

ARTIKEL

**PENERAPAN ALGORITMA KRIPTOGRAFI MENGGUNAKAN
METODE RSA UNTUK DOKUMEN PADA BALAI DESA PUHRUBUH**



Oleh:

Melinda Dwi Asnonawati

13.1.03.02.0300

Dibimbing oleh :

- 1. Ahmad Bagus Setiawan, S.T.,M.M.,M.Kom.**
- 2. Lilia Sinta Wahyuniar, M.Pd.**

PROGRAM STUDI

FAKULTAS

UNIVERSITAS NUSANTARA PGRI KEDIRI

2018



SURAT PERNYATAAN ARTIKEL SKRIPSI TAHUN 2018

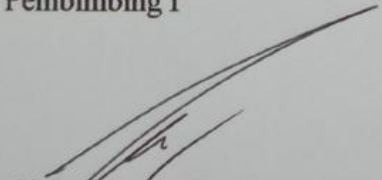
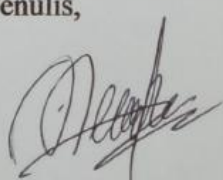
Yang bertanda tangan di bawah ini:

Nama Lengkap : Melinda Dwi Asnonawati
NPM : 13.1.03.02.0300
Telepon/HP : 085773790232
Alamat Surel (Email) : melindadwi25@gmail.com
Judul Artikel : PENERAPAN ALGORITMA KRIPTOGRAFI
MENGUNAKAN METODE RSA UNTUK
DOKUMEN PADA BALAI DESA PUHRUBUH
Fakultas – Program Studi : Teknik – Teknik Informatika
Nama Perguruan Tinggi : Universitas Nusantara PGRI Kediri
Alamat Perguruan Tinggi : Jl KH Achmad Dahlan 76 Kediri

Dengan ini menyatakan bahwa :

- artikel yang saya tulis merupakan karya saya pribadi (bersama tim penulis) dan bebas plagiarisme;
- artikel telah diteliti dan disetujui untuk diterbitkan oleh Dosen Pembimbing I dan II.

Demikian surat pernyataan ini saya buat dengan sesungguhnya. Apabila di kemudian hari ditemukan ketidaksesuaian data dengan pernyataan ini dan atau ada tuntutan dari pihak lain, saya bersedia bertanggungjawab dan diproses sesuai dengan ketentuan yang berlaku.

Mengetahui		Kediri, 7 Februari 2019
Pembimbing I  <u>Ahmad Bagus Setiawan, S.T., M.M., M.Kom.</u> NIDN.0703018704	Pembimbing II  <u>Lilia Sinta Wahyuniar, M.Pd.</u> NIDN.07051290001	Penulis,  <u>Melinda Dwi Asnonawati</u> NPM. 13.1.03.02.0300



PENERAPAN ALGORITMA KRIPTOGRAFI MENGGUNAKAN METODE RSA UNTUK DOKUMEN PADA BALAIDESIA PUHRUBUH

Melinda Dwi Asnonawati

13.1.03.02.0300

Teknik- Teknik Informatika

Melindadwi25@gmail.com

Ahmad Bagus Setiawan, S.T.,M.,M.Kom. dan Lilia Sinta Wahyuniar, M.Pd.

UNIVERSITAS NUSANTARA PGRI KEDIRI

ABSTRAK

KATA KUNCI : *Kriptografi, RSA, Enkripsi, Dekripsi*

Untuk menjaga keamanan dan kerahasiaan dokumen merupakan salah satu aspek yang sangat penting dalam sistem informasi pada saat ini. Munculnya teknologi internet dan multimedia telah mendorong berbagai macam usaha untuk melindungi, mengamankan, dan menyembunyikan data pada file digital dari pihak-pihak yang tidak mempunyai otoritas untuk mengakses file-file tersebut. Salah satu usaha untuk mengamankan data dan informasi diantaranya dengan menggunakan kriptografi RSA berbasis web.

