Djtechno : Jurnal Teknologi Informasi
Vol.5, No. 1, April 2024
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

IMPLEMENTASI ALGORITMA ELGAMAL DALAM MENJAGA KEASLIAN DOKUMEN DIGITAL

Rospita Sihombing[1], Amru Yasir [2], Welnof Satria [3]

1,2,3) Teknologi Informasi, Fakultas Teknik dan Ilmu Komputer, Universitas Dharmawangsa Medan, Indonesia

Article Info

Article history:

Received: 15 April 2024
Revised: 23 April 2024
Accepted: 29 April 2024

ABSTRACT

Abstrak

Saat ini dokumen dapat disimpan dalam bentuk digital bukan hanya dokumen dalam bentuk teks, tetapi dalam bentuk lainnya seperti foto, suara, video ataupun file-file lainnya. Kemudahan dalam hal pengarsipan dan distribusi, menyebabkan penggunaan dokumen digital menjadi pilihan utama untuk menyimpan informasi. Untuk menjaga keaslian dan originalitas suatu dokumen digital, dokumen digital dapat diaplikasikan pada dokumen tersebut. dokumen digital dan konvensional mempunyai fungsi yang sama yaitu menjaga keaslian dan kepemilikan dokumen. dokumen digital tidak berbentuk coretan tinta seperti pada dokumen konvensional. Pada bentuk dokumen digital berupa kombinasi dari kumpulan angka dan huruf unik yang disisipkan ke dalam seluruh isi dokumen digital. Dokumen digital dapat dibuat dengan menerapkan ilmu kriptografi. Dokumen digital dibuat melalui dua proses utama, yaitu proses signing untuk pembuatan kunci dan implementasinya ke dalam dokumen digital serta proses verifikasi yang digunakan untuk membandingkan Dokumen digital dengan file yang diterima. Salah satu algoritma yang dapat digunakan untuk membentuk Dokumen digital adalah algoritma ElGamal.

Kata Kunci : Arsip, Dokumen Digital, Algoritma Elgamal.

Abstract

Nowadays, documents can be stored in digital form, not only documents in the form of text, but in other forms such as photos, sounds, videos or other files. The ease of archiving and distribution, causing the use of digital documents to be the main choice for storing information. To maintain the authenticity and originality of a digital document, digital documents can be applied to the document. digital and conventional documents have the same function of maintaining the authenticity and ownership of documents. digital documents are not in the form of ink strokes as in conventional documents. In the form of digital documents in the form of a combination of a unique set of numbers and letters that are inserted into the entire contents of the digital document.

Digital documents can be created by applying the science of cryptography. Digital documents are created through two main processes, namely the signing process for key generation and implementation into digital documents and the verification process used to compare digital documents with received files. One of the algorithms that can be used to form digital documents is the ElGamal algorithm.

Keywords**: **Archives, Digital Documents, Elgamal Algorithm.

Corresponding Author:

E-mail : sihombing_rospita@ymail.com

1. PENDAHULUAN

Untuk menjaga keaslian dan originalitas suatu dokumen digital, dokumen digital dapat diaplikasikan pada dokumen tersebut. dokumen digital dan konvensional mempunyai fungsi yang sama yaitu menjaga keaslian dan kepemilikan dokumen. dokumen digital tidak berbentuk coretan tinta seperti pada dokumen konvensional.

Pada bentuk dokumen digital berupa kombinasi dari kumpulan angka dan huruf unik yang disisipkan ke dalam seluruh isi dokumen digital. Dokumen digital dapat digunakan untuk mencegah penyangkalan kepemilikan dokumen, menjaga keaslian dan otentikasi pemilik.

Dokumen digital dapat dibuat dengan menerapkan ilmu kriptografi. Dokumen digital dibuat melalui dua proses utama, yaitu proses *signing* untuk pembuatan kunci dan implementasinya ke dalam dokumen digital serta proses verifikasi yang digunakan untuk membandingkan Dokumen digital dengan file yang diterima.

