

Implementasi Algoritma RSA Untuk Kerahasiaan File Pada SMK TI Gajah Mada Medan

Implementation of the RSA Algorithm for File Confidentiality at Gajah Mada IT Vocational School, Medan

Mefor Elfantari Hulu¹, Ok Muhammad Ihsan²

^aProgram Studi Informatika Universitas Potensi Utama, Jl.K.L Yos Sudarso KM 6.5 Tj.Mulia, Medan, 20241, Indonesia

^bProgram Studi Informatika Universitas Potensi Utama, Jl.K.L Yos Sudarso KM 6.5 Tj.Mulia, Medan, 20241, Indonesia
elfanhulu8@gmail.com¹, okm.ihsan@gmail.com²

ABSTRAK

SMK TI Gajah Mada Medan terletak di Jl HM Said No 19 Gaharu, Medan Timur merupakan sebuah lembaga pendidikan yang mana didalam sekolah tersebut sering melakukan berbagai macam transaksi keuangan, seperti penggajian untuk guru, pembayaran uang bulanan bagi siswa, dan pengeluaran maupun pemasukan lainnya. Dalam melakukan transaksi keuangan tersebut, SMK TI Gajah Mada Medan masih menggunakan pencatatan secara konvensional, yang mana petugas masih mencatat setiap transaksi keuangan sekolah tersebut ke dalam sebuah buku besar atau buku kas sekolah, sehingga dikhawatirkan akan rentan terhadap manipulasi dan penyalahgunaan pada data keuangan tersebut. Maka dari itu di buat suatu sistem komputerisasi sekaligus pengamanan terhadap data tersebut. Keuangan sekolah perlu dikelola dengan baik. Pengelolaan keuangan sekolah penting untuk dilak ukan agar dana yang diperoleh dapat digunakan secara efektif dan efisien. Keuangan memberikan gambaran mengenai perancangan anggaran, penata usahaan, pengeluaran dan penerimaan kas maupun pelaporan. Untuk mengatasi permasalahan pada keamanan data keuangan di SMK TI Gajah Mada Medan tersebut, maka dapat memanfaatkan perkembangan ilmu teknologi yang ada saat ini salah satunya adalah ilmu kriptografi. Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan dengan cara menyandikannya ke dalam bentuk yang tidak dapatdimengerti lagimaknya. Dalam ilmu kriptografi, terdapat dua proses yaitu enkripsi dan dekripsi. Dalam kriptografi ada beberapa metode yang dapat menyelesaikan permasalahan pada SMK TI Gajah Mada Medan tersebut salah satunya metode RSA

Kata Kunci : Keuangan , RSA, Enkrip, Dekrip

ABSTRACT

Gajah Mada Medan IT Vocational School, located on Jl HM Said No 19 Gaharu, East Medan, is an educational institution where the school often carries out various kinds of financial transactions, such as salaries for teachers, monthly payments for students, and other expenses and income. In carrying out these financial transactions, Gajah Mada Medan IT Vocational School still uses conventional recording, where officers still record every school financial transaction in a ledger or school cash book, so that borrowing will be vulnerable to manipulation and protection of the financial data. Therefore, a computerized system was created as well as security for this data. School finances need to be managed well. School financial management is important so that the funds obtained can be used effectively and efficiently. Finance provides an overview of budget design, administration, cash expenditures and receipts and reporting. To overcome the problem of financial data security at Gajah Mada Medan IT Vocational School, we can take advantage of current technological developments, one of which is cryptography. Cryptography is the science and art of maintaining confidentiality by encoding it in a form whose meaning is no longer understandable. In cryptography, there are two processes of encryption, namely and decryption. In cryptography there are several methods that can solve problems at the Gajah Mada IT Vocational School, Medan, one of which is the RSA method.

Keywords : Finance, RSA, Encryption, Decryption

Info Artikel :

Disubmit:15 Agustus 2024

Direview:12 September 2024

Diterima : 05 Oktober 2024

Copyright © 2024 – senadimu. All rights reserved.

1. PENDAHULUAN

Pendidikan merupakan fondasi pembangunan bangsa yang tidak dapat dipisahkan dari Data ini mencakup informasi keuangan penting, seperti penerimaan dan pengeluaran, yang harus dijaga kerahasiaannya (Benny & Sewaka, 2022; Hendri Syaputra & Herdiyatomoko Fery Hendrik, 2020). Maka dari itu di buat suatu sistem komputerisasi sekaligus pengamanan terhadap data tersebut. Keuangan sekolah perlu dikelola dengan baik (Apdilah & Swanda, 2019). Pengelolaan keuangan sekolah penting untuk dilakukan agar dana yang diperoleh dapat digunakan secara efektif dan efisien. Keuangan memberikan gambaran mengenai perancangan anggaran, penata usahaan, pengeluaran dan penerimaan kas maupun pelaporan (Sandy et al., 2023; Sumiah & Hakim, 2020). Dalam ilmu kriptografi, terdapat dua proses yaitu enkripsi dan dekripsi. Dalam kriptografi ada beberapa metode yang dapat menyelesaikan permasalahan pada SMK TI Gajah Mada Medan tersebut salah satunya metode RSA (Perbawa & Diana, 2022).

Tujuan menggunakan Ilmu kriptografi pada kasus ini yaitu pada saat data keuangan akan di buka dan di ubah isinya, maka isinya akan berubah menjadi kode yang tidak mudah di pahami. Dan data keuangan tersebut hanya dapat di ubah kembali isinya menjadi teks yang mudah di pahami dengan melakukan proses dekrip oleh orang yang memiliki akses tersebut (Alfiani Fauzan & Fathurrozi, 2023; Pahrizal, 2019).

