Journal of Informatics Management and Information Technology
ISSN 2774-4744 (Media Online)
Vol 1, No 3, Juli 2021
Hal 101-107
https://hostjournals.com/jimat

Pengamanan Data Pelanggan dan Penjualan Menggunakan Implementasi Algoritma Kriptografi

Sri Vivi Wahdini[1,*], Dedy Hartama[1], Ika Okta Kirana[1], Poningsih[2], Sumarno[1]

[1] STIKOM Tunas Bangsa, Pematangsiantar, Indonesia
[2] AMIK Tunas Bangsa, Pematangsiantar, Indonesia
Email: [1,*]sriviviwahdini@gmail.com, [2]dedyhartama@amiktunasbangsa.ac.id, [3]ikaoktakirana@stikomtb.ac.id,
[4]poningsih@amiktunasbangsa.ac.id, [5]sumarno@amiktunasbangsa.ac.id

Abstrak−Keamanan data merupakan hal penting yang menjadi prioritas, karena berkaitan dengan privasi, integritas, otentikasi dan kerahasiaan, begitu pula halnya pada data pelanggan dan penjualan. Faktor kerahasiaan dan keamanan data pelanggan dan penjualan, merupakan hal yang paling utama dari pelaksanaan bisnis di era industri 4.0 yang kini serba digital. Oleh karena itu tujuan penelitian pada makalah ini untuk melakukan pengamanan data pelanggan menggunakan implementasi algoritma kriptografi RSA (Rivest Shamir Adleman). Kekuatan dan kelebihan keamanan algoritma RSA terletak pada tingkat kesulitan dalam memfaktorkan bilangan menjadi faktor-faktor prima, Penelitian pada makalah ini menggunakan data pelanggan dan penjualan mobil pada PT. Sutan Indo Aneka Mobil Pematangsiantar. Berdasarkan data-data tersebut, akan dibangun aplikasi enkripsi dekripsi dengan mengunakan algoritma RSA. Algoritma kriptografi RSA ini menggunakan panjang kunci 1024 bit dan plainteks berupa file Microsoft Office. Langkah yang akan dilakukan terlebih dahulu adalah mengubah plaintext dan kunci tersebut menjadi bentuk heksadesimal. Hasil penelitian menunjukkan bahwa panjang file yang digunakan akan mempengaruhi waktu yang dibutuhkan untuk proses enkripsi dan dekripsi. Apabila semakin panjang ukuran file maka semakin lama pula waktu yang dibutuhkan untuk melakukan enkripsi dan proses dekripsi. Sehingga dapat disimpulkan bahwa algoritma RSA efektif digunakan untuk mengamankan data yang tidak terlalu besar ukuran file nya.

Kata Kunci: Keamanan; Data Pelanggan; Kriptografi; RSA; Data Penjualan

Abstract−Data security is an important priority, as it relates to privacy, integrity, authentication, confidentiality, and customer and sales data. The confidentiality and security of customer and sales data is the most important thing in conducting business in the industrial 4.0 era, which is now all-digital. Therefore, the research objective in this paper is to secure customer data using the RSA (Rivest Shamir Adleman) cryptographic algorithm implementation. The strength and security of the RSA algorithm lie in the level of difficulty in factoring numbers into prime factors. The research in this paper uses customer data and car sales at PT. Sutan Indo Various Cars Pematangsiantar. Based on these data, a decryption encryption application will be built using the RSA algorithm. This RSA cryptographic algorithm uses a key length of 1024 bits and plaintext in the form of files with the extension Microsoft Office. The first step is to convert the plaintext and the key into hexadecimal form. The results showed that the length of the file used would affect the encryption and decryption process time. The longer the file size, the longer it will take for the encryption and decryption process. So it can be concluded that the RSA algorithm is effectively used to secure data that is not too large in file size.