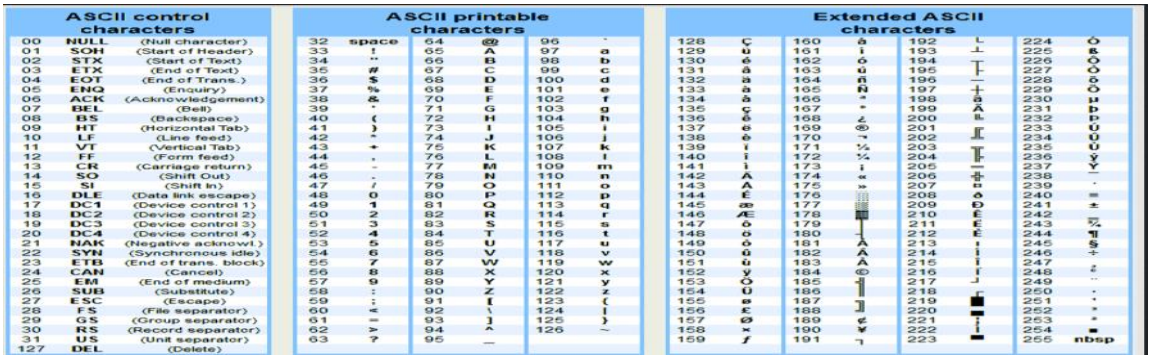
2. METODE PENELITIAN

Observasi, data dikumpulkan dari pengamatan dan pencatatan tentang cara pengarsipan dan penentuan keabsahan dokumen, baik secara digital maupun konvensional.

Studi kepustakaan, pengumpulan data melalui buku-buku tentang kriptografi, pengamanan file digital dan tanda tangan digital. Studi dokumentasi, pengumpulan data dilakukan melalui studi dari literaturliteratur, jurnal-jurnal, artikel *online* yang sudah memiliki standar ISSN mengenai kriptografi, dokumen digital dan tanda tangan digital. Sistem dapat melakukan proses enkripsi pesan berupa *plaintext* yang diinputkan oleh *user.* Sistem dapat melakukan proses dekripsi untuk mengembalikan pesan asli yangtelah terenkripsi. Sistem dapat mengubah *plaintext* menjadi *ciphertext* dari proses enkripsi. Dan mengembalikan *ciphertext* ke *plaintext* dengan proses dekripsi. Sistem dapat melakukan proses perhitungan enkripsi dan dekripsi kriptografielgamal.

3. HASIL DAN PEMBAHASAN

Tujuan dari analisa kebutuhan adalah untuk mendefinisikan apa yang harus dikerjakan oleh sistem, yaitu memenuhi keinginan pengguna/*user* untuk melakukan enkripsi dan dekripsi pada pesan atau informasi yang dimiliki.



ASCII control characters

00	NULL	(Null character)
01	SOH	(Start of Header)
02	STX	(Start of Text)
03	ETX	(End of Text)
04	EOT	(End of Trans.)
05	ENQ	(Enquiry)
06	ACK	(Acknowledgement)
07	BEL	(Bell)
08	BS	(Backspace)
09	HT	(Horizontal Tab)
10	LF	(Line feed)
11	VT	(Vertical Tab)
12	FF	(Form feed)
13	CR	(Carriage return)
14	SO	(Shift Out)
15	SI	(Shift In)
16	DLE	(Data link escape)
17	DC1	(Device control 1)
18	DC2	(Device control 2)
19	DC3	(Device control 3)
20	DC4	(Device control 4)
21	NAK	(Negative acknowl.)
22	SYN	(Synchronous idle)
23	ETB	(End of trans. block)
24	CAN	(Cancel)
25	EM	(End of medium)
26	SUB	(Substitute)
27	ESC	(Escape)
28	FS	(File separator)
29	GS	(Group separator)
30	RS	(Record separator)
31	US	(Unit separator)
127	DEL	(Delete)