Berdasarkan penelitian Moch dan Iswan Perangin-Angin (2021) mengenai Implementasi Algoritma Rivest Shamir Adleman (RSA) Untuk Keamanan Data Nilai Siswa Pada SMK Multi Karya Medan. Menggunakan metode criptogrfi RSA untuk infomasi rahasia (Irma Listiani et al., 2022).

Erik Iman Heri Ujjianto (2020) melakukan implementasi Kriptografi untuk keamanan data teks menggunakan Algoritma Asimetris Rivest Shamir Adleman (RSA), dengan mengenkripsi teks dan teks hasil enkripsi tersebut didekripsi kembali dengan menggunakan dua kunci agar keamanan data informasi tersebut dapat terjaga keamanannya (Rizkyansyah & Saifudin, 2018; Sutejo, 2021).

Dari beberapa penelitian terdahulu yang telah berhasil menggunakan metode algoritma RSA untuk mengatasi kasus kerahasiaan data, maka peneliti menggunakan metode algoritma RSA untuk kerahasiaan data pada teks laporan keuangan sekolah SMK TI Gajah Mada Medan.

2. METODE

Di dalam penelitian ini penulis menggunakan 2 (dua) metode studi pengumpulan data yaitu:

1. Studi Lapangan

Metode ini dilakukan dengan mengamati dan mengumpulkan data langsung ke lapangan terkait keamanan data laporan keuangan di SMK TI Gajah Mada Medan Adapun teknik pengumpulan data yang dilakukan penulis adalah :

a. Pengamatan (*Observation*)

suatu aktivitas pengamatan secara cermat dan secara langsung di lokasi penelitian yaitu di SMK TI Gajah Mada Medan dengan mengambil contoh-contoh data yang di perlukan, seperti data laporan keuangan. Berikut ini merupakan data laporan keuangan pada SMK TI Gajah Mada Medan:

RENCANA ANGGARAN PENDAPATAN DAN BELANJA SEKOLAH (RAPBS)

SMK TI GAJAH MADA TAHUN PELAJARAN 2023/2024

No.	Sumber Dana	Jumlah	No	Kegiatan Pembiayaan	Jumlah
1	Dana BOS	Rp 105,280,000	1	Gaji/honorarium tenaga pendidik (guru)	Rp 220,800,000
2	Iuran Sekolah (Komite)	Rp 332,760,000	2	Gaji/honorarium tenaga kependidikan (pegawai)	Rp 79,200,000
3	Uang Pembangunan	Rp 37,600,000	3	Gaji/honorarium pelatih ekskul	Rp 46,800,000
4	Donasi	Rp	4	Pengadaan daya dan jasa	Rp 12,000,000
		Rp	5	Pengadaan bahan dan peralatan/sarana	Rp 15,000,000
		Rp	6	Pemeliharaan sarana dan prasarana	Rp 8,200,000
		Rp	7	Biaya kegiatan belajar mengajar	Rp 14,400,000
		Rp	8	Biaya kegiatan kesiswaan dan ekstra kurikuler	Rp 7,200,000
		Rp	9	Promosi sekolah dan penerimaan siswa baru	Rp 3,800,000
		Rp	10	Evaluasi dan penilaian pembelajaran dan kelulusan	Rp 5,200,000
		Rp	11	Rehab/perbaikan dan pengembangan prasarana	Rp 14,500,000
		Rp	12	Pengadaan buku teks dan buku referensi	Rp 32,500,000
		Rp	13	Pengadaan alat-alat dan bahan praktikum	Rp 12,500,000
		Rp	14	Kegiatan manajemen pengelolaan sekolah	Rp 3,540,000
	Total	Rp 475,640,000		Total	Rp 475,640,000

Gambar 1. Laporan Keuangan Pada SMK TI Gajah Mada Medan

KERTAS KERJA RENCANA KEGIATAN DAN ANGGARAN SEKOLAH (RKAS) PER TAHAP TAHUN ANGGARAN : 2023

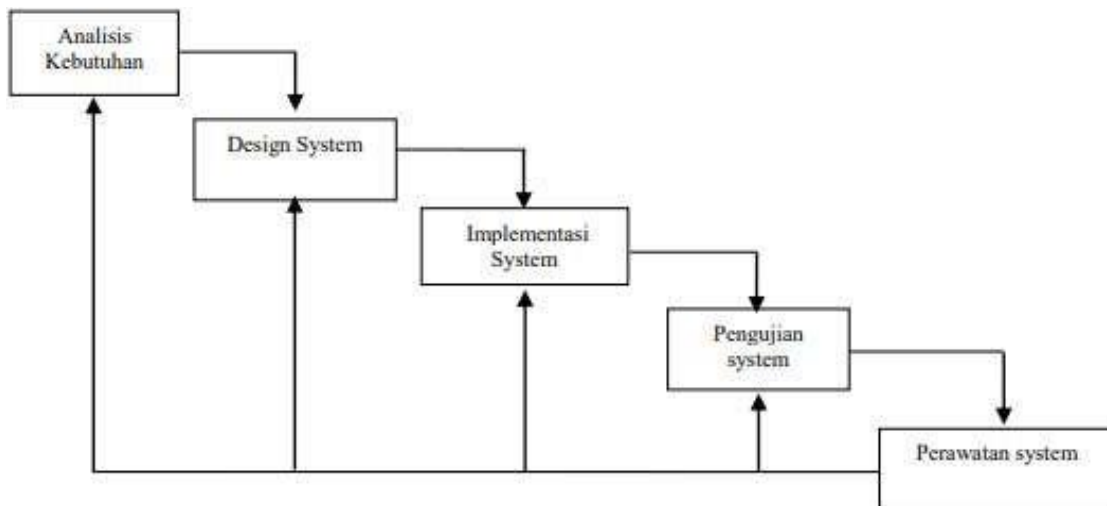
MPSN		: 99877410		URAIAN		DITERIMA		Jumlah	
Nama Sekolah		: SMK TI GAJAH MADA		TAHAP I		Rp		186.840.000	
Alamat Kabupaten Provinsi		: JL. HM. SANJ NO. 15, Kes. Medan Timur		TAHAP II		Rp		37.920.000	
Kabupaten/Kota		: Kota Medan		TAHAP III		Rp		37.920.000	
Propinsi		: Sumatera Utara		TOTAL		Rp		186.840.000	
Tahap		: I, II dan III		TOTAL PERKEMAHAN BOS 2023		Rp		186.840.000	
Jumlah Siswa		: 128 Orang							