Keywords: Security; Customer Data; Cryptography; RSA; Sales Data

1. PENDAHULUAN

Keamanan data pribadi pelanggan maupun transaksi yang telah dilakukan merupakan hal yang vital bagi kelangsungan sebuah bisnis [1], sehingga haruslah menjadi prioritas utama karena berkaitan dengan privasi, integritas, otentikasi dan kerahasiaan [2]. Faktor kerahasiaan dan keamanan data pelanggan dan penjualan, merupakan hal yang harus dijaga dari pelaksanaan bisnis di era industri 4.0 yang kini serba digital [3]. Seiring dengan perkembangan teknologi informasi yang berkembang semakin modern maka memerlukan keamanan yang kuat dan mumpuni [4]. Komputer memiliki peranan penting sebagai alat bantu dalam menjembatani hal ini, dimana dalam proses tersebut, kecepatan dan ketepatan data yang diolah menjadi informasi yang lebih berguna dan bermanfaat haruslah berbanding lurus dengan tingkat keamanan dari informasi yang akan disajikan. Perkembangan teknologi digital juga membawa dampak pada ancaman keamanan data [5][6][7][8][9]. Hal tersebut memberikan gambaran pentingnya pengamanan data digital [10][11][12]. Namun, sekali lagi, masalah keamanan siber (cyber security) dan kasus kebocoran data pelanggan dan penjualan masih membayangi dan berpotensi menggerus penjualan. Kasus kebocoran data pelanggan dan penjualan memunculkan kekhawatiran yang membutuhkan perhatian khusus, terutama bagi organisasi / perusahaan yang memfokuskan bisnisnya melalui platform digital [13]. Korporasi berbasis digital memang menerima detail pribadi milik pelanggan, dan tentu saja para pelanggan mempercayai data penting itu untuk dijaga agar tetap aman dan tidak jatuh di tangah orang yang salah [14].

Makalah ini akan membahas masalah data pelanggan dan penjualan pada PT. Sutan Indo Aneka Mobil Pematangsiantar. Salah satu cara untuk mengatasi masalah tersebut dengan melakukan pengamanan data pelanggan dan penjualan menggunakan implementasi algoritma kriptografi RSA (Rivest Shamir Adleman). Kekuatan dan kelebihan keamanan algoritma RSA terletak pada tingkat kesulitan dalam memfaktorkan bilangan menjadi faktor-faktor prima. Sebenarnya banyak algoritma-algoritma kriptografi selain RSA, seperti yang tergolong pada algoritma simetri (Data Encryption Standard (DES) [15], Rivest Cipher [16], International Data Encryption Algorithm (IDEA) [17], Advanced Encryption Standard (AES) [18], On Time Pad (OTP) [19]) dan lain sebagainya. Selain itu algoritma yang termasuk dalam jenis Asimetri (Digital Signature Algorithm (DSA) [20], Diffle-Hellman (DH) [21], Elliptic Curve Cryptography

(ECC) [22], Kriptografi Quantum [23], RSA [24], dan lain sebaginya. Algoritma lain selain Simetri dan Asimetri adalah Fungsi Hash sering disebut dengan funsi satu arah (one-way function) [25].

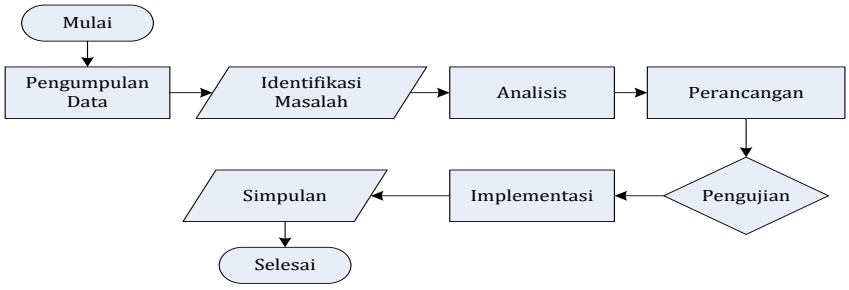
Penelitian-penelitian terkait yang menjadi rujukan terhadap masalah ini diantaranya: Penelitian yang dilakukan oleh Anshori, dkk (2019) tentang penerapan algoritma kriptografi Rivest Shamir Adleman (RSA) pada tanda tangan digital. Proses pembuatan tanda tangan digital diawali dengan pembuatan message digest dari sebuah dokumen kemudian proses pembangkitan kunci publik dan kunci privat untuk mengamankan data dan untuk membuat tanda tangan digital. Kunci privat akan dikirimkan kepada penerima pesan untuk memverifikasi tanda tangan digital. Tanda tangan digital dan dokumen dikirmkan kepada penerima. Selanjutnya, pada proses verifikasi, penerima akan mengecek apakah tanda tangan tersebut cocok atau tidak dengan menggunakan kunci privat dan menghitung nilai hash (message digest) dari dokumen yang diterima [26]. Penelitian yang dilakukan oleh Riswanto, dkkl (2020) tentang pengamanan data pengiriman SMS menggunakan RSA. Sistem ini dibangun pada platform Android, karena hampir semua orang memiliki smartphone Android dengan sistem yang menjalankan panjang karakter pesan tidak mempengaruhi kecepatan pada saat pengiriman pesan ke penerima, dan tidak ada batasan pada panjang karakter pesan selama proses enkripsi, sehingga setiap panjang karakter dapat dienkripsi dengan baik [27]. Selanjutnya Putra, dkk (2021) melakukan penerapan RSA untuk mengamankan database Program Keluarga Harapan (PKH). Algoritma RSA digunakan sebagai pelindung database PKH. Sistem akan membangkitkan kunci public dan kunci private, untuk mengamankan database PKH dienkripsi dengan kunci public. Seluruh data akan dienkripsi, sedangkan kunci private akan melakukan dekripsi atau mengembalikan dalam keadaan asli. Penerapan algoritma kriptografi RSA menjadi solusi yang baik pada sistem pengamanan database sql server yang akan digunakan untuk mengamankan database PKH [28]. Anwar, dkk (2021) menerapkan algoritma RSA untuk mengamankan nilai siswa pada SMP HKBP Padang Bulan Medan [29]. Sutejo (2021) melakukan implementasi algoritma RSA untuk mengamankan data rekam medis pasien pada Klinik Citra Bunda Kecamatan Tapung Hulu. Hasil dari penelitian ini berupa sistem rekam medis berbasis web yang dapat membantu Klinik Citra Bunda untuk meningkatkan keamanan data rekam medis pasien [30].

