan bagaimana alur tersebut berakhir[11]

2.5.2 *Use Case Diagram*

Use Case Diagram adalah pemodelan untuk prilaku sistem informasi yang akan dibuat, *use case* bekerja dengan mengilustrasikan tipikal interaksi antara *user* sebuah sistem dengan sistem itu sendiri melalui sebuah cerita bagaimana sistem itu dipakai[12].

2.5.3 *Class Diagram*

Diagram Class ialah mendeskripsikan struktur sistem asal segi pendefinisian kelas-kelas yang akan dirancang untuk menciptakan sistem[11]

2.6 Penerapan Metode *RSA*

Sistem keamanan yang digunakan untuk mengamankan data pengiriman barang adalah dengan menggunakan metode *RSA*. Berikut perhitungannya:

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 1; Januari 2025 ; Page 73-82
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

1. Pemilihan Bilangan Prima

Pemilihan bilangan prima menjadi langkah awal dalam tahapan pembangkitan kunci dalam algoritma *RSA*. Setiap pengguna memiliki dua buah bilangan prima yang masing-masing nilainya dipresentasikan oleh p dan q, dalam penelitian ini, bilangan prima yang dipilih adalah bilangan prima 2 digit (puluhan). Persamaan dan nilai dapat dilihat sebagai berikut :

p dan q = bilangan prima (1)

Dimana p dan q adalah bilangan prima 2 digit.
p = 37
q = 83

2. Penentuan Nilai Modulus

Setelah dua buah bilangan prima setiap pengguna didapatkan, langkah selanjutnya adalah penentuan nilai *modulus* yang dipresentasikan dengan simbol n penentuan nilai *modulus* dan hasil dari operasi dapat dilihat dari rumus sebagai berikut :

$$n = p \times q \quad (2)$$

Dimana n adalah modulus, p adalah bilangan prima pembangkit, dan q adalah bilangan prima pembangkit.
n = p * q
n = 37 * 83
n = 3071

3. Kalkulasi *Totient* Dari Nilai *Modulus* (φ(n))

Kalkulasi *Totient* adalah langkah selanjutnya dalam pembangkitan kunci, dimana *totient* akan digunakan untuk menentukan *public key* dan *private key* setiap pengguna. Persamaan yang digunakan dan hasil dari penerapannya dalam langkah ini adalah sebagai berikut:

$$\varphi(n) = (p-1) \times (q-1) \quad (3)$$

Dimana φ(n) adalah *totient* dari *modulus*, n adalah *modulus*, p adalah bilangan prima pembangkit dan q adalah bilangan prima pembangkit.
φ(n) = (37-1) x (83-1)
φ(n) = (36) x (82)
φ(n) = 2952

2. Penentuan *Public Key*

Setelah nilai *totient* dari masing-masing pengguna sudah didapatkan, *public key* sudah dapat ditentukan dengan ketentuan :

$$gcd\ (e, \varphi(n)) = 1 \quad (4)$$

Dimana *gcd* adalah *factor* pembagi terbesar, e adalah eksponen dari *public key* dan φ(n) adalah nilai *totient* dari *modulus* dan nilai e awal ditentukan secara statis.
e = 5, φ(n) = 2952
e = 5 sehingga *gcd* (5, 2952) = 1

3. Penentuan *Private Key*

Untuk penentuan *private key* milik masing-masing pengguna dapat ditentukan dengan ketentuan :

$$d_e\ (mod\ \varphi(n)) = 1 \quad (5)$$

Dimana d adalah *Private key*, e adalah *public key*, *φ(n)* adalah *totient* dari *modulus* dan nilai dari d awal ditentukan secara statis.
5, d = 4133
5 x 4133 = 20665 *mod* (φ(n) = 2952)) = 1
Maka didapatlah hasil untuk pasangan kunci adalah :
kunci *public key (e, n)* = (5, 3071)
kunci *private key (d, n)* = (4133, 3071)

Untuk memperjelas data pada tahap pembangkitan kunci yang telah dikalkulasi, berikut adalah data dalam bentuk tabular.