A. PERKEMAHAN		Pemerintah		Jumlah	
Sumber Dana				186.840.000	
No. Kode		Kode Kegiatan		Jumlah	
2.3.011		BOS Kegiatan		186.840.000	
		Total Perencanaan		186.840.000	

B. BELAJAR		Kode Rincian		Kode Program		Uraian		Rincian Perhitungan Per Tahun Anggaran				Rincian Pembagian Per Tahap				TOTAL	
No. Urut								Volume	Unit	Harga per unit	Jumlah	Volume	MLA	Volume	MLA	Volume	MLA
1.	83.	83.01	83.01.01	83.01.01.01	83.01.01.01.01	83.01.01.01.01.01	Pengembangan Sistem Praktek	40	sat	1.325.000	53.000.000	40	53.000.000	40	53.000.000	40	53.000.000
2.	83.	83.02	83.02.01	83.02.01.01	83.02.01.01.01	83.02.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	575.000	23.000.000	40	23.000.000	40	23.000.000	40	23.000.000
3.	83.02	83.02.02	83.02.02.01	83.02.02.01.01	83.02.02.01.01.01	83.02.02.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000
4.	83.02	83.02.03	83.02.03.01	83.02.03.01.01	83.02.03.01.01.01	83.02.03.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000
5.	83.02	83.02.04	83.02.04.01	83.02.04.01.01	83.02.04.01.01.01	83.02.04.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000
6.	83.02	83.02.05	83.02.05.01	83.02.05.01.01	83.02.05.01.01.01	83.02.05.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000
7.	83.02	83.02.06	83.02.06.01	83.02.06.01.01	83.02.06.01.01.01	83.02.06.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000
8.	83.02	83.02.07	83.02.07.01	83.02.07.01.01	83.02.07.01.01.01	83.02.07.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000
9.	83.02	83.02.08	83.02.08.01	83.02.08.01.01	83.02.08.01.01.01	83.02.08.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000
10.	83.02	83.02.09	83.02.09.01	83.02.09.01.01	83.02.09.01.01.01	83.02.09.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000
11.	83.02	83.02.10	83.02.10.01	83.02.10.01.01	83.02.10.01.01.01	83.02.10.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000
12.	83.02	83.02.11	83.02.11.01	83.02.11.01.01	83.02.11.01.01.01	83.02.11.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000
13.	83.02	83.02.12	83.02.12.01	83.02.12.01.01	83.02.12.01.01.01	83.02.12.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000
14.	83.02	83.02.13	83.02.13.01	83.02.13.01.01	83.02.13.01.01.01	83.02.13.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000
15.	83.02	83.02.14	83.02.14.01	83.02.14.01.01	83.02.14.01.01.01	83.02.14.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000
16.	83.02	83.02.15	83.02.15.01	83.02.15.01.01	83.02.15.01.01.01	83.02.15.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000
17.	83.02	83.02.16	83.02.16.01	83.02.16.01.01	83.02.16.01.01.01	83.02.16.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000
18.	83.02	83.02.17	83.02.17.01	83.02.17.01.01	83.02.17.01.01.01	83.02.17.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000
19.	83.02	83.02.18	83.02.18.01	83.02.18.01.01	83.02.18.01.01.01	83.02.18.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000
20.	83.02	83.02.19	83.02.19.01	83.02.19.01.01	83.02.19.01.01.01	83.02.19.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000
21.	83.02	83.02.20	83.02.20.01	83.02.20.01.01	83.02.20.01.01.01	83.02.20.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000
22.	83.02	83.02.21	83.02.21.01	83.02.21.01.01	83.02.21.01.01.01	83.02.21.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000
23.	83.02	83.02.22	83.02.22.01	83.02.22.01.01	83.02.22.01.01.01	83.02.22.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000
24.	83.02	83.02.23	83.02.23.01	83.02.23.01.01	83.02.23.01.01.01	83.02.23.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000
25.	83.02	83.02.24	83.02.24.01	83.02.24.01.01	83.02.24.01.01.01	83.02.24.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000
26.	83.02	83.02.25	83.02.25.01	83.02.25.01.01	83.02.25.01.01.01	83.02.25.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000
27.	83.02	83.02.26	83.02.26.01	83.02.26.01.01	83.02.26.01.01.01	83.02.26.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000
28.	83.02	83.02.27	83.02.27.01	83.02.27.01.01	83.02.27.01.01.01	83.02.27.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000
29.	83.02	83.02.28	83.02.28.01	83.02.28.01.01	83.02.28.01.01.01	83.02.28.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000
30.	83.02	83.02.29	83.02.29.01	83.02.29.01.01	83.02.29.01.01.01	83.02.29.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000
31.	83.02	83.02.30	83.02.30.01	83.02.30.01.01	83.02.30.01.01.01	83.02.30.01.01.01.01	Pembinaan Kegiatan Pembelajaran dan Bimbingan	40	sat	60.000	2.400.000	40	2.400.000	40	2.400.000	40	2.400.000