Penelitian-penelitian inilah yang melatar belakangi dilakukannya penelitian untuk melakukan pengamanan data pelanggan dan penjualan berupa enkripsi dan deskripsi pada PT. Sutan Indo Aneka Mobil Pematangsiantar, dengan tujuan untuk mengatasi masalah terjadinya pencurian data oleh pihak ketiga atau pihak lain yang tidak bertanggungjawab.

2. METODOLOGI PENELITIAN

2.1 Flowchart Rancangan Penelitian

Diagram alur model rancangan penelitian disajikan dalam rancangan flowchart berikut.



Gambar 1. Flowchart Rancangan Penelitian

Berikut merupakan penjelasan dari tahapan di atas.

a. Teknik Pengumpulan Data
   Pada penelitian ini data diperoleh dari PT. Sutan Indo Aneka Mobil, dengan melakukan metode pengumpulan data melalui wawancara, obervasi, studi literatur.
b. Identifikasi Masalah
   Menganalisa pada masalah yang mana terhadap data pelanggan Sutan Indo Aneka Mobil, adalah pengenalan terhadap masalah dan tahap awal pada proses penelitian.
c. Analisis
   Pada tahapan ini dilakukan terlebih dahulu proses analisis terhadap algoritma *Rivest Shamir Adleman* (RSA), agar dapat mengimplementasikan pada keamanan data penjualan.
d. Perancangan
   Tahapan ini menjelaskan apa saja yang akan dirancang oleh penulis dengan menggunakan aplikasi *NetBeans* dengan bahasa pemrograman java.
e. Pengujian
   Pada tahap ini akan dilakukan sebuah proses pengujian aplikasi keamanan data penjualan.
f. Implementasi

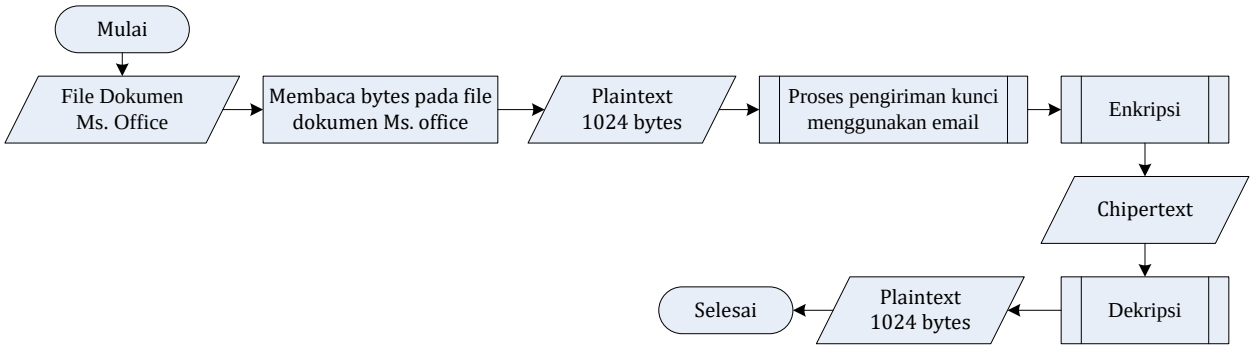
ISSN 2774-4744 (Media Online)
Vol 1, No 3, Juli 2021
Hal 101-107
https://hostjournals.com/jimat

Pada tahapan ini penulis membuat beberapa tahapan dengan implementasi diantaranya melakukan penginstalan *NetBeans* dan membuat program dengan membangun aplikasi sesuai pada fitur yang ditentukan.

g. Simpulan
Kesimpulan yang diperoleh setelah melakukan tahap analisis, rancangan, pengujian, dan implementasi aplikasi yang dibuat dengan menggunakan algorita RSA.