Permasalahan dalam skripsi ini adalah bagaimana membangun aplikasi yang dapat digunakan untuk penilaian mengenkripsi teks dokumen yang bersifat rahasia. Metode yang digunakan dalam skripsi ini adalah kriptografi RSA berbasis web. Penelitian bertujuan untuk mengamankan dokumen pada balaidesa puhribuh metode RSA dengan menggunakan aplikasi *PHP* dan menggunakan *MySQL* sebagai database. Dengan aplikasi ini supaya pegawai dan pemimpin bisa mengamankan file tanpa ada yang bisa membukanya.

Dalam penelitian ini memberikan kesimpulan bahwa telah berhasil dibuat sebuah aplikasi untuk mengenkripsi dan dekripsi dokumen dengan menggunakan metode RSA dengan menggunakan kunci *public* dan *privat*, semakin besar nilai kunci p dan q untuk proses enkripsi maka semakin kuat keamanan enkripsi datanya, Aplikasi dapat memberikan alternative untuk mengamankan dokumen dengan menggunakan kriptografi Cara menggunakan aplikasi ini yaitu pegawai hanya perlu memasukkan *username* dan *password* lalu *user* menginputkan bilangan prima yang tersedia lalu memilih nilai p dan q pada proses enkripsi digunakan untuk merubah *plaintext* menjadi *chipertext*, *User* dapat mengetik langsung ke dalam inputan ataupun menginput *text* kedalam aplikasi. Pada proses dekripsi digunakan untuk merubah *chipertext* menjadi *plaintext* dengan menginputkan nilai N dan D yang didapat saat melakukan enkripsi dokumen.

1. LATAR BELAKANG

Dokumen dalam arti luas yaitu meliputi semua sumber tertulis saja, baik tertulis maupun lisan. Dalam arti sempit yaitu yang meliputi semua sumber tertulis saja. Dokumen dalam arti spesifik yaitu hanya meliputi surat-surat perjanjian. (Nurjanah, 2014)

Secara umum ada dua tipe algoritma kriptografi berdasarkan kuncinya algoritma simetris dan algoritma asimetris. Algoritma simetris adalah algoritma yang memiliki kunci dekripsi dan enkripsi yang sama sedangkan algoritma asimetris memiliki kunci yang berbeda. Dalam algoritma kunci asimetris kunci yang didistribusikan adalah kunci *public* yang tidak diperlukan kerahasiaannya sedangkan kunci *privat* disimpan atau tidak didistribusikan. Saat ini dokumen yang bersifat rahasia di Balaidesa Puhubuh Kediri tidak ada keamanan khusus untuk menjaga kerahasiaannya. Dokumen yang bersifat rahasia yang hanya ditujukan pada salah satu pegawai masih bisa dibaca pegawai lainnya.

Dengan adanya kelemahan di Balaidesa Puhubuh penulis tertarik melakukan penelitian untuk mengankan

dokume menggunakan algoritma Kriptografi RSA pada Balaidesa Puhubuh.

2. METODE

Penelitian yang diambil ialah penelitian kualitatif dimana penelitian ini diambil berdasarkan data yang sudah ada (data sekunder) berdasarkan observasi.

1. Pengumpulan Data

Teknik pengambilan data pada penelitian ini adalah sebagai berikut:

a. Studi Literatur

Pada tahap ini dalam pemahaman serta penjelasan konsep didapat dari buku-buku referensi, jurnal penelitian ataupun artikel yang didapat dari internet. Setelah materi yang dibutuhkan untuk pembuatan sistem ini telah terkumpul dan terseleksi, maka dapat dilakukan pembelajaran materi.

b. Wawancara

Wawancara dilakukan untuk mendapatkan data atau informasi tentang sistem yang ingin penulis buat secara rinci. Data itu didapat dari tanya jawab dengan narasumber guru.

c. Observasi

Pengamatan secara langsung untuk memperoleh data yang akurat. Ini dilakukan untuk mensinkronkan hasil wawancara yang didapat dengan melakukan observasi langsung.

