Desain Sistem Pengamanan Database Sismik Menggunakan Algoritma RSA

1st Sudirman Sudirman
Teknologi Informasi
Universitas Bosowa
Makassar, Indonesia
sudirman.dymand@universitasbosowa.ac.id

2nd Aswin Setiawan
Teknologi Informasi
Universitas Bosowa
Makassar, Indonesia
aswinhantaz19@gmail.com

3rd Muh Syuaib
Teknologi Informasi
Universitas Bosowa
Makassar, Indonesia
muhsyuaib.info@gmail.com

***Abstrak*—Salah satu teknologi yang banyak digunakan oleh kampus adalah sistem informasi akademik (sismik). Data-data yang disimpan adalah data rahasia yang isinya tidak boleh diketahui orang lain. Akan tetapi sebagian besar kampus tidak menyediakan fitur untuk mengamankan data sehingga database yang disimpan hanya berbentuk plain text yang isinya bisa langsung dibaca oleh orang lain. Untuk mengamankan data dalam database dapat dilakukan dengan teknik penyamaran atau penyandian data yang disebut dengan kriptografi. Kriptografi merupakan ilmu dan seni teknik penyamaran atau penyandian pesan untuk melindungi data dengan mengubah kode tertentu dan hanya orang tertentu (encryptor) mempunyai kunci yang dapat menjamin kerahasiaan data. Pada jurnal ini dibuat sebuah rancangan untuk menyimpan data dengan menerapkan metode kriptografi yakni Algoritma Rivest Shamir Adleman (RSA) untuk pengamanan isi database. Dengan mengharapkan algoritma tersebut isi database akan diubah menjadi suatu informasi yang tidak dapat dimengerti oleh siapapun dan diharapkan keamanan dalam menyimpan informasi di database dapat terjamin kerahasiaan dari sebuah informasi tersebut.**

Kata kunci— Data base, Sismik, Kriptografi, RSA, Enkrip, Dekrip.

I. PENDAHULUAN

A. Latar belakang

Sistem informasi akademik (Sismik) menyimpan berbagai data penting. Data yang ada dalam sismik berisi data informasi yang penting bahkan sangat rahasia dan harus dijaga keamanannya. Kemudian dengan adanya ancaman kejahatan seperti interception (penyadapan), akibatnya data bisa jatuh pada orang yang tidak berhak bahkan data akan disalahgunakan oleh pihak yang tidak berwenang.

Dengan semakin banyaknya orang yang menggunakan layanan sismik, ditambah dengan adanya hacker dan cracker, hal ini menuntut kita agar data yang disimpan harus mempunyai keamanan yang kuat. Untuk menjaga keamanan data, dapat dilakukan dengan menggunakan teknik kriptografi. Dalam hal keamanan data, ada 4 aspek layanan keamanan yaitu kerahasiaan, keutuhan, autentikasi dan nirpenyangkalan (Munir, 2006). Banyak algoritma kriptografi yang digunakan untuk melakukan pengamankan data, Salah satu dari algoritma tersebut adalah RSA.

Algoritma kriptografi RSA merupakan algoritma kriptografi kunci publik (nirsimetri). Ditemukan pertama kali pada tahun 1977 oleh R. Rivest, A. Shamir, dan L. Adleman. Nama RSA sendiri diambil dari ketiga penemunya tersebut. Sebagai algoritma kunci publik, RSA mempunyai dua kunci, yaitu kunci publik dan kunci rahasia. Kunci publik boleh diketahui oleh siapa saja, dan digunakan untuk proses enkripsi. Sedangkan kunci rahasia hanya pihak-pihak tertentu saja yang boleh mengetahuinya, dan digunakan untuk proses dekripsi. Algoritma kriptografi RSA terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi.

Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci privat. Selama pemfaktoran bilangan besar menjadi faktor-faktor prima belum ditemukan algoritma yang mangkus, maka selama itu pula keamanan algoritma RSA tetap terjamin.

B. Rumusan Masalah

Berdasarkan latar belakang diatas, maka pokok permasalahan yang dihadapi yaitu: Bagaimana cara yang tepat dalam mengamankan database sismik dengan menggunakan Algoritma RSA.