ASCII printable characters

32	space	64	@	96	`
33	!	65	A	97	a
34	"	66	B	98	b
35	#	67	C	99	c
36	$	68	D	100	d
37	%	69	E	101	e
38	&	70	F	102	f
39	'	71	G	103	g
40	(	72	H	104	h
41	)	73	I	105	i
42	*	74	J	106	j
43	+	75	K	107	k
44	,	76	L	108	l
45	-	77	M	109	m
46	.	78	N	110	n
47	/	79	O	111	o
48	0	80	P	112	p
49	1	81	Q	113	q
50	2	82	R	114	r
51	3	83	S	115	s
52	4	84	T	116	t
53	5	85	U	117	u
54	6	86	V	118	v
55	7	87	W	119	w
56	8	88	X	120	x
57	9	89	Y	121	y
58	:	90	Z	122	z
59	;	91	[	123	{
60	<	92	\	124	|
61	=	93	]	125	}
62	>	94	^	126	~
63	?	95	_		

Extended ASCII characters

128	Ç	160	á	192	└	224	Ó
129	ü	161	í	193	┴	225	ß
130	é	162	ó	194	┬	226	Ô
131	â	163	ú	195	├	227	Ò
132	ä	164	ñ	196	─	228	õ
133	à	165	Ñ	197	┼	229	Õ
134	å	166	ª	198	ã	230	µ
135	ç	167	º	199	Ã	231	þ
136	ê	168	¿	200	╚	232	Þ
137	ë	169	®	201	╔	233	Ú
138	è	170	¬	202	╩	234	Û
139	ï	171	½	203	╦	235	Ù
140	î	172	¼	204	╠	236	ý
141	ì	173	¡	205	═	237	Ý
142	Ä	174	«	206	╬	238	¯
143	Å	175	»	207	¤	239	´
144	É	176	░	208	ð	240	≡
145	æ	177	▒	209	Ð	241	±
146	Æ	178	▓	210	Ê	242	‗
147	ô	179	│	211	Ë	243	¾
148	ö	180	┤	212	È	244	¶
149	ò	181	Á	213	ı	245	§
150	û	182	Â	214	Í	246	÷
151	ù	183	À	215	Î	247	¸
152	ÿ	184	©	216	Ï	248	°
153	Ö	185	╣	217	┘	249	¨
154	Ü	186	║	218	┌	250	·
155	ø	187	╗	219	█	251	¹
156	£	188	╝	220	▄	252	³
157	Ø	189	¢	221	¦	253	²
158	×	190	¥	222	▌	254	■
159	ƒ	191	┐	223	▀	255	nbsp

Gambar 3.2 Tabel Kode ASCII

Contoh Kasus :

Rospita akan mengrim pesan " selamat Pagi " Kepada Badriah melalui Kartika. Rospita tidak ingin pesan tersebut diketahui oleh badriah maka rospita mengenkripsi pesan tersebut untuk sampai kepada kartika (Private key) untuk proses deskripsi kepada badriah melalui kartika.

Penyelesaian perhitungan manula enskripsi dengan metode Elgamal sebagai beikut :

1. Pembentukan kunci

   Siti membangkitkan pasangan kunci dengan memilih

   bilangan :p = 787 g = 185 x = 32

   Kemudian p, g, x digunakan untuk menghitung y :

   $y = g^x \bmod p$

   $y = 185^{32} \bmod 787$

   y = 754

   jadi kunci public yang dimiliki Siti adalah y = 754, g = 185, p = 787 dan kunci private yang akan dikirim kepada Nunuy untuk proses dekripsi adalah adalah x =32, p = 787

2. Enskripsi Pesan

   Nilai ASCII dari pesan “Selamat PAGI” adalah 83 101 108 97 109 97 116 32 80 65 71 73

   Kemudian nilai ASCII tersebut dimasukkan kedalam blok-blok nilai m secara Berurutan.

4. SIMPULAN

Berdasarkan hasil pembahasan dapat disimpulkan beberapa hal sebagai berikut:

Telah dihasilkan suatu aplikasi untuk penandaan dokumen dengan proses enkripsi dan deskripsi.Proses pengujian aplikasi menggunakan metode *Elgamal,* hasilnya adalah proses enkripsi dan deskripsi. mplementasi program ini menghasilkan suatu aplikasi yang dapat mengubah dokumen untuk menandai bahwasanya dokumen tersebut telah diamankan. Aplikasi disini hanya menandakan dokumen telah di enskripsi. Dan belum memproteksi dokumen.

