IMPLEMENTASI ALGORITMA *AES* DAN *ELGAMAL* UNTUK ENKRIPSI DAN DEKRIPSI FILE DATA VIDEO MP4 BERBASIS WEB

Imam Hafaz, Nur Wulan, Munjiat Setiani Asih
Teknik Informatika, Universitas Harapan Medan
Jalan HM Joni No 70 Medan
Imam007p@gmail.com

ABSTRAK

Dalam era perkembangan teknologi saat ini, pertukaran data melalui jaringan internet telah menjadi suatu keharusan yang dilakukan manusia sehari-hari, konten video menjadi salah satu teknologi media komunikasi yang banyak digunakan. Era saat ini data video telah mengalami pertumbuhan yang sangat signifikan. Banyak individu dan organisasi menghasilkan, menyebarkan, dan menyimpan video dalam format MP4. metode *Advanced Encryption Standard (AES)* dan *Elgamal* dapat dilakukan dengan meng*implementasi*kan algoritma enkripsi dan dekripsi pada web *server*. Data video akan di enkripsi menggunakan kunci *Elgamal* yang telah terenkripsi menggunakan kunci *Advanced Encryption Standard (AES)* yang dipilih secara acak, dimana kunci *Elgamal* tersebut akan dienkripsi terlebih dahulu menggunakan kunci *Advanced Encryption Standard (AES)*, lalu akan menghasilkan kunci pribadi dan kunci publik *Elgamal*, kunci publik *Elgamal* digunakan untuk enkripsi data video dan kunci pribadi *Elgamal* digunakan untuk dekripsi data video, sehingga hanya pihak yang memiliki kunci pribadi *Elgamal* yang dapat mengakses dan membuka data video. Dengan cara ini, data video dapat dijamin keamanan dan kerahasiaanya saat di bagikan atau disimpan dalam jaringan internet.

***Kata kunci**: Enkripsi Data Video, AES, Elgamal, Keamanan Data, Aplikasi Berbasis*

1. PENDAHULUAN

Dalam era perkembangan teknologi saat ini, pertukaran data melalui jaringan internet telah menjadi suatu keharusan yang dilakukan manusia sehari-hari, konten video menjadi salah satu teknologi media komunikasi yang banyak digunakan. Era saat ini data video telah mengalami pertumbuhan yang sangat signifikan. Banyak individu dan organisasi menghasilkan, menyebarkan, dan menyimpan video dalam format MP4. Ini mencakup konten seperti video streaming, rekaman konferensi, tutorial online, hiburan, dan banyak lagi. Seiring berjalannya waktu, data video menjadi salah satu media komunikasi yang harus dijaga kerahasiaan dan keamanannya karena sangat rentan terhadap resiko keamanan, seperti penyadapan, peretasan, dan perubahan data. Ini dapat mengakibatkan kerugian serius, baik dalam hal privasi pengguna maupun integritas konten video itu sendiri.

Data video MP4 yang disimpan dan ditransmisikan melalui web rentan terhadap risiko keamanan, seperti penyadapan, peretasan, dan perubahan data. Ini dapat mengakibatkan kerugian serius, baik dalam hal privasi pengguna maupun integritas konten video itu sendiri. Oleh karena itu, perlindungan data video yang efektif menjadi sangat penting.

Kriptografi bertujuan untuk menjaga keamanan dan kerahasian informasi dalam bentuk yang tidak dapat dipahami hal ini agar terhindar dari pihak yang tidak berkepentingan atas akses data tersebut [1] . Enkripsi data merupakan proses mengubah pesan atau data asli menjadi bentuk yang tidak dapat dibaca atau dimengerti oleh pihak yang tidak berwenang [1]

