Jurnal Riset Multidisiplin Edukasi
https://journal.hasbaedukasi.co.id/index.php/jurmie
Halaman : 343 - 360

IMPLEMENTASI ALGORITMA HOMOMORPHIC ENCRYPTION UNTUK PENGAMANAN DATA FILE TEKS

Jihan Mahira Irza[1], Khairuddin Nasution[2], Satria Yudha Prayogi[3]
Universitas Islam Sumatera Utara, Medan, Indonesia [1,2,3]
Email: jihanmahirairza@gmail.com

Informasi

Volume : 3
Nomor : 11
Bulan : November
Tahun : 2026
E-ISSN : 3062-9624

Abstract

The development of information technology has led to an increasing use of digital documents, particularly in the storage and exchange of information. Digital documents stored in information systems are vulnerable to unauthorized access; therefore, security mechanisms are required to maintain the confidentiality of the information they contain. This study aims to implement the Paillier Partially Homomorphic Encryption (PHE) algorithm to secure document files in Microsoft Word (.docx) and Portable Document Format (.pdf) formats. The data collection methods used in this study include literature review and observation. The literature review was conducted by examining theories and previous studies related to cryptography and the Paillier algorithm, while observation was carried out to identify the characteristics of document files and the requirements for the security process. The security process involves generating a public key and a private key, followed by representing the contents of the files as numerical blocks so that they can be processed using the Paillier PHE algorithm. The encryption process uses the public key, while the decryption process uses the private key to restore the data to its original form. The encrypted results are stored in the system without modifying the original input files. The developed system is expected to help secure digital documents and enable files to be restored to their original formats through the decryption process. By implementing the Paillier PHE algorithm, this study is expected to provide an alternative cryptographic technique for maintaining the confidentiality of digital document files.

Keyword: *Homomorphic Encryption, Paillier, Encryption, Decryption, File Security, DOCX, PDF.*

Abstrak

Perkembangan teknologi informasi menyebabkan penggunaan dokumen digital semakin meningkat, terutama dalam penyimpanan dan pertukaran informasi. Dokumen digital yang disimpan dalam sistem memiliki risiko terhadap akses oleh pihak yang tidak berwenang, sehingga diperlukan mekanisme pengamanan untuk menjaga kerahasiaan informasi di dalamnya. Penelitian ini bertujuan untuk mengimplementasikan algoritma Homomorphic Encryption (PHE) Paillier dalam mengamankan File dokumen berformat Microsoft Word (.docx) dan Portable Document Format (.pdf). Metode pengumpulan data yang digunakan meliputi studi literatur dan observasi. Studi literatur dilakukan dengan mempelajari teori serta penelitian terdahulu yang berkaitan dengan kriptografi dan algoritma Paillier, sedangkan observasi dilakukan untuk mengetahui karakteristik File dokumen serta kebutuhan proses pengamanan. Proses pengamanan dilakukan melalui pembangkitan kunci publik dan kunci privat, kemudian isi File direpresentasikan ke dalam blok bilangan agar dapat diproses menggunakan algoritma PHE Paillier. Proses enkripsi menggunakan kunci publik, sedangkan proses dekripsi menggunakan kunci privat untuk mengembalikan data ke bentuk aslinya. Hasil enkripsi disimpan di dalam sistem tanpa mengubah File asli yang digunakan sebagai masukan. Sistem yang dibangun

diharapkan dapat membantu mengamankan dokumen digital serta memungkinkan proses pengembalian File ke format semula melalui proses dekripsi. Dengan penerapan algoritma PHE Paillier, penelitian ini diharapkan dapat menjadi salah satu alternatif dalam penerapan teknik kriptografi untuk menjaga kerahasiaan File dokumen digital.

Kata Kunci : *Homomorphic Encryption, Paillier, Enkripsi, Dekripsi, Keamanan File, DOCX, PDF.*

A. PENDAHULUAN

Perkembangan teknologi informasi menyebabkan pertukaran dan penggunaan dokumen digital semakin meningkat. File teks sering digunakan untuk menyimpan berbagai informasi, mulai dari catatan pribadi, dokumen akademik, hingga data administrasi. Kemudahan dalam membuat, mengirim, dan menyimpan file teks juga menimbulkan kebutuhan untuk menjaga kerahasiaan informasi, terutama apabila file memuat data yang tidak boleh diketahui oleh pihak lain. File yang disimpan tanpa perlindungan kriptografi dapat dibaca oleh siapa pun yang berhasil memperoleh akses terhadap file tersebut. Oleh karena itu, diperlukan mekanisme pengamanan yang dapat mengubah isi file menjadi bentuk yang tidak dapat dipahami tanpa kunci yang sesuai. (Aljohani & Ahmad, 2023).

Salah satu pendekatan untuk melindungi informasi digital adalah kriptografi. Kriptografi mengubah pesan asli (plaintext) menjadi bentuk tersandi (ciphertext) melalui proses enkripsi dan mengembalikannya melalui proses dekripsi. Salah satu pengembangan kriptografi adalah Homomorphic Encryption (HE), yaitu teknik yang memungkinkan operasi tertentu dilakukan terhadap data terenkripsi tanpa terlebih dahulu membuka isi data aslinya. Konsep ini telah diterapkan dalam penelitian sistem e-voting dan pengamanan data finansial menggunakan skema homomorfik (Soleh et al., 2024; Sukmana & Muliantara, 2025).

Homomorphic Encryption memiliki beberapa skema, salah satunya Partially Homomorphic Encryption (PHE). PHE mendukung operasi homomorfik tertentu, sehingga sesuai untuk kebutuhan komputasi terbatas pada data terenkripsi.

Salah satu algoritma PHE adalah Paillier Cryptosystem yang memiliki sifat homomorfik aditif. Sifat tersebut memungkinkan ciphertext dikombinasikan sehingga hasil dekripsinya ekuivalen dengan penjumlahan plaintext yang bersesuaian. Penerapan Paillier pada pengolahan data terenkripsi telah dibahas dalam penelitian e-voting dan pengamanan data finansial (Soleh et al., 2024; Sukmana & Muliantara, 2025).

Algoritma Paillier menggunakan pasangan kunci publik dan kunci privat. Kunci publik digunakan dalam proses enkripsi, sedangkan kunci privat digunakan untuk dekripsi. Pesan yang akan dienkripsi direpresentasikan sebagai bilangan bulat dalam ruang pesan modulo n.

Oleh karena itu, file teks perlu melalui tahap pengkodean menjadi byte dan pembagian menjadi blok-blok bilangan yang nilainya berada dalam rentang yang didukung algoritma. Pembagian blok tersebut merupakan penyesuaian teknis sistem agar data file dapat diproses oleh skema Paillier (Soleh et al., 2024; Sukmana & Muliantara, 2025).

Dalam penelitian ini, algoritma Paillier diterapkan untuk mengamankan file teks berformat .txt. File teks dipilih karena berisi karakter yang dapat direpresentasikan dalam bentuk byte sehingga dapat diproses melalui tahapan pengkodean sebelum dienkripsi. Sistem berbasis web dirancang agar pengguna dapat memilih file TXT, menjalankan proses enkripsi, menyimpan hasil ciphertext, serta melakukan dekripsi untuk memperoleh kembali file teks semula. Fokus penelitian adalah menguji keberhasilan pemulihan isi file dan mengukur waktu proses enkripsi serta dekripsi.

Meskipun Paillier mempunyai sifat homomorfik aditif, sifat tersebut tidak berarti algoritma dapat langsung melakukan seluruh operasi pengolahan teks seperti menggabungkan kalimat atau mengedit karakter pada ciphertext. Operasi homomorfik Paillier berlaku pada representasi bilangan yang dienkripsi. Dengan demikian, penelitian ini membatasi pembahasan komputasi homomorfik pada operasi penjumlahan bilangan terenkripsi, sedangkan tujuan utama aplikasi adalah pengamanan dan pemulihan file teks (Soleh et al., 2024; Sukmana & Muliantara, 2025).

Berdasarkan latar belakang yang telah diuraikan, rumusan masalah dalam penelitian ini adalah bagaimana mengimplementasikan algoritma Homomorphic Encryption Paillier untuk mengenkripsi dan mendekripsi file teks berformat TXT, serta bagaimana hasil pengujian keberhasilan pemulihan isi file dan kinerja proses enkripsi dan dekripsi file teks menggunakan algoritma Paillier.

Agar penelitian lebih terarah dan tidak menyimpang dari tujuan yang telah ditetapkan, penelitian ini dibatasi pada penggunaan jenis Partially Homomorphic Encryption (PHE) dengan algoritma Paillier. Sistem yang dikembangkan berupa aplikasi pengamanan file teks berbasis web dan bukan merupakan layanan penyimpanan awan. Objek file yang diproses dibatasi pada file teks berformat .txt dengan karakter yang dapat direpresentasikan menggunakan UTF-8. Ukuran file yang diuji dibatasi maksimal 100 KB pada tahap pengujian awal atau disesuaikan dengan kapasitas implementasi dan parameter kunci Paillier yang digunakan, dengan batas akhir ditetapkan berdasarkan hasil pengujian. Pengujian penelitian difokuskan pada keberhasilan proses enkripsi dan dekripsi, kesesuaian isi file sebelum dan sesudah dekripsi, ukuran ciphertext, serta waktu yang dibutuhkan dalam proses enkripsi dan dekripsi. Selain itu,

pengujian operasi homomorfik dilakukan terhadap nilai numerik dan tidak mencakup operasi penyuntingan teks.

Adapun tujuan dari penelitian ini adalah untuk mengimplementasikan algoritma Homomorphic Encryption Paillier pada aplikasi berbasis web sebagai metode pengamanan file teks berformat TXT serta menguji keberhasilan proses dekripsi dalam mengembalikan isi file teks ke bentuk semula dan mengukur kinerja sistem berdasarkan waktu yang dibutuhkan dalam proses enkripsi dan dekripsi.

B. METODE PENELITIAN

Penelitian ini dilaksanakan di Laboratorium Komputer Universitas Islam Sumatera Utara, Medan, pada tanggal 9 Juni hingga 9 Agustus 2026. Perangkat yang digunakan meliputi laptop dengan prosesor Intel Core i5, RAM 8 GB, dan SSD 512 GB, serta perangkat lunak Windows 10, Visual Studio Code, XAMPP, PHP, JavaScript, dan MySQL. Teknik pengumpulan data dilakukan melalui studi literatur dan observasi. Studi literatur dilakukan dengan mengkaji buku, jurnal ilmiah, artikel, serta penelitian terdahulu yang berkaitan dengan Homomorphic Encryption Paillier. Sementara itu, observasi dilakukan untuk mengamati karakteristik, pengelolaan, penyimpanan, pengaksesan, serta kebutuhan pengamanan file dokumen melalui proses enkripsi dan dekripsi. Implementasi algoritma Paillier diawali dengan inisialisasi sistem dan pembangkitan pasangan kunci publik (public key) serta kunci privat (private key). Selanjutnya, file diunggah, dibaca dalam bentuk byte, dibagi menjadi blok numerik, kemudian dienkripsi menggunakan kunci publik dan disimpan dalam bentuk ciphertext.

Proses dekripsi dilakukan menggunakan kunci privat untuk mengembalikan ciphertext menjadi plaintext sehingga file dapat diakses kembali dalam bentuk aslinya. Implementasi algoritma Paillier meliputi tahapan pembentukan kunci, enkripsi, dan dekripsi dengan menggunakan parameter matematis berupa bilangan prima p dan q, modulus n, nilai λ, generator g, serta μ. Perancangan sistem dilakukan menggunakan Use Case Diagram, Sequence Diagram, Activity Diagram, dan Class Diagram untuk menggambarkan alur kerja, interaksi pengguna, serta struktur sistem. Sistem memiliki dua kelas utama, yaitu Pengguna dan File, yang berfungsi mengelola autentikasi akun dan penyimpanan file. Selain itu, dirancang tabel database Pengguna dan File untuk menyimpan informasi akun, identitas file, lokasi penyimpanan, ukuran hasil enkripsi, serta waktu pemrosesan. Perancangan antarmuka meliputi halaman login, pendaftaran, beranda, informasi sistem, unggah file, enkripsi, dan dekripsi. Seluruh tahapan tersebut menjadi dasar pembangunan aplikasi pengamanan file

berbasis web menggunakan algoritma Paillier Homomorphic Encryption.

C. HASIL DAN PEMBAHASAN

Hasil Pengujian Sistem

Pengujian dilakukan dengan beberapa skenario:

Tabel 1 Tabel Hasil Pengujian Sistem

No	Proses	Hasil
1	Upload *File*	Berhasil
2	Enkripsi	Berhasil
3	Simpan ke sistem	Berhasil
4	Unduh *File*	Berhasil
5	Dekripsi	Berhasil

Dari hasil tersebut, semua fungsi sistem berjalan dengan baik.

Pengujian Keamanan Data Sebelum dan Sesudah Enkripsi

Jika *file* PDF dan word disimpan ke dalam *database* tanpa melalui proses enkripsi. Hasil pengujian menunjukkan bahwa *file* tetap tersimpan dalam format PDF atau word sehingga dapat langsung dibuka menggunakan aplikasi pembaca PDF atau word. Dengan kondisi tersebut, apabila pihak yang tidak berwenang memperoleh akses terhadap media penyimpanan server, maka isi dokumen dapat langsung dibaca tanpa memerlukan proses autentikasi maupun dekripsi. Hal ini menunjukkan bahwa penyimpanan *file* tanpa enkripsi memiliki risiko kebocoran data yang tinggi.

Pada skenario kedua, *file* PDF atau word terlebih dahulu dienkripsi menggunakan algoritma *Paillier* sebelum disimpan pada sistem. Setelah proses enkripsi selesai, *file* berubah menjadi *ciphertext* sehingga tidak lagi dapat dikenali oleh sistem. Ketika *file* hasil enkripsi diakses secara langsung dari media penyimpanan server, *file* tersebut tidak dapat dibuka karena seluruh isi data telah berubah menjadi bentuk terenkripsi. *File* hanya dapat dikembalikan ke bentuk semula melalui proses dekripsi menggunakan private key yang dimiliki sistem.

Dengan demikian, meskipun terjadi akses langsung terhadap *file* yang tersimpan pada server *database* informasi yang terdapat di dalam *file* tetap terlindungi karena isi *file* tidak dapat dibaca tanpa melalui proses dekripsi. Hal ini menunjukkan bahwa implementasi algoritma *Paillier* mampu meningkatkan keamanan penyimpanan data dibandingkan penyimpanan *file* tanpa enkripsi.

Tabel 2 Perbandingan Penyimpanan *File*

Aspek Pengujian	**Tanpa Enkripsi**	**Menggunakan *Paillier* HE**
Bentuk *file* pada server	*File* PDF atau Word asli	*File* terenkripsi (*ciphertext*)
File dapat dibuka langsung dari server	Ya	Tidak
Isi dokumen dapat langsung dibaca	Ya	Tidak
Memerlukan proses dekripsi	Tidak	Ya
Risiko kebocoran data	Tinggi	Rendah
Tingkat keamanan	Rendah	Tinggi

Pembahasan

Berdasarkan hasil pengujian pada Tabel 2 dapat diketahui bahwa terdapat perbedaan yang signifikan antara penyimpanan *file* tanpa enkripsi dan penyimpanan *file* menggunakan algoritma *Paillier*. Pada penyimpanan tanpa enkripsi, *file* yang berada di server masih berupa dokumen PDF asli sehingga dapat dibuka dan dibaca apabila *file* berhasil diakses oleh pihak yang tidak memiliki hak akses. Kondisi tersebut berpotensi menyebabkan kebocoran informasi penting yang tersimpan di dalam dokumen.

Sebaliknya, pada penyimpanan menggunakan algoritma *Paillier*, *file* yang tersimpan di server telah berubah menjadi *ciphertext* sehingga tidak dapat dibuka secara langsung menggunakan aplikasi pembaca PDF. *File* hanya dapat dikembalikan ke bentuk aslinya melalui proses dekripsi menggunakan private key pada sistem. Dengan mekanisme tersebut, data tetap terlindungi meskipun *file* berhasil diperoleh oleh pihak lain.

Hasil pengujian ini menunjukkan bahwa penerapan algoritma *Partially Homomorphic Encryption* (*Paillier*) memberikan peningkatan keamanan pada sistem. Walaupun proses enkripsi menambah waktu pemrosesan beberapa milidetik sebagaimana telah dijelaskan pada pengujian waktu enkripsi, tambahan waktu tersebut masih tergolong kecil dibandingkan dengan manfaat yang diperoleh berupa perlindungan terhadap kerahasiaan data. Oleh karena itu, algoritma *Paillier* layak digunakan sebagai mekanisme pengamanan *file* pada sistem yang dibangun dalam penelitian ini.

Waktu Enkripsi

Perhitungan waktu enkripsi dilakukan menggunakan persamaan berikut.

$T_e = T_{selesai} - T_{mulai}$

Keterangan:

T_e = waktu enkripsi (detik)

$T_{selesai}$ = waktu saat proses enkripsi dimulai

T_{mulai} = waktu setelah proses enkripsi selesai

Sebagai contoh, pada salah satu proses pengujian diperoleh waktu mulai enkripsi sebesar 1752041410,214563 detik dan waktu selesai sebesar 1752041410,236891 detik, sehingga waktu enkripsi dihitung sebagai berikut.

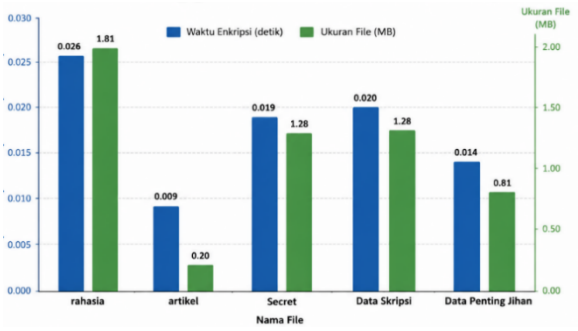
$T_e = 1752041410214563 - 1752041410262891 = 0026$ detik

Hasil tersebut menunjukkan bahwa sistem hanya memerlukan waktu sekitar 0,026 detik atau 26 milidetik untuk menyelesaikan proses enkripsi metadata *file* menggunakan algoritma *Paillier*. Waktu tersebut menunjukkan bahwa proses enkripsi dapat dilakukan dengan cepat sehingga tidak memberikan jeda yang signifikan terhadap aktivitas pengguna ketika melakukan unggah dokumen ke dalam sistem.

Secara umum, lamanya proses enkripsi dipengaruhi oleh beberapa faktor, seperti ukuran data yang diproses, spesifikasi perangkat keras yang digunakan, serta kompleksitas operasi matematika pada algoritma *Paillier*. Semakin besar data yang dienkripsi atau semakin besar parameter kunci yang digunakan, maka waktu komputasi yang dibutuhkan juga akan meningkat. Namun, pada penelitian ini data yang dienkripsi berupa metadata *file*, sehingga beban komputasi relatif kecil dan proses enkripsi dapat diselesaikan dalam waktu yang singkat.

Tabel 3 Tabel Waktu Enkripsi

No	**Nama *File***	**Ukuran *File* (KB)**	**Ukuran (MB)**	**Waktu Enkripsi (detik)**
1	rahasia	1.806 KB	1,81 MB	0,026
2	artikel	200 KB	0,20 MB	0,009
3	Secret	1.278 KB	1,28 MB	0,019
4	Data Skripsi	1.278 KB	1,28 MB	0,020
5	Data Penting Jihan	811 KB	0,81 MB	0,014



Gambar 1 Gambar Grafik Hasil Pengujian Waktu Enkripsi

Gambar 1 di atas merupakan grafik yang menggambarkan hasil pengujian waktu enkripsi *file* teks berformat dokomen dan PDF. Grafik digunakan untuk memperlihatkan perbandingan durasi yang dibutuhkan sistem ketika mengenkripsi *file* dengan ukuran yang berbeda. Sumbu horizontal menunjukkan ukuran *file* yang diuji, sedangkan sumbu vertikal menunjukkan waktu

enkripsi dalam satuan detik. Setiap titik atau batang pada grafik harus disesuaikan dengan data hasil pengujian aktual pada Tabel 4.3. Berdasarkan grafik tersebut, pembaca dapat mengamati perubahan waktu enkripsi seiring bertambahnya ukuran *file* dan jumlah blok data yang diproses oleh algoritma *Paillier*.

Implementasi Hasil

Halaman *Login* Pengguna



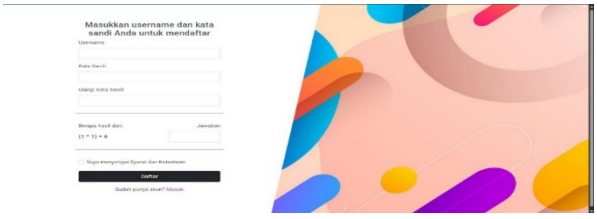
Gambar 2 Tampilan Halaman *Login* Pengguna

Gambar 2 merupakan halaman *login* (masuk) dari sistem aplikasi yang telah dibuat. Halaman ini digunakan oleh pengguna untuk masuk ke dalam sistem sebelum dapat mengakses fitur seperti *upload* dan *download file*.

Pada bagian kiri terdapat *form login* yang berisi beberapa *input*, yaitu: (1) *Username*, digunakan untuk memasukkan nama pengguna yang sudah terdaftar. (2) Kata Sandi (*Password*), digunakan untuk menjaga keamanan akun agar tidak bisa diakses sembarangan. (3) Pertanyaan sederhana (*captcha*) berupa operasi matematika, misalnya (9 + 4) + 9, yang harus dijawab oleh pengguna. Tujuannya adalah untuk memastikan bahwa yang *login* adalah manusia, bukan bot.

Di bawah *form* terdapat tombol "Masuk" yang digunakan untuk mengirim data *login* ke sistem. Jika data yang dimasukkan benar, maka pengguna akan berhasil masuk ke halaman utama sistem. Selain itu, terdapat juga tulisan "Belum punya akun? Daftar" yang berfungsi untuk mengarahkan pengguna ke halaman registrasi jika belum memiliki akun.

Halaman Daftar Pengguna



Gambar 3 Tampilan Halaman Daftar Pengguna

Gambar 3 merupakan halaman registrasi (daftar akun) pada sistem aplikasi. Halaman ini digunakan oleh pengguna baru untuk membuat akun sebelum bisa masuk ke dalam sistem.

Pada bagian kiri terdapat form pendaftaran yang berisi beberapa input, yaitu: (1) *Username*, digunakan untuk membuat nama pengguna yang nantinya dipakai saat *login*. (2) Kata Sandi (*Password*), digunakan untuk mengamankan akun. (3) Ulangi Kata Sandi, digunakan untuk memastikan bahwa *password* yang dimasukkan tidak salah.

Di bawah itu terdapat pertanyaan matematika sederhana (*captcha*) seperti (5 - 9) - 1, yang harus dijawab oleh pengguna. Tujuannya adalah untuk memastikan bahwa pendaftaran dilakukan oleh manusia, bukan bot. Selanjutnya terdapat pilihan "Saya menyetujui Syarat dan Ketentuan", yang harus dicentang sebelum akun dapat dibuat. Ini menandakan bahwa pengguna setuju dengan aturan penggunaan sistem. Kemudian ada tombol "Daftar" yang digunakan untuk mengirim data pendaftaran ke sistem. Jika semua data sudah benar, maka akun akan berhasil dibuat. Di bagian bawah juga terdapat tulisan "Sudah punya akun? Masuk", yang berfungsi untuk mengarahkan pengguna ke halaman *login* jika sudah memiliki akun.

Halaman Beranda



Gambar 4 Halaman Beranda

Gambar 4 merupakan tampilan halaman utama (beranda) dari sistem *Partial Homomorphic Encryption* (PHE) yang dirancang sebagai media untuk mengamankan dokumen PDF pada layanan penyimpanan. Pada bagian atas halaman terdapat menu navigasi yang terdiri dari Beranda, Tentang, *Form* Unggah, Enkripsi, Dekripsi, dan Keluar yang berfungsi untuk memudahkan pengguna dalam mengakses setiap fitur yang tersedia. Di sisi kiri halaman ditampilkan judul sistem beserta deskripsi singkat mengenai fungsi utama aplikasi, yaitu menerapkan algoritma *Partial Homomorphic Encryption* (PHE) agar data tetap berada dalam kondisi terenkripsi selama proses penyimpanan dan hanya dapat dibuka kembali melalui proses dekripsi oleh pengguna yang berwenang.

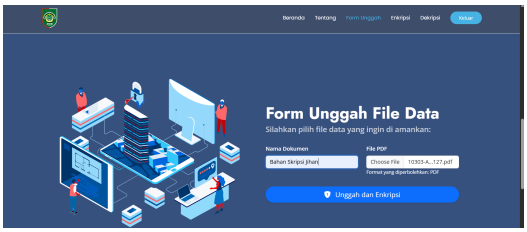
Halaman Tentang Sistem



Gambar 5 Halaman Tentang Sistem

Gambar 5 menampilkan halaman Tentang pada sistem *Partial Homomorphic Encryption* (PHE) yang berisi penjelasan mengenai tujuan, konsep, dan manfaat dari sistem yang dikembangkan. Pada halaman ini dijelaskan bahwa *Partial Homomorphic Encryption* merupakan metode kriptografi yang memungkinkan data tetap diproses dalam keadaan terenkripsi tanpa harus membuka isi data terlebih dahulu, sehingga tingkat keamanan informasi dapat lebih terjaga. Selain itu, dijelaskan pula bahwa sistem ini dikembangkan sebagai bagian dari implementasi keamanan data, khususnya untuk mengamankan dokumen PDF melalui proses enkripsi dan dekripsi. Beberapa manfaat utama yang ditampilkan meliputi kemampuan menjaga kerahasiaan *file* selama proses penyimpanan, mempertahankan data dalam kondisi terenkripsi sehingga tidak dapat diakses oleh pihak yang tidak berwenang, serta meningkatkan keamanan data dengan menerapkan metode kriptografi modern. Tampilan halaman disusun secara sederhana dengan pembagian informasi ke dalam dua bagian sehingga isi penjelasan lebih mudah dipahami oleh pengguna sebelum menggunakan fitur-fitur yang tersedia pada sistem.

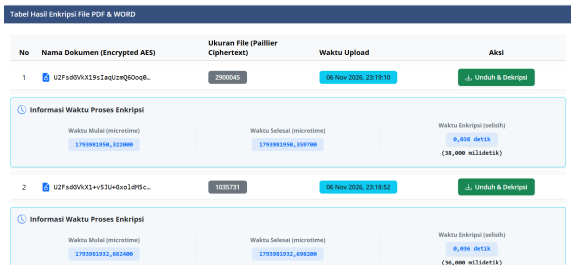
Halaman Unggah *File*



Gambar 6 Tampilan Halaman Unggah *File*

Gambar 6 menampilkan halaman Form Unggah *File* Data yang digunakan sebagai media untuk mengunggah dokumen PDF sebelum dilakukan proses enkripsi menggunakan metode *Partial Homomorphic Encryption* (PHE). Pada halaman ini tersedia beberapa komponen input yang harus diisi oleh pengguna, yaitu kolom Nama *File* untuk memberikan identitas dokumen, dan pilihan Pilih *File* untuk menentukan *file* PDF yang akan diproses. Setelah seluruh data diisi, pengguna dapat menekan tombol Unggah dan Enkripsi untuk memulai proses unggah sekaligus mengenkripsi dokumen sehingga *file* yang tersimpan berada dalam kondisi aman.

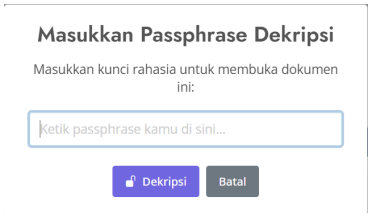
Halaman Data Enkripsi



Gambar 7 Halaman Data Enkripsi

Gambar 7 merupakan tampilan halaman Enkripsi & Dekripsi *File* PDF dan Word pada sebuah sistem berbasis web yang digunakan untuk mengamankan dokumen PDF dan Word. Pada halaman ini, sistem menampilkan daftar *file* PDF dan Word yang telah melalui proses enkripsi dalam bentuk tabel. Informasi yang ditampilkan meliputi nomor, nama dokumen yang telah dienkripsi, ukuran *file* hasil enkripsi atau *ciphertext*, waktu proses enkripsi, serta waktu ketika *file* diunggah. Selain itu, tersedia tombol "Unduh & Dekripsi" pada bagian aksi yang dapat digunakan pengguna untuk melakukan proses dekripsi dan mengunduh kembali *file* dalam bentuk aslinya. Dengan demikian, halaman ini berfungsi sebagai tempat untuk menampilkan dan mengakses kembali *file* PDF dan Word yang telah diamankan melalui proses enkripsi.

Halaman Data Dekripsi



Gambar 8 Halaman Data Dekripsi

Gambar 8 menampilkan formulir untuk memasukkan *passphrase* dekripsi yang digunakan untuk membuka atau mengakses dokumen yang telah dienkripsi. Pada bagian atas terdapat judul "Masukkan Passphrase Dekripsi", kemudian disertai keterangan yang meminta pengguna memasukkan kunci rahasia untuk membuka dokumen. Pengguna dapat memasukkan passphrase pada kolom yang tersedia dengan tulisan *"Ketik passphrase kamu di sini..."*. Setelah *passphrase* dimasukkan, pengguna dapat menekan tombol "Dekripsi" untuk memproses pembukaan dokumen menggunakan kunci tersebut. Sementara itu, tombol "Batal" digunakan untuk membatalkan proses dan menutup formulir tanpa melakukan dekripsi.

Hasil Pengujian Algoritma

Tabel 4 Tabel Hasil Pengujian Algoritma

No	Nama *File*	Jenis *File* Teks	Ukuran Enkripsi	Waktu Enkripsi (detik)	Ukuran Dekripsi
1	Daftar isi 1	word	2.900 KB	0,036	27.5 KB

2	abstrak	pdf	1.035 KB	0,038	10.3 KB
3	Lamiran	Word	3.210 KB	0,033	31.1 KB
4	Cover	Pdf	17.498 KB	0,081	173 KB
5	Skripsi revisi 1	Word	780.135 KB	1,893	7.53 MB
6	Skripsi revisi 1 pdf	Pdf	190.153 KB	0,424	1.83 MB
7	Skripsi revisi 4	Word	752.724 KB	1,770	7.26 MB
8	Skripsi revisi 2 word	Word	752.927 KB	1,948	7.26 MB
9	Artikel	Pdf	20.229 KB	0,069	200 KB
10	*File* bahan	Word	37.524 KB	0,105	371 KB
11	Daftar isi revisi	Word	2.832 KB	0,031	27.5 KB
12	Abstrak word	Word	2.124 KB	0,026	20.7 KB
13	Skripsi full	Word	839.608 KB	2,062	8.10 MB
14	Skripsi 2	Pdf	190.153 KB	0,427	1.83 MB
15	Skripsi revisi seminar	Word	714.896 KB	1,655	6.90B

Berdasarkan tabel hasil pengujian terhadap 15 file dokumen berformat DOCX dan PDF, dapat diketahui bahwa waktu enkripsi dipengaruhi oleh ukuran *file* yang diproses. Semakin besar ukuran *file*, waktu yang dibutuhkan untuk proses enkripsi cenderung semakin lama. Waktu enkripsi tercepat adalah 0,026 detik, sedangkan waktu terlama adalah 2,062 detik. Selain itu, ukuran *file* hasil enkripsi lebih kecil dibandingkan ukuran *file* setelah dekripsi. Ukuran *file* setelah dekripsi kembali sama dengan ukuran *file* aslinya, sehingga dapat disimpulkan bahwa proses dekripsi berhasil mengembalikan *file* ke ukuran semula.

D. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa algoritma Paillier Homomorphic Encryption berhasil diimplementasikan untuk mengamankan file PDF melalui proses enkripsi dan dekripsi. File PDF yang telah dienkripsi tidak dapat dibaca secara langsung dan hanya dapat dikembalikan ke bentuk semula melalui proses dekripsi menggunakan kunci yang sesuai. Hasil pengujian menunjukkan bahwa proses pengamanan data dilakukan melalui tahapan pengunggahan file, konversi data menjadi ciphertext menggunakan algoritma Paillier, penyimpanan file terenkripsi, serta proses dekripsi menggunakan private key untuk mengembalikan data menjadi plaintext. Selain itu, karakteristik additive homomorphic pada algoritma Paillier memungkinkan operasi penjumlahan dilakukan terhadap data dalam bentuk ciphertext tanpa harus mengetahui isi data aslinya. Pengujian terhadap lima file PDF dengan ukuran berbeda menunjukkan bahwa ukuran file memengaruhi waktu proses enkripsi. File artikel berukuran 200 KB memiliki waktu

enkripsi tercepat, yaitu 0,009 detik, sedangkan file rahasia berukuran 1.806 KB membutuhkan waktu paling lama, yaitu 0,026 detik. Dengan demikian, semakin besar ukuran file yang diproses, semakin lama waktu yang dibutuhkan untuk melakukan enkripsi, meskipun peningkatan waktu tersebut relatif kecil sehingga tidak memberikan pengaruh signifikan terhadap kinerja sistem.

E. DAFTAR PUSTAKA

Abdulloh, R. (2018). 7 in 1 pemprograman web untuk pemula. PT Elex Media Komputindo.

Adobe Systems. (2023). PDF reference and Portable Document Format specification. Adobe Inc.

Aghili, S., Shojafar, M., Peris-Lopez, P., & Baccarelli, E. (2024). Secure cloud computing and application services: Challenges and opportunities. Journal of Cloud Computing, 13(1), 1–19.

Ahamed, K. (2023). Enhancing privacy in cloud anomaly detection with lightweight Homomorphic Encryption. International Journal of Computer Science & Information System, 8(8), 1–4.

Aljohani, A., & Ahmad, M. (2023). Privacy-preserving data processing in cloud computing using Homomorphic Encryption: A survey and future directions. Journal of Cloud Computing, 12(1), 1–25. https://doi.org/10.1186/s13677-023-00425-7

Aljohani, A., & Ahmad, M. (2023). Privacy-preserving data processing in cloud computing using Homomorphic Encryption: A survey and future directions. Journal of Cloud Computing, 12(1), 1–25. https://doi.org/10.1186/s13677-023-00425-7

Aljohani, A., & Ahmad, M. (2023). Privacy-preserving data processing in cloud computing using Homomorphic Encryption: A survey and future directions. Journal of Cloud Computing, 12(1), 1–25. https://doi.org/10.1186/s13677 023-00425-7

Almeida, R., & Costa, P. (2023). Digital document management and PDF technology in modern information systems. International Journal of Digital Information Management, 8(2), 115–128.

Amorim, I., & Costa, I. (2023). Leveraging searchable encryption through Homomorphic Encryption: A comprehensive analysis. Mathematics, 11(13), 2948. https://doi.org/10.3390/math11132948

Amorim, I., & Costa, I. (2023). Leveraging searchable encryption through homomorphic encryption: A comprehensive analysis. Mathematics, 11(13), 2948. https://doi.org/10.3390/math11132948

Anardani, S., Yunitasari, Y., & Sussolaikah, K. (2023). Analisis perancangan sistem informasi monitoring dan evaluasi kerjasama menggunakan UML. REMIK: Riset dan E-Jurnal Manajemen Informatika Komputer, 7(1), 522–532. https://doi.org/10.33395/remik.v7i1.12070

Annisa Medina. (2023). Pengertian PHP, Sejarah, Sintak Dasar dan Kelebihannya. https://fikti.umsu.ac.id/pengertian-php-sejarah-sintak-dasar-dankelebihannya/

Azad, M. A. K., Sharma, V., & Kumar, N. (2023). Secure key management techniques for cloud-based cryptographic systems. Journal of Information Security and Applications, 73, 103423.

Bkakria, A. (2023). Modern encryption techniques for data confidentiality in cloud environments. International Journal of Information Security, 22(4), 645–662.

Cahyono, M. R. A., Maulana, A., & Sunarsa, T. (2024). Perancangan Unified Modelling Language sistem informasi surat jalan dan lembaran permintaan perbaikan berbasis website. Jurnal Instrumentasi dan Teknologi Informasi, 6(1). https://jurnal.poltek-gt.ac.id/jiti/id/article/view/75

Chaitanya, N. S., Bhargavi, A. J., & Geetha, J. (2024). Secure file storage using Homomorphic Encryption in cloud. Journal of Computational Analysis and Applications, 33(8), 5394–5411.

Dan, A. (2025). Pengertian HTML, PHP, CSS, JavaScript dan XML. https://andreasdan.com/html-php-css-javascript-xml/

El-Yahyaoui, A., & Dafir, M. (2016). Fully Homomorphic Encryption: State of the art and comparison. https://doi.org/10.6084/M9.FIGSHARE.3362338

Fauziah, R. Z., Khudzaifah, M., & Herawati, E. (2024). Pengamanan pesan teks menggunakan Affine Cipher dan algoritma Goldbach Code. CyberSecurity dan Forensik Digital, 7(1), 1–6. https://doi.org/10.14421/csecurity.2024.7.1.4406

Fintri Indriyani, Yunita, Muthia, D. A., Surniandari, A., & Sriyadi. (2019). Analisa perancangan sistem informasi. Bina Sarana Informatika.

Harahap, H. R. S., & Yahfizham. (2023). Konsep dan fungsi algoritma pemrograman. Konstanta: Jurnal Matematika dan Ilmu Pengetahuan Alam, 1(3), 245–257. https://doi.org/10.59581/konstanta-widyakarya.v1i4.1875

Harahap, H. R. S., & Yahfizham. (2023). Konsep dan fungsi algoritma pemrograman. Konstanta: Jurnal Matematika dan Ilmu Pengetahuan Alam, 1(3), 245–257. https://doi.org/10.59581/konstanta-widyakarya.v1i4.1875

Hasanah, F. N., & Untari, R. S. (2020). Rekayasa perangkat lunak. UMSIDA Press.

Johan, J., Suwandhi, A., Jimmy, J., Simanihuruk, T., & Benny. (2025). Homomorphic Encryption & Confidential Computing: Teknologi untuk perlindungan data dalam pemrosesan terenkripsi. Jurnal Minfo Polgan, 14(1), 578–584. https://doi.org/10.33395/jmp.v14i1.14792

Johnson, M., & Miller, S. (2023). Comparative analysis of text document formats for digital archiving. Journal of Information Technology Research, 16(3), 45–59.

Kaendung, E., Pangemanan, F., & Undap, G. (2021). Implementasi kebijakan tentang rencana induk teknologi informasi dan komunikasi di Kota Manado. Jurnal Governance, 1(2).

Kishiyama, T., & Alsmadi, I. (2023). Security challenges in web-based cloud applications. Journal of Cyber Security Technology, 7(3), 215–231.

Kumar, A., & Singh, R. (2023). Text document formats and information management in digital environments. International Journal of Computer Applications, 185(8), 12–20.

Kumar, S., & Verma, P. (2023). Security challenges in PDF document management systems. International Journal of Information Security Research, 13(2), 101–112.

Kusumawati, F. I., Hidayat, W. N., & Riaji, D. (2024). Pengembangan media pembelajaran e-modul interaktif pada mata pelajaran orientasi dasar PPLG materi flowchart. Journal of Innovation and Teacher Professionalism, 2(2), 124–131. https://doi.org/10.17977/um084v2i22024p124-131

Laouid, A., Hammoudeh, M., Kara, M., Bejaoui, T., Eleyan, A., & Al-Khalidi, M. (2023). A multi-key with Partially Homomorphic Encryption scheme for low-end devices ensuring data integrity. Information, 14(5), 263. https://doi.org/10.3390/info14050263

Laouid, A., Hammoudeh, M., Kara, M., Bejaoui, T., Eleyan, A., & Al-Khalidi, M. (2023). A multi-key with partially homomorphic encryption scheme for low-end devices ensuring data integrity. Information, 14(5), 263. https://doi.org/10.3390/info14050263

Li, X., Zhang, Y., & Chen, H. (2025). Fully Homomorphic Encryption for secure cloud data computation: Challenges and performance evaluation. Journal of Cloud Computing, 14(1), 1–19. https://doi.org/10.1186/s13677-025-00774-5

Liu, Y., & Chen, H. (2023). Portable document technologies for modern digital communication. Journal of Digital Documentation, 7(1), 66–78.

Maharani, P. (2025). Pengembangan Website PT. Rantangin Digital Indonesia Menggunakan Framework Next Js dan Tailwind CSS. Repeater: Publikasi Teknik Informatika dan Jaringan, 3(1), 129-137. https://doi.org/10.62951/repeater.v3i1.355

Mishra, P., & Gupta, V. (2023). Evolution of word processing document formats in digital systems. International Journal of Advanced Computing Research, 14(4), 88–99.

Morris, L. (2013). Analysis of partially and fully Homomorphic Encryption.

Mulyasa. Kurikulum Berbasis Kompetensi Konsep, Karakteristik, Implementasi, dan Inovasi. (Bandung: Remaja Rosdakarya. 2005).93

Narulita, S., Nugroho, A., & Abdillah, M. Z. (2024). Diagram Unified Modelling Language (UML) untuk perancangan sistem informasi manajemen penelitian dan pengabdian masyarakat (SIMLITABMAS). BRIDGE: Jurnal Publikasi Sistem Informasi dan Telekomunikasi, 2(3), 244–256. https://doi.org/10.62951/bridge.v2i3.174.

Nova, S. (2025). Pembuatan website inventory urban material: Pendekatan PHP & MYSQL. Jurnal Minfo Polgan, 13(2), 2248-2256. https://doi.org/10.33395/jmp.v13i2.14425

Park, J., Lee, S., Kang, H., Kim, Y., & Kim, D. (2023). Secure decryption mechanisms and access control in modern cryptographic systems. Journal of Information Processing Systems, 19(2), 245–259.

Patel, R., & Sharma, K. (2023). Plain text file structures and applications in computing systems. Journal of Computer Science Applications, 11(2), 34–42.

Pötzelsberger, G., & Eng, B. (2013). KV web security: Applications of Homomorphic Encryption.

Sakinah, K., Ghofur, A., & Lutfi, A. (2024). Perancangan dan implementasi aplikasi e-learning berbasis website dengan menggunakan PHP dan MySQL pada SMK Ibrahimy Miftahul Ulum Bengkak-Wongsorejo. SENADA (Seminar Nasional Manajemen, Desain dan Aplikasi Bisnis Teknologi), 7, 122–129.

Sakinah, K., Ghofur, A., & Lutfi, A. (2024, April). Perancangan Dan Implementasi Aplikasi E-Learning Berbasis Website Dengan Menggunakan Php & Mysql Pada Smk Ibrahimy Miftahul Ulum Bengkak-Wongsorejo. In SENADA (Seminar Nasional Manajemen, Desain dan Aplikasi Bisnis Teknologi) (Vol. 7, pp. 122-129).

Samanth, K., Prema, K. V., & Balachandra, M. (2023). Data encryption methods for protecting sensitive information in cloud computing. International Journal of Advanced Computer Science and Applications, 14(5), 145–154

Saputra, D., Dharmawan, W. S., Syarif, M., & Risdiansyah, D. (2023). Analisis & perancangan sistem informasi. Penerbit Insan Cendekia Mandiri.

Silalahi, F. D. (2022). Manajemen database MySQL (Structured Query Language). Yayasan Agus Prima Teknik.

Sinambela, M. R., Waidah, D. F., Susilo, T., Jaya, N. A., & Friansyah, I. G. (2024). Rancang bangun

perpustakaan digital berbasis website pada SD Swasta 001 PT. KG Meral Barat di Kabupaten Karimun. Tikar: Jurnal Teknik Informatika Karimun, 5(1), 12–23. https://doi.org/10.51742/teknik_informatika.v5i1.1231.

Sinlae, F., Maulana, I., Setiyansyah, F., & Ihsan, M. (2024). Pengenalan pemrograman web: Pembuatan aplikasi web sederhana dengan PHP dan MySQL. Jurnal Siber Multi Disiplin, 2(2), 68–82. https://doi.org/10.38035/jsmd.v2i2.156

Siswanto, E. (2021). PHP uncover (Kupas tuntas pemrograman PHP). Yayasan Prima Agus Teknik.

Soleh, M. N. Z., Hadiana, A. I., & Kasyidi, F. (2024). Kriptografi homomorfik dalam anonimisasi data untuk pengolahan data pada sistem e-voting. Jurnal Masyarakat Informatika, 15(2), 107–124. https://doi.org/10.14710/jmasif.15.2.66317

Suganya, R., & Sasipraba, T. (2023). Security enhancement in cloud storage systems using cryptographic techniques. Journal of Cloud Computing, 12(1), 1–14.

Sukmana, I. B. M. W. T., & Muliantara, A. (2025). Pengamanan data finansial menggunakan enkripsi homomorfik Paillier. Jurnal Nasional Teknologi Informasi dan Aplikasinya, 3(2), 255–260. https://doi.org/10.24843/JNATIA.2025.v03.i02.p04

Supriyadi, S., Ronal, R., & Yuliana, Y. (2023). Studi perbandingan skema enkripsi homomorfik dalam voting system e-suara. JSR: Jaringan Sistem Informasi Robotik, 7(1), 61–65. https://doi.org/10.58486/jsr.v7i1.215

Suwandi, R., Nasution, S. M., & Azmi, F. (2018). Secure e-voting system by utilizing homomorphic properties of the encryption algorithm. TELKOMNIKA (Telecommunication Computing Electronics and Control), 16(2), 862–867. https://doi.org/10.12928/TELKOMNIKA.v16i2.8420

Syarifuddin Nurdin, Guru Profesional dan Implementasi Kurikulum. (Jakarta: Ciputat Press, 2005). 70

Syed Arafath, M., & Amutha, R. (2023). Cryptography and data security in cloud computing environments. International Journal of Progressive Research in Science and Engineering, 4(7), 56–64.

Tantowi, L., & Wijayanti, L. (2023). Peluang dan tantangan penyimpanan Cloud storage pada dokumen digital. Shaut Al-Maktabah: Jurnal Perpustakaan, Arsip dan Dokumentasi, 15(1), 118–131.

Vyas, A., & Abimannan, S. (2023). Use of Homomorphic Encryption techniques for secure cloud computing. AIP Conference Proceedings, 2755(1), 020022.

https://doi.org/10.1063/5.0148262

Wang, X., & Zhao, L. (2023). Adoption of PDF documents in academic and professional environments. International Journal of Information Systems and Technology, 9(1), 21–33.

Yuan, Z., Chang, W., & Xu, L. (2023). Web application architecture for scalable cloud services. International Journal of Web Information Systems, 19(4), 355–370.

Zhang, Y., & Wang, T. (2023). Classification and utilization of text-based digital file formats. Journal of Information Management and Technology, 15(2), 77–89.

Zhang, Y., Chen, H., & Li, W. (2025). A comparative study of partially, somewhat, and fully Homomorphic Encryption in modern cryptographic libraries. Electronics, 14(23), 4753. https://doi.org/10.3390/electronics14234753.