C. Tujuan

Tujuan dari jurnal ini adalah untuk mengetahui cara yang tepat dalam mengamankan database sismik menggunakan algoritma RSA.

D. Manfaat

- Dapat menjadi sumber referensi atau konsep dalam memberikan pengamanan terhadap database sismik
- Memberi pengenalan lebih jauh terhadap kriptografi serta algoritma RCA.

II. TINJAUAN PUSTAKA

- Penelitian [1] dari Seungkwang Lee dengan judul "Rcryptect: Real-time detection of cryptographic function in the user-space filesystem" Tahun 2021. Menggunakan metode penyelesaian Rcryptect (Real time + CRYPto + deTECT) untuk mendeteksi fungsi kriptografi yang berpotensi berbahaya saat run-time di sistem file. Ini adalah teknik berbasis entropi untuk menyaring blok berbahaya yang dienkripsi dalam sistem file ruang pengguna. Berdasarkan hasil percobaan kami,Rcryptect dapat mendeteksi fungsi kriptografi dengan menggunakan blok yang mencurigakan sehingga 90% atau lebih darinblok berturut-turut tampaknya entropi tinggi. Kami menunjukkan bahwa Rcryptect dapat mendeteksi dan mencegah ransomware terkenal. Ini dapat diterapkan ke berbagai platform tanpa menginstal pembaruan kernel, dan biaya tambahannya kira-kira meningkat 13% dari waktu penulisan di sistem file.
- Penelitian [2] dari Sonal Kukreja dengan judul "Copyright protection scheme for color images using extended visual cryptography" Tahun 2020. Menggunakan metode DCuT, yaitu transformasi multiresolusi yang memberikan representasi gambar yang lebih jarang

dibandingkan dengan transformasi wavelet lainnya seperti FrFT dan Transformasi Wavelet Diskrit (DWT). FrFT dan DWT membutuhkan jumlah yang lebih besar dari koefisien frekuensi dan fungsi dasar wavelet, masing-masing untuk mewakili gambar. DcuT memiliki kemampuan yang efisien untuk merepresentasikan informasi tepi dan kurva pada citra. Mengambil gambar dua dimensi dari bentuk (,) sebagai masukan, DcuT menghasilkan Koefisien Curvelet. Eksperimen telah dilakukan pada gambar yang berbeda dengan melakukan serangan yang berbeda untuk memeriksa ketahanan skema.NCnilai tanda air yang diekstraksi dipertahankan pada 0,99 atau lebih, yang menunjukkan bahwa skema tersebut memiliki ketahanan yang luar biasa terhadap serangan. Keuntungan dari skema yang diusulkan adalah ketahanan tinggi, imperceptibility, keamanan dan deteksi buta.

- Penelitian [3] dari Luca Ferretti dengan judul "A symmetric cryptographic scheme for data integrity verification in cloud databases" tahun 2017. Menggunakan metodologi analitik, filter Bloom dan enkripsi simetris. Penelitian ini mengusulkan metodologi analitik yang memungkinkan untuk menghitung ukuran terbaik filter Bloom untuk meminimalkan penyimpanan dan overhead jaringan serta biaya layanan cloud. Penelitian ini menunjukkan bahwa skema dan metodologi yang diusulkan efektif dan mengurangi penggunaan sumber daya dalam skenario yang realistis.
- Penelitian [4] dari Hubin Zhang dengan judul "A comprehensive test framework for cryptographic accelerators in the cloud" tahun 2020. Menggunakan metodologi algoritme tipikal, yaitu RSA 2048-bit, ECDSAP256, dan chained cipher. Untuk benchmark makro, framework mengadopsi Nginx yang dimodifikasi yang mendukung mode asynchronous offloading sebagai sisi server dan memperkenalkan MySQL serta Redis untuk jenis beban kerja yang intensif pada disk atau memori. Beban kerja tambahan dapat dengan mudah dimasukkan ke dalam kerangka kerja. Selain itu, ABFork dirancang dan diimplementasikan berdasarkan alat ApacheBench standar sebagai klien untuk mengukur throughput sistem, latency, dll, sehingga mencerminkan kinerja operasi kriptografi. Kerangka kerja penelitian ini mampu mencakup beberapa mode operasi dan jenis beban kerja variabel perangkat keras heterogen.

