Merkurius: Jurnal Riset Sistem Informasi dan Teknik Informatika
Volume. 3 Nomor. 6 November 2025
e-ISSN : 3031-8912, p-ISSN : 3031-8904, Hal. 176-190
DOI: https://doi.org/10.61132/merkurius.v3i6.1160
Tersedia: https://journal.arteii.or.id/index.php/Merkurius

Super Enkripsi Kriptografi Pengamanan Pesan File Audio Record Mp3 dengan Algoritma Riverst Shamir Adleman (RSA) dan Elgamal

Dhymaz Haiqal Azhari[1*], Achmad Fauzi[2], Herman Sembiring[3]
[1-3]Informatics Engineering, STMIK Kaputama, Indonesia
[*]*Penulis korespondensi: haiqaldhymaz@gmail.com[1]*

Abstract. *MP3 audio files are often used in a variety of fields, but they are prone to security risks such as eavesdropping and illegal access. This study proposes a super encryption method by combining the algorithms of Rivest Shamir Adleman (RSA) and ElGamal to improve the protection of audio data. RSA was chosen for its efficiency and ease of implementation, while ElGamal offers a high level of security through discrete logarithmic complexity. The combination of the two is expected to address the weaknesses of each algorithm and strengthen file security. The system is developed using the Python programming language with the Visual Studio Code environment. The encryption process is done in layers: MP3 files are first encrypted with RSA, and then the results are encrypted again with ElGamal. The decryption is done in reverse order. Tests are conducted with various MP3 file sizes to measure the effectiveness and performance of the system. The results show that this method is able to secure audio files so that they cannot be accessed without the private keys of both algorithms. Although processing times are increased compared to single encryption, the level of security obtained is much higher. This approach can be an effective solution for protecting digital audio data, particularly MP3 format, and could potentially be applied to a wide range of other data types that require a high level of security.*

Keywords: *Algorithm Cryptography; Audio Security; Digital Protection; RSA ElGamal; Super Encryption*

Abstrak. File audio MP3 sering digunakan dalam berbagai bidang, namun rawan terhadap risiko keamanan seperti penyadapan dan akses ilegal. Penelitian ini mengusulkan metode *super enkripsi* dengan menggabungkan algoritma Rivest Shamir Adleman (RSA) dan ElGamal untuk meningkatkan perlindungan data audio. RSA dipilih karena efisiensi dan kemudahan implementasinya, sedangkan ElGamal menawarkan tingkat keamanan tinggi melalui kompleksitas logaritma diskrit. Kombinasi keduanya diharapkan mengatasi kelemahan masing-masing algoritma dan memperkuat keamanan file. Sistem dikembangkan menggunakan bahasa pemrograman Python dengan lingkungan Visual Studio Code. Proses enkripsi dilakukan secara berlapis: file MP3 terlebih dahulu dienkripsi dengan RSA, lalu hasilnya dienkripsi kembali dengan ElGamal. Dekripsi dilakukan dengan urutan terbalik. Pengujian dilakukan dengan berbagai ukuran file MP3 untuk mengukur efektivitas dan kinerja sistem. Hasil menunjukkan bahwa metode ini mampu mengamankan file audio sehingga tidak dapat diakses tanpa kunci privat kedua algoritma. Walaupun waktu pemrosesan meningkat dibandingkan enkripsi tunggal, tingkat keamanan yang diperoleh jauh lebih tinggi. Pendekatan ini dapat menjadi solusi efektif untuk melindungi data audio digital, khususnya format MP3, dan berpotensi diterapkan pada berbagai jenis data lain yang memerlukan tingkat keamanan tinggi.

Kata Kunci: Algoritma Kriptografi; Keamanan Audio; Proteksi Digital; RSA ElGamal; Super Enkripsi

1. PENDAHULUAN

Perkembangan teknologi digital mempermudah pengiriman dan berbagi data, termasuk file audio MP3 yang banyak digunakan pada berbagai platform seperti media sosial dan pendidikan. Namun, kemudahan ini juga diiringi risiko keamanan, seperti penyadapan, pencurian data, dan akses ilegal. File audio MP3 sering memuat informasi penting sehingga memerlukan perlindungan yang efektif.

Kriptografi menjadi salah satu solusi utama untuk mengamankan data digital. RSA dikenal cepat dan mudah diimplementasikan, sementara ElGamal menawarkan keamanan tinggi melalui kompleksitas logaritma diskrit. Penelitian sebelumnya menunjukkan RSA

Naskah Masuk: 20 September 2025; Revisi: 14 Oktober 2025; Diterima: 15 November 2025;
Terbit: 17 November 2025

efektif melindungi file MP3, meskipun performa dipengaruhi ukuran file dan panjang kunci (Diarse and Bendi 2016). Sementara itu, ElGamal memiliki tingkat keamanan tinggi, namun masih terdapat tantangan implementasi yang perlu diatasi (R.V.bolung, S.Moniharapon 2018).