Gambar 2. Laporan Anggaran Keuangan Pada SMK TI Gajah Mada Medan

Metodologi penelitian merupakan tata cara dan langkah - langkah yang diperlukan untuk mencapai tujuan perancangan yang dilakukan. Langkah - langkahnya adalah :



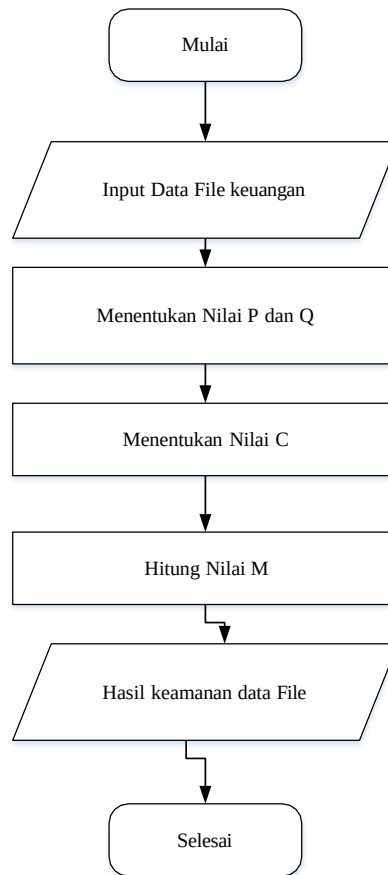
Gambar 3. Perancangan Waterfall

3. HASIL DAN PEMBAHASAN

3.1. Pembahasan

Ilmu kriptografi adalah teknik menyampaikan pesan secara tersembunyi dengan memanfaatkan fitur enkripsi data (Ginting et al., 2020; Waruwu et al., 2020). Kriptografi adalah sebuah metode pengamanan informasi dan komunikasi melalui penggunaan kode khusus, sehingga hanya orang yang tertentu saja yang dapat memproses informasi tersebut (Alfin Fisar et al., 2020; Muis et al., 2021).

Berikut ini merupakan flowchart dari metode RSA sebagai berikut :



Gambar 4. Flowchart Metode RSA

Akan dilakukan enkripsi menggunakan algoritma RSA terhadap plaintext $M = \text{KEUANGAN}$. Pertama-tama plaintext tersebut diubah menjadi format ASCII sebagai berikut :

Tabel 1. Tabel ASCII Karakter "KEUANGAN":

Huruf	ASCII
K	75
E	69
U	85
A	65
N	78
G	71
A	65
N	78

Data yang Sudah Ditetapkan:

- ☐ $p=61, q=53$
- ☐ $n=p \times q=61 \times 53=3233$
- ☐ $\phi(n)=(p-1) \times (q-1)=3120$
- ☐ Eksponen publik $e=17$
- ☐ Eksponen privat $d=2753$

Enkripsi dengan Kunci Publik

Enkripsi dilakukan dengan menggunakan rumus:

$$C = M^e \bmod n$$

di mana:

- M adalah nilai ASCII dari huruf
- e=17 adalah eksponen publik
- n=3233

1. Huruf "K" (ASCII = 75):

$$C = 75^{17} \bmod 3233$$

Langkah perhitungan:

$$75^{17} = 169518829100544703125$$

$$C = 169518829100544703125 \bmod 3233 = 2201$$

Jadi, ciphertext untuk "K" adalah 2201.

2. Huruf "E" (ASCII = 69):

$$C = 69^{17} \bmod 3233$$

Langkah perhitungan:

$$69^{17} = 1041273502979112415329$$

$$C = 1041273502979112415329 \bmod 3233 = 1313$$

Ciphertext untuk "E" adalah 1313.

3. Huruf "U" (ASCII = 85):

$$C = 85^{17} \bmod 3233$$

Langkah perhitungan:

$$85^{17} = 418211942557747392265625$$

$$C = 418211942557747392265625 \bmod 3233 = 2535$$

Ciphertext untuk "U" adalah 2535.

4. Huruf "A" (ASCII = 65):

$$C = 65^{17} \bmod 3233$$

Langkah perhitungan:

$$65^{17} = 8650415919381337933$$

$$C = 8650415919381337933 \bmod 3233 = 2790$$

Ciphertext untuk "A" adalah 2790.

5. Huruf "N" (ASCII = 78):

$$C = 78^{17} \bmod 3233$$

Langkah perhitungan:

$$78^{17} = 82724026188633676417793$$

$$C = 82724026188633676417793 \bmod 3233 = 2591$$

Ciphertext untuk "N" adalah 2591.

6. Huruf "G" (ASCII = 71):

$$C = 71^{17} \bmod 3233$$

Langkah perhitungan:

$$71^{17} = 16448102661888121144271$$

$$C = 16448102661888121144271 \bmod 3233 = 1730$$

Ciphertext untuk "G" adalah 1730.