Tabel 2. Data Pembangkitan Kunci

Bilangan Pembangkit Kunci (p dan q)	*Totient* *(φ)*	*Modulus* *(n)*	*Public Key* *(e)*	*Private Key* *(d)*
37 dan 83	2952	3071	5	4133

4. Konversi *Plaintext* Kedalam Bentuk *ASCII.* (6)

Dari data sampel yang telah dikumpulkan, berikut adalah bentuk data sampel yang dikonversikan menjadi bentuk *ASCII.*

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 1; Januari 2025 ; Page 73-82
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

Tabel 3. *Plaintext* Dalam Bentuk *ASCII*

Plaintext	*ASCII*
DEWITA SIBORO	068, 069, 087, 073, 084, 065, 083, 073, 066, 079, 082, 079

5. Enkripsi *Plaintext* Menjadi *Ciphertext*

$$C = m^e \ mod \ (n) \quad (7)$$

Dimana c adalah *ciphertext*, m adalah angka *ASCII* dari data Pengiriman barang, e adalah *public key* dan n adalah modulo. Untuk Nama "DEWITA SIBORO" salah satu nama Pelanggan yang mengirimkan paket ke Nias Barat, berikut adalah perhitungannya :

"D" = 068^5 mod 3071 = 2399
"E" = 069^5 mod 3071 = 1759
"W" = 087^5 mod 3071 = 775
"I" = 073^5 mod 3071 = 2256
"T" = 084^5 mod 3071 = 914
"A" = 065^5 mod 3071 = 2334
"S" = 083^5 mod 3071 = 996
"I" = 073^5 mod 3071 = 2256
"B" = 066^5 mod 3071 = 273
"O" = 079^5 mod 3071 = 387
"R" = 082^5 mod 3071 = 1244
"O" = 079^5 mod 3071 = 387

Kemudian untuk merangkum nama pelanggan yang mengirim barang, telah di *enkripsi*, berikut adalah data DEWITA SIBORO dalam bentuk tabular.

Tabel 4. Nama Pelanggan Yang Telah Di *enkripsi*

Plaintext	*ASCII*	*Ciphertext*
DEWITA SIBORO	068, 069, 087, 073, 084, 065, 083, 073, 066, 079, 082, 079	2399, 1759, 775, 2256, 914, 2334, 996, 2256, 273, 387, 1244, 387.

6. Dekripsi *Ciphertext* Menjadi *Plaintext*

Dalam proses melakukan *dekripsi*, persamaan atau rumus yang digunakan adalah sebagai berikut :

$$m = c^d \ mod \ (n) \quad (8)$$

Dimana m adalah *plaintext*, c adalah *ciphertext*, d adalah *private key*, dan n adalah *modulo*.

Pada nama " DEWITA SIBORO " yang diketahui bentuk dari *Ciphertext* nya adalah 2399, 1759, 775, 2256, 914, 2334, 996, 2256, 273, 387, 1244, 387. Kemudian untuk proses *dekripsi*nya adalah sebagai berikut :

2399^{4133} mod 3071 = 068 = "D"
1759^{4133} mod 3071 = 069 = "E"
775^{4133} mod 3071 = 087 = "W"
2256^{4133} mod 3071 = 073 = "I"
914^{4133} mod 3071 = 084 = "T"
2334^{4133} mod 3071 = 065 = "A"
996^{4133} mod 3071 = 083 = "S"
2256^{4133} mod 3071 = 073 = "I"
273^{4133} mod 3071 = 066 = "B"
387^{4133} mod 3071 = 079 = "O"
1244^{4133} mod 3071 = 082 = "R"
387^{4133} mod 3071 = 079 = "O"

Kemudian untuk merangkum salah satu nama pelanggan yang telah di *dekripsi*, berikut adalah nama pelanggan dalam bentuk tabular :

Tabel 5. Nama Pelanggan Yang Telah Di *dekripsi*

Ciphertext	*Plaintext* Bentuk *ASCII*	*Plaintext* Bentuk Karakter
2399,1759, 775, 2256, 914, 2334, 996, 2256, 273, 387, 1244, 387.	068, 069, 087, 073, 084, 065, 083, 073, 066, 079, 082, 079	DEWITA SIBORO

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 1; Januari 2025 ; Page 73-82
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

3. HASIL DAN PEMBAHASAN

3.1 Hasil

Hasil dari perancangan sistem yang telah dibangun yaitu aplikasi Kriptografi dalam pengamanan data pengiriman barang. Implementasi Kriptografi metode *RSA* yang digunakan dalam pengamanan data pengiriman barang di rancang berbasis *web*. Hasil yang akan ditampilkan adalah hasil tampilan *interface* dari sistem yang telah dibangun serta hasil pengujian sistem yang telah dilakukan.