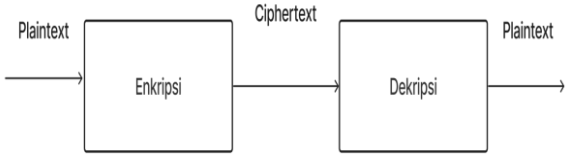
Dalam lingkup keamanan data, enkripsi dan dekripsi merupakan cara yang efektif untuk melindungi data dari akses yang tidak sah. Keamanan informasi adalah suatu hal yang sangat penting untuk dilakukan, karena pada perkembangan teknologi sekarang ini informasi sangat rawan atas peretasan dan pencurian data oleh pihak yang tidak berwenang atas data tersebut [2]. Salah satu keamanan yang dapat digunakan yaitu dengan algoritma Advanced Encryption Standard (AES) dan Elgamal adalah dua algoritma enkripsi yang telah terbukti aman dan banyak digunakan karena memiliki tingkat keamanan dan kecepatan enkripsi yang tinggi. Implementasi keduanya untuk enkripsi dan dekripsi file data video MP4 di lingkungan web adalah solusi yang terbaik untuk mengatasi masalah keamanan data [3].

Dalam konteks implementasi berbasis web, enkripsi dan dekripsi data video menggunakan algoritma Advanced Encryption Standard (AES) dan Elgamal dapat dilakukan dengan mengimplementasikan algoritma enkripsi dan dekripsi pada web server. Data video akan di enkripsi menggunakan kunci Elgamal yang telah terenkripsi menggunakan kunci Advanced Encryption Standard (AES) yang dipilih secara acak, dimana kunci Elgamal tersebut akan dienkripsi terlebih dahulu menggunakan kunci Advanced Encryption Standard (AES), lalu akan menghasilkan kunci pribadi dan kunci publik Elgamal, kunci publik Elgamal digunakan untuk enkripsi data video dan kunci pribadi Elgamal digunakan untuk dekripsi data video, sehingga hanya pihak yang memiliki kunci pribadi Elgamal yang dapat mengakses dan membuka data video. Dengan cara ini, data video dapat dijamin

keamanan dan kerahasiaanya saat di bagikan atau disimpan dalam jaringan internet.

2. TINJAUAN PUSTAKA

Kriptografi adalah ilmu dan seni untuk melindungi informasi dengan mengubahnya menjadi format yang tidak dapat dimengerti oleh siapa pun kecuali pihak yang memiliki kunci khusus untuk mengembalikannya ke bentuk asli. Proses ini dikenal sebagai enkripsi, sedangkan proses untuk mengembalikan informasi yang telah dienkripsi ke bentuk aslinya disebut dekripsi [4].



Gambar 1. Mekanisme Enkripsi dan Dekripsi.

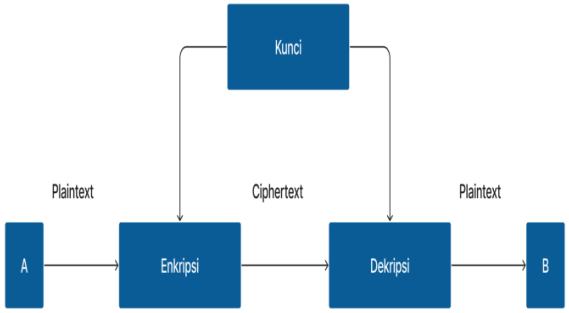
Dalam kriptografi, terdapat dua jenis utama algoritma yang digunakan untuk enkripsi dan dekripsi data: algoritma Simetris dan algoritma asimetris. Kedua jenis ini memiliki karakteristik, keuntungan, dan kelemahan yang berbeda, yang membuat mereka cocok untuk berbagai aplikasi [5]

Terdapat 4 aspek keamanan pada algoritma kriptografi:[3]

a. Kerahasiaan. Pesan (Plaintext) hanya dapat dimengerti oleh pihak yang memliki kewenangan.
b. Autentikasi. Pengirim pesan harus dapat menetapkan dengan pasti, bahwa penyusup harus dipastikan tidak bisa diam-diam menjadi orang lain.
c. Integritas. Penerima pesan harus dapat menetapkan bahwa pesan yang diterima tidak ada perubahan ketika sedang dalam proses pengiriman data.
d. Non-Repudiation. Pengirim pesan harus tidak bisa membantah pesan yang dia kirimkan.