7. Huruf "A" (ASCII = 65):

Karena "A" sudah dienkripsi sebelumnya, ciphertext-nya adalah:

$$C = 2790$$

8. Huruf "N" (ASCII = 78):

Ciphertext untuk "N" sudah dihitung:

$$C = 2591$$

Hasil Enkripsi:

Setelah dienkripsi, teks "KEUANGAN" berubah menjadi deretan ciphertext:

- 2201 1313 2535 2790 2591 1730 2790 2591

Dekripsi dengan Kunci Privat

Dekripsi dilakukan dengan menggunakan rumus:

$$M = C^d \bmod n$$

di mana:

- C adalah nilai ciphertext
- d=2753 adalah eksponen privat
- n=3233

Dekripsi setiap ciphertext untuk mendapatkan kembali teks asli.

1. Ciphertext 2201 (untuk "K"):

$$M = 2201^{2753} \bmod 3233$$

Dengan menggunakan metode eksponensiasi modular:

$$M = 75$$

Ini mengembalikan huruf "K".

2. Ciphertext 1313 (untuk "E"):

$$M = 1313^{2753} \bmod 3233$$

Hasilnya adalah:

$$M = 69$$

Ini mengembalikan huruf "E".

3. Ciphertext 2535 (untuk "U"):

$$M = 2535^{2753} \bmod 3233$$

Hasilnya adalah:

$$M = 85$$

Ini mengembalikan huruf "U".

4. Ciphertext 2790 (untuk "A"):

$$M = 2790^{2753} \bmod 3233$$

Hasilnya adalah:

$$M = 65$$

Ini mengembalikan huruf "A".

5. Ciphertext 2591 (untuk "N"):

$$M = 2591^{2753} \bmod 3233$$

Hasilnya adalah:

$$M = 78$$

Ini mengembalikan huruf "N".

6. Ciphertext 1730 (untuk "G"):

$$M = 1730^{2753} \bmod 3233$$

Hasilnya adalah:

$$M = 71$$

Ini mengembalikan huruf "G".

7. Ciphertext 2790 (untuk "A"):

$$M = 2790^{2753} \bmod 3233$$

Hasilnya adalah:

$$M = 65$$

Ini mengembalikan huruf "A".

8. Ciphertext 2591 (untuk "N"):

$$M = 2591^{2753} \bmod 3233$$

Hasilnya adalah:

M=78

Ini mengembalikan huruf "N".

Hasil Dekripsi:

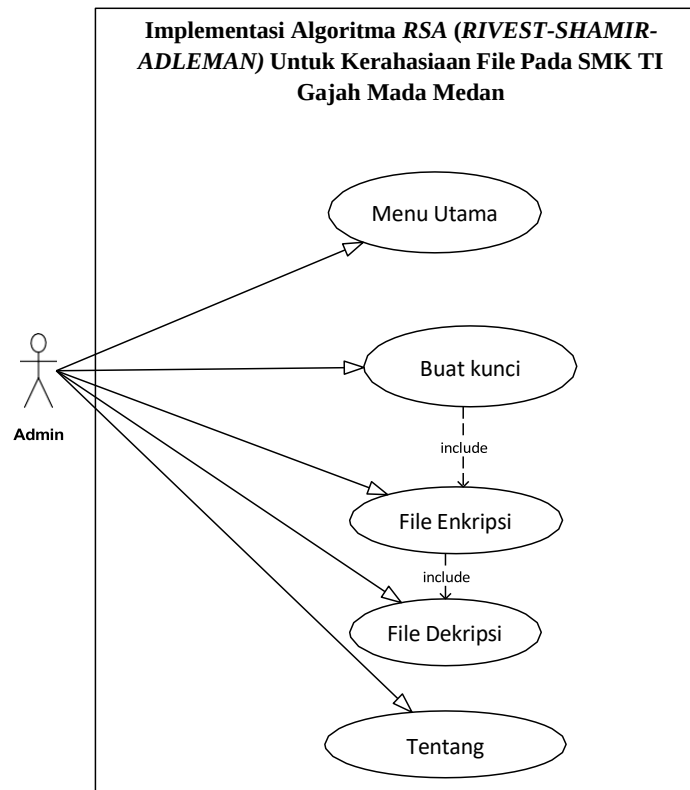
Setelah dekripsi, maka mendapatkan kembali teks asli:

- **KEUANGAN**

Kesimpulan:

- **Enkripsi** mengubah teks "KEUANGAN" menjadi deretan ciphertext 2201 1313 2535 2790 2591 1730 2790 2591 menggunakan kunci publik.
- **Dekripsi** menggunakan kunci privat mengembalikan ciphertext tersebut menjadi teks asli "KEUANGAN".

Secara garis besar, bisnis proses sistem yang akan dirancang digambarkan dengan *usecase diagram* yang terdapat pada gambar 5:



Gambar 5. Use Case Diagram

3.2. Hasil

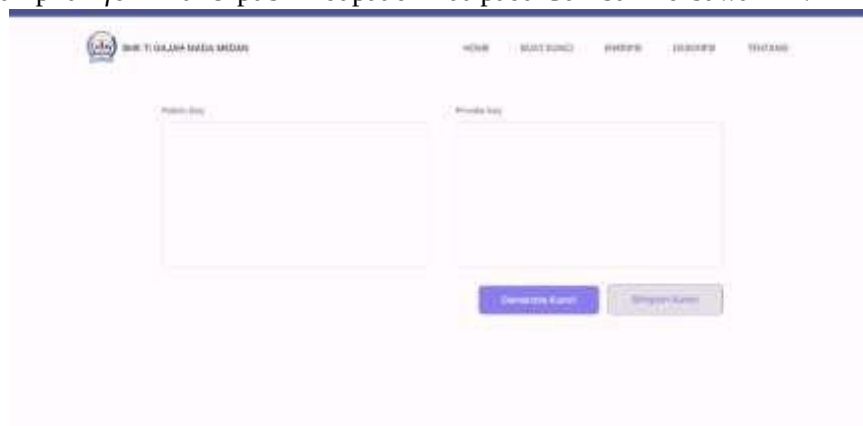
1. Tampilan Menu beranda

Tampilan beranda merupakan tampilan yang pertama kali muncul ketika program dijalankan. Pada menu beranda ini ada beberapa elemen yang membantu pengguna dalam mengoperasikan aplikasinya, dan sebagai *form* beranda admin program. Gambar tampilan beranda dapat ditunjukkan pada gambar 6 :