3.1.1 Hasil Tampilan Antarmuka

Berikut ini adalah hasil tampilan antarmuka *(interface)* dari aplikasi kriptografi dalam pengamanan data pengiriman barang yang telah dibangun:

1. Tampilan Halaman *Login*

Halaman ini digunakan untuk *administrator* saat membatasi hak akses kedalam halaman tertentu dimana hanya dapat diakses oleh admin yang memiliki *username* dan *password* yang benar.

Gambar 3. Tampilan Halaman *Login*

2. Tampilan Halaman Menu Utama

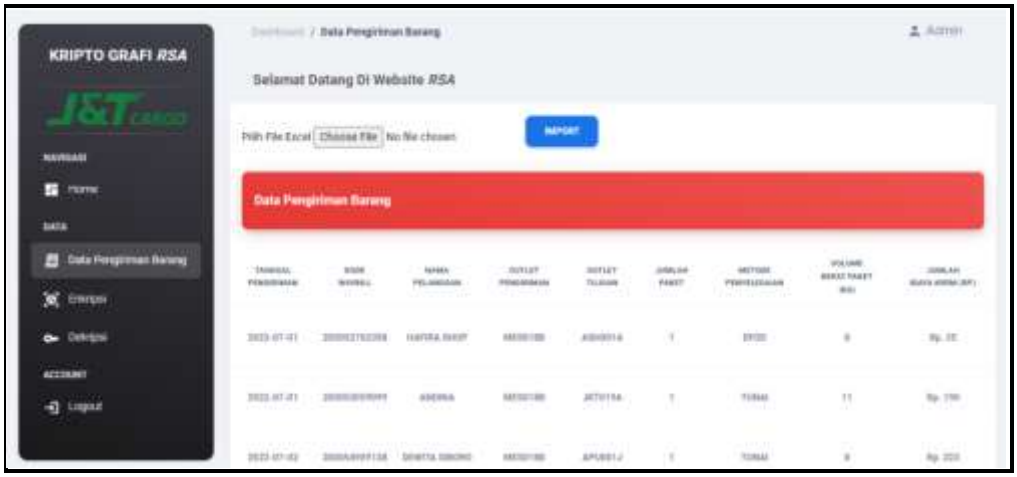
Halaman menu utama admin merupakan halaman yang hanya dapat diakses oleh seorang admin yang telah memiliki hak akses ke *web*, yang digunakan untuk menampilkan halaman utama dari aplikasi kriptografi *RSA*.

Gambar 4. Tampilan Halaman Menu Utama

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 1; Januari 2025 ; Page 73-82
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

3. Tampilan Halaman Data Pengiriman Barang

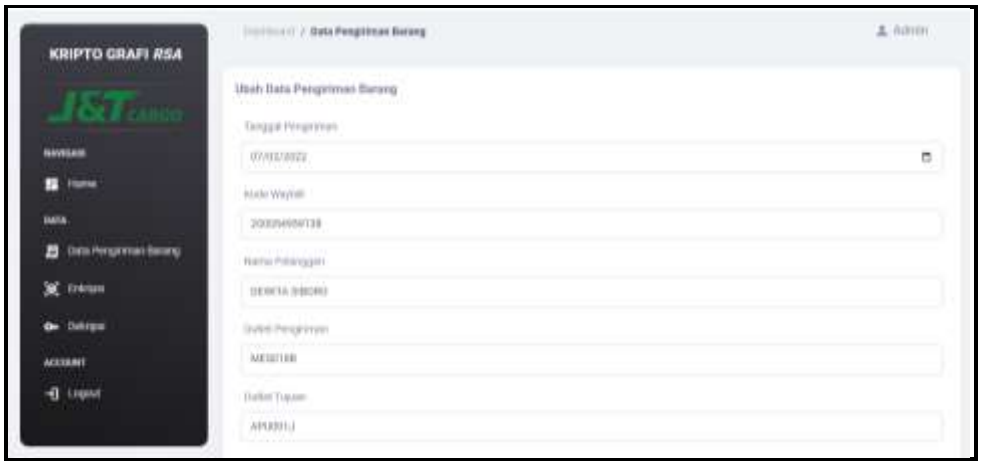
Halaman data pengiriman yang berfungsi untuk mengelola data pengiriman barang dari aplikasi kriptografi *RSA*.



Gambar 5. Tampilan Halaman Data Pengiriman Barang

4. Tampilan Halaman Ubah Data Pengiriman Barang

Halaman ubah data pengiriman barang merupakan halaman yang bertujuan untuk melakukan pengeditan data pengiriman barang.