Penelitian ini mengusulkan metode super enkripsi dengan menggabungkan RSA dan ElGamal secara berlapis untuk meningkatkan keamanan file MP3. Kombinasi ini diharapkan dapat mengatasi keterbatasan masing-masing algoritma, menghasilkan sistem yang aman tanpa mengorbankan efisiensi proses. Sistem akan diuji berdasarkan ukuran file dan tingkat keamanan yang dihasilkan, dengan harapan dapat menjadi solusi efektif perlindungan data audio di era digital.

2. LANDASAN TEORITIS

Kriptografi

Kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika untuk menjaga keamanan informasi, meliputi kerahasiaan, integritas data, dan otentikasi. Selain itu, kriptografi juga dapat dipandang sebagai seni dan teknik untuk menjaga keamanan pesan. Algoritma kriptografi adalah fungsi matematika yang digunakan dalam proses enkripsi dan dekripsi, yang terdiri dari dua fungsi saling terkait, yaitu satu untuk enkripsi dan satu lagi untuk dekripsi (Fauzi, Maulita, and Novriyenni 2017).

Proses kriptografi yang efektif memerlukan Komponen utama:

a. Plaintext: pesan asli yang disandikan.
b. Chipertexs: pesan yang telah dienkripsi dan tidak dapat dibaca tanpa dekripsi.
c. Kunci Kriptografi: nilai yang digunakan untuk enkripsi dan dekripsi, berperan mengontrol proses kriptografi.
d. Algoritma Enkripsi/Dekripsi: fungsi matematika yang mengubah plainteks menjadi chiperteks dan sebaliknya (H. Kridalaksana, Rangan, and Ansharie 2021).

Super Enkripsi

Super enkripsi merupakan penggabungan dua atau lebih algoritma kriptografi, seperti metode substitusi dan permutasi, untuk menghasilkan algoritma yang lebih sulit dipecahkan. Proses ini diawali dengan mengenkripsi pesan menggunakan teknik substitusi, kemudian dilanjutkan dengan teknik permutasi. Dekripsi dilakukan dengan urutan terbalik (Agustina, Sujarwo, and Khudzaifah 2023).

Algoritma RSA

Algoritma RSA (Rivest–Shamir–Adleman) pertama kali diperkenalkan pada tahun 1977 oleh Ron Rivest, Adi Shamir, dan Leonard Adleman. Nama RSA sendiri berasal dari

gabungan huruf awal nama ketiga penemunya. RSA termasuk dalam kriptografi kunci publik yang hingga kini masih banyak digunakan, karena memiliki tingkat keamanan yang tinggi berkat penggunaan kunci dengan panjang variatif serta penerapannya yang semakin matang.

Dalam RSA terdapat dua jenis kunci, yaitu kunci publik dan kunci privat. Kunci publik dapat diketahui oleh siapa saja dan berfungsi dalam proses enkripsi, sedangkan kunci privat hanya diketahui oleh pihak tertentu dan digunakan dalam proses dekripsi. Proses pembangkitan pasangan kunci RSA dilakukan melalui serangkaian algoritma khusus (Hakim et al. 2025).

Pembangkit kunci

Pilih bilangan prima besar: p dan q

Menghitung nilai: n = p x q.

Hitung fungsi Euler (φ): φ(n) = (p-1).(q-1).

Pilih bilangan buat e yang relatif prima terhadap φ(n), Sehingga gcd (e, φ(n)) = 1 e adalah kunci Publik.

Hitung d sengai invers modulo dari e terhadap φ(n), yaitu d x e ≡ 1 (mod φ(n)). d adalah kunci Privat.

Kunci publik: (e, n) dan Kunci privat (d, n).

Enkripsi

Proses enkripsi menggunakan e, dimana e adalah kunci Publik.

$$\mathbf{C = m^e \bmod n}$$

Dekripsi

Proses dekripsi menggunakan d sebagai kunci privat.

$$\mathbf{M = c^d \bmod n}$$

Dengan: m adalah plainteks dan c adalah chiperfile (Prastya, Pardede, and Fauzi 2022).

Algoritma Elgamal

Algoritma ElGamal diperkenalkan pada tahun 1985 oleh seorang ilmuwan asal Mesir bernama Taher ElGamal. Algoritma ini berbasis pada konsep kriptografi kunci publik. Meskipun awalnya dirancang untuk keperluan tanda tangan digital, dalam perkembangannya ElGamal juga dapat diterapkan dalam proses enkripsi dan dekripsi (Rio Andika et al. 2025). Tahapan penyelesaian metode kriptografi ElGamal dijelaskan sebagai berikut:

Pembangkit kunci

Pilih bilangan Prima besar p.

Plih bilangan aca g < p.

Pilih bilangan acak x dengan $1 \leq x \leq p - 2$ (Kunci Privat).

Hitung y dengan rumus: $y = g^x \bmod p$ (Kunci Publik).

Kunci publik: (y, g, p).

Kunci privat: (x, p).

Enkripsi

Pilh bilangan acak k dengan $1 \leq k \leq p - 2$.

Hitung :

$a = g^x \bmod p$

$b = y^k.Mi \bmod p$

Dekripsi

Hitung s: $s = a^x \bmod p$.

Cari invers modulo: $s^{-1} \bmod p$.