Gambar 6. Tampilan *Form* Beranda

2. Tampilan *Form* Buat Kunci Publik

Form buat kunci publik merupakan *interface* untuk pembuatan kunci public dan private dengan menggunakan metode RSA, kunci publik ini di gunakan saat mengenkripsi dan mendekripsi file. Untuk lebih jelasnya tampilan *form* kunci publik dapat dilihat pada Gambar 7 dibawah ini.

Gambar 7. Tampilan *Form* Menu Kunci Publik

3. Tampilan *Form* Data Unggah File Enkripsi

Form unggah file enkripsi ini berfungsi untuk merubah isi data unggah file enkripsi dalam bentuk *chipertext*, menyimpan hasil enkripsi (*chipertext*), dan keluar dari *form* data enkripsi. Berikut ini tampilan *form* data unggah file enkripsi dapat dilihat pada gambar 8 berikut ini:

Gambar 8. Tampilan *Form Data* unggah file enkripsi

3. Tampilan *Form Data* dekripsi

Form unggah file deksripsi ini berfungsi sebagai tempat merubah isi data unggah file deksripsi. Berikut ini tampilan *form* data unggah file deksripsi dapat dilihat pada gambar 9 berikut ini:

Gambar 9. Tampilan *Form* Dekripsi

4. Tampilan *Form* Tentang

Form tentang berfungsi untuk melihat tentang aplikasi, aplikasi ini merupakan aplikasi enkripsi dan deskripsi data keuangan dalam bentuk file word dan excel yang dapat dilihat sebagai berikut ini:

Gambar 10. Tampilan *Form* Tentang

4. KESIMPULAN

Berdasarkan hasil pembahasan dan uji coba yang telah dilakukan pada Implementasi Algoritma RSA (*RIVEST-SHAMIR-ADLEMAN*) Untuk Kerahasiaan File pada SMK TI Gajah Mada Medan, dapat disimpulkan :

1. Aplikasi yang dirancang dapat dapat memanipulasi data file data keuangan pada SMK TI Gajah Mada Medan dan terhadap isi suatu *file* data keuangan pada SMK TI Gajah Mada Medan dengan system penyandian Aplikasi algoritma RSA
2. Sistem yang dibangun sudah mampu melakukan enkripsi dan dekripsi terhadap data Sehingga dapat Melindungi data-data data keuangan pada SMK TI Gajah Mada Medan dengan menggunakan metode RSA.
3. Sistem yang dibangun mempunyai tampilan yang sangat sederhana dan dengan menggunakan kunci berupa huruf dan angka dan dapat diimplementasikan untuk menjaga kerahasiaan data keuangan.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Bapak Ok Muhammad Ihsan M.kom atas bimbingan dan dukungannya selama proses penelitian ini. Kepada LPPM Universitas potensi utama yang telah banyak memberikan masukan dan saran dalam penyelesaian penelitian ini.

Semoga semua ilmu yang telah diberikan menjadi bekal di masa depan saya, sekali lagi saya ucapkan terimakasih atas semua dukungan dan bimbingan yang tak ternilai ini.

REFERENSI

- [1] Alfiani Fauzan, D., & Fathurrozi, A. (2023). Perancangan Aplikasi Pengamanan Data Menggunakan Algoritma RSA (Rivest Shamir Adleman) dan AES (Advanced Encryption Standard) Berbasis Web. *Journal of Information and Information Security (JIFORTY)*, 4(1), 2722–4058. <http://ejurnal.ubharajaya.ac.id/index.php/jiforty>
- [2] Alfin Fisar, M., Adriansyah, A. F., & Nazahrani, S. L. (2020). Pemanfaatan Digital Signature Pada Sertifikat Digital Berbasis Blockchain. *TRIPLE A: Jurnal Pendidikan Teknologi Informasi*, 1(2), 103–107. <https://blockchain.alphabetincubator.id/>
- [3] Apdilah, D., & Swanda, H. (2018). Penerapan Kriptografi RSA Dalam Mengamankan File Teks Berbasis PHP. *Jurnal Teknologi Informasi*, 2(1), 45. <https://doi.org/10.36294/jurti.v2i1.407>
- [4] Benny, S., & Sewaka. (2022). Aplikasi Pengamanan Data Menggunakan Kriptografi Dengan Metode Wake dan Algoritma Des Bebasis Java Desktop. *OKTAL : Jurnal Ilmu Komputer Dan Science*, 1(7), 808–817. <https://journal.mediapublikasi.id/index.php/oktal>
- [5] Ginting, A., Isnanto, R. R., & Windasari, I. P. (2015). Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email. *Jurnal Teknologi Dan Sistem Komputer*, 3(2), 253. <https://doi.org/10.14710/jtsiskom.3.2.2015.253-258>
- [6] Hendri Syaputra, & Herdiyatomoko Fery Hendrik. (2012). Aplikasi enkripsi data pada file teks dengan algoritma rsa (. *Seminar Nasional Teknologi Informasi & Komunikasi Terapan 2012 (Semantik 2012)* Semarang, ISBN 979-(Semantik), 229–234.
- [7] Irma Listiani, Maimanah Salsabila Nasution, Wini Istya Sari, & Adnan Buyung Nasution. (2022). Perancangan Keamanan Data Pasien Di Klinik Kecantikan Ratu Beauty Studio Menggunakan Metode <https://senadimu.potensi-utama.ac.id | redaksijurnalupu@gmail.com>