III. METODOLOGI

Metodologi yaitu suatu tata cara atau metode dalam melakukan sesuatu (Mouton, 1996)

Metode yang digunakan dalam jurnal ini adalah metode kuantitatif.

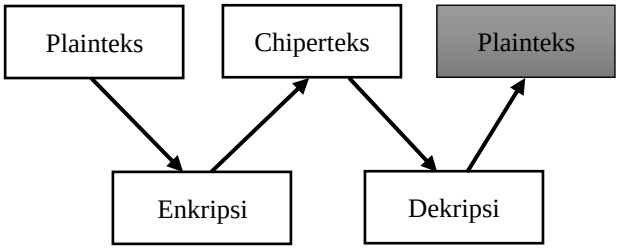
A. Landasan Teori

2.1 Kriptografi

2.1.1 Definisi

Kriptografi berasal dari bahasa Yunani yaitu kryptos yang artinya "yang tersembunyi" dan graphein yang artinya "tulisan", jadi kriptografi adalah seni dan ilmu untuk menjaga keamanan data. Dan ahlinya disebut sebagai cryptographer. Cryptanalst merupakan orang yang melakukan cryptanalysis, yaitu seni dan ilmu untuk membuka ciphertext menjadi plaintext tanpa melalui cara yang seharusnya. Data yang dapat dibaca disebut plaintext dan teknik untuk membuat data tersebut menjadi tidak dapat dibaca disebut enkripsi. Data hasil dari enkripsi disebut ciphertext, dan proses untuk mengembalikan ciphertext menjadi plaintext disebut dekripsi. Cabang matematika yang mencakup kriptografi dan cryptanalysis disebut cryptology dan pelakunya disebut cryptologist.

Secara umum, kriptografi merupakan teknik pengamanan informasi yang dilakukan dengan cara mengolah informasi awal (plainteks) dengan suatu kunci tertentu menggunakan suatu metode enkripsi tertentu sehingga menghasilkan suatu informasi baru (chiperteks) yang tidak dapat dibaca secara langsung. Chiperteks tersebut dapat dikembalikan menjadi informasi awal (plainteks) melalui proses deskripsi. Urutan proses kriptografi secara umum dapat dilihat pada gambar.



Gambar 1. Urutan proses kriptografi

Kriptografi berkembang sedemikian rupa sehingga melahirkan bidang yang berlawanan yaitu kriptanalisis. Kriptanalis (cryptanalysis) adalah ilmu dan seni untuk memecahkan cipherteks menjadi plainteks, tanpa memerlukan kunci yang digunakan. Pelakunya disebut dengan kriptanalis. Jika seorang kriptopgrafer (istilah bagi pelaku kriptografi) mentransformasikan plainteks ke cipherteks dengan menggunakan kunci, maka sebaliknya seorang kriptanalis berusaha memecahkan cipherteks tersebut untuk menemukan plainteks atau kunci.

2.1.2 Algoritma Kriptografi

Berdasarkan kunci yang dipakai, aigoritma kriptografi dapat dibedakan atas dua golongan, yaitu :

1. Algoritma Simetris
2. Algoritma Asimetris

2.1.2.1 Algoritma simetris

Algoritma kriptografi simetris atau disebut juga algoritma kriptografi konvensional adalah algoritma yang menggunakan kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi. Algoritma kriptografi simetcris dibagi menjadi 2 kategori yaitu aigoritma aliran (Stream Ciphers) dan aigoritma blok (Block Ciphers).

Pada algoritma aliran, proses penyandiannya beroricntasi pada satu bit atau satu byte data. Scdang pada algoritma blok, proses penyandiannya berorientasi pada sckumpulan bit atau byte data (per blok). Contoh aigoritma kunci simetris yang terkenal adalah DES (Data Encryption Standard).