2.1. Algoritma Kriptografi Simetris

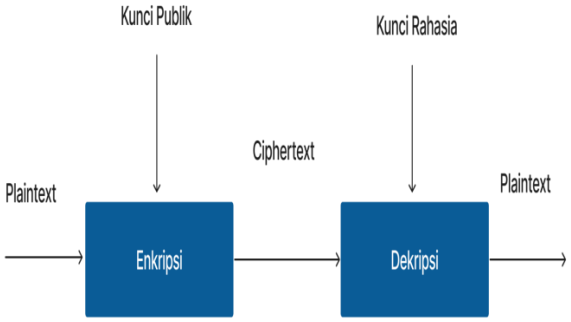
Algoritma kriptografi Simetris menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi. Kunci ini harus dijaga kerahasiaannya dan hanya diketahui oleh pihak yang berwenang.



Gambar 2. Algoritma Kriptografi *Simetris*.

2.2. Algoritma Kriptografi Asimetris

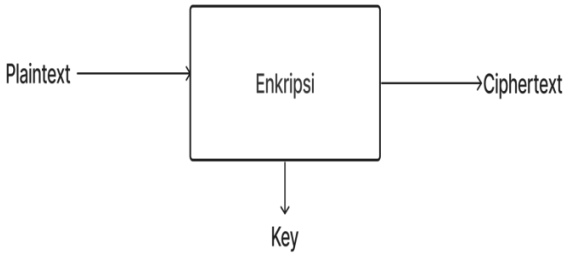
Algoritma kriptografi asimetris menggunakan dua kunci yang berbeda namun berkaitan: kunci publik dan kunci pribadi. Kunci publik digunakan untuk enkripsi, sementara kunci pribadi digunakan untuk dekripsi.



Gambar 3. Algoritma Kriptografi Asimetris.

2.3. Enkripsi

Enkripsi adalah proses mengubah informasi asli (Plaintext) menjadi bentuk yang tidak dapat dimengerti (ciphertext) menggunakan algoritma enkripsi dan kunci enkripsi. Tujuan dari enkripsi adalah untuk melindungi kerahasiaan data sehingga hanya pihak yang memiliki kunci yang sesuai dapat mengakses informasi asli.



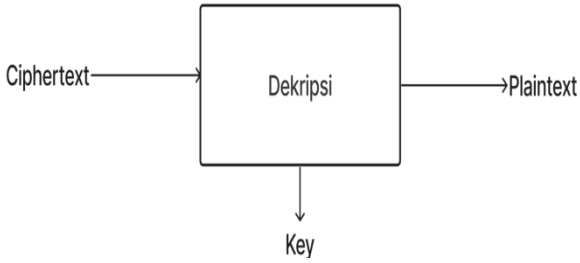
Gambar 4. Proses Enkripsi.

Proses Enkripsi

a. Plaintext: Data asli yang ingin dilindungi.
b. Algoritma Enkripsi: Serangkaian instruksi matematis yang mengubah Plaintext menjadi ciphertext.
c. Kunci Enkripsi: Nilai rahasia yang digunakan oleh algoritma enkripsi untuk melakukan transformasi.

2.4. Dekripsi

Dekripsi adalah proses mengubah ciphertext kembali menjadi informasi asli (Plaintext) menggunakan algoritma dekripsi dan kunci dekripsi [6].



Gambar 5. Proses Dekripsi

Proses Dekripsi

a. Ciphertext: Data terenkripsi yang tidak dapat dimengerti.
b. Algoritma Dekripsi: Serangkaian instruksi matematis yang mengubah ciphertext kembali menjadi Plaintext.
c. Kunci Dekripsi: Nilai rahasia yang digunakan oleh algoritma dekripsi untuk melakukan transformasi.

2.5. AES (Advanced Encryption Standard)

AES (Advanced Encryption Standard) adalah algoritma enkripsi Simetris yang diadopsi sebagai standar oleh pemerintah Amerika Serikat dan banyak digunakan di seluruh dunia untuk mengamankan data sensitif. AES menggantikan algoritma DES (Data Encryption Standard) yang sebelumnya digunakan secara luas. AES termasuk algoritma enkripsi Simetris yang kuat dan efisien. AES termasuk dalam kategori kriptografi Key satu arah (Simetris) [7]. Ada tiga kriteria utama pemilihan *AES* yaitu: keamanan, harga dan karakteristik algoritma beserta *implementasi*nya [8].