2. Analisa

Analisa merupakan bentuk penelitian yang dilakukan secara terorganisir dalam melihat suatu peristiwa atau kejadian, untuk menentukan tema apa yang akan dipakai dalam pembuatan sistem agar dapat tersampaikan dan menjadi solusi sesuai dengan permasalahan yang ada.

3. Perancangan Sistem

Perancangan sistem yang dibuat merupakan perancangan awal bentuk dari sistem yang akan dibuat untuk diterapkan dan dibahas permasalahan, dimana sistem yang dibuat ini harus benar-benar sesuai dengan permasalahan dan harus mampu untuk diterapkan pada program

4. Desain Sistem

Setelah tahap perancangan sistem selesai maka mulai dilakukan tahapan pembuatan program. Pembuatan program ini meliputi pembuatan desain antar muka dan pengkodean. Desain antar muka yang dimaksud merupakan tindak lanjut penerapan rancangan desain antar muka yang telah dibuat pada tahapan pembuatan sistem.

5. Implementasi

Tahap ini melibatkan latihan bagi pemakai untuk menggunakan atau mengendalikan sistem aplikasi yang telah dibuat tersebut. Pada tahap implementasi akan diketahui bagaimana sistem pada program tersebut berjalan serta akan dilakukan perbaikan jika ditemui kesalahan.

6. Uji Coba

Melinda Dwi Asnonawati | 13.1.03.02.0300
Teknik – Teknik Informatika

Program yang telah dibuat apakah sudah sesuai dengan hasil yang diharapkan. Dengan mengadakan uji program ini berguna untuk mengetahui tingkat kesuksesan yang telah dicapai dalam pembuatan Program yang telah dibuat apakah sudah sesuai dengan hasil yang diharapkan. Dengan mengadakan uji program ini berguna untuk mengetahui tingkat kesuksesan yang telah dicapai dalam pembuatan sistem dan mengetahui kekurangan sehingga pada tahap berikutnya dapat terselesaikan.

7. Laporan

Dari program yang sudah sukses dalam uji coba akan dibuat laporan pada tahap akhirnya

ALGORITMA RSA

Berdasarkan hasil dari analisa sistem, maka diputuskan untuk membangun sebuah sistem untuk mengamankan dokumen rahasia agar tidak sembarang orang bisa membacanya.

Dengan menggunakan Algoritma Kriptografi RSA dokumen yang berisi teks biasa diubah menjadi teks yang tidak bisa dibaca secara langsung. Berikut adalah tahapan untuk melakukan enkripsi dan dekripsi dokumen :

a. Pilih 2 buah bilangan prima p dan q .



- b. Hitung nilai $n = p * q$, (usahakan agar setidaknya $n > 255$ agar dapat mewakili seluruh karakter ASCII).
- c. Hitung nilai $m = (p-1) * (q-1)$.
- d. Cari nilai e , dimana e merupakan relatif prima dari m .
- e. Cari nilai d , yang memenuhi persamaan $ed \equiv 1 \pmod m$ atau $d = e^{-1} \pmod m$.
- f. Kunci *public* (e, n) dan kunci *private* (d, n).
- g. Fungsi enkripsi $\rightarrow E(t_a) = t_a^e \pmod n$; dimana t_a merupakan karakter ke- a dari *message* (pesan) yang akan dienkripsi.
- h. Fungsi dekripsi $\rightarrow D(c_a) = c_a^d \pmod n$; dimana c_a merupakan karakter ke- a dari *ciphertext* yang akan didekripsikan.

Dari hasil *testing* program, didapatkan program berjalan dengan lancar dan menghasilkan *output* yang sesuai dengan perhitungan. Adapun perhitungan data *testing* yang dilakukan sebagai berikut :

- a. Menentukan nilai p dan q secara acak dimana untuk syarat penentuan nilai p dan q merupakan bebas yang termasuk bilangan prima.