Kriptografi Rsa. *Jurnal Informatika Teknologi Dan Sains*, 4(4), 437–443.
<https://doi.org/10.51401/jinteks.v4i4.2173>

- [8] Muis, M. D., Sukarno, P., & ... (2021). Analisis Dan Implementasi Sistem Pendeteksi Ijazah Dan Transkrip Palsu Dengan Menggunakan Ipfs Dan Smart Contract Blockchain. *EProceedings* ..., 8(5), 9872–9884.
<https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/15751>
- [9] Pahrizal, D. P. (2019). Implementasi Algoritma Rsa Untuk Pengamanan Data Berbentuk Teks. *Jurnal Pseudocode*, III(1), ISSN : 2355 – 5920.
- [10] Perbawa, K. A., & Diana, D. (2022). Application of Linear Congruential Generator (LCG) Algorithm in Android Based Mathematics Education Game. *Jurnal Komputer, Informasi Dan Teknologi*, 2(1), 47–56.
<https://doi.org/10.53697/jkomitek.v2i1.599>
- [11] Rizkyansyah, Y. F., & Saifudin, A. (2018). Integrasi Algoritma RSA (Rivest Shamir Adleman) dan Caesar Cipher untuk Meningkatkan Keamanan Enkripsi SMS (Short Message Service). *Jurnal Informatika Universitas Pamulang*, 3(3), 208. <https://doi.org/10.32493/informatika.v3i3.2238>
- [12] Sandy, C. L. M., Fadlisyah, F., & Reyhan Achmad Rizal. (2023). Sistem Informasi E-Voting Berbasis Web Menggunakan Metode RSA dan Base64. *Jurnal CoSciTech (Computer Science and Information Technology)*, 4(1), 200–206. <https://doi.org/10.37859/coscitech.v4i1.4753>
- [13] Sumiah, A., & Hakim, R. R. (2020). Implementasi Metode Linear Generator Pada Game Congruential Puzzle Berbasis Android. *JEJARING : Jurnal Teknologi Dan Manajemen Informatika*, 5(1), 1–10.
<https://doi.org/10.25134/jejaring.v5i1.6748>
- [14] Sutejo, S. (2021). Implementasi Algoritma Kriptografi Rsa (Rivest Shamir Adleman) Untuk Keamanan Data Rekam Medis Pasien. *INTECOMS: Journal of Information Technology and Computer Science*, 4(1), 104–114.
<https://doi.org/10.31539/intecom.v4i1.2437>
- [15] Waruwu, E. V., A. A., Sonata, F., & Zulkarnain, I. (2020). Penerapan Digital Signature Menggunakan Metode Rsa Untuk Menvalidasi Keaslian Ijazah Sma Swasta Bina Artha. *J-SISKO TECH (Jurnal Teknologi Sistem Informasi Dan Sistem Komputer TGD)*, 3(2), 45. Surbakti, A. S. B., & Pohan, Y. A. (2024). Pengaruh lingkungan kerja, stres kerja dan budaya organisasi terhadap kinerja karyawan. *Jurnal Manajemen dan Bisnis Jayakarta*, 5(2), 180–189.
<https://www.journal.stiejayakarta.ac.id/index.php/JMBJayakarta/article/view/197>
- [16] Purba, S. E., & Pohan, Y. A. (2024). Pengaruh keterampilan dan pengalaman kerja terhadap kemampuan kerja perawat pada Rumah Sakit Umum Wulan Windy. *Jurnal Dunia Pendidikan*, 4(3), 1213–1226. <https://doi.org/10.55081/jurdip.v4i3.2039>
- [17] Zagoto, E., & Pohan, Y. A. (2024). Pengaruh pelatihan kerja, motivasi kerja dan disiplin kerja, terhadap kinerja karyawan Rumah Sakit Umum Mitra Medika Medan. *Jurnal Dunia Pendidikan*, 4(3), 1159–1179.
<https://doi.org/10.55081/jurdip.v4i3.1981>
- [18] Gulo, A. F., & Pohan, Y. A. (2024). Pengaruh disiplin kerja, kompensasi dan motivasi kerja terhadap kinerja karyawan pada PT. Yumeida Utama Industry. *Jurnal Dunia Pendidikan*, 4(3), 1125–1137. <https://doi.org/10.55081/jurdip.v4i3.1978>
- [19] Mauliza, P., Prabowo, A., & Aspan, H. (2023). Analisis social media promotion, perceived value, dan customer satisfaction terhadap revisit intention wisatawan pada Sawah Lukis Binjai. *Jurnal Menara Ekonomi: Penelitian dan Kajian Ilmiah Bidang Ekonomi*, 9(1). <https://doi.org/10.31869/me.v9i1.4788>
- [20] Prabowo, A., & Risal, T. (2023). Peran entrepreneurial orientation dan social media marketing terhadap peningkatan strategi bersaing (UMKM) coffee shop pada era modern customer di Kota Medan. *Menara Ekonomi*, 9(1).
<https://senadimu.potensi-utama.ac.id | redaksijurnalupu@gmail.com>