Empat prosesutama algoritma *AES* yaitu sebagai berikut : [9].

a. *SubBytes* (Transformasi *Substitusi Byte*)
b. *ShiftRow* (Transfornasi Pergeseran Baris)
c. *MixColumns* (Transformasi Percampuran Kolom)
d. *AddRoundKey* (Transformasi Penambahan Kunci)

2.6. *Elgamal*

Elgamal adalah algoritma kriptografi *asimetris* yang digunakan untuk enkripsi dan dekripsi data serta pembuatan dan verifikasi tanda tangan digital. Algoritma ini didasarkan pada konsep logaritma diskret, dan diperkenalkan oleh Taher *Elgamal* pada tahun 1985. Keamanan *Elgamal* bergantung pada kesulitan komputasi masalah logaritma diskret dalam kelompok bilangan besar. Algoritma *Elgamal* memiliki dua kunci yaitu kunci publik dan kunci pribadi [10].

2.7. Algoritma *Elgamal*

Algoritma *Elgamal* memerlukan 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 yang memenuhi persamaan [10].

Dari persamaan y= gx mod p nilai y, g dan p merupakan pasangan kunci publik sedangkan x, p merupakan pasangan kunci pribadi. Besaran-besaran yang digunakan dalam algoritma kriptografi *Elgamal* adalah : [10].

a. Bilangan prima *p* bersifat tidak rahasia.
b. Bilangan acak g (g <p) bersifat tidak rahasia
c. Bilangan acak x (x <p) bersifat rahasia.
d. Bilangan y bersifat tidak rahasia.
e. m (*Plaintext*) bersifat rahasia merupakan pesan
f. asli yang digunakan untuk data
g. sumber dalam proses enkripsi dan merupakan data hasil pada proses dekripsi.
h. a dan b (*ciphertext*) bersifat tidak rahasia.

Algoritma ini memproses enkripsi dilakukan dengan memilih bilangan acak k yang berada dalam himpunan $1 \leq k \leq p-2$. Setiap blok *Plaintext* m dienkripsi dengan persamaan:

a = gk mod p
b = yk mod p

Proses dekripsi menggunakan kunci pribadi x dan p untuk mendekripsi a dan b menjadi *Plaintext* m dengan persamaan :

(ax)-1 = ap-1-x mod p
m =b*ax mod p .

Sehingga *Plaintext* dapat ditemukan kembali dari pasangan *ciphertext* adan b.

2.8. Keamanan Informasi

Pada saat ini informasi adalah salah satu hal yang sangat penting dalam suatu komoditi bagi sebuahl embaga pemerintahan, perguruan tinggi, organisasi serta individu [7].

2.9. Data Video

Video merupakan salah satu media *elektronik* yang didalamnya terdapat serangkaian gambar gerak yang disertai gabungan teknologi audio dan visual yang menghasilkan bentuk frame atau gambar yang bergerak menjadi dinamis dan menarik [12]. Data video merupakan bentuk data yang gampang diakses oleh siapa saja. Data video merujuk pada informasi yang direkam dalam format visual bergerak, yang biasanya disimpan sebagai file *digital*. Video data mencakup sejumlah frame gambar yang ditampilkan dalam urutan cepat untuk menciptakan ilusi gerakan, sering kali disertai dengan audio untuk memperkaya pengalaman penonton.

2.10. *Flowchart*

Flowchart adalah diagram yang menggambarkan alur kerja atau proses secara visual menggunakan simbol-simbol standar. *Flowchart* membantu dalam memahami, menganalisis, dan mendokumentasikan berbagai proses atau sistem dalam berbagai bidang. Kegunaan flowchart yaitu untuk memberikan gambaran *visualisasi* jalur

eksekusi dan logika pada suatu program secara jelas dan mudah untuk dipahami [9].

2.11. *Diagram Unified Modeling Language (UML)*

Unified Modeling Language (UML) bekerja dalam *OOAD* (*Object-Oriented Analysis Design*) pada sistem arsitektur yang menggunakan satu bahasa konsisten untuk mem*visualisasi*, membangun dan mendokumentasi *artifact*. *UML* adalah alat yang sangat berguna dalam pengembangan perangkat lunak, memberikan cara yang terstruktur untuk memahami dan mendokumentasikan desain sistem, serta membantu dalam komunikasi yang efektif di antara semua pihak yang terlibat.*UML(Unified Modeling Language)* merupakan salah satu bahasa yang populer dan banyak digunakan untuk membantu membuat suatu analisis desain dan menggambarkan bentuk arsitektur objek [13].