Jika p bernilai 13 maka q bernilai 31

- b. Hitung modulus n (*public key*) dan fungsi *Euler's Totient* $\phi(n)$ dengan rumus

$$n = p \times q$$

$$= 13 \times 31$$

$$= 403$$

$$\phi(n) = (p - 1)(q - 1)$$

$$= (13 - 1)(31 - 1)$$

$$= 12 \times 30$$

$$= 360$$

- c. Menentukan nilai K_p . Karena nilai K_p tidak boleh merupakan nilai factorial dari $\phi(n)$ yang bersifat bilangan prima, maka sebelumnya dicari nilai factorial dari $\phi(n)$, yaitu

$$: \phi(n) = 360$$

$$= 23 \times 32 \times 5$$

Jadi untuk nilai K_p tidak boleh bernilai 2, 3 atau 5. Dan disini ditentukan $K_p = 7$

- d. Menentukan nilai K_s , Nilai K_s dapat ditentukan dengan rumus sebagai berikut :

$$(K_p \times K_s) \pmod{\phi(n)} = 1$$

$$(7 \times K_s) \pmod{360} = 1$$

Sehingga untuk menentukan nilai K_s dengan cara termudah adalah

$$K_s = "(m \times 360 + 1) / 7"$$

Hasil dari Ks adalah bilangan bulat dengan mencoba nilai-nilai m (bilangan integer) = 1, 2, 3, ..., sehingga diperoleh Ks adalah 103 dengan m = 2

e. Cek nilai Ks

$$(7 \times Ks) \bmod 360 = 1$$

$$(7 \times 103) \bmod 360 = 1$$

$$721 \bmod 360 = 1$$

kemudian

$$(721 - 1) / 360 = \text{modulo } 0$$

$$720 / 360 = 2 \text{ modulo } 0$$

Jadi dapat ditentukan bahwa nilai Ks adalah 103.

f. Setelah didapat semua parameter yang akan digunakan dalam proses enkripsi dan dekripsi, yaitu :

$$N = 403$$

$$Kp = 7$$

$$Ks = 103$$

Contoh *Plaintext* :

Nanti Sore Ada Rapat Mendadak Khusus Kabag Di Ruang Pimpinan

Untuk melakukan enkripsi, pertama ubah *plaintext* menjadi kode ascii. Kode dapat dilihat pada gambar di bawah ini :

ASCII TABLE

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	(NUL)	32	20	SPACE	64	40	@	96	60	h
1	1	(START OF HEADING)	33	21	!	65	41	A	97	61	i
2	2	(START OF TEXT)	34	22	"	66	42	B	98	62	j
3	3	(END OF TEXT)	35	23	#	67	43	C	99	63	k
4	4	(BACKSPACE)	36	24	\$	68	44	D	100	64	l
5	5	(TAB)	37	25	%	69	45	E	101	65	m
6	6	(BELL)	38	26	&	70	46	F	102	66	n
7	7	(BACKSPACE)	39	27	'	71	47	G	103	67	o
8	8	(BACKSPACE)	40	28	(72	48	H	104	68	p
9	9	(BELL)	41	29)	73	49	I	105	69	q
10	A	(LINE FEED)	42	2A	*	74	4A	J	106	6A	r
11	B	(VERTICAL TAB)	43	2B	+	75	4B	K	107	6B	s
12	C	(FORM FEED)	44	2C	,	76	4C	L	108	6C	t
13	D	(CARRIAGE RETURN)	45	2D	-	77	4D	M	109	6D	u
14	E	(SHIFT OUT)	46	2E	.	78	4E	N	110	6E	v
15	F	(SHIFT IN)	47	2F	:	79	4F	O	111	6F	w
16	10	(DATA LINK ESCAPE)	48	30	0	80	50	P	112	70	x
17	11	(DEVICE CONTROL 1)	49	31	1	81	51	Q	113	71	y
18	12	(DEVICE CONTROL 2)	50	32	2	82	52	R	114	72	z
19	13	(DEVICE CONTROL 3)	51	33	3	83	53	S	115	73	[
20	14	(DEVICE CONTROL 4)	52	34	4	84	54	T	116	74	\
21	15	(NEGATIVE ACKNOWLEDGE)	53	35	5	85	55	U	117	75]
22	16	(SYNCHRONOUS END)	54	36	6	86	56	V	118	76	^
23	17	(END OF TRANSMISSION)	55	37	7	87	57	W	119	77	_
24	18	(CANCEL)	56	38	8	88	58	X	120	78	`
25	19	(END OF MESSAGE)	57	39	9	89	59	Y	121	79	a
26	1A	(SUBSTITUTE)	58	3A	:	90	5A	Z	122	7A	b
27	1B	(IGNORE)	59	3B	;	91	5B	[123	7B	c
28	1C	(FILE SEPARATOR)	60	3C	<	92	5C	\	124	7C	d
29	1D	(GROUP SEPARATOR)	61	3D	=	93	5D]	125	7D	e
30	1E	(INCR SEPARATOR)	62	3E	>	94	5E	^	126	7E	f
31	1F	(UNIT SEPARATOR)	63	3F	?	95	5F	_	127	7F	(DEL)