<https://jurnal.umsb.ac.id/index.php/menaraekonomi/article/download/4785/pdf>

- [21]Aspan, H., Rozaini, Prabowo, A., & Zahara, A. N. (2024). Analysis of work discipline and job satisfaction on lecturer performance in Medan City. *International Journal of Economic, Business, Accounting, Agriculture Management and Sharia Administration (IJEBAS)*, 4(4), 1193–1205. <https://doi.org/10.54443/ijebas.v4i4.1857>
- [22]Aspan, H., Rozaini, Prabowo, A., & Lestari, D. M. (2024). Implementation of lecturer performance: Through career paths and work environment on private lecturers in Medan City. *International Conference on Health Science, Green Economics, Educational Review and Technology (IHERT)*, 6(1), 114–126. <https://doi.org/10.54443/ihert.v6i1.379>
- [23]Aspan, H., Rozaini, Wahyuni, E. S., & Prabowo, A. (2024). Personal resources and job crafting: Implications work engagement for modern coffee shops employee in Medan City. *Multidisciplinary Output Research for Actual and International Issue (MORFAI)*, 4(2), 556–567. <https://doi.org/10.54443/morfai.v4i2.1859>
- [24]Prabowo, A., Aspan, H., Wahyuni, E. S., & Lestari, I. (2024). Anteseden shopping emotion konsumen dalam berbelanja brand fashion Uniqlo. *Management Studies and Business Journal (PRODUCTIVITY)*, 1(5), 826–834. <https://doi.org/10.62207/ebtme684>
- [25]Azzahri, S., & Prabowo, A. (2024). Pengaruh content creator, price promotion, sosial media marketting terhadap impulsive buying dalam pembelian produk skincare pada aplikasi Tik Tok Shop (Studi kasus mahasiswa/i Fakultas Ekonomi dan Bisnis Universitas Potensi Utama). *Jurnal Widya*, 5(2). <https://doi.org/10.54593/awl.v5i2.366>
- [26]Kadariah, S., & binti Noor Azman, F. K. (2023). Product marketing strategy Muamalat DIN (Digital Islamic Network) at PT. Bank Muamalat Indonesia Tbk. *Journal of Islamic Financial Technology*, 2(2), 40–59. <https://doi.org/10.24952/jiftech.v2i2.10981>
- [27]Kadariah, S., & Utama, U. P. (2023). The impact of online loans on the community. *Journal of Islamic Financial Technology*, 2(1), 132–144. <https://jurnal.uinsyahada.ac.id/index.php/jiftech/article/view/9718>
- [28]Kadariah, S., Nasution, A. W., & Siregar, S. (2023). Penerapan konsep peringkat risiko pada manajemen risiko hukum di perbankan syariah. *Jurnal EMT KITA*, 7(2), 301–307. <https://doi.org/10.35870/emt.v7i2.890>
- [29]Kadariah, S., & Majid, M. S. A. (2023). Krisis ekonomi dalam perspektif Islam. *Jurnal EMT KITA*, 7(1), 18–24. <https://doi.org/10.35870/emt.v7i1.717>
- [30]Nazli, P. (2024). Implementasi perpanjangan masa angsuran pembiayaan murabahah di bank syariah pada masa pandemi Covid-19. *Jurnal Ekonomi, Bisnis dan Manajemen*, 3(1), 174–189. <https://doi.org/10.58192/ebismen.v3i1.1760>
- [31]Aisyah, S., Natasha, S. F., Nazli, P., Anindya, D. A., Anggraini, D. P., & Habibie, M. (2024). Analysis of supporting factors in performance quality of Medan City tourism services for free daily employees. *Economic and Business Horizon*, 3(1), 1–12. <https://doi.org/10.54518/ebh.3.1.2024.239>
- [32]Ridwan, M., Hutagalung, M. A. K., Riski, B., & Rambe, R. (2024). Analisis pengaruh pembiayaan musyarakah, dana pihak ketiga terhadap profitabilitas Bank Sumut Syariah Medan. *J-EBIS (Jurnal Ekonomi dan Bisnis Islam)*, 9(1), 97–116. <https://doi.org/10.32505/j-ebis.v9i1.8786>

- [33]Budimansyah, M., & Ridwan, M. (2023). Analisis penyelesaian akad akad pembiayaan bermasalah di BPRS Al Washliyah Medan. *Innovative: Journal of Social Science Research*, 3(6), 7112–7120. <https://j-innovative.org/index.php/Innovative/article/view/6937>
- [34]Arafah, S., Hutagalung, M. A. K., Mushliha, & Sembiring, E. A. (2024). Determinan keputusan masyarakat dalam berinvestasi di pasar modal syariah. *MUTLAQAH: Jurnal Kajian Ekonomi Syariah*, 5(1), 1–13. <https://doi.org/10.30743/mutlaqah.v5i1.9715>
- [35]Ridwan, M., Hutagalung, M. A. K., Riski, B., & Rambe, R. (2024). Analisis pengaruh pembiayaan musyarakah, dana pihak ketiga terhadap profitabilitas Bank Sumut Syariah Medan. *J-EBIS (Jurnal Ekonomi dan Bisnis Islam)*, 9(1), 97–116. <https://doi.org/10.32505/j-ebis.v9i1.8786>
- [36]Yamin, M., & Murtani, A. (2024). The influence of halal lifestyle, halal knowledge and promotion on Rabbani brand purchasing decisions: (Study on Rabbani consumers in Medan City). *International Journal of Education, Social Studies, and Management (IJESSM)*, 4(3), 1120–1132. <https://doi.org/10.52121/ijessm.v4i3.501> <https://doi.org/10.53513/jsk.v3i2.2033>