2.1.2.2 Algoritma Asimetris

Algoritma kriptografi asimetris adalah aigoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Algoritma ini disebut juga algoritma kunci umum (public key algorithm) karena kunci untuk enknpsi dibuatumum (public key) atau dapat diketahui oleh sctiap

orang, tapi kunci untuk dekripsi hanya diketahui oleh orang yang berwenang mengetahui data yang disandikan atau sering disebut kunci pribadi (private key). Contoh algoritma terkenal yang menggunakan kunci asimetris adalah RSA, PGP dan ECC

2.2. Algoritma RSA

Sistem kriptografi RSA adalah salah satu sistem kriptografi kunci publikyang ditemukan oleh Rivest, Shamir dan Adleman. Sejak skema sistem iniditemukan, sistem ini menguasai sebagai satu-satunya sistem yang diterima danditerapkan secara luas sebagai sistem kriptografi kunci publik. Sistem ini termasuk sistem enkripsi blok, karena data asli dan data sandi adalah bilangan integer antara 0 sampai (n -1), untuk semua nilal n positif[STA951.

RSA merupakan sebuah terobosan baru dalam sistcm enkripsi data, kita sebelumnya mengenal enkripsi data dimana cara untuk meng-enkripsi dan cara men-dekripsi sebuah data dilakukan dengan kunci yang sama sebagai contoh enkripsi data sedcrhana scmisal kita punya data ABC dan dienkn'psi meniadi BCD (tiap huruf diganti menjadi huruf yang ada pada urutan berikutnya) maka saat teman kita akan mendckrip data BCD kembali menjadi ABC. cara ini lah yang disebut juga enkripsi symctric dimana aigoritma dalam mendekripsi dan mengenkripsi mempunyai kesamaan aigoritma (tinggal membalik proses/simctris).

RSA hadir dengan cara baru yaitu enkripsi yang asimetris (algoritma untuk mengenkrip dan men-dekrip merupakan dua hal yang berbeda namun mempunyai hasil yang sama). teknik RSA ini disebut juga sistem enkripsi dengan public key - private key. berikut adalah konsep pemikiran dari RSA :
Dianggap semua orang sudah mempunyai 2 buah kunci (kode untuk enkripsi dan dekripsi seterusnya akan disebutkan sebagai sebuah "kunci"), kedua kunci ini yang satu dinamakan Private key dan yang satu lagi dinamakan Public key, private key sesuai namanya maka harus disimpan / hanya diketahui oleh si pemilik kemudian public key dibcrikan ke orang lam atau ditaruh pada sebuah sumber yang bebas seperti Internet.

2.2.1 Pembangkit kunci RSA

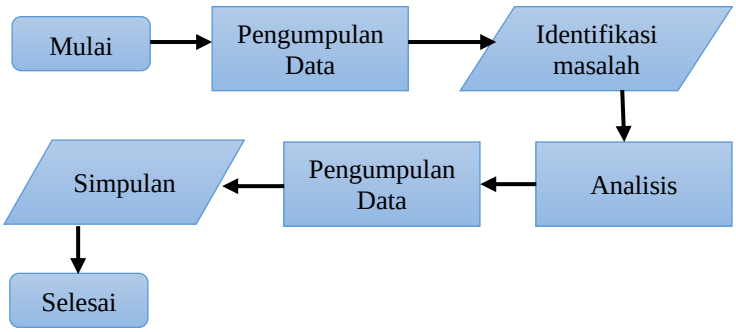
1. Pilih dua buah bilangan prima acak p,q (sangat rahasia).
2. Hitung n = p*q.
3. Hitung m = (p-1) * (q -1)
4. Pilih bilangan bulat yang yang relatif prima terhadap M dan memenuhi persyaratan pada rumus gcd (e, m) = 1
5. Hitung kunci untuk dekripsi (d) dengan rumus (e*d) mod m = 1.