Gambar 6. Tampilan Halaman Ubah Data Pengiriman Barang

5. Tampilan Halaman *Enkripsi*

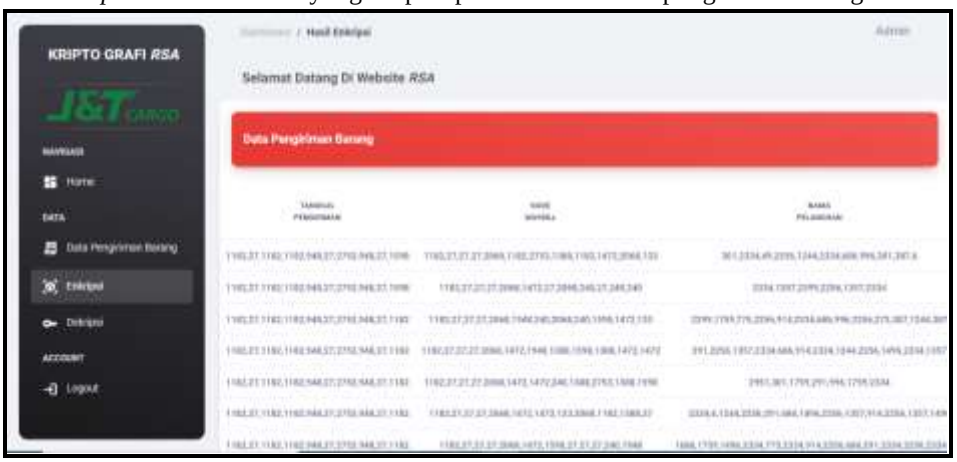
Halaman *enkripsi* berfungsi untuk melakukan proses *enkripsi* terhadap seluruh data pengiriman barang.

Gambar 7. Tampilan Halaman *Enkripsi*

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 1; Januari 2025 ; Page 73-82
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

6. Tampilan Halaman Hasil *Enkripsi*

Halaman hasil *enkripsi* adalah halaman yang tampil apabila seluruh data pengiriman barang sudah di *enkripsi*.



Gambar 8. Tampilan Halaman Hasil *Enkripsi*

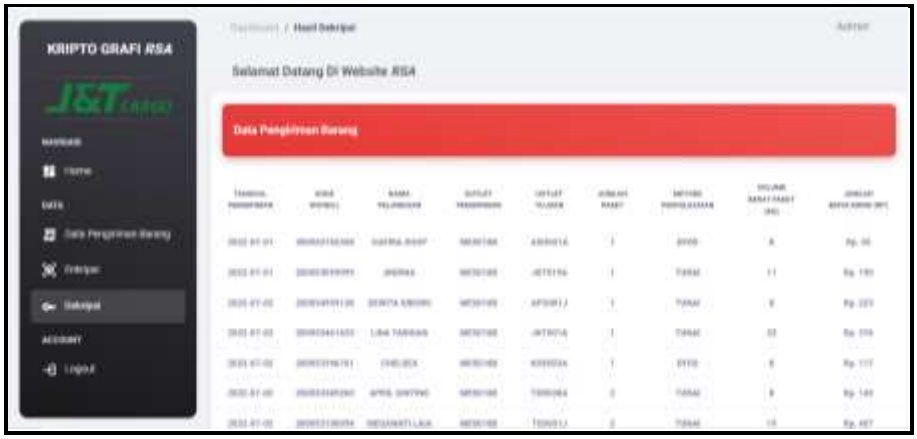
7. Tampilan Halaman *Dekripsi*

Halaman *dekripsi* berfungsi untuk melakukan proses *dekripsi* terhadap seluruh data pengiriman barang yang telah di *enkripsi*.

Gambar 9. Tampilan Halaman *Dekripsi*

8. Tampilan Halaman Hasil *Dekripsi*

Halaman hasil *dekripsi* adalah halaman yang tampil apabila seluruh data pengiriman barang sudah di *dekripsi*.



Gambar 10. Tampilan Halaman Hasil *Dekripsi*

9. KESIMPULAN

Algoritma *RSA* telah berhasil digunakan dalam aplikasi dengan baik, sehingga data pengiriman barang dapat terjaga, dan meningkatkan keamanan data pada J&T Cargo Padang Bulan Medan. Penerapan Kriptografi untuk pengamanan data pengiriman barang pada J&T Cargo Padang Bulan Medan menggunakan algoritma *RSA* dirancang melalui proses yang diawali dengan mencari masalah, lalu menemukan solusinya, kemudian merancang sebuah sistem yang dapat memecahkan masalah tersebut.