Dapatkan plainteks:

$M1 = (b \times s^{-1}) \bmod p$

Setelah M1 diperoleh, pesan dapat dikembalikan ke bentuk awal (Nugraha 2024).

3. ANALISIS DAN DESAIN

Metode Penelitian

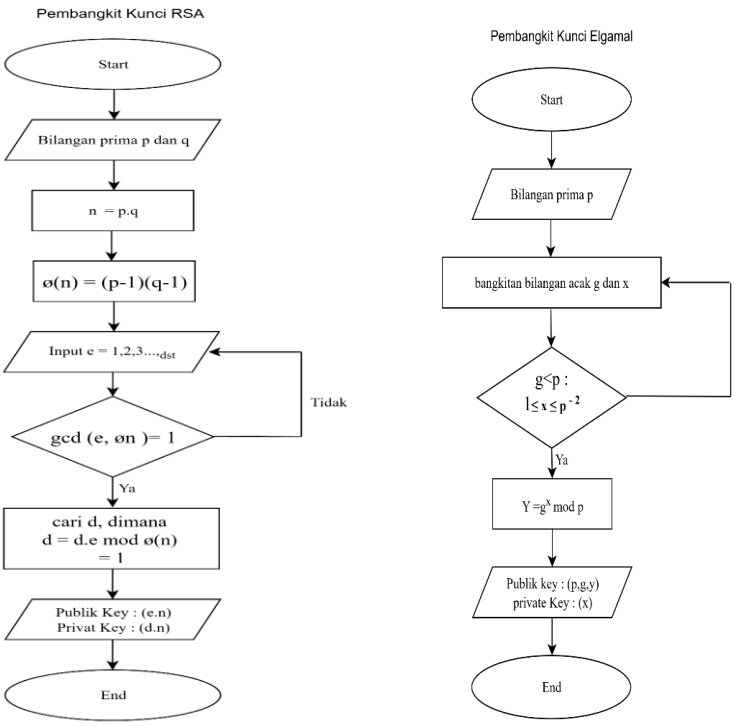
Penelitian ini dilakukan secara bertahap untuk memastikan pengembangan, penerapan, dan evaluasi sistem super enkripsi pada file audio MP3 berjalan sistematis:

a. Studi Literatur – Meninjau referensi jurnal, penelitian terdahulu, dan teori terkait kriptografi, algoritma RSA, ElGamal, serta metode pengamanan file audio MP3.
b. Perancangan Program – Membuat rancangan sistem super enkripsi berlapis menggunakan RSA dan ElGamal, dilengkapi bagan alur kerja untuk proses enkripsi dan dekripsi.
c. Implementasi Program – Mengembangkan sistem menggunakan bahasa Python pada Visual Studio Code, dipilih karena populer dan sesuai dengan kebutuhan penelitian.

Dengan langkah-langkah ini, pengembangan sistem dilakukan secara terstruktur untuk menghasilkan metode perlindungan data audio digital yang optimal.

Key generator

Alur proses pembangkitan kunci dan proses super enkripsi file MP3 menggunakan algoritma RSA dan ElGamal. Diagram ini berfungsi sebagai panduan yang mempermudah pemahaman, analisis, serta implementasi sistem secara bertahap dan terstruktur. Dengan adanya flowchart, setiap tahapan mulai dari pembangkitan kunci, enkripsi, hingga dekripsi, dapat terlihat jelas sehingga meminimalkan kesalahan dan memastikan proses berjalan sesuai rancangan.



Gambar 1. diagram alur generator kunci RSA dan Elgamal.

Gambar 1 menjelaskan diagram alur proses pembangkitan kunci RSA dan Elgamal digunakan untuk kunci saat proses enkripsi dan dekripsi.

RSA key generation process

Sebelum proses enkripsi dan dekripsi dilakukan, terlebih dahulu dibangkitkan kunci RSA melalui beberapa tahapan sebagai berikut:

a. Pilih dua bilangan prima p dan q. (nilai p dan q bersifat rahasia).

   p = 79

   q = 71

b. Menghitung nilai n = p x q.

   n = 79 x 71 = 5609

c. Menghitung φ(n) untuk pembentukan kunci privat: φ(n) = (p-1).(q-1).

   φ(n) = 78 x 70 = 5460

d. Memilih bilangan bulat sebagai kunci publik, yang relatif prima terhadap φ(n) artinya faktor pembagian terbesar kedua adalah 1, secara matematis disebut GCD(e, φ(n))= 1.

   e = 97

e. Menenutkan kunci privat d, dengan menggunakan persamaan.

   d = d.e mod φ(n) = 1

   d adalah bilangan yang jika dikalikan dengan e dan kemudian dibagikan φ(n), sisanya adalah 1.

d = d.97 mod 5460 = 1

d = 2533.97 mod 5460 = 1

d= 245701 mod 5460 = 1

sehingga diperoleh nilai d = 2533

f. Pasangan kunci publik dan privat, dengan nilai nilai tersebut. Kunci adalah:

Kunci publik: (e, n) = (97, 5609).

Kunci Privat: (d, n) = (2533, 5609).