Terdapat empat macam diagram yang sering digunakan, yaitu :

a. *Use Case*
b. *Class Diagram*
c. *Activity Diagram*
d. *Sequence Diagram.*

3. METODE PENELITIAN

3.1. Analisis Sistem

Analisis sistem merupakan suatu sistem informasi yang lengkap dengan beberapa bagian di dalamnya, tujuannya adalah agar dapat mengevaluasi dan *mengidentifikasi* berbagai bentuk permasalahan yang menghambat sistem, oleh karena itu analisis sistem dibuat untuk dapat mempertahankan, memitigasi, memperbaiki dan mengembangkan.

Berikut merupakan analisis sistem aplikasi data video menggunakan algoritma *AES* dan *Elgamal* berbasis web:

a. Tujuan Sistem
   - Memiliki tingkat keamanan yang tinggi untuk melindungi data video dalam proses enkripsi data video.
   - Memiliki tingkat kecepatan yang optimal dalam proses enkripsi dan dekripsi.

b. Fungsi Utama Sistem
   Aplikasi ini memiliki dua fungsi utama, yaitu :
   - *Generate* kunci
   - Enkripsi dan dekripsi.

c. Arsitektur Sistem
   - Komponen sistem
   - Aplikasi web
   - *Server*
   - Penyimpanan
   - Algoritma enkripsi
   - Manajemen kunci.
   - Enkripsi dan dekripsi

d. Proses Enkripsi
   - *Generate* kunci
   - Enkripsi kunci *simetris*
   - Enkripsi data video

e. Proses Dekripsi
   - Dekripsi kunci *Elgamal*
   - Dekripsi data video

f. Keamanan
   - Keamanan *Elgamal*
   - Keamanan *AES*

g. Pengujian dan Validasi
   - Uji keamanan
     Untuk *mengidentifikasi* kerentanan dan perbaikan diperlukan pengujian keamanan untuk melihat seberapa efesien tingkat keamanan data.
   - Uji kinerja
     Untuk mengukur waktu respon dan kecepatan proses enkripsi dan dekripsi data diperlukan uji kinerja.

3.2. Analisis Masalah

Dalam mengembangkan sistem aplikasi data video berbasis web yang menggunakan algoritma enkripsi *AES* dan *Elgamal*, terdapat beberapa aspek yang perlu dianalisis untuk memastikan bahwa sistem tersebut dapat berjalan dengan optimal dan aman.

Berikut adalah analisis masalah berdasarkan beberapa aspek penting :

a. Keamanan Data
   Masalah:
   - Ancaman Peretasan: Data video yang tidak terenkripsi bisa saja diakses oleh pihak yang tidak berwenang jika *server* diretas.
   - *Man-in-the-Middle Attack*: Selama proses pengiriman kunci atau video terenkripsi, ada risiko serangan *man-in-the-middle* yang dapat memintas data.
   - Kehilangan atau Pencurian Kunci Pribadi: Jika kunci pribadi pengguna dicuri atau hilang, semua data video terenkripsi dapat terancam.

   Solusi:
   - Menggunakan *HTTPS* untuk semua komunikasi data.
   - *Implementasi* algoritma pengelolaan kunci yang aman seperti penyimpanan
   - kunci pribadi di perangkat pengguna dan perlindungan dengan *password* kuat.
   - *Otentikasi* dua faktor untuk mengamankan akun pengguna.