2.2 Enkripsi dan Dekripsi File Secara Umum

Berikut tahapan umum enkripsi.

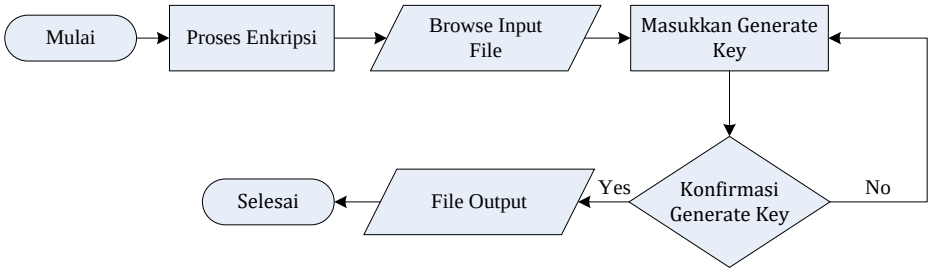


Gambar 2. Tahapan Enkripsi dan Dekripsi File Secara Umum

Proses pembentukan kunci pada aplikasi ini menggunakan teknik *Sieve Of Eratosthenes* untuk pencarian bilangan prima. Setelah menemukan kumpulan bilangan prima, proses selanjutnya adalah memilih dua bilangan prima yang terbesar. Setelah memilih dua bilangan prima yang terbesar, maka proses berikutnya adalah membaca *byte-byte* yang ada di dalam file tersebut dan diambil sepanjang 1024 *bytes* untuk dilakukan proses enkripsi. Selanjutnya dilakukan proses enkripsi menggunakan dua buah kunci yang telah dibangkitkan yaitu kunci publik dan kunci privat dengan cara mengubah *plaintext* dari file dokumen menjadi sebuah *chipertext*. Proses yang terakhir adalah proses dekripsi. Pada proses ini dilakukan pengubahan kembali sebuah *chipertext* menjadi sebuah *plaintext* yang dapat dibaca kembali dengan menggunakan kunci privat yang tercipta pada saat proses enkripsi sebelumnya.

2.3 Tahapan Enkripsi File

Berikut tahapan umum enkripsi.



Gambar 3. Tahapan Enkripsi File Secara Khusus

Tahapan enkripsi file dengan implementasi riptografi RSA antara lain : Lakukan enkripsi file. Pilih file yang akan dienkripsi. Masukan password dan konfirmasi password, password yang dimasukan sesuai keinginan user. Program akan melakukan proses enkripsi file dan kemudian akan menuliskan file ouput. File hasil enkripsi akan tersimpan secara langsung direktori yang sama dengan menggantikan file asli.

3. HASIL DAN PEMBAHASAN

Berikut ini contoh perhitungan Enkripsi dan dekripsi Algoritma RSA disimulasikan secara manual dengan plaintext "ADLI". Proses pertama adalah melakukan enkripsi plaintext dengan menggunakan algoritma RSA. Langkah yang akan dilakukan terlebih dahulu adalah mengubah plaintext dan kunci tersebut menjadi bentuk heksadesimal. Konverensi plaintext ke dalam bentuk heksadesimal dapat dilihat seperti tabel berikut:

Tabel 1. Tabel ASCII

Dec	Hex	Binary	Character	Dec	Hex	Binary	Character	Dec	Hex	Binary	Character
32	20	00100000	Space	64	40	01000000	@	96	60	01100000	.
33	21	00100001	!	65	41	01000001	A	97	61	01100010	a
34	22	00100010	"	66	42	01000010	B	98	62	01100010	b

ISSN 2774-4744 (Media Online)
Vol 1, No 3, Juli 2021
Hal 101-107
https://hostjournals.com/jimat

Dec	Hex	Binary	Character
35	23	00100011	#
36	24	00100100	$
37	25	00100101	%
38	26	00100110	&
39	27	00100111	‘
40	28	00101000	(
41	29	00101001	)
42	2A	00101010	*
43	2B	00101010	+
44	2C	00101100	,
45	2D	00101101	-
46	2E	00101110	.
47	2F	00101111	/
48	30	00110000	0
49	31	00110001	1
50	32	00110010	2
51	33	00110011	3
52	34	00110100	4
53	35	00110101	5
54	36	00110110	6
55	37	00110111	7
56	38	00111000	8
57	39	00111001	9
58	3A	00111010	:
59	3B	00111011	;
60	3C	00111100	<
61	3D	00111101	=
62	3E	00111110	>
63	3F	00111111	?