ElGamal key generation process

Sebelum melakukan proses enkripsi dan dekripsi dilakukan terlebih dahulu dibangkitkan kunci Elgamal melalui beberapa tahapan sebagai berikut:

a. Pilih bilangan prima p, bilangan prima pada Elgamal harus lebih besar dari nilai n RSA.

p = 5623

b. Elemen primitf g, bilangan acak yang lebih kecil dari p sebagai elemen primitf.

g = 257

c. Kunci privat x, bilangan acak bersifat rahasia.

x = 71

d. Kunci publik y, dihitung dengan persamaan $y = g^x \bmod p$. Digunakan pada proses enkripsi.

$257^{71} \bmod 5623$

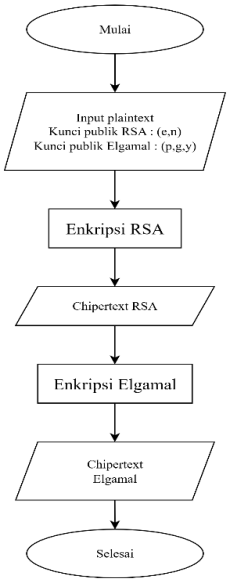
e. Pasangan kunci publik dan privat Elgamal, dengan nilai nilai tersebut. Kunci adalah:

Kunci publik: (p, g, y).

Kunci privat: (x).

Enkripsi RSA dan Elgamal

Super enrkipsi merupakan metode yang mengombinasikan dua algoritma kriptografi untuk berkerja secara berlapis dalam satu sistem, sehingga meningkatkan tingkat keamanan data, pada penelitian ini, algoritma yang digunakan adalah RSA dan Elgamal. Adapun tahapan yang dilakukan dalam proses enkripsi RSA dan elgamal sebagai berikut:



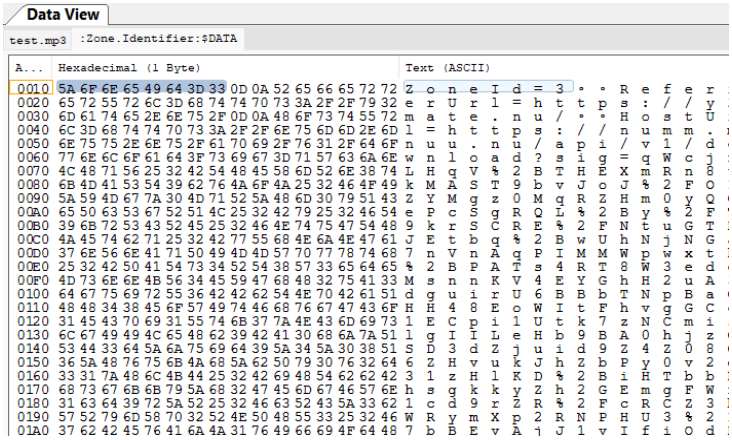
Gambar 2. Enkripsi RSA dan Elgamal.

Proses Enkripsi RSA Dan Elgamal

Analisis terhadap proses enkripsi superenkripsi adalah sebagai berikut:

Gambar 3. File To Be Secured.

Sebelum dilakukan proses enkripsi dan dekripsi, file terlebih dahulu diekstraksi untuk memperoleh nilai heksadesimal. Sebanyak 8 byte diambil untuk sampel dengan menggunakan software Binarry viewer., seperti ditunjuk pada gambar berikut:



Gambar 4. Hexadecimal From File.

Dari gambar tersebut diambil sempel berupa nilai heksadesimal: 5A, 6F, 6E 65, 49, 64, 3D, 33. Nilai-nilai heksadesimal ini digunakan sebagai plainfile dalam proses super enkripsi menggunakan algoritma RSA dan Elgamal, kemudian di konversi menjadi bentuk desimal: 90, 111, 110, 101, 73,100, 61, 51. Setelah di konversi dalam bilangan desimal maka akan di enkripsi menggunakan algoritma RSA dengan kunci Publik (e, n) = 97, 5609

Adapun proses perhitungan enkripsi RSA dan elgamal sebagai berikut:

Enkripsi RSA

Dengan rumus RSA: $\mathbf{M^e \bmod n}$

C1 = 90^{97} mod 5609 = 1495

C2 = 111^{97} mod 5609 = 4198

C3 = 110^{97} mod 5609 = 761

C4 = 101^{97} mod 5609 = 684

C5 = 73^{97} mod 5609 = 5008

C6 = 100^{97} mod 5609 = 2220

C7 = 61^{97} mod 5609= 2174

C8 = 51^{97} mod 5609= 4157

Maka dari perhitungan dari atas didapatkan chiperfile sebagai berikut: 1495, 4189, 3557, 684, 5008, 2220, 2174, 4157

Enkripsi elgamal

Lalu di proses dengan elgamal dengan angka desimal: 1495, 4189, 3557, 684, 5008, 2220, 2174, 4157. Angka-angka desimal ini akan dienkripsi dengan elgamal untuk menjadi superchiperfile.

Untuk enkripsi dilakukan secara manual menggunakan rumus Elgamal dengan rumus: $\mathbf{A = g^k \bmod p}$ **dan** $\mathbf{B = y^k.m \bmod p.}$

A1 = 257^{31} mod 5623 = 4349

A2 = 257^{31} mod 5623 = 4349

A3 = 257^{31} mod 5623 = 4349

A4 = 257^{31} mod 5623 = 4349

A5 = 257^{31} mod 5623 = 4349

A6 = 257^{31} mod 5623 = 4349

A7 = 257^{31} mod 5623 = 4349

A8 = 257^{31} mod 5623 = 4349

Lanjut dengan enkripsi yang ke dua dengan rumus: $\mathbf{y^k.m \bmod p}$

B1 = 4207^{31}. 1495 mod 5623 = 5315

B2 = 4207^{31}. 4198 mod 5623 = 1610

B3 = 4207^{31}. 761 mod 5623 = 1784

B4 = 4207^{31}. 684 mod 5623 = 2601

B5 = 4207^{31}. 5008 mod 5623 = 5430

B6 = 4207^{31}. 2220mod 5623 = 1931

B7 = 4207^{31}. 2174 mod 5623 = 2200

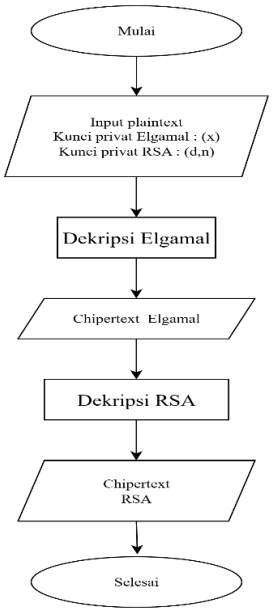
Setelah mendapatkan nilai enkripsi A dan B, hasil perhitungan tersebut disusun dengan pola selang seling:

A1 B1, A2 B2, A3 B3, A4 B4, A5 B5, A6 B6, A7 B7, A8 B8.

(4349,5315), (4349,1610), (4349,1784), (4349,2601), (4349,5430), (4349,1931), (4349,2200), (4349,1972).

Dekripsi Elgamal Dan RSA

Langkah-langkah yang dilakukan dalam proses dekripsi pada metode *super enkripsi* menggunakan algoritma RSA dan ElGamal dapat dilihat pada gambar 5:



Gambar 5. Dekripsi Elgamal dan RSA.

Proses Dekripsi Elgamal Dan RSA

Setelah diperoleh cipherfile hasil proses enkripsi RSA dan ElGamal dengan metode super enkripsi, yaitu: (4349,5315), (4349,1610), (4349,1784), (4349,2601), (4349,5430), (4349,1931), (4349,2200), (4349,1972), tahap berikutnya adalah mengembalikan cipherfile

tersebut ke bentuk aslinya melalui proses dekripsi, yang diawali dengan dekripsi menggunakan algoritma ElGamal, kemudian dilanjutkan dengan dekripsi RSA.

Dekripsi elgamal

Proses dekripsi elgamal ini dilakukan dengan rumus invers modular digunakan dalam proses dekripsi karena pembagian tidak bisa dilakukan secara langsung pada bilangan biasa. Maka sebagai gantinya digunakan perkalian dengan invers modular.

Dengan rumus :

Hitung $s = a^x \bmod p$

Hitung invers $s_{inv} = s^{-1} \bmod p$

$s = a^x \bmod p = 4349^{71} \bmod 5623 = 4517$

$s_{inv} = s^{-1} \bmod p = 4517 * 1693 \bmod 5623 = 1$

Lalu dekripsi bagian b setelah mendapatkan s_{inv} dengan hasil: 1693

dengan menggunakan rumus: **$m = (b.s_{inv}) \bmod p$**

$m1 = (b.s_{inv}) \bmod p = 5315 * 1693 \bmod 5623 = 1495$

$m1 = (b.s_{inv}) \bmod p = 1610 * 1693 \bmod 5623 = 4198$

$m1 = (b.s_{inv}) \bmod p = 1784 * 1693 \bmod 5623 = 761$

$m1 = (b.s_{inv}) \bmod p = 2601 * 1693 \bmod 5623 = 684$

$m1 = (b.s_{inv}) \bmod p = 5430 * 1693 \bmod 5623 = 5008$

$m1 = (b.s_{inv}) \bmod p = 1931 * 1693 \bmod 5623 = 2220$

$m1 = (b.s_{inv}) \bmod p = 2200 * 1693 \bmod 5623 = 2174$

$m1 = (b.s_{inv}) \bmod p = 1972 * 1693 \bmod 5623 = 4157$

Maka didapatkan hasil dari plainfile dekripsi Elgamal : 1495, 4198, 761, 684, 5008, 2220, 2174, 4157.

Dekripsi RSA

Pada tahap ini, plainfile hasil dekripsi ElGamal dikonversi menjadi cipherfile untuk didekripsi menggunakan algoritma RSA dengan kunci privat (d, n) sesuai rumus berikut: **$m = c^d \bmod p$**

$m = c^d \bmod n = 1495^{2533} \bmod 5609 = 90$

$m = c^d \bmod n = 4198^{2533} \bmod 5609 = 111$

$m = c^d \bmod n = 761^{2533} \bmod 5609 = 110$

$m = c^d \bmod n = 684^{2533} \bmod 5609 = 101$

$m = c^d \bmod n = 5008^{2533} \bmod 5609 = 73$

$m = c^d \bmod n = 2220^{2533} \bmod 5609 = 100$

$m = c^d \bmod n = 2174^{2533} \bmod 5609 = 61$

$m = c^d \bmod n = 4157^{2533} \bmod 5609 = 51$

Setelah mendapatkan hasil decimal: 90, 111, 110, 101, 73, 100, 61, 51. Lalu di ubah menjadi bilangan hexadecimal, yang menghasikan nilai berikut: 5A, 6F, 6E 65, 49, 64, 3D, 33. Dengan adanya proses-proses diatas, maka pesan dapat dikembalikan ke pesan asli.

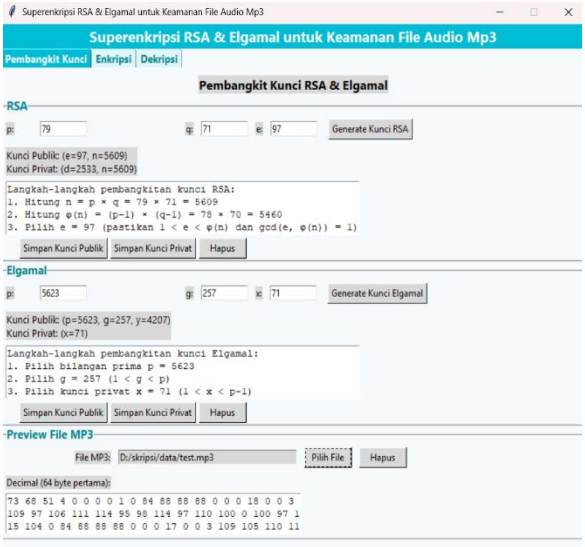
4. IMPLEMENTASI DAN DISKUSI

Implementasi

Sistem yang telah dianalisis dan dirancang selanjutnya diimplementasikan untuk membahas penerapan aplikasi kriptografi dengan metode super enkripsi, yaitu kombinasi algoritma RSA dan ElGamal. Program dikembangkan menggunakan Python di Visual Studio Code untuk memudahkan integrasi dan pengujian. Pengujian dilakukan guna memastikan sistem berjalan sesuai harapan, mampu mengenkripsi data dengan benar, serta menjaga kerahasiaan dan integritas file audio.

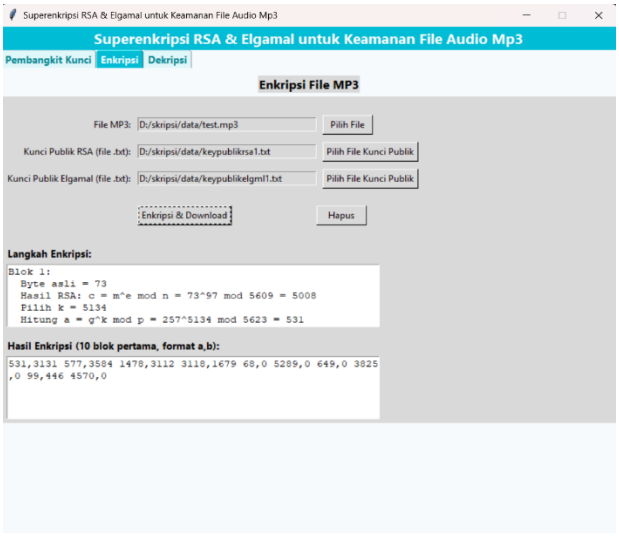
Pengujian

Uji coba ini menggunakan algoritma RSA dan ElGamal untuk meningkatkan keamanan file audio MP3. Kunci RSA dibangkitkan dengan nilai p, q, dan e, sedangkan kunci ElGamal dengan nilai p, g, dan x. Setelah tombol generate key ditekan, sistem otomatis menghitung dan menampilkan kunci yang dapat disimpan sebagai kunci publik atau privat untuk proses enkripsi dan dekripsi. Terakhir, fitur *preview* memungkinkan pengguna memilih file MP3, kemudian sistem menampilkan hasil konversi awal file ke bentuk desimal. Proses pembangkit kunci dapat dilihat pada gambar 6.



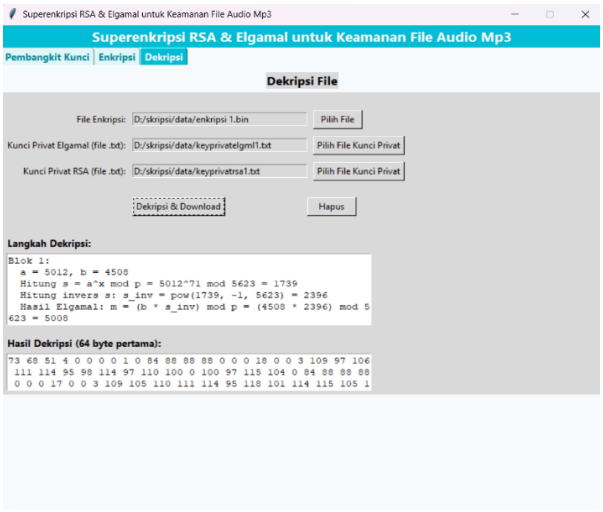
Gambar 6. Proses Pengujian Pembangkit Kunci RSA Dan Elgmal.

Uji coba enkripsi ini bertujuan memastikan kombinasi algoritma RSA dan ElGamal dapat digunakan secara efektif untuk mengenkripsi file audio MP3. Tanpa dekripsi yang tepat, file terenkripsi tidak dapat diakses. Form menyediakan tombol *Pilih File* untuk memilih MP3 serta kunci publik RSA dan ElGamal dalam format .txt. Setelah semua file dipilih, tombol *Enkripsi* ditekan untuk memulai proses, dimulai dari hasil enkripsi RSA hingga pembentukan pasangan kunci ElGamal. Hasil enkripsi sepuluh blok pertama ditampilkan sebagai output awal untuk memastikan keberhasilan proses. Dapat dilihat pada Gambar 6.



Gambar 7. Proses Pengujian Enkripsi.

Uji coba ini bertujuan memastikan dekripsi dengan kombinasi algoritma ElGamal dan RSA dapat digunakan secara efektif untuk memulihkan file audio MP3 terenkripsi. Proses dilakukan dengan menginput file MP3 terenkripsi serta pasangan kunci privat ElGamal dan RSA dalam format .txt. Setelah semua file dipilih, tombol *Dekripsi* ditekan untuk memulai proses, dimulai dari dekripsi ElGamal hingga RSA. Hasil dekripsi 64 byte pertama ditampilkan sebagai output awal untuk memastikan keberhasilan proses, seperti terlihat pada Gambar 8.

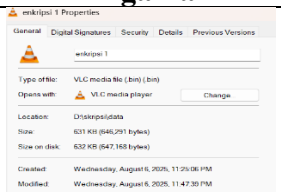
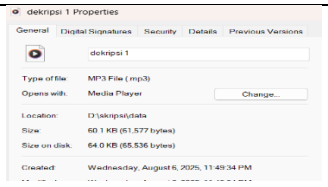
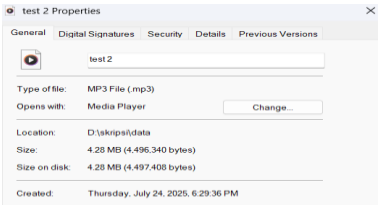
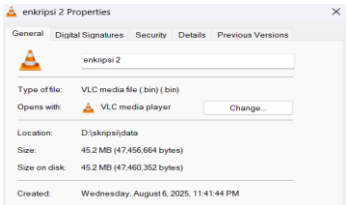
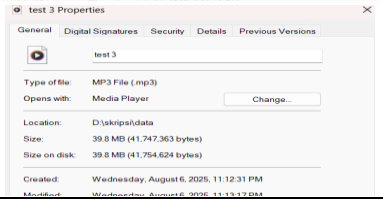
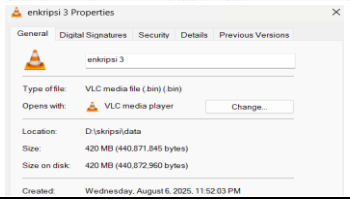
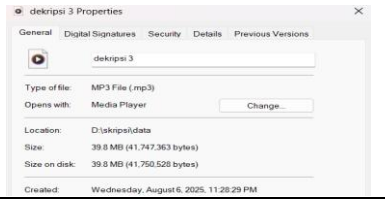


Gambar 8. Proses Pengujian Dekripsi.

Hasil tes

Berikut Adalah hasil uji coba program Teknik super enkripsi algoritma RSA dan Elgamal dengan file audio Mp3 yang dibangun untuk proses enkrips dan dekripsi sesuai dengan rancangan file. File di uji dengan beberapa ukuran file audio Mp3 berhasil dienkripsi sehingga tidak dapat dibuka dengan aplikasi normal, dan setelah dilakukan proses dekripsi file dapat kembali ke bentuk semula tanpa perubahan isi file dan suara. Hasil pengujian mencata ukuran file sebelum dienkripsi dan sesudah dienkripsi. Hasil uji coba dapat dilihat pada tabel dibawah ini:

Tabel 1. Hasil Tes.

No	File Asli	File Enkripsi RSA Dan Elgamal	File Dekripsi Elgamal Dan RSA
1.			
2.			
3.			