Aplikasi Kriptografi untuk pengamanan data pengiriman barang pada J&T Cargo Padang Bulan Medan menggunakan algoritma *RSA* yang telah dirancang tentu saja dapat diaplikasikan untuk menjaga data pengiriman barang yang berbentuk file *XLSX (Microsoft Excel Spreadsheet)* dari pihak-pihak yang tidak bertanggung jawab dengan tujuan untuk mengambil keuntungan pribadi.

UCAPAN TERIMAKASIH

Terima Kasih diucapkan kepada kedua orang tua serta keluarga yang selalu memberi motivasi, Doa dan dukungan moral maupun materi, serta pihak-pihak yang telah mendukung dalam proses pembuatan jurnal ini yang tidak dapat disebutkan satu persatu. Kiranya jurnal ini bisa memberi manfaat bagi pembaca dan dapat meningkatkan kualitas jurnal selanjutnya.

DAFTAR PUSTAKA

[1] Fatonah and Dadang Iskandar Mulyana, "Implementasi Metode Rivest Shamir Adleman untuk Enkripsi dan Dekripsi Text," *J. Inform. dan Teknol. Komput. (J-ICOM)*, vol. 3, no. 1, pp. 32–39, 2022, doi: 10.33059/j-icom.v3i1.4990.

[2] 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.

[3] B. Anwar, R. Kustini, and I. Zulkarnain, "J-SISKO TECH Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD Penerapan Algoritma RSA (Rivest Shamir Adelman) Untuk Mengamankan Nilai Siswa SMP HKBP P. Bulan," □, vol. 88, no. 1, pp. 88–91, 2021.

[4] H. Saputra Djong and S. Siswanto, "Implementasi Kriptografi Dengan Menggunakan Metode Rc4 Dan Aes-256 Untuk Mengamankan File Dokumen Pada Pt Varnion Technology Semesta," *Semin. Nas. Mhs. Fak. Teknol. Inf. Jakarta-Indonesia*, no. September, pp. 149–158, 2022.

[5] Indra Gunawan, *Keamanan Data: Teori dan Implementasi*. Jawa Barat: CV Jejak, Anggota IKAPI, 2021. [Online]. Available: https://books.google.co.id/books?id=JcQwEAAAQBAJ&lpg=PP1&ots=EU5NK8Alst&dq=Indra Gunawan%2C Keamanan Data%3A Teori dan Implementasi. Jawa Barat%3A CV Jejak%2C Anggota IKAPI%2C 2021.&lr&hl=id&pg=PP1#v=onepage&q=Indra Gunawan, Keamanan Data: Teori dan Imple

[6] D. Febriyanto, "Sistem Keamanan Data Pada IoT Berbasis MQTT Dan Database MySQL Menggunakan Metode RSA," vol. 8, no. 6, pp. 3932–3943, 2022.

[7] S. J. Siregar, N. B. Nugroho, and H. Sigalingging, "Implementasi Algoritma Kriptografi RSA (Rivest Shamir Adleman) Dalam Pengamanan Data Gaji Karyawan Di Kantor BSPJI," *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 22, no. 2, p. 528, 2023, doi: 10.53513/jis.v22i2.9409.

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

[9] 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

[10] M. Affandi, "Implementasi Kriptografi Untuk Keamanan Data Teks Menggunakan Algoritma Asimetris Rivest Shamir Adleman," 2020, [Online]. Available: http://eprints.uty.ac.id/6325/%0Ahttp://eprints.uty.ac.id/6325/1/Naskah Publikasi-5150411254-Muhammad Pandu Affandi.pdf

[11] P. M. Ariansyah and K. Wijaya, "Rancang Bangun Sistem Informasi Akademik Berbasis Web: Studi Kasus: SD Negeri 18 Tanah Abang," *J. Pengemb. Sist. Inf. dan Inform.*, vol. 2, no. 3, pp. 138–156, 2021, doi: 10.47747/jpsii.v2i3.562.

[12] N. W. Al Hafiz and E. Erlinda, "Perancangan Sistem Penyiraman Tanaman Otomatis Meggunakan Arduino," *J. Teknol. Dan Open Source*, vol. 3, no. 2, pp. 245–260, 2020, doi: 10.36378/jtos.v3i2.831.