Dec	Hex	Binary	Character
67	43	01000011	C
68	44	01000100	D
69	45	01000101	E
70	46	01000110	F
71	47	01000111	G
72	48	01001000	H
73	49	01001001	I
74	4A	01001010	J
75	4B	01001011	K
76	4C	01001100	L
77	4D	01001101	M
78	4E	01001110	N
79	4F	01001111	O
80	50	01010000	P
81	51	01010001	Q
82	52	01010010	R
83	53	01010011	S
84	54	01010100	T
85	55	01010101	U
86	56	01010110	V
87	57	01010111	W
88	58	01011000	X
89	59	01011000	Y
90	5A	01011010	Z
91	5B	01011011	[
92	5C	01011100	\
93	5D	01011101	]
94	5E	01011110	^
95	5F	01011111	-

Dec	Hex	Binary	Character
99	63	01000110	c
100	64	01100100	d
101	65	01100101	e
102	66	01100110	f
103	67	01100111	g
104	68	01101000	h
105	69	01101001	i
106	6A	01101010	j
107	6B	01101011	k
108	6C	01101100	l
109	6D	01101101	m
110	6E	01101110	n
111	6F	01101111	o
112	70	01110000	p
113	71	01110001	q
114	72	01110010	r
115	73	01110011	s
116	74	01110100	t
117	75	01110101	u
118	76	01110110	v
119	77	01110111	w
120	78	01111000	X
121	79	01111001	Y
122	7A	01111010	Z
123	7B	01111011	{
124	7C	01111100	|
125	7D	01111110	}
126	7E	01111110	~
127	7F	01111111	DEL

Berikut ini merupakan langkah-langkah enkripsi dengan menggunakan algoritma RSA:

a. Pilih bilangan prima misalnya p = 13 dan q = 17, (n = p.q = 221 < 256)
b. Dihasilkan n = p*q = 13*17 = 221
c. Hitunglah m = (13 - 1) (17 - 1) = 12 * 16 = 192
d. Pilih sembarang bilangan e, dengan *gcd* (e, m) = 1 Karena e mempunyai ketentuan e > 1 dan e < m, maka e dimulai dari e = 2
   Nilai e = 2
   Jadi, *gcd* (2,192) = 2.
   Karena *gcd* (2,192) = 2, maka tidak memenuhi *gcd* (e, m) = 1.
   Nilai e = 3
   Jadi, *gcd* (3,192) = 3
   Karena *gcd* (3,192) = 3, maka tidak memenuhi *gcd* (e, m) = 1.
   Nilai e = 4
   Jadi, *gcd* (4,192) = 4.
   Karena *gcd* (4,192) = 4, maka tidak memenuhi *gcd* (e, m) = 1.
   Nilai e = 5
   Jadi, *gcd* (5,192) = 1.
   Karena *gcd* (5,192) = 1, maka memenuhi *gcd* (e, m) = 1.
e. Menghitung kunci private, disebut namanya *d* sedemikian agar *(d x e) mod m* = 1 (77 x 5) mod 192 = 1 jadi nilai d = 77
f. Maka public key nya = (e, n) = (5, 221)
g. Private key = (d, n) = (77, 221)
h. Proses enkripsi dengan menggunakan persamaan c = ple mod n.
   Diketahui :
   e = 5, n = 221, plainteks = ”ADLI”, dengan
   pl1 = A = 65
   pl2 = D = 68
   pl3 = L = 76
   pl4 = I = 73
   Maka enkripsi datanya sebagai berikut :
   C1 = 65^5 mod 221