5. KESIMPULAN

Berdasarkan hasil perancangan dan implementasi program *Super Enkripsi Kriptografi Pengamanan Pesan File Audio Record MP3* menggunakan algoritma RSA dan ElGamal, diperoleh kesimpulan bahwa penggabungan dua algoritma kriptografi yang memiliki tingkat keamanan tinggi, yaitu RSA dan ElGamal, secara berlapis mampu meningkatkan keamanan file audio MP3 secara signifikan. Penerapan teknik *super enkripsi*, berupa enkripsi ganda berturut-turut, menjadikan file audio sangat aman dan sulit untuk dipecahkan atau diakses tanpa otorisasi. Implementasi algoritma RSA dan ElGamal yang dikembangkan menggunakan bahasa pemrograman Python pada lingkungan pengembangan Visual Studio Code berjalan dengan baik, mencakup seluruh tahapan mulai dari pembangkitan kunci, proses enkripsi berlapis, hingga dekripsi bertahap sesuai urutan algoritma yang digunakan.

Meskipun penerapan metode pengamanan ganda ini mengakibatkan waktu pemrosesan enkripsi dan dekripsi menjadi relatif lebih lama, khususnya pada file audio berukuran besar, sistem tetap mampu beroperasi secara optimal. File audio MP3 yang telah melalui proses *super enkripsi* menggunakan algoritma RSA dan ElGamal tidak dapat dibuka atau diputar tanpa akses terhadap kunci privat dari kedua algoritma tersebut. Kondisi ini memastikan bahwa hanya pihak yang memiliki otorisasi yang dapat mengakses dan memanfaatkan file tersebut, sehingga keamanan, kerahasiaan, dan integritas data tetap terjamin. Hasil akhir dari pengujian menunjukkan peningkatan signifikan pada tingkat keamanan data tanpa mengorbankan kestabilan serta konsistensi performa sistem.

DAFTAR PUSTAKA

Agustina, L., Sujarwo, I., & Khudzaifah, M. (2023). Membangun super enkripsi untuk mengamankan pesan. *Jurnal Riset Mahasiswa Matematika*, 2(3), 84–89. https://doi.org/10.18860/jrmm.v2i3.16335

Alani, M. M. (2016). Guide to elliptic curve cryptography. Springer.

Alsmadi, I., Xu, D., & Nyeem, H. (2020). A survey on multimedia encryption: Current trends, challenges, and opportunities. *IEEE Access*, 8, 124–140. https://doi.org/10.1109/ACCESS.2019.2963725

Bolung, R. V., Moniharapon, S., & Lumintang, G. G. (2018). Implementasi kriptografi hibrid dengan algoritma ElGamal dan algoritma one time pad (OTP) dalam pengamanan file audio berbasis desktop. *Jurnal EMBA: Jurnal Riset Ekonomi, Manajemen, Bisnis dan Akuntansi*, 6(3), 1838–1847.

Diarse, N. N., & Bendi, J. K. (2016). Penerapan algoritma RSA pada sistem kriptografi file audio MP3.

El-Said, W., & Wahba, K. (2018). Secure audio encryption technique using chaotic maps and advanced cryptographic algorithms. *International Journal of Network Security*, 20(5), 881–890.

Fauzi, A., Maulita, Y., & Novriyenni, N. (2017). Perancangan aplikasi keamanan pesan menggunakan algoritma ElGamal dengan memanfaatkan algoritma one time pad sebagai pembangkit kunci. *JTIK (Jurnal Teknik Informatika Kaputama)*, 1(1), 1–9. https://doi.org/10.59697/jtik.v1i1.680

Hakim, A., Anggraini, Z., Sillfani, D., Ayuni, R., & Fauzi, A. (2025). Penerapan super enkripsi Hill Cipher dan RSA untuk pengamanan data file audio MP3. *Jurnal Sistem Informasi Kaputama (JSIK)*, 9(1), 55–64. https://doi.org/10.59697/jsik.v9i1.959

Kridalaksana, A., Rangan, A. Y., & Ansharie, A. (2021). Enkripsi data audio menggunakan metode kriptografi RSA. *Sebatik*, 17(1), 6–10. https://doi.org/10.46984/sebatik.v17i1.79

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (2018). Handbook of applied cryptography**.** CRC Press.

Nugraha, S. N. (2024). Penerapan algoritma kriptografi ElGamal pada aplikasi pengamanan pesan berbasis website.

Prastya, R., Pardede, A. M. H., & Fauzi, A. (2022). Teknik pembangkit kunci algoritma RSA menggunakan algoritma Diffie Hellman pada keamanan citra. *KAKIFIKOM (Kumpulan Artikel Karya Ilmiah Fakultas Ilmu Komputer)*, 4(1), 16–22. https://doi.org/10.54367/kakifikom.v4i1.1872

Rio Andika, Sitepu, R. F., Ramadhani, P., Fitria, R. N., & Fauzi, A. (2025). Penerapan super enkripsi algoritma Autokey Cipher dan El-Gamal file gambar. *Jurnal Sistem Informasi Kaputama (JSIK)*, 9(1), 45–54. https://doi.org/10.59697/jsik.v9i1.957

Singh, G., & Supriya, M. (2013). A study of encryption algorithms for audio data security. *International Journal of Computer Applications*, 74(6), 1–6. https://doi.org/10.5120/12931-9723

Zhang, L., & Xiao, D. (2021). A hybrid audio encryption scheme based on RSA and chaotic systems. *Journal of Information Security and Applications*, 58, 102–110. https://doi.org/10.1016/j.jisa.2020.102610