3.3. Analisis Kebutuhan *Hardware* Dan *Software*

Dalam proses merancang sistem enkripsi dan dekripsi data video berbasis web, penulis membutuhkan beberapa perangkat yang dapat mendukung berjalannya sistem ini, di antaranya yaitu:

3.3.1. *Hardware* (Perangkat Keras)

Kebutuhan *hardware* diantaranya, yaitu :

a. *Server*
   - *CPU*
   - Penyimpanan

- *RAM*

b. *Klien* (Pengguna)
- Perangkat
- *RAM*

3.3.2. *Software* (Perangkat Lunak)

Kebutuhan Software diantaranya, yaitu :

a. Sistem operasi
- *Server*
  Dibutuhkan sistem operasi yang dapat mendukung pengembangakn aplikasi web, maka bisa memilih salah satu sistem operasi seperti windows *server* atau linux (contohnya *CentOS* atau *Ubuntu*).
- *Klien* (pengguna)
  Ada beberapa sistem operasi yang digunakan seperti windows, linux, atau macOS.

b. Library dan algoritma
- *Elgamal*
  Pada bagian ini menggunakan library dan modul yang mencakup *implementasi* algoritma *Elgamal* seperti *cryptography library.*
- *AES*
  Pada *AES* ini memakai library atau modul yang mencakup *implementasi* algoritma *AES* seperti *pycryptodome* atau *cryptojs*.
- Analisis Perancangan Sistem
  Analisis perancangan sistem merupakan tahap yang menggambarkan proses apa saja yang akan dibuat pada sistem berbasis web ini. Berikut analisis beberapa aspek perancangan sistem aplikasi enkripsi data video dengan menggunakan algoritma *Elgamal* dan *AES* berbasis web :

3.4. Arsitektur Aplikasi

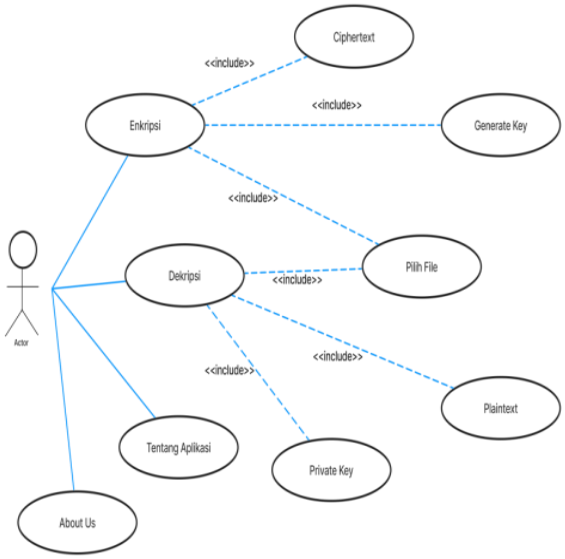
a. Antarmuka pengguna
b. *Server*
c. Basis data
d. Modul enkripsi dan dekripsi
e. Manajemen kunci
f. Antarmuka user

3.5. Perancangan Sistem

Pada bagian ini penulis merancang dan memberikan penjelasan mengenai alur dan tahapan dari sistem enkripsi dan dekripsi data video berbasis web menggunakan algoritma *AES* dan *Elgamal* yang akan dibuat.

3.6. *Use Case* Enkripsi dan Dekripsi

Berikut ini penulis membuat rancangan dan penjelasan dari *use case* pada gambar 6 menunjukan tahapan proses terjadinya enkripsi dan dekripsi data video. Berikut penjelasan alur *use case* tersebut :



Gambar 6. *Use Case* Enkripsi dan Dekripsi

Pengguna mengakses situs web dan akan menuju halaman utama enkripsi, dekripsi, halaman tentang aplikasi menggunakan algoritma *AES* dan *Elgamal* dan halaman *about us*.

a. Pengguna bisa memilih enkripsi untuk mengenkripsikan data video caranya pengguna hanya mengunggah atau mengupload data video dan memasukkan kunci *Plaintext* lalu *Generate key*.
b. Sistem akan menghasilkan sepasang kunci *Elgamal*, yaitu kunci publik dan kunci pribadi yang telah terenkripsi menggunakan kunci *AES*.
c. Lalu ketika melakukan *Generate key*, pengguna akan mendapatkan *private key* yang akan langsung terdownload, yang mana *private key* ini akan digunakan untuk mendekripsikan data video yang telah terenkripsi.
d. Selanjutnya ketika pengguna mengklik tombol submit, maka pengguna akan mendapatkan *ciphertext* yang akan langsung terdownload.
e. Dalam prosesnya video akan terbