Perancangan Aplikasi Keamanan Bank Soal Ujian Sekolah Menggunakan Algoritma Kriptografi Elgamal Berbasis Web

Mahmubin Haibah[1], Ferdy Riza[2]
[1,2]Program Studi Sistem Informasi, Universitas Muhammadiyah Sumatera Utara, Indonesia
Email : sayahaibah@gmail.com; ferdyriza@umsu.ac.id

ABSTRAK

Keamanan data menjadi aspek krusial dalam sistem pendidikan, terutama dalam pengelolaan bank soal ujian sekolah. Kebocoran soal dapat mengganggu integritas proses evaluasi dan berdampak pada kredibilitas instansi pendidikan. Untuk menjawab tantangan tersebut, penelitian ini merancang sebuah aplikasi keamanan bank soal berbasis web dengan menerapkan keamanan algoritma kriptografi ElGamal. Algoritma ini dipilih karena kemampuannya dalam menjaga kerahasiaan data melalui proses enkripsi dan dekripsi serta pemilihan kunci publik dan kunci privat yang berbeda. Aplikasi ini memungkinkan user atau guru untuk mengunggah soal ujian dalam bentuk file berekstensi PDF yang kemudian dienkripsi menggunakan algoritma kriptogragi ElGamal, sehingga hanya pihak yang memiliki kunci privat yang dapat mengakses isi soal tersebut. Pengujian dilakukan untuk memastikan fungsionalitas aplikasi berjalan baik, mulai dari proses unggah, enkripsi, penyimpanan file serta kunci privat, hingga proses dekripsi file soal. Hasil implementasi menunjukkan bahwa sistem mampu mengamankan soal ujian secara efektif dan dapat diakses dengan mudah oleh pengguna yang berwenang. Dengan adanya sistem ini, diharapkan proses distribusi dan penyimpanan soal ujian menjadi lebih aman, efisien, dan terjaga kerahasiaannya.
Keyword: Keamanan Data; Bank Soal; Kriptografi ElGamal

ABSTRACT

Data security is a crucial aspect of the education system, particularly in the management of school exam question banks. Leakage of exam questions can compromise the integrity of the evaluation process and affect the credibility of educational institutions. To address this challenge, this study designs a web-based application for securing exam question banks by implementing the ElGamal cryptographic algorithm. This algorithm is chosen for its ability to maintain data confidentiality through encryption and decryption processes, as well as its use of distinct public and private keys. The application allows users or teachers to upload exam questions in PDF format, which are then encrypted using the ElGamal algorithm, ensuring that only those with the private key can access the contents. Testing was conducted to ensure that the application's functionalities work properly, from the upload process, encryption, file and private key storage, to the decryption of the exam file. The implementation results show that the system effectively secures exam questions and can be easily accessed by authorized users. With this system, the distribution and storage of exam questions are expected to be more secure, efficient, and confidential.
Keyword: Data Security; Question Bank; ElGamal Cryptography

Corresponding Author:
Ferdy Riza,
Universitas Muhammadiyah Sumatera Utara,
Jl. Kapten Muchtar Basri No.3, Glugur Darat II, Kec. Medan Tim., Kota Medan, Sumatera Utara 20238, Indonesia
Email: ferdyriza@umsu.ac.id

1. PENDAHULUAN

Dalam perkembangan sistem pendidikan saat ini, penggunaan bank soal pada suatu institusi pendidikan memiliki peran yang sangat penting sebagai media penyimpanan data soal ujian sekolah. Bank soal

berfungsi untuk meningkatkan efisiensi dalam pengelolaan soal dan menjadi indikator perkembangan proses penilaian dalam institusi pendidikan.

Bank soal merupakan kumpulan soal dari berbagai materi yang disusun secara terstruktur untuk mempermudah dalam penyusunan soal ujian. Umumnya, bank soal dilengkapi dengan informasi seperti nomor soal, kunci jawaban, dan indeks soal yang merujuk pada materi yang telah diajarkan (Qhorifadillah et al., 2022). Selain dalam bidang akademik, konsep bank soal juga dapat digunakan di disiplin ilmu lainnya. Secara umum, bank soal memberikan berbagai keuntungan seperti kemudahan dalam fasilitasi, hasil yang cepat, serta efisiensi biaya karena tidak memerlukan kertas kerja dan pemeriksaan hasil dapat dilakukan secara langsung (Annas, 2020).

Beberapa langkah penting dalam pengembangan bank soal meliputi penulisan soal, validasi, kalibrasi, penyimpanan, serta pengamanan soal. Namun, pada praktiknya, tahapan-tahapan ini seringkali tidak dilakukan secara menyeluruh (Suhardi, 2023). Banyak institusi pendidikan masih menggunakan metode penyimpanan konvensional atau digital tanpa sistem keamanan yang memadai, sehingga rentan terhadap ancaman *cybercrime* seperti pencurian dan kebocoran soal sebelum pelaksanaan ujian (Butarbutar, 2023). *Cybercrime* adalah aktivitas kriminal yang dilakukan melalui komputer dan jaringan internet dengan tujuan mengeksploitasi kelemahan dalam sistem digital.

Untuk mengatasi permasalahan tersebut, salah satu solusi yang dapat diterapkan adalah membangun sistem bank soal yang dilengkapi dengan algoritma kriptografi agar data soal hanya dapat diakses oleh pihak yang berwenang. Kriptografi berasal dari bahasa Yunani *kryptos* yang berarti tersembunyi dan *graphein* yang berarti menulis. Kriptografi merupakan ilmu dan seni mengamankan data melalui teknik pengkodean agar informasi tidak dapat diakses oleh pihak yang tidak memiliki kewenangan (Riza et al., 2020).

Kriptografi terbagi menjadi dua jenis, yaitu kriptografi simetris dan asimetris. Kriptografi simetris menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi, sedangkan kriptografi asimetris menggunakan dua kunci berbeda, yaitu *public key* untuk enkripsi dan *private key* untuk dekripsi. Algoritma kriptografi asimetris dianggap lebih aman dibandingkan dengan algoritma simetris (Saputro et al., 2020). Salah satu algoritma kriptografi asimetris yang dikenal adalah ElGamal. Algoritma ElGamal didasarkan pada masalah logaritma diskret dan memiliki tiga tahapan utama yaitu pembentukan kunci, proses enkripsi, dan proses dekripsi (Riza et al., 2020). ElGamal dikenal memiliki tingkat keamanan yang tinggi karena menghasilkan *ciphertext* yang kompleks, meskipun prosesnya relatif lebih lambat. ElGamal juga dinilai lebih aman dibandingkan algoritma RSA (Mallouli et al., 2019).

Berdasarkan solusi yang telah dijelaskan, penelitian ini bertujuan untuk membangun sistem bank soal berbasis *web* yang menggunakan algoritma kriptografi ElGamal. Metode ini dipilih karena memiliki tingkat keamanan yang tinggi dan kompleksitas dalam memecahkan kunci privat, sehingga mampu melindungi data soal ujian dari akses pihak yang tidak berwenang. Oleh karena itu, penelitian ini diangkat dalam judul: "Perancangan Aplikasi Keamanan Bank Soal Ujian Sekolah Menggunakan Algoritma Kriptografi ElGamal Berbasis Web".

2. KAJIAN PUSTAKA

A. Bank Soal

Secara singkat, bank soal dapat diartikan sebagai kumpulan dari beberapa soal. Namun, bank soal tidak hanya merupakan kumpulan dari beberapa soal saja, tetapi juga dapat diartikan pada proses pengumpulan soal, pemantauan dan mengelola informasi yang terkait sehingga mempermudah pendistribusiannya (Wardani et al., 2024). Bank soal merupakan kumpulan soal-soal dari berbagai materi yang terstruktur, untuk mempermudah penyusunan soal untuk ujian, bank soal terdiri dari beberapa soal dari berbagai materi yang teroganisir dimulai dari menata hingga menyimpan dengan merujuk pada materi yang sudah diberikan, seperti nomor soal, kunci soal, dan indeks soal (Qhorifadillah et al., 2022).

B. Kriptografi

Kriptografi adalah ilmu yang mempelajari cara menyembunyikan pesan. Namun, pada era modern saat ini kriptografi adalah ilmu yang didasarkan pada teknik matematika untuk menangani keamanan informasi, termasuk kerahasiaan, keutuhan data dan otentikasi entitas. Akibatnya, definisi kriptografi saat ini tidak hanya berkaitan dengan menyembunyikan pesan, tetapi juga mencakup berbagai metode untuk menjaga keamanan informasi tersebut (Nugraha, 2024). Keamanan sistem informasi didasarkan pada lima aspek utama yang dikenal sebagai CIAAN: Confidentiality (Kerahasiaan), Integrity (Integritas), Availability (Ketersediaan), Authentication (Autentikasi), dan Non-repudiation (Nirpenyangkalan). Kerahasiaan memastikan bahwa informasi hanya dapat diakses oleh pihak berwenang melalui enkripsi dan kontrol akses. Integritas menjaga keakuratan data dengan metode seperti checksum dan hashing untuk mencegah manipulasi. Ketersediaan memastikan layanan tetap dapat diakses, meskipun ada serangan seperti DDoS (Riza et al., 2020).

C. Enkripsi dan Dekripsi

Enkripsi adalah salah satu komponen kunci dalam kriptografi, yaitu proses mengubah data asli (plaintext) menjadi bentuk terenkripsi (ciphertext) menggunakan algoritma enkripsi dan kunci enkripsi yang sesuai. Enkripsi memainkan peran penting dalam menjaga kerahasiaan, integritas, dan keamanan data dalam keamanan komputer (Wijoyo et al., 2023).

Sementara Dekripsi adalah kegiatan untuk mengembalikan pesan yang telah tersandi atau terenkripsi menjadi pesan asli atau plaintext. Proses mengembalikan isi ciphertext menggunakan kunci yang telah ditentukan sebelumnya. Dekripsi adalah kebalikan dari proses enkripsi, yaitu mengubah pesan asli menjadi pesan tersandi atau ciphertext (Alfirdaus et al., 2023).

D. Kriptografi Kunci Simetris dan Asimetris

Algoritma kriptografi kunci simetris adalah algoritma kriptografi dengan menggunakan kunci enkripsi dan dekripsi yang sama. Saat menggunakan algoritma ini untuk mengirim pesan, orang yang menerima pesan harus mengetahui kunci yang digunakan agar mereka dapat mendekripsi pesan tersebut. Dengan demikian, keamanan pesan yang dikirim dengan algoritma ini bergantung pada kunci yang digunakan. Orang lain dapat melakukan enkripsi dan dekripsi pesan jika mereka tahu kuncinya. (Alfirdaus et al., 2023).

Sementara Kriptografi kunci asimetris adalah salah satu jenis kriptografi yang menggunakan dua kunci yang berbeda namun saling terkait untuk mengamankan informasi. Kedua kunci ini disebut kunci publik atau public key dan kunci privat atau private key. Berbeda dengan kriptografi simetris yang hanya menggunakan satu kunci untuk mengenkripsi dan mendekripsi data, kriptografi asimetris memastikan bahwa apa yang dienkripsi dengan kunci publik hanya dapat didekripsi dengan kunci privat, dan sebaliknya (Riza, F. et al., 2020).

E. Public Key dan Private Key

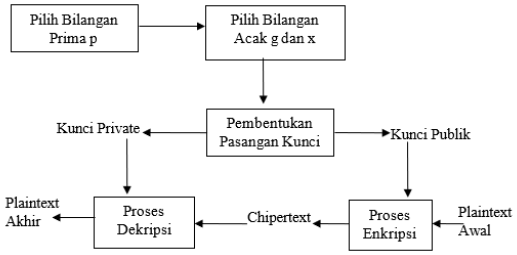
Public key adalah kunci yang dapat dibagikan kepada pihak lain digunakan untuk mengenkripsi data. (Baraka, 2023). Kegunaan kunci ini adalah untuk mengenkripsi data atau pesan. Siapapun yang memiliki kunci publik dapat menggunakannya untuk mengenkripsi pesan, tetapi hanya mereka yang memiliki kunci privat yang diizinkan untuk membuka pesan setelah dienkripsi. Karena kunci publik tidak dapat digunakan untuk mendekripsi informasi, kunci publik dapat dibagikan secara bebas kepada siapa saja (Riza, F. et al., 2020).

Semetara Private key adalah kunci yang hanya diketahui oleh pemiliknya, dan untuk mendekripsi data (Baraka, 2023). Kunci ini hanya dimiliki oleh satu orang atau entitas dan digunakan untuk mendekripsi data yang telah dienkripsi sebelumnya dengan kunci publik yang tepat. Karena bersifat rahasia, kunci ini harus dijaga dengan sangat hati-hati. Jika kunci privat jatuh ke tangan orang yang salah, orang yang tidak bertanggung jawab dapat mendekripsi data yang dienkripsi dengan kunci publik, yang dapat menyebabkan pelanggaran keamanan yang signifikan (Riza et al., 2020).

F. Kriptografi ElGamal

Algoritma ElGamal diciptakan oleh ilmuwan asal Mesir, Taher ElGamal pada tahun 1985. Konsep dasar algoritma ElGamal terletak pada kunci publik dan awalnya digunakan untuk tanda tangan digital, namun kemudian algoritma ini dimodifikasi sehingga dapat digunakan untuk proses enkripsi dan dekripsi pesan. Algoritma kunci publik ElGamal merupakan algoritma blok cipher yang mengenkripsi blok-blok plaintext menjadi blok-blok ciphertext, yang kemudian akan didekripsi kembali menggunakan kunci privat dan digabungkan menjadi plaintext semula (Nugraha, 2024).

Algoritma kriptografi ElGamal unggul dalam pembangkitan kunci dengan menggunakan logaritma diskrit pada modulo prima yang besar, sehingga upaya untuk menyelesaikan masalah logaritma ini menjadi sulit untuk dipecahkan. Metode enkripsi dekripsi yang menggunakan proses komputasi yang besar sehingga hasil enkripsinya berukuran dua kali dari ukuran semula. Kekurangan algoritma ini adalah membutuhkan resource yang besar karena ciphertext yang dihasilkan dua kali panjang plaintext serta membutuhkan processor yang mampu untuk melakukan komputasi yang besaruntuk perhitungan logaritma perpangkatan besar. Untuk proses dekripsi, algoritma ini membutuhkan waktu yang lebih lama karena kompleksitas proses dekripsinya yang rumit. Dibutuhkan dua kali komputasi karena ukuran ciphertext yang lebih besar dibandingkan plaintext-nya (Harahap et al., 2022).



(Sumber: Nugraha, 2024)

Gambar 1. Tahapan Penyelesaian Algoritma ElGamal

1) Proses Pembangkitan Kunci Elgamal (*Elgamal Generate Key*)

Algoritma ElGamal merupakan sepasang kunci yang dibangkitkan dengan memilih bilangan prima p dan dua buah bilangan acak (random) g dan x, dengan syarat bahwa nilai g dan x lebih kecil dari p. Nilai y, g dan p merupakan kunci publik, sedangkan x, p merupakan pasangan kunci pribadi. Langkah-langkah dalam pembangkitan kunci pada algoritma kriptografi ElGamal (Elgamal Generate Key) adalah sebagai berikut:

a) Kunci Publik (Public Key)

- Pilih p adalah bilangan prima dengan syarat p > 255.
- Pilih bilangan acak g dengan syarat g < p.
- Hitung nilai y dengan persamaan dibawah ini:

  $y= g^x \mod p$ (1)

  Keterangan:
  g = kunci publik g.
  x = Kunci privat x.
  mod = Perhitungan modulus.
  p = kunci publik p (Ramadhani & Tanti, 2024).

b) Kunci Private (Private Key)

- Pilih p adalah bilangan prima dengan syarat p > 255.
- Pilih bilangan acak x dengan syarat x < p.

c) Bilangan Acak Pengirim (Random k)

- Pilih bilangan acak k (random k), dengan syarat $1 \leq k \leq p - 2$.

2) Proses Enkripsi ElGamal (*ElGamal Encryption Process*)

Proses enkripsi merupakan proses mengubah pesan asli (plaintext) menjadi pesan rahasia (chipertext). Pada proses ini digunakan public key (p, g, y). Langkah-langkah dalam mengenkripsi plaintext adalah:

- Potong plaintext menjadi blok-blok m1, m2, …, mN.
- Konversi nilai blok-blok pesan kedalam nilai ASCII.
- Setiap blok m dienkripsi dengan persamaan dibawah ini:

  $a = g^k \mod p$ (2)

  $b = y^k . m \mod p$ (3)

  Keterangan:
  a = Pasangan ciphertext pertama.
  b = Pasangan ciphertext kedua.
  g = kunci publik g.
  k = Bilangan acak (random k).
  m = nilai ASCII karakter plaintext.
  mod = perhitungan modulus.
  p = kunci publik p.
- Susun ciphertext dengan urutan a1, b1; a2, b2; …; aN, bN (Ramadhani & Tanti, 2024).

3) Proses Dekripsi ElGamal (*ElGamal Decryption Process*)

Untuk proses dekripsi pesan ciphertext membutuhkan nilai ciphertext dari proses enkripsi dan kunci privat x. Selanjutnya ciphertext dilakukan proses dekripsi dengan perhitungan sebagai berikut:

- Gunakan kunci privat x untuk menghitung persamaan dibawah ini:

  $(a^x)^{-1} = a^{p-1-x} \; mod \; p$ (4)
- Lalu, hitung plaintext (m) dengan persamaan dibawah ini:

  $m = b(a^x)^{-1} \; mod \; p$ (5)

  Keterangan:
  a = Pasangan ciphertext pertama.
  b = Pasangan ciphertext pertama.
  x = kunci privat x.

p = kunci publik p.
mod = perhitungan modulus.
m = nilai ASCII karakter plaintext (Nugraha, 2024).

3. METODE PENELITIAN

A. Tahapan Penelitian

1) Analisis Kebutuhan

Tahap ini merupakan proses identifikasi dan analisis terhadap kebutuhan sistem yang akan dibangun. Kegiatan utama meliputi pengumpulan data dan perangkat yang diperlukan untuk merancang sistem.

Adapun kebutuhan yang diidentifikasi meliputi:

- Data soal ujian sekolah dari SMA Adlin Murni.
- Perangkat lunak server lokal (XAMPP).
- Layanan hosting (anymhost.id).
- Peramban web (Google Chrome).
- Teks editor (Sublime Text versi 3).

2) Desain Sistem

Desain sistem bertujuan menerjemahkan kebutuhan fungsional dan non-fungsional menjadi rancangan teknis yang siap diimplementasikan. Proses ini mencakup perancangan struktur data, keamanan data, arsitektur perangkat lunak, antarmuka pengguna, dan alur prosedural. Pemodelan dilakukan menggunakan Unified Modeling Language (UML) melalui flowchart, use case diagram, class diagram, activity diagram, dan sequence diagram.

3) Implementasi Sistem

Tahap ini merupakan penerjemahan desain sistem ke dalam bahasa pemrograman. Pengembangan dimulai dengan pembuatan antarmuka menggunakan HTML dan CSS, dilanjutkan dengan pemrograman logika sistem menggunakan PHP dan JavaScript, serta pengelolaan database dengan MySQL.

4) Pengujian Sistem

a) Fungsionalitas:
   - Enkripsi data menggunakan algoritma ElGamal.
   - Dekripsi data untuk memastikan kesesuaian dengan plaintext awal.
   - Pembuatan public key dan private key sesuai algoritma.
   - Fitur unggah dan unduh file.

b) Antarmuka:
   - Kesesuaian alur sistem dengan desain.
   - Kemudahan penggunaan sistem bagi pengguna akhir.

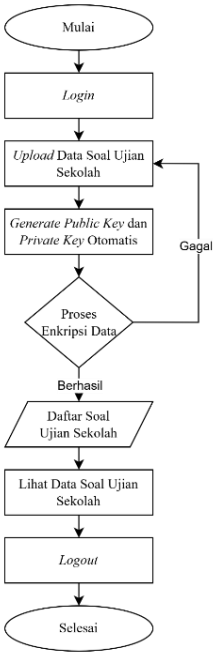
5) Penerapan dan Pemeliharaan Sistem

Tahap akhir melibatkan penerapan sistem kepada pengguna serta pemeliharaan untuk menjamin keberlangsungan dan keamanan sistem. Aktivitas ini mencakup:

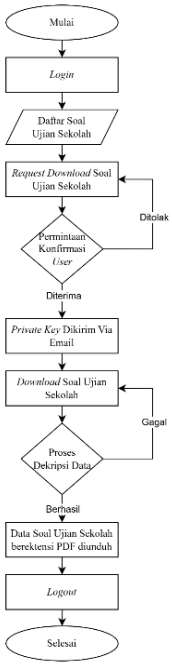
a) Penerapan sistem kepada pengguna.
b) Pemeliharaan berkala, termasuk perbaikan kesalahan (bug fixing), pembaruan keamanan, optimasi performa, dan peningkatan fitur.

B. Perancangan Sistem

1) *Flowchart* Sistem

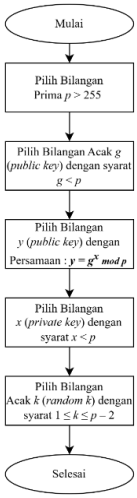


Gambar 2. Flowchart Alur Program User



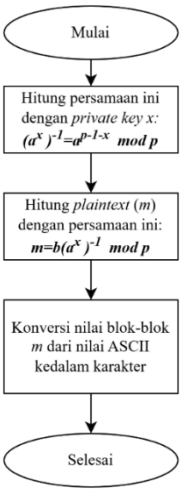
Gambar 3. Flowchart Alur Program Administrator

2) *Flowchart Algoritma ElGamal*



Gambar 4. Flowchart Alur Program User

Gambar 5. Flowchart Alur Program Administrator



Gambar 6. Flowchart Dekripsi

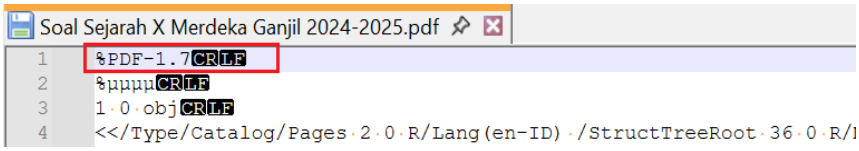
4. HASIL DAN PEMBAHASAN

A. Pengujian Perhitungan Algoritma Kriptografi ElGamal

Pengujian terhadap implementasi algoritma kriptografi ElGamal guna mengukur validitas proses enkripsi dan dekripsi data dalam sistem dengan membangkitkan kunci privat dan kunci public tertentu. Pengujian dilakukan menggunakan satu file soal ujian sekolah berekstensi PDF sebagai sampel data uji. Adapun spesifikasi data uji yang digunakan adalah sebagai berikut:

- Nama file plaintext: Soal Sejarah X Merdeka Ganjil 2024–2025.pdf

- Jumlah sampel plaintext: Karakter pada baris pertama dalam struktur file plaintext, sebanyak 10 karakter.



Gambar 7. Sampel 10 Karakter Awal Pada File Plaintext Sampel

Pada gambar diatas, terlihat bahwa 10 karakter awal berisi karakter %PDF-1.7CR LF yang akan dijadikan sampel untuk dilakukan proses perhitungan enkripsi dan dekripsi algoritma kriptografi ElGamal.

1) Pembangkitan Kunci Publik dan Kunci Privat

Tabel 1. Pembangkitan Kunci Publik Dan Kunci Privat

No	Kunci	Cara Pembangkitan	Nilai	Jenis Kunci
1	p	Statis / Tidak berubah	2503	*Public Key*
2	g	Statis / Tidak berubah	2	*Public Key*
3	y	$y = g^x \bmod p$ $y = 2^{582} \bmod 2503 = 829$	829	*Public Key*
4	x	Dinamis / Berubah tiap data soal ujian	582	*Private Key*

2) Perhitungan Proses Enkripsi Algoritma ElGamal

Tabel 2. Perhitungan Proses Enkripsi Pada ElGamal

No	Karakter	Nilai *ASCII*	Acak k	Proses Perhitungan Enkripsi Elgamal	*Ciphertext*
1	%	37	463	$a = g^k \bmod p$ $a = 2^{463} \bmod 2503 = 631$ $b = y^k m \bmod p$ $b = 829^{463} \bmod 2503$ $b = 1230 * 37 \bmod 2503 = 456$	$a1 = 631$ $b1 = 456$
2	P	80	881	$a = g^k \bmod p$ $a = 2^{881} \bmod 2503 = 358$ $b = y^k m \bmod p$ $b = 829^{881} \bmod 2503$ $b = 949 * 80 \bmod 2503 = 830$	$a2 = 358$ $b2 = 830$
3	D	68	947	$a = g^k \bmod p$ $a = 2^{947} \bmod 2503 = 973$ $b = y^k m \bmod p$ $b = 829^{947} \bmod 2503$ $b = 1171 * 68 \bmod 2503 = 2035$	$a3 = 973$ $b3 = 2035$
4	F	70	415	$a = g^k \bmod p$ $a = 2^{415} \bmod 2503 = 1558$ $b = y^k m \bmod p$ $b = 829^{415} \bmod 2503$ $b = 792 * 70 \bmod 2503 = 374$	$a4 = 1558$ $b4 = 374$
5	-	45	1829	$a = g^k \bmod p$ $a = 2^{1829} \bmod 2503 = 834$ $b = y^k m \bmod p$ $b = 829^{1829} \bmod 2503$ $b = 1117 * 45 \bmod 2503 = 205$	$a5 = 834$ $b5 = 205$
6	1	49	293	$a = g^k \bmod p$ $a = 2^{293} \bmod 2503 = 1402$ $b = y^k m \bmod p$ $b = 829^{293} \bmod 2503$ $b = 412 * 49 \bmod 2503 = 164$	$a6 = 1402$ $b6 = 164$
7	.	46	1175	$a = g^k \bmod p$ $a = 2^{1175} \bmod 2503 = 129$ $b = y^k m \bmod p$ $b = 829^{1175} \bmod 2503$ $b = 564 * 46 \bmod 2503 = 914$	$a7 = 129$ $b7 = 914$
8	7	55	1573	$a = g^k \bmod p$ $a = 2^{1573} \bmod 2503 = 2083$ $b = y^k m \bmod p$ $b = 829^{1573} \bmod 2503$ $b = 1195 * 55 \bmod 2503 = 647$	$a8 = 2083$ $b8 = 647$

No	Karakter	Nilai *ASCII*	Acak *k*	Proses Perhitungan Enkripsi Elgamal	*Ciphertext*
9	CR	13	259	$a = g^k \bmod p$ $a = 2^{259} \bmod 2503 = 1915$ $b = y^k m \bmod p$ $b = 829^{259} \bmod 2503$ $b = 2429 * 13 \bmod 2503 = 1541$	*a9* = 1915 *b9* = 1541
10	LF	10	1841	$a = g^k \bmod p$ $a = 2^{1841} \bmod 2503 = 1972$ $b = y^k m \bmod p$ $b = 829^{1841} \bmod 2503$ $b = 2096 * 10 \bmod 2503 = 936$	*a10* = 1972 *b10* = 936

3) Perhitungan Proses Dekripsi Algoritma ElGamal

Tabel 3. Perhitungan Proses Dekripsi Pada ElGamal

No	*Ciphertext*	Proses Perhitungan dekripsi ElGamal	Nilai *ASCII* (*m*)	Karakter
1	*a1* = 631	$(a^x)^{-1} = a^{p-1-x} \bmod p$ $(a^x)^{-1} = 631^{2503-1-582} \bmod 2503$ $(a^x)^{-1} = 631^{1920} \bmod 2503 = 291$	37	%
	b1 = 456	$m = b(a^x)^{-1} \bmod p$ $m = 456 * 291 \bmod 2503 = 37$		
2	*a2* = 358	$(a^x)^{-1} = a^{p-1-x} \bmod p$ $(a^x)^{-1} = 358^{2503-1-582} \bmod 2503$ $(a^x)^{-1} = 358^{1920} \bmod 2503 = 2292$	80	P
	b2 = 830	$m = b(a^x)^{-1} \bmod p$ $m = 830 * 2292 \bmod 2503 = 80$		
3	*a3* = 973	$(a^x)^{-1} = a^{p-1-x} \bmod p$ $(a^x)^{-1} = 973^{2503-1-582} \bmod 2503$ $(a^x)^{-1} = 973^{1920} \bmod 2503 = 171$	68	D
	b3 = 2035	$m = b(a^x)^{-1} \bmod p$ $m = 2035 * 171 \bmod 2503 = 68$		
4	*a4* = 1558	$(a^x)^{-1} = a^{p-1-x} \bmod p$ $(a^x)^{-1} = 1558^{2503-1-582} \bmod 2503$ $(a^x)^{-1} = 1558^{1920} \bmod 2503 = 1419$	70	F
	b4 = 374	$m = b(a^x)^{-1} \bmod p$ $m = 374 * 1419 \bmod 2503 = 70$		
5	*a5* = 834	$(a^x)^{-1} = a^{p-1-x} \bmod p$ $(a^x)^{-1} = 834^{2503-1-582} \bmod 2503$ $(a^x)^{-1} = 834^{1920} \bmod 2503 = 997$	45	-
	b5 = 205	$m = b(a^x)^{-1} \bmod p$ $m = 205 * 997 \bmod 2503 = 45$		
6	*a6* = 1402	$(a^x)^{-1} = a^{p-1-x} \bmod p$ $(a^x)^{-1} = 1402^{2503-1-582} \bmod 2503$ $(a^x)^{-1} = 1402^{1920} \bmod 2503 = 565$	49	1
	b6 = 164	$m = b(a^x)^{-1} \bmod p$ $m = 164 * 565 \bmod 2503 = 49$		
7	*a7* = 129	$(a^x)^{-1} = a^{p-1-x} \bmod p$ $(a^x)^{-1} = 129^{2503-1-582} \bmod 2503$ $(a^x)^{-1} = 129^{1920} \bmod 2503 = 608$	46	.
	b7 = 914	$m = b(a^x)^{-1} \bmod p$ $m = 914 * 608 \bmod 2503 = 46$		
8	*a8* = 2083	$(a^x)^{-1} = a^{p-1-x} \bmod p$ $(a^x)^{-1} = 2083^{2503-1-582} \bmod 2503$ $(a^x)^{-1} = 2083^{1920} \bmod 2503 = 886$	55	7
	b8 = 647	$m = b(a^x)^{-1} \bmod p$ $m = 647 * 886 \bmod 2503 = 55$		
9	*a9* = 1915	$(a^x)^{-1} = a^{p-1-x} \bmod p$ $(a^x)^{-1} = 1915^{2503-1-582} \bmod 2503$ $(a^x)^{-1} = 1915^{1920} \bmod 2503 = 575$	13	CR
	b9 = 1541	$m = b(a^x)^{-1} \bmod p$ $m = 1541 * 575 \bmod 2503 = 13$		
10	*a10* = 1972	$(a^x)^{-1} = a^{p-1-x} \bmod p$ $(a^x)^{-1} = 1972^{2503-1-582} \bmod 2503$ $(a^x)^{-1} = 1972^{1920} \bmod 2503 = 2380$	10	LF

No	*Ciphertext*	Proses Perhitungan dekripsi ElGamal	Nilai *ASCII* (*m*)	Karakter
	$b10 = 936$	$m = b(a^x)^{-1} \; mod \; p$		
		$m = 936 * 2380 \; mod \; 2503 = 10$		

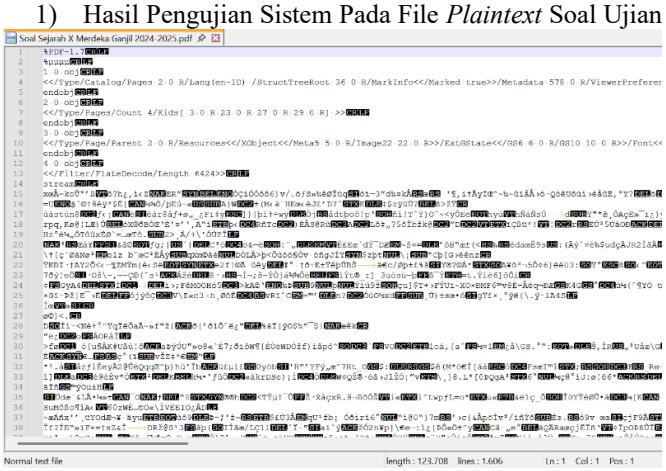
B. Hasil Pengujian Pada Sistem

Pengujian difokuskan pada proses enkripsi dan dekripsi terhadap file sampel untuk mengevaluasi kinerja algoritma ElGamal dalam mengamankan data soal ujian. Sampel file ini digunakan untuk menguji keakuratan proses enkripsi plaintext menjadi ciphertext dan sebaliknya, serta untuk memastikan bahwa hasil dekripsi identik dengan data asli tanpa terjadi perubahan atau kehilangan informasi.

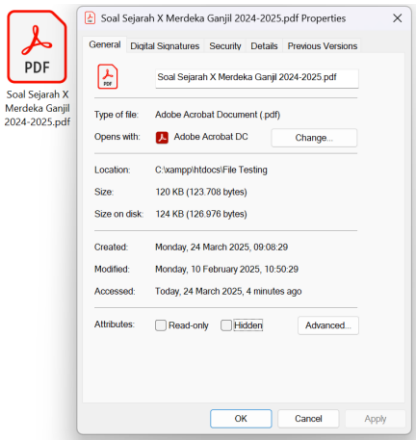
Adapun spesifikasi data uji yang digunakan adalah sebagai berikut:

- Nama file plaintext: Soal Sejarah X Merdeka Ganjil 2024–2025.pdf
- Ukuran file plaintext: 120 kilobyte atau setara dengan 123.708 byte

1) Hasil Pengujian Sistem Pada File *Plaintext* Soal Ujian



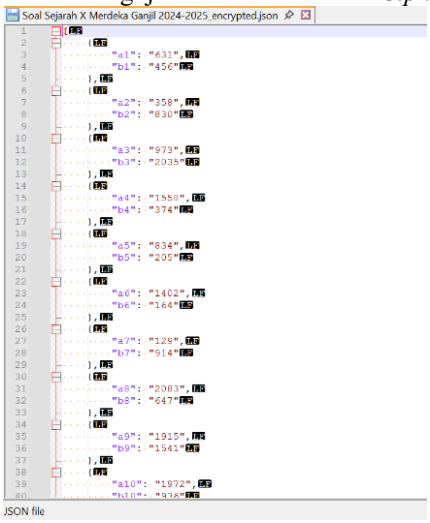
Gambar 8. Struktur File Plaintext Berekstensi PDF



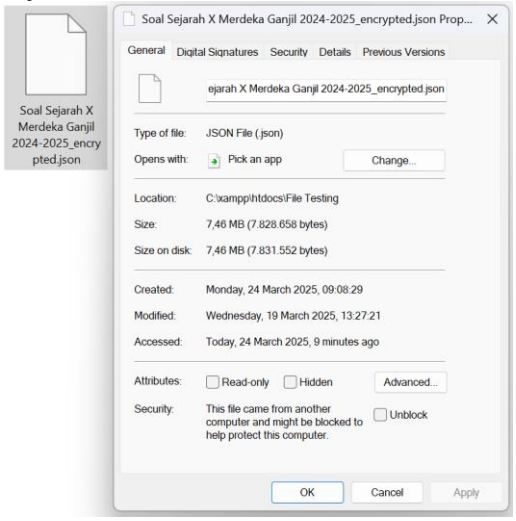
Gambar 9. Ukuran File Plaintext Berekstensi PDF

Hasil pengujian sistem terhadap file *plaintext* soal ujian dalam format PDF menunjukkan struktur internal file yang diamati melalui aplikasi Notepad++ berisi sekumpulan karakter yang disusun sedemikian rupa, tiap-tiap karakter ini yang nantinya akan dilakukan perhitungan hingga seluruh karakter dienkripsi menggunakan algoritma kriptografi ElGamal. Pengamatan selanjutnya dilakukan untuk membandingkan struktur file sebelum proses enkripsi menggunakan algoritma kriptografi ElGamal. Selain itu, ditampilkan pula ukuran file PDF sebelum dilakukan proses enkripsi yaitu sebesar 120KB atau setara 123.708 bytes.

2) Hasil Pengujian Sistem Pada File *Ciphertext* Soal Ujian



Gambar 10. Struktur File Ciphertext Berekstensi JSON



Gambar 11. Ukuran File Ciphertext Berekstensi JSON

Hasil pengujian terhadap *file ciphertext* pada sistem, menunjukkan perubahan struktur *file* soal ujian setelah dienkripsi menggunakan algoritma ElGamal. *File* yang semula berekstensi PDF diubah menjadi JSON sesuai dengan format *array* yang berisi nilai [{"a1": "631", "b1": "456"}, {"a2": "358", "b2": "830"}, {"aN": "…", "bN": "…"}]. Nilai-nilai diatas adalah nilai yang mewakili *a* dan *b* hasil *ciphertext* pada perhitungan algoritma kriptografi ElGamal. Pada ukuran *file* juga menunjukkan bahwa *file ciphertext* soal ujian dengan ekstensi JSON mngalami perubahan mencapai 7,47 MB (7.828.658 bytes). Terjadi peningkatan signifikan dari ukuran file asli yang semula sebesar 120 KB (123.708 bytes) menjadi 7,47 MB setelah proses enkripsi.

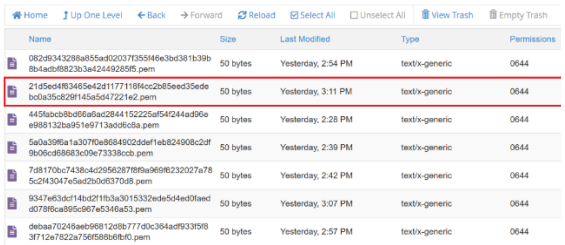
3) Hasil Pengujian Sistem *Generate Key* Pada *Public Key* dan *Private Key*

Hasil pengujian terhadap proses pembangkitan kunci menunjukkan bagaimana sistem menghasilkan pasangan *public key* dan *private key*. Pada sistem ini, terdapat dua jenis mekanisme pembangkitan kunci: (1) *public key* yang dibangkitkan secara statis dan hanya berubah apabila terdapat modifikasi pada struktur kode PHP, serta (2) *private key* yang dibangkitkan secara dinamis setiap kali *file* soal ujian diunggah. Gambar berikut memperlihatkan hasil pembentukan kedua jenis kunci tersebut oleh sistem.

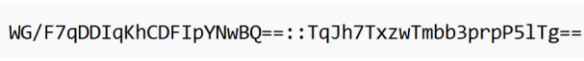
```php
// Konfigurasi ElGamal
$p = 2503; // Bilangan prima besar
$g = 2;     // Generator untuk grup

// Fungsi untuk membangkitkan publik key dan private key
function generate_keys($p, $g) {
    $x = random_int(1, $p - 2); // Kunci privat harus berada di antara 1 dan p-2
    $y = bcpowmod($g, $x, $p); // Kunci publik: y = g^x mod p

    return [
        'public' => ['p' => $p, 'g' => $g, 'y' => $y],
        'private' => $x
    ];
}
```

Gambar 12. Penulisan Code Generate Key Pada Public Key dan Private Key

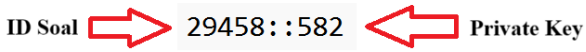
Gambar di atas menunjukkan bahwa kunci publik terdiri dari nilai *p* dan *g* yang dibangkitkan secara statis. Sementara itu, kunci privat *x* dibangkitkan secara acak menggunakan fungsi *random_int*, yang menghasilkan angka acak antara 1 hingga dua angka sebelum nilai maksimum *p* (yaitu 2503). Nilai kunci publik *y* kemudian dihitung menggunakan fungsi *bcpowmod*, yang merupakan hasil perpangkatan modular antara *g* dan *x* dengan modulo *p*. Setelah public key digunakan untuk perhitungan enkripsi, selanjutnya *private key x* akan disimpan dalam *file* kunci dengan ekstensi PEM yang juga akan dilakukan proses *hashing* menggunakan kunci PIN agar menjaga keamanan *private key* tidak dapat terbaca dan diliat oleh pihak yang tidak berwenang.



Gambar 13. Pembangkitan Private Key Pada File PEM

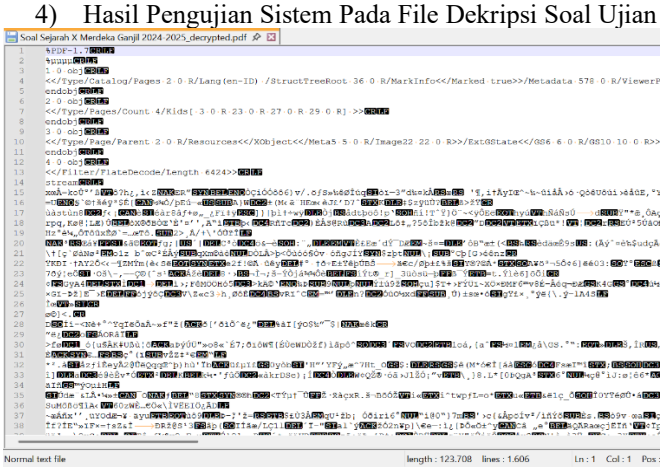


Gambar 14. Isi Private Key File PEM yang Dienkripsi

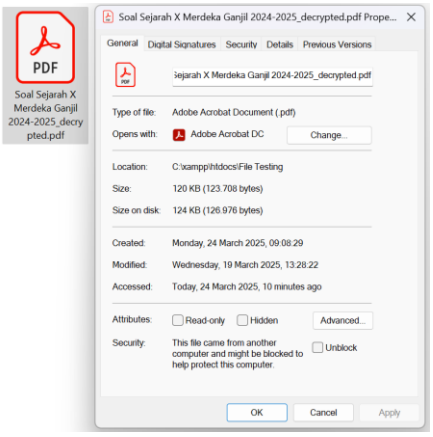


Gambar 15. Isi Private Key File PEM yang Didekripsi

4) Hasil Pengujian Sistem Pada File Dekripsi Soal Ujian



Gambar 16. Struktur File Ciphertext Berekstensi JSON



Gambar 17. Ukuran File Plaintext Berekstensi JSON

Hasil pengujian sistem terhadap *file* dekripsi soal ujian dalam format PDF menunjukkan struktur internal *file* yang diamati melalui aplikasi *Notepad++* kembali menjadi sekumpulan karakter yang disusun sedemikian rupa seperti struktur *file plaintext*. Dengan struktur yang identik persis seperti sebelumnya, maka *file* soal ujian berekstensi PDF ini sudah dapat dibuka kembali seperti sebelum dilakukan enkripsi. Pada ukuran *file* juga kembali seperti sebelum dilakukan enkripsi yaitu sebesar 120KB atau setara 123.708 *bytes*.