Tabel 1 tabel ASCII

Jadi kode ASCII dari *plain text* adalah:

78 97 110 116 105 32 83 111 114 101 32
65 100 97 32 82 97 112 97 116 32 77
101 110 100 97 100 97 107 32 75 104
117 115 117 115 32 75 97 98 97 103 32
68 105 32 82 117 97 110 103 97 110 32
80 105 109 112 105 110 97 110

g. Proses Enkripsi (*chipper code*) = $(Character)Kp \bmod n$:

$$N = 78^7 \bmod 403 = 39$$

$$a = 97^7 \bmod 403 = 202$$

$$n = 110^7 \bmod 403 = 384$$

$$t = 116^7 \bmod 403 = 246$$

$$i = 105^7 \bmod 403 = 365$$

$$(\text{spasi}) = 32^7 \bmod 403 = 280$$

$$S = 83^7 \bmod 403 = 73$$

$$o = 111^7 \bmod 403 = 71$$

$$r = 114^7 \bmod 403 = 166$$

$$e = 101^7 \bmod 403 = 374$$

$$(\text{spasi}) = 32^7 \bmod 403 = 280$$

$$A = 65^7 \bmod 403 = 234$$

$$d = 100^7 \bmod 403 = 152$$



$$\begin{aligned} a &= 97^7 \bmod 403 = 202 \\ (\text{spasi}) &= 32^7 \bmod 403 = 280 \\ R &= 82^7 \bmod 403 = 173 \\ a &= 97^7 \bmod 403 = 202 \\ p &= 112^7 \bmod 403 = 317 \\ a &= 97^7 \bmod 403 = 202 \\ t &= 116^7 \bmod 403 = 246 \\ (\text{spasi}) &= 32^7 \bmod 403 = 280 \\ M &= 77^7 \bmod 403 = 116 \\ e &= 101^7 \bmod 403 = 374 \\ n &= 110^7 \bmod 403 = 384 \\ d &= 100^7 \bmod 403 = 152 \\ a &= 97^7 \bmod 403 = 202 \\ d &= 100^7 \bmod 403 = 152 \\ a &= 97^7 \bmod 403 = 202 \\ k &= 107^7 \bmod 403 = 81 \\ (\text{spasi}) &= 32^7 \bmod 403 = 280 \\ K &= 75^7 \bmod 403 = 270 \\ h &= 104^7 \bmod 403 = 13 \\ u &= 117^7 \bmod 403 = 65 \\ s &= 115^7 \bmod 403 = 145 \\ u &= 117^7 \bmod 403 = 65 \\ s &= 115^7 \bmod 403 = 145 \\ (\text{spasi}) &= 32^7 \bmod 403 = 280 \\ K &= 75^7 \bmod 403 = 270 \\ a &= 97^7 \bmod 403 = 202 \\ b &= 98^7 \bmod 403 = 253 \\ a &= 97^7 \bmod 403 = 202 \\ g &= 103^7 \bmod 403 = 51 \\ (\text{spasi}) &= 32^7 \bmod 403 = 280 \end{aligned}$$