= 1160290625 mod 221
= 182

C2 = 68^5 mod 221
= 1453933568 mod 221
= 204

C3 = 76^5 mod 221
= 2535525376 mod 221
= 111

C4 = 73^5 mod 221
= 2073071593 mod 221
= 99

Jadi, chipertext nya adalah 182 204 111 99

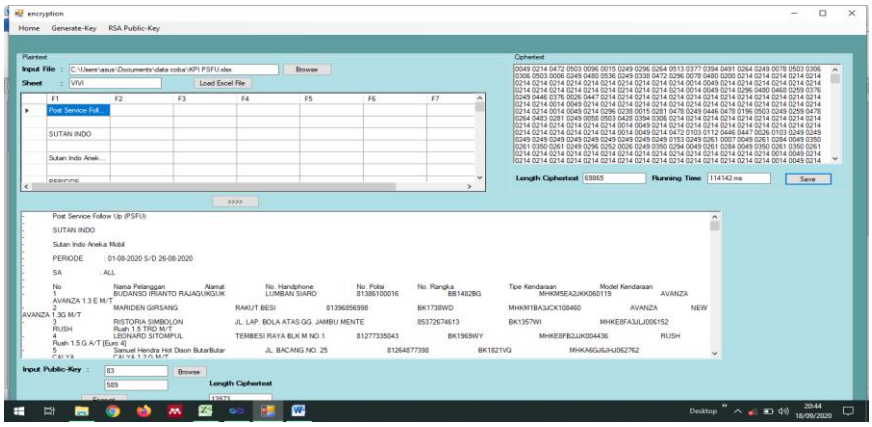
Setelah mendapatkan ciphertext yaitu "182, 204, 111, 99" (dalam nilai ASCII), kemudian melakukan proses dekripsi ciphertext yang dihasilkan. Berikut langkah-langkahnya:

Ciphertext = [182, 204, 111, 99]
pl1 = 18277 mod 221
pl1 = 65
pl2 = 20477 mod 221
pl2 = 68
pl3 = 11177 mod 221
pl3 = 76
pl4 = 21177 mod 221
pl4 = 73

Jadi hasil dekripsinya adalah 65 68 76 73.

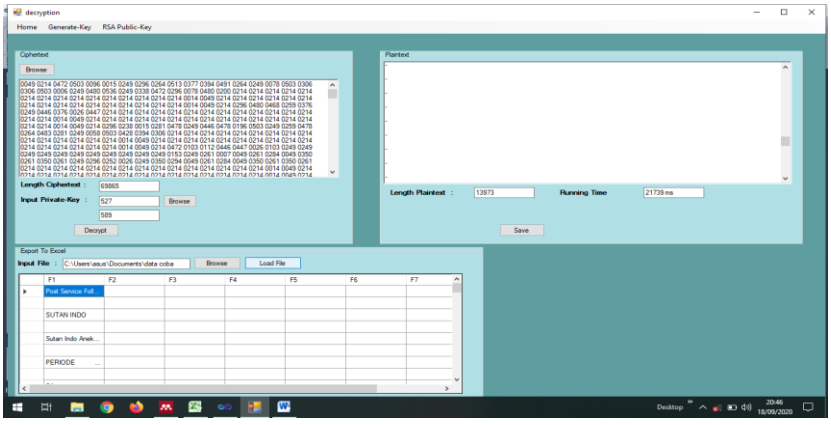
3.1 Hasil Pengujian

Hasil pengujian untuk ekripsi dan dekripsi data pelanggan ataupun data penjualan dapat dilihat pada gambar 4 dan gambar 5.



Gambar 4. Pengujian Enkripsi

Gambar 4 merupakan tampilan pengujian Enkripsi dari file *.Excel yang akan diamankan untuk kemudian dikirmkan kepada kantor pusat PT. Sutan Indo Aneka Mobil.



Gambar 5. Pengujian Dekripsi

Gambar 5 merupakan tampilan pengujian Dekripsi dari file *.Excel yang telah di enkripsi sebelumnya yang diperoleh dari kiriman email untuk kemudian dilakukan proses dekripsi. Terdapat Hubungan keterkaitan antara ukuran panjang file dengan waktu proses enkripsi dan dekripsi yang dapat dilihat pada Tabel 2.

Tabel 2. Hubungan Ukuran File

No	Nama File	Kunci			Panjang File	Waktu Enkripsi (ms)	Waktu Dekripsi (ms)
		E	N	d			
1	KPI PSFU	7	6557	3655	1465	4837	1606
2	Outbond	7	6557	3655	7027	97090	25435
3	Standarisasi	7	6557	3655	373	439	415
4	JARINGAN	7	6557	3655	4677	45404	13084

Tabel 2 menunjukan kecenderungan kenaikan waktu yang dibutuhkan untuk melakukan proses enkripsi dan proses dekripsi. Perbedaan panjang file yang digunakan mempengaruhi waktu yang dibutuhkan untuk proses enkripsi dan dekripsi. Apabila semakin panjang ukuran file maka semakin lama pula waktu yang dibutuhkan untuk melakukan enkripsi dan proses dekripsi.

4. KESIMPULAN

Berdasarkan analisis terhadap permasalahan dan pengujian aplikasi yang telah dilakukan, bahwa panjang file yang digunakan akan mempengaruhi waktu yang dibutuhkan untuk proses enkripsi dan dekripsi. Apabila semakin panjang ukuran file maka semakin lama pula waktu yang dibutuhkan untuk melakukan enkripsi dan proses dekripsi. Sehingga dapat disimpulkan bahwa algoritma RSA efektif digunakan untuk mengamankan data yang tidak terlalu besar ukuran file nya, seperti pada data pelanggan dan penjualan PT. Sutan Indo Aneka Mobil Pematangsiantar. Implementasi enkripsi dekripsi algoritma kriptografi RSA pada data pelanggan dan penjualan PT. Sutan Indo Aneka Mobil Pematangsiantar berhasil dilakukan dan meningkatkan keamanan data yang akan dikirim ke pusat, sehingga tidak bisa dibajak oleh pihak ketiga karena data yang dikirim sudah dienkripsi sampai ke penerima, selanjutnya penerima akan melakukan proses dekripsi untuk mengembalikan data pelanggan dan penjualan ke data yang sebenarnya.

REFERENCES

[1] H. Agusta, "Keamanan dan Akses Data Pribadi Penerima Pinjaman Dalam Peer to Peer Lending di Indonesia," *Krtha Bhayangkara*, vol. 15, no. 1, pp. 11–38, 2021.

[2] R. B. Anjasworo, "Penerapan MD5 Pada Verifikasi dan Validasi Keaslian Data," *Kumpulan Karya Ilmiah Mahasiswa Fakultas sains dan Tekhnologi*, vol. 1, no. 1, pp. 1–20, 2019.

[3] T. S. Alasi, R. Wanto, and V. H. Sitanggang, "Implementasi Kriptografi Algoritma Idea Pada Keamanan Data Teks Berbasis Android," *Jurnal Informasi Komputer Logika*, vol. 2, no. 1, pp. 1–4, 2021.

[4] E. D. Hastri, "Cyber Espionage Sebagai Ancaman Terhadap Pertahanan dan Keamanan Negara Indonesia," *Law and Justice Review Journal*, vol. 1, no. 1, pp. 12–25, 2021.

[5] R. Raodia, "Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime)," *Jurisprudentie*, vol. 6, no. 2, pp. 230–239, 2019.

[6] I. J. Alfreda, R. R. Permata, and T. S. Ramli, "Pelindungan Dan Tanggung Jawab Kebocoran Informasi Pada Penyedia Platform Digital Berdasarkan Perspektif Rahasia Dagang," *Jurnal Sains Sosio Humaniora*, vol. 5, no. 1, pp. 1–16, 2021.

[7] M. R. Ramadhani and & A. R. Pratama, "Analisis Kesadaran Cyber Security Pada Pengguna Media Sosial Di Indonesia," *Jurnal Aotomata*, vol. 3, no. 2, pp. 1–8, 2020.

[8] N. Ma'rufah, H. K. Rahmat, and I. D. K. K. Widana, "Degradasi Moral Sebagai Dampak Kejahatan Siber Pada Generasi Millenial di Indonesia," *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, vol. 7, no. 1, pp. 191–201, 2020.

[9] E. F. Pakpahan, K. Chandra, and A. Tanjaya, "Urgensi Pengaturan Financial Technology di Indonesia," *Jurnal Darma Agung*, vol. 28, no. 3, pp. 444–456, 2020.

[10] F. P. Nugroho, R. W. Abdullah, S. Wulandari, and Hanafi Hanafi, "Keamanan Big Data Di Era Digital di Indonesia," *Jurnal INFORMA*, vol. 5, no. 1, pp. 28–34, 2019.

[11] M. Fadlan, S. Sinawati, A. Indriani, and E. D. Bintari, "Pengamanan Data Teks Melalui Perpaduan Algoritma Beaufort dan Caesar Cipher," *Jurnal Teknik Informatika*, vol. 12, no. 2, pp. 149–158, 2019.

[12] A. Widarma, H. F. Siregar, and M. D. Irawan, "Teknik Keamanan Data Menggunakan Vigenere Cipher Dan Electronic Code Book (ECB)," *J-SAKTI (Jurnal Sains Komputer dan Informatika)*, vol. 3, no. 2, p. 393, 2019.

[13] L. L. A. Rahman, "Implikasi Diplomasi Pertahanan terhadap Keamanan Siber dalam Konteks Politik Keamanan," *Jurnal Diplomasi Pertahanan*, vol. 6, no. 2, pp. 1–93, 2020.