5. KESIMPULAN

Hasil pengujian sistem menunjukkan adanya perubahan signifikan pada struktur dan ukuran *file* soal ujian setelah proses enkripsi menggunakan algoritma ElGamal. File asli berformat PDF dengan ukuran 120 KB (123.708 *bytes*) mengalami perubahan menjadi *file ciphertext* berformat JSON dengan ukuran 7,47 MB (7.828.658 *bytes*). Perubahan ini diamati melalui aplikasi *Notepad++* untuk membandingkan struktur *file* sebelum dan sesudah enkripsi, menunjukkan bahwa proses enkripsi berhasil mengubah format dan meningkatkan kompleksitas data secara signifikan. Meskipun terjadi pembesaran ukuran *file*, hasil dekripsi menunjukkan bahwa *file* soal ujian berhasil dikembalikan ke format dan isi aslinya secara utuh, baik dari segi struktur maupun kontennya, sehingga membuktikan bahwa proses enkripsi dan dekripsi menggunakan algoritma ElGamal berjalan dengan baik dan benar.

Tabel 4. Data Perbandingan File Sebelum dan Sesudah Enkripsi Serta Dekripsi

Aspek	Sebelum Enkripsi	Sesudah Enkripsi	Sesudah Dekripsi
Nama File	*Soal Sejarah X Merdeka Ganjil 2024–2025.pdf*	*Soal Sejarah X Merdeka Ganjil 2024–2025_encrypted.json*	*Soal Sejarah X Merdeka Ganjil 2024–2025_decryped.pdf*
Ekstensi File	PDF	JSON	PDF
Ukuran File	120 KB (123.708 *bytes*)	7,47 MB (7.828.658 bytes)	120 KB (123.708 *bytes*)
Struktur File	Format PDF standar	Format JSON (nilai *a* & *b*)	Format PDF standar
Pembaca pdf	Dapat dibaca langsung	Tidak dapat dibaca langsung	Dapat dibaca langsung

REFERENSI

Alfirdaus, M. H., Tahir, M., Dewanti, N. E., Ardianto, R., Azurah, N. N., & Cahyono, N. F. (2023). Perancangan aplikasi enkripsi deskripsi menggunakan metode Caesar Chiper berbasis web. *Jurnal Teknik Mesin, Industri, Elektro dan Informatika (JTMEI)*, *2*(2), 64–76.

Annas, F. (2020). Perancangan sistem informasi bank soal online di SMP Negeri 3 Matur. *Journal Educative: Journal of Educational Studies*, *4*(2), 150. https://doi.org/10.30983/educative.v4i2.2522

Baraka. (2023). Mengenal apa itu private dan public key dalam dunia digital? *Biro Perencanaan Sumber Daya Manusia dan Karir (BARAKA)*. https://baraka.uma.ac.id/mengenal-apa-itu-private-dan-public-key-dalam-dunia-digital

Butarbutar, R. (2023). Kejahatan siber terhadap individu: Jenis, analisis, dan perkembangannya. *Jurnal Hukum & Pembangunan*, *2*(2). https://doi.org/10.21143/telj.vol2.no2.1043

Harahap, A. Y. N., Gunawan, H., Nst, A. B., & Sari, R. E. (2022). Penerapan ElGamal guna meningkatkan keamanan data text dan docx. *IT (Informatic Technique) Journal*, *10*(1), 76. https://doi.org/10.22303/it.10.1.2022.76-86

Mallouli, F., Hellal, A., Saeed, N. S., & Alzahrani, F. A. (2019). A survey on cryptography: Comparative study between RSA vs ECC algorithms, and RSA vs El-Gamal algorithms. In *Proceedings of the 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud 2019) and the 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom 2019)* (pp. 173–176). https://doi.org/10.1109/CSCloud/EdgeCom.2019.00022

Nugraha, S. N. (2024). Penerapan algoritma kriptografi ElGamal pada aplikasi pengamanan pesan berbasis website. *Jurnal Informatika dan Teknik Elektro Terapan*, *12*(3). https://doi.org/10.23960/jitet.v12i3.4794

Qhorifadillah, U., Lestari, S., & Chulkamdi, M. T. (2022a). Perancangan aplikasi bank soal berbasis website dengan algoritma Fisher-Yates shuffle dan cosine similarity (Studi kasus di SMK Indraprasta Wlingi). *JATI (Jurnal Mahasiswa Teknik Informatika)*, *6*(1), 352–359. https://doi.org/10.36040/jati.v6i1.4232

Ramadhani, S., & Tanti, L. (2024). Rancang bangun aplikasi keamanan data penjualan menggunakan metode ElGamal berbasis web pada PT Pixelindo. *Jurnal Teknologi dan Informatika*, *1*, 985–1001.

Riza, F., Muttaqin, M., Pandia, S., Mufida, F. D., Siregar, R., Adytia, P., Wahyuni, W., Simarmata, T. M. D. J., & Lubis, M. (2020). *Pengantar ilmu kriptografi*. *Journal GEEJ*, *7*(2).

Saputro, T. H., Hidayati, N., & Ujianto, E. I. H. (2020). Survei tentang algoritma kriptografi asimetris. *Jurnal Informatika Polinema*, *6*(2), 67–72. https://doi.org/10.33795/jip.v6i2.345

Suhardi, I. (2023). *Pengembangan bank soal berbasis computer-based testing*. [Laporan/Artikel tidak diterbitkan atau tanpa informasi jurnal]

Wardani, W. K., Faruq, H. A. A., & Bakti, B. S. (2024). Desain dan implementasi aplikasi bank soal berbasis web pada lembaga kursus tingkat sekolah dasar "Pak Slamet". *Jurnal Smart Teknologi*, *5*(5). http://jurnal.unmuhjember.ac.id/index.php/JST

Wijoyo, A., Rahmawati, T., Agustin, W., Saputra, B. M., & Kurdi. (2023). Perlindungan data sensitif: Enkripsi sebagai pilar utama keamanan komputer. *CHIPSET: Jurnal Ilmu Komputer, Teknik, dan Multimedia*, *1*(2), 84–91. https://jurnal.publikasimahasiswa.id/index.php/chipset

Ziaurrahman, M., Utami, E., & Wibowo, F. W. (2019). Modifikasi kriptografi klasik Vigenère cipher menggunakan one time pad dengan enkripsi berlanjut. *Jurnal Informasi Interaktif*, *4*(2).