2.3 Database

Pengertian basis data atau disebut juga sebagai database dalam bahasa inggris adalah kumpulan informasi yang disimpan dalam media elektronik atau komputer secara sistematik. Data tersebut juga diolah sedemikian rupa supaya bisa digunakan dengan mudah. Biasanya, istilah basis data atau database dipelajari dalam ilmu informasi. Pada awalnya, database ada dalam ilmu komputer selanjutnya meluas ke bidang elektronika. Selain itu, pengertian basis data secara sederhana juga bisa diartikan sebagai kumpulan data yang saling berhubungan satu sama lain dan mempunyai penggunaan yang beragam. Data base juga berarti kumpulan data yang bersifat mekanis, terdefinisi, dan terbagi dengan formal melalui suatu pengorganisasian. Data base adalah data operasional yang dipergunakan oleh sistem dari aplikasi dari pengorganisasian. Database juga didefinisikan sebagai sistem file yang terintegrasi serta mempunyai paling tidak satu primary key untuk sebuah pengulangan.

Pengolahan database dalam media komputer ditujukan untuk mempermudah dan tentunya mengikut i perkembangan zaman yang semakin menerapkan era komputerisasi. Suatu pengelolaan sistem database dalam dunia IT biasa dikenal dengan istilah DBMS (Database Management System). Suatu database juga dapat didefinisikan terdiri dari kumpulan tabel – tabel yang menyimpan data serta informasi. Namun pada hakikatnya penerapan database tidak hanya terdapat dalam lingkup IT saja, namun lebih dari itu. Contohnya pada sekolah atau universitas terdapat database mahasiswa, murid, tenaga pengajar, sarana prasarana dan lain lain. Dalam lingkungan perusahaan juga pastinya terdapat data – data perusahaan mencakup database karyawan, keuangan, dan lain – lain.

B. Rancangan Sistem

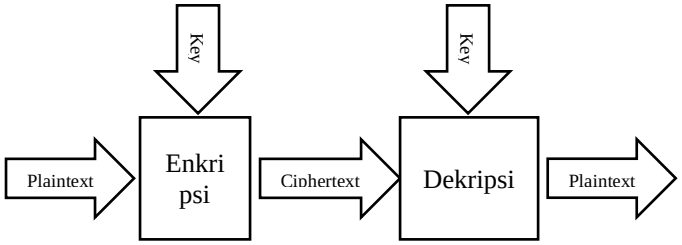


Gambar 2. Flowchart Rancangan Penelitian

Berikut merupakan penjelasan dari tahapan di atas:

a. Teknik Pengumpulan Data
   Jurnal ini menyajikan data yang diperoleh setelah melakukan pengumpulan data melalui obervasi yang dilakukan terhadap situs Sismik Unversitas Bosowa
b. Identifikasi Masalah
   Menganalisa pada masalah yang ada pada database sismik Universitas Bosowa, merupakan tahap awal pada proses penelitian.
c. Analisis
   Pada tahapan ini dilakukan terlebih dahulu proses analisis terhadap algoritma Rivest Shamir Adleman (RSA), agar dapat realisasikan pada keamanan database sismik.
d. Perancangan
   Tahapan ini menjelaskan apa saja yang akan dirancang oleh penulis dengan menggunakan algoritma RSA.
e. Simpulan
   Kesimpulan yang diperoleh setelah melakukan tahap analisis, dan rancangan menggunakan algoritma RSA.

C. Algoritma



Gambar 3. Alur Algoritma RSA

RSA dikenal juga sebagai salah satu algoritma kriptografi yang menggunakan konsep kriptografi kunci publik. RSA membutuhkan tiga langkah dalam prosesnya, yaitu: pembangkitan kunci, enkripsi, dan dekripsi. Dimana proses enkripsi dan dekripsi merupakan proses yang hampir sama, maksudnya jika bilangan acak yang dibangkitkan kuat, maka akan lebih sulit untuk melakukan cracking terhadap pesan. Parameter yang dijadikan kuat tidaknya suatu kunci yaitu terdapat pada besarnya bilangan acak yang digunakan.

IV. HASIL DAN PEMBAHASAN

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.

Berikut ini contoh perhitungan Enkripsi dan Dekripsi Algoritma RSA disimulasikan secara manual dengan plaintext "MUH. SYUAIB". 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:

Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
0	00	Null	32	20	Space	64	40	@	96	60	`
1	01	Start of heading	33	21	!	65	41	A	97	61	a
2	02	Start of text	34	22	"	66	42	B	98	62	b
3	03	End of text	35	23	#	67	43	C	99	63	c
4	04	End of transmit	36	24	$	68	44	D	100	64	d
5	05	Enquiry	37	25	%	69	45	E	101	65	e
6	06	Acknowledge	38	26	&	70	46	F	102	66	f
7	07	Audible bell	39	27	'	71	47	G	103	67	g
8	08	Backspace	40	28	(	72	48	H	104	68	h
9	09	Horizontal tab	41	29	)	73	49	I	105	69	i
10	0A	Line feed	42	2A	*	74	4A	J	106	6A	j
11	0B	Vertical tab	43	2B	+	75	4B	K	107	6B	k
12	0C	Form feed	44	2C	,	76	4C	L	108	6C	l
13	0D	Carriage return	45	2D	-	77	4D	M	109	6D	m
14	0E	Shift out	46	2E	.	78	4E	N	110	6E	n
15	0F	Shift in	47	2F	/	79	4F	O	111	6F	o
16	10	Data link escape	48	30	0	80	50	P	112	70	p
17	11	Device control 1	49	31	1	81	51	Q	113	71	q
18	12	Device control 2	50	32	2	82	52	R	114	72	r
19	13	Device control 3	51	33	3	83	53	S	115	73	s
20	14	Device control 4	52	34	4	84	54	T	116	74	t
21	15	Neg. acknowledge	53	35	5	85	55	U	117	75	u
22	16	Synchronous idle	54	36	6	86	56	V	118	76	v
23	17	End trans. block	55	37	7	87	57	W	119	77	w
24	18	Cancel	56	38	8	88	58	X	120	78	x
25	19	End of medium	57	39	9	89	59	Y	121	79	y
26	1A	Substitution	58	3A	:	90	5A	Z	122	7A	z
27	1B	Escape	59	3B	;	91	5B	[	123	7B	{
28	1C	File separator	60	3C	<	92	5C	\	124	7C	|
29	1D	Group separator	61	3D	=	93	5D	]	125	7D	}
30	1E	Record separator	62	3E	>	94	5E	^	126	7E	~
31	1F	Unit separator	63	3F	?	95	5F	_	127	7F	□

Gambar 4. Tabel Ascii

A. Pembangkit Kunci RSA :

1. Pilih dua buah bilangan prima acak p,q (sangat rahasia).
   p = 13
   q = 17

2. Hitung n = p*q.
   n = p*q
   n = 13 * 17
   n = 221

3. Hitung m = (p-1) * (q -1)
   m = (p-1) * (q -1)
   m = (13-1) *(17-1)
   m = 12 * 16
   m = 192

4. Pilih bilangan bulat yang yang relatif prima terhadap m dan memenuhi persyaratan pada rumus gcd (e, m) = 1
   Nilai e = 5
   Jadi, gcd (5,192) = 1.
   Karena gcd (5,192) = 1, maka memenuhi gcd (e, m) = 1.

5. Hitung kunci untuk dekripsi (d) dengan rumus (e*d) modm = 1.
   Nilai d = 77
   (5 * 77) mod 192 = 1
   Karena (5 * 77) mod 192 = 1, maka memenuhi rumus (e*d) mod m = 1.

6. Public Key = (e, n) (5, 221)

7. Private Key = (d, n) (77, 221)

B. Langkah-langkah Kritografi algoritma RSA:

TEXT	M	U	H	.	SPACE	S	Y	U	A	I	B
ASCII	77	85	72	46	32	83	89	85	65	73	66

Tabel 1. Konversi Teks ke Ascii Heksa Desimal

Plaintext : 77 85 72 46 23 83 89 85 65 73 66
Rumus Enkripsi :

c = pl^e mod n

C1 = 77^5 mod 221
C1 = 25

C2 = 85^5 mod 221
C2 = 102

C3 = 72^5 mod 221
C3 = 89

C4 = 46^5 mod 221
C4 = 37

C5 = 32^5 mod 221
C5 = 2

C6 = 83^5 mod 221

C6 = 70

C7 = 89^5 mod 221
C7 = 72

C8 = 85^5 mod 221
C8 = 102
C9 = 65^5 mod 221
C9 = 182

C10 = 73^5 mod 221
C10 = 99

C11 = 66^5 mod 221
C11 = 53

Chipertext : 25 102 89 37 2 70 72 102 182 99 53

Langkah-langkah proses Dekripsi:
Rumus Dekripsi:
pl = c^d mod 221

PL1 = 25^77 mod 221 = 77
PL2 = 102^77 mod 221 = 85
PL3 = 89^77 mod 221 = 72
PL4 = 37^77 mod 221 = 46
PL5 = 2^77 mod 221 = 32
PL6 = 70^77 mod 221 = 83
PL7 = 72^77 mod 221 = 89
PL8 = 102^77 mod 221 = 85
PL9 = 182^77 mod 221 = 65
PL10 = 99^77 mod 221 = 73
PL11 = 53^77 mod 221 = 66

C. Hasil enkripsi pada database sismik

Database	Text	Enkripsi
Nama	MUH. SYUAIB	25 102 89 37 2 70 72 102 182 99 53
NIM	4521048003	52 66 33 121 29 52 218 29 29 51
Jurusan	TI	67 99
Kelas	A-R	182 197 114
Angkatan	2021	33 29 33 121

Tabel 2. Hasil Enkripsi Database Sismik

KESIMPULAN

Dari hasil pembahasan analisis diatas dapat di simpulkan bahwa, keamanan informasi sangatlah penting. Perharinya pertukaran informasi semakin besar, untuk itu diharapkan setiap transaksinya memiliki keamanan agar tetap terjaga kerahasiaannya. Maka di kembangkanlah sebuah sistem keamanan pada jaringan komputer, salah satunya ialah Metode RSA (Rivest Shamir Adleman), dimana hasil dari studi literatur kemudian penulis melakukan analisis dan perancangan sehingga menjadi suatu program yang dapat di pakai untuk merahasiakan sebuah teks. Algoritma kriptografi RSA digunakan untuk mencegah agar tidak adanya sembarang orang dapat menerima suatu informasi yaitu memberikan keamanan terhadap keaslian data. Berikut kesimpulan yang dapat diambil dari hasil desain sistem pengamanan database sismik menggunakan algoritma RSA, Terdapat tiga langkah dalam proses penerapan desain sistem ini, pertama melakukan pembangkitan kunci, kedua melakukan proses enkripsi dan terakhir melakukan proses dekripsi.

SARAN

Saran kami yaitu diadakannya pengimplementasian penggunaan metode RSA di dalam database sismik agar lebih bisa menjaga kerahasiaan serta keamanan dari database sismik.

DAFTAR PUSTAKA

[1] Lee, S., Jho, N. S., Chung, D., Kang, Y., & Kim, M. Rcryptect: Real-time detection of cryptographic function in the user-space filesystem. Computers & Security, 112, 102512, 2022.

[2] Kukreja, Sonal, Geeta Kasana, and Singara Singh Kasana. "Copyright protection scheme for color images using extended visual cryptography." Computers & Electrical Engineering 91 (2021): 106931.

[3] Ferretti, L., Marchetti, M., Andreolini, M., & Colajanni, M. A symmetric cryptographic scheme for data integrity verification in cloud databases. Information Sciences, 422, 497-515, 2018.

[4] Zhang, H., Hu, X., Li, J., & Guan, H. A comprehensive test framework for cryptographic accelerators in the cloud. Journal of Systems Architecture, 113, 101873, 2021.

[5] Sudirman, S. (2021). Machine Learning Deteksi Jatuh Menggunakan Algoritma Human Posture Recognition. Proceeding KONIK (Konferensi Nasional Ilmu Komputer), 5, 462-466.

[6] Sudirman, S., Zainuddin, Z., & Suyuti, A. (2021). Fall Detection in the Elderly With Android Mobile IoT Devices Using Nodemcu And Accelerometer Sensors.