$$\begin{aligned} D &= 68^7 \bmod 403 = 68 \\ i &= 105^7 \bmod 403 = 365 \\ (\text{spasi}) &= 32^7 \bmod 403 = 280 \\ R &= 82^7 \bmod 403 = 173 \\ u &= 117^7 \bmod 403 = 65 \\ a &= 97^7 \bmod 403 = 202 \\ n &= 110^7 \bmod 403 = 384 \\ g &= 103^7 \bmod 403 = 51 \\ a &= 97^7 \bmod 403 = 202 \\ n &= 110^7 \bmod 403 = 384 \\ (\text{spasi}) &= 32^7 \bmod 403 = 280 \\ P &= 80^7 \bmod 403 = 102 \\ i &= 105^7 \bmod 403 = 365 \\ m &= 109^7 \bmod 403 = 8 \\ p &= 112^7 \bmod 403 = 317 \\ i &= 105^7 \bmod 403 = 365 \\ n &= 110^7 \bmod 403 = 384 \\ a &= 97^7 \bmod 403 = 202 \\ n &= 110^7 \bmod 403 = 384 \end{aligned}$$

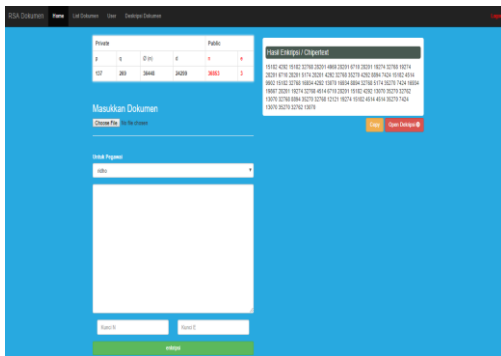
3. HASIL DAN KESIMPULAN

Keamanan dan kerahasiaan dokumen merupakan salah satu aspek yang sangat penting dalam sistem informasi pada saat ini. Munculnya teknologi internet dan multimedia telah mendorong berbagai macam usaha untuk melindungi, mengamankan, dan menyembunyikan data pada *file* digital dari pihak-pihak yang tidak mempunyai otoritas untuk mengakses file-

file tersebut. Salah satu usaha untuk mengamankan data dan informasi diantaranya dengan menggunakan kriptografi.

Rancangan *output* merupakan rancangan hasil dari semua data yang sudah diinputkan kedalam sistem. Adapun beberapa rancangan *output* tersebut adalah :

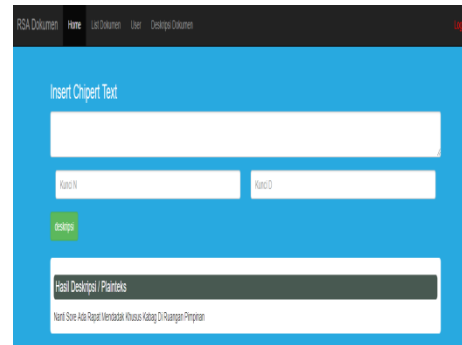
a. Halaman enkripsi



Gambar 1 halaman enkripsi

Pada halaman enkripsi digunakan untuk merubah *plaintext* menjadi *chiphertext*. *User* dapat mengetik langsung teks ke dalam inputan ataupun menginput dokumen berupa *text* kedalam aplikasi dan memasukkan kunci E dan kunci D lalu proses *User*. untuk merubah *chiphertext* menjadi *plaintext* dengan menginputkan kunci N dan kunci D yang didapat saat melakukan enkripsi dokumen

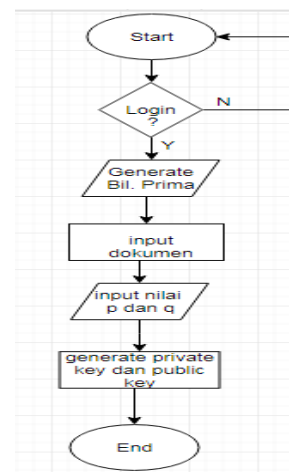
b. Halaman dekripsi



Gambar 2 halaman dekripsi

Pada halaman dekripsi digunakan untuk merubah *chiphertext* menjadi *plaintext* dengan menginputkan kunci N dan kunci D yang didapat saat melakukan enkripsi dokumen

c. Flowchart sistem



Gambar 3 flowchart sistem

KESIMPULAN

Berdasarkan penelitian yang dilakukan dalam membuat enkripsi dan dekripsi pada Balaidesa Puhubuh, maka dapat ditarik kesimpulan sebagai berikut:

1. Telah berhasil dibuatnya sebuah aplikasi untuk mengenkripsi dan dekripsi dokumen dengan menggunakan metode RSA dengan menggunakan kunci *public* dan *privat*
2. Semakin besar nilai kunci p dan q untuk proses enkripsi maka semakin kuat keamanan enkripsi datanya.
3. Aplikasi dapat memberikan alternatif untuk mengamankan dokumen dengan menggunakan kriptografi.

SARAN

Algoritma kriptografi yang dibuat ini masih memiliki banyak kekurangan. Untuk pengembangan sistem ini, perlu diperhatikan agar algoritma kriptografi berikutnya menjadi lebih baik lagi. Beberapa hal yang dapat dikembangkan antara lain:

1. Penambahan system untuk menghubungkan pada bagian organisasi agar tiap organisasi bisa saling terhubung.
2. Meningkatkan tampilan aplikasi supaya lebih *user friendly* dan mudah dipahami.

4. DAFTAR PUSTAKA

Agustina, A.N, Aryanti dan Nasron. 2015. Implementasi Algoritma RSA Untuk Enkripsi dan Dekripsi Email. *Jurnal Teknologi dan Sistem Komputer*, Vol 3, No 2 April 2015. (Online), tersedia: <https://ojs.amikom.ac.id>.

Ariyus, D. 2013. Aplikasi Algoritma RSA untuk Keamanan Data pada Sistem Informasi Berbasis Web. *Jurnal DASI*, 14 (2). (Online), tersedia: <https://ojs.amikom.ac.id>.

Asroni, Ronald Andrian., 2015. Aplikasi Enkripsi dan Dekripsi menggunakan Algoritma RSA Berbasis Web. *Jurnal Ilmiah Semesta Teknika*, 18 (1). (Online), tersedia: <https://journal.umy.ac.id>.

Fina, N. 2014 Penerapan Algoritma Kriptografi Asimetris RSA untuk Keamanan Data Oracle. Makalah diseminarkan pada Seminar Nasional Teknologi Informasi dan Multimedia, 2015. (Online),



- tersedia: <https://ojs.amikom.ac.id>,
diunduh 11 Agustus 2018.
- Dony, A. 2013. Penerapan kriptografi RSA untuk mengidentifikasi pesan digital. *Jurnal TEKNOIF*, 1 (1). (Online), tersedia: <https://ejournal.itp.ac.id>, diunduh 20 November 2018
- Kadir, Abdul. 2008a. *Belajar Database Menggunakan MySQL*. Yogyakarta: Penerbit Andi.
- Kadir, Abdul. 2008b. *Dasar Pemrograman Web Dinamis Menggunakan PHP (Revisi)*. Yogyakarta: Penerbit Andi.
- Kusrini, Luthfi, TA. 2009. *Algoritma Kriptografi RSA*. Yogyakarta: Penerbit Andi.
- Liliana, Sila. 2013. Penerapan Algoritma C.45 untuk Penentuan Jurusan Mahasiswa. *Jurnal GEMA AKTUALITA*, 2 (1). (Online), tersedia: <https://documentslide.com>, diunduh 20 November 2016
- Munir, Rinaldi. 2016. *Kriptografi*. Bandung: Penerbit Andi
- Nurjanah, Enung., 2014. Aplikasi Enkripsi Menggunakan Algoritma RSA Berbasis Web. *Jurnal Ilmiah JURNAL INFORMATIKA*, VOLUME 1 NOMOR 2, MARET 2016. [:http://kbbi.web.id/konsentrasi](http://kbbi.web.id/konsentrasi). diakses 18 November 2016.