[14] K. A. Seputra and G. A. J. Saskara, "Kriptografi Simetris RC4 Pada Transaksi Online Booking Engine System," *Jurnal Pendidikan Teknologi dan Kejuruan*, vol. 17, no. 2, pp. 286–295, 2020.

[15] A. Vuppala, R. S. Roshan, S. Nawaz, and J. V. R. Ravindra, "An Efficient Optimization and Secured Triple Data Encryption Standard Using Enhanced Key Scheduling Algorithm," *Procedia Computer Science*, vol. 171, no. 2019, pp. 1054–1063, 2020.

[16] R. Donev, A. Alsadoon, P. W. C. Prasad, A. Dawoud, S. Haddad, and A. Alrubaie, "A novel secure solution of using mixed reality in data transmission for bowel and jaw surgical telepresence: enhanced rivest cipher RC6 block cipher," *Multimedia Tools and Applications*, vol. 80, pp. 5021–5046, 2021.

[17] V. S. Prajwal and K. V. Prema, "User Defined Encryption Procedure for IDEA Algorithm," *2018 International Conference*

on Advances in Computing, Communications and Informatics (ICACCI), pp. 1668–1671, 2018.
[18] B. Langenberg, H. A. I. Pham, and R. Steinwandt, "Reducing the Cost of Implementing the Advanced Encryption Standard as a uantum Engineering," *IEEE Transactions on Quantum Engineering*, vol. 1, no. 2500112, pp. 1–12, 2020.
[19] O. K. Sulaiman, K. Nasution, and S. Y. Prayogi, "Base64 Sebagai Kunci Keamanan pada One Time Pad (OTP)," *CESS (Journal of Computer Engineering, System and Science)*, vol. 5, no. 2, p. 241, 2020.
[20] N. Mehibel and M. Hamadouche, "A new enhancement of elliptic curve digital signature algorithm," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 23, no. 3, pp. 743–757, 2020.
[21] A. El Emine Sejad, K. Wane Keita, K. Tall, and I. Diop, "Proposal of a DH optimization model," *2020 International Conference on Computer, Information and Telecommunication Systems (CITS)*, pp. 1–5, 2020.
[22] M. M. Islam, M. S. Hossain, M. D. Shahjalal, M. K. Hasan, and Y. M. Jang, "Area-Time Efficient Hardware Implementation of Modular Multiplication for Elliptic Curve Cryptography," *IEEE Access*, vol. 8, pp. 73898–73906, 2020.
[23] T. Shang, Y. Tang, R. Chen, and J. Liu, "Full quantum one-way function for quantum cryptography," *Quantum Engineering*, vol. 2, no. 1, pp. 1–11, 2020.
[24] S. Ambika, S. Rajakumar, and A. S. Anakath, "A novel RSA algorithm for secured key transmission in a centralized cloud environment," *International Journal of Communication Systems*, vol. 33, no. 5, pp. 1–9, 2020.
[25] G. M. Nikolopoulos, "Cryptographic one-way function based on boson sampling," *Quantum Information Processing*, vol. 18, no. 8, pp. 1–25, 2019.
[26] Y. Anshori, A. Y. Erwin Dodu, and D. M. P. Wedananta, "Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) pada Tanda Tangan Digital," *Techno.Com*, vol. 18, no. 2, pp. 110–121, 2019.
[27] Ainafatul Nur Muslikah, H. R. Riswanto, K. Safinah, and K. F. H. Holle, "Implementasi Teknik Kriptografi Rsa Untuk Pengamanan Data Pengiriman Sms," *Jurnal Ilmiah Informatika*, vol. 5, no. 1, pp. 61–66, 2020.
[28] A. Cahya Putra, M. Simanjuntak, and Nurhayati, "Penerapan Algoritma Rivest Shamir Adleman (Rsa) Untuk Mengamankan Database Program Keluarga Harapan (PKH)," *Jurnal Teknik Informatika Kaputama (JTIK)*, vol. 5, no. 1, pp. 76–84, 2021.
[29] M. Nilai, S. Smp, and H. P. Bulan, "Penerapan Algoritma RSA (Rivest Shamir Adelman) Untuk Mengamankan Nilai Siswa SMP HKBP P. Bulan," *Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD (J-SISKO TECH)*, vol. 4, no. 1, pp. 88–91, 2021.
[30] Sutejo, "Implementasi Algoritma Kriptografi RSA (Rivest Shamir Adleman) Untuk Keamanan Data Rekam Medis Pasien," *Journal of Information Technology and Computer Science (INTECOMS)*, vol. 4, no. 1, pp. 104–114, 1967.