UCAPAN TERIMAKASIH

Puji dan syukur Kepada Tuhan Yesus, yang telah memberikan kesehatan dan nafas kehidupan sampai saat ini, sehingga pada akhirnya penulis dapat menyelesaikan skripsi ini dengan baik. Terimakasih untuk orangtua saya yang menjadi pendukung dalam bentuk finansial dan mendoakan selama penulis menyusun skripsi. Terimakasih untuk kekasih saya yang selalu memberikan semangat dan doanya. Terimakasih untuk para pamong yang selalu memberikan nasehat dan semangat. Terimakasih untuk para Dosen Pembina dan Pembimbing yang membantu penulis dalam menyelesaikan skripsi.

PUSTAKA

Ariyus. (2013). Kemanan Data. Retrieved June 30, 2018, from http://repository.usu.ac.id/bitstream/handle/123456789/39071/Chapter II.pdf?sequence=4&isAllowed=y

A.S, R., & Shalahudin. (2014). Metode Waterfall. Retrieved June 28, 2018, from http://eprints.polsri.ac.id/2203/3/BAB II.pdf

Bunafit. (2013). Pengertian MYSQL. Retrieved June 25, 2018, from http://eprints.polsri.ac.id/1082/3/BAB II .pdf

Imaniawan, F. F. D., & Wati, F. F. (2017). Sistem Informasi Administrasi Kependudukan Berbasis Web Pada Desa Bogangin Sumpiuh. *IndonesianJournal on Networking and Security*, *7*. Retrieved from ijns.org/journal/index.php/ijns/article/download/1516/1472

Indrawati, Hartatik, S., & Utami, I. G. (2013). Penerapan Enkripsi Dan Deskripsi Menggunakan Algoritma Rc4. Retrieved June 30, 2018, fromhttps://www.academia.edu/22370187/Penerapan_Enkripsi_Dan_Deskripsi_ Menggunakan_Algoritma_Rc4

Indrajani. (2015). Pengertian Basis Data. Retrieved May 20, 2018, from http://library.binus.ac.id/eColls/eThesisdoc/Bab2/2014-2-00296-IF Bab2001.pdf

L, I. (2017). Pengertian Kriptografi. Retrieved June 20, 2018, fromhttps://pojokteknologi.com/item/140-kriptografi

Lestari. (2013). Pengertian LRS. Retrieved June 30, 2018, from http://repository.nusamandiri.ac.id/index.php/unduh/item/1836/10-BAB-II- landasan-teori.pdf

Prayitno, A., & Safitri, Y. (2015). Pemanfaatan Sistem Informasi Perpustakaan Digital Berbasis Website Untuk Para Penulis. *IJSE – Indonesian Journal on Software Engineering*, *1*(1), 1–10.

Rizaniar, F. N., & Sardiarinto. (2015). Perancangan Sistem Informasi Wisata Air Di Daerah Istimewa Yogyakarta Berbasis Web. Retrieved August 30, 2016, from https://ejournal.bsi.ac.id/ejurnal/index.php/evolusi/article/view/625/516

Sukmaindrayana, A., & Sidik, R. (2017). Jurnal Manajemen. *Sistem Informasi Akademik Sekolah Berbasis Web Di Sekolah Menengah Pertama Negeri 11 Tasikmalaya*, *4*(2), 1–158. https://doi.org/10.1017/CBO9781107415324.004

Sukmaindyarana, A., & Sidik, R. (2017). Aplikasi Grosir Pada Toko RsidikBungursari Tasikmalaya.

Triase. (2015). Kriptografi-Elgamal-Menggunakan-Metode-Mersenne. RetrievedJune 30, 2018,

fromhttps://www.researchgate.net/profile/Triase_St_Mkom/publication/319181684_Kriptografi_Elgamal_Menggunakan_Metode_Mersenne/Links/59987 2eaa6fdcc2615843d09/Kriptografi Elgamal-Menggunakan-Metode- Mersenne.pdf?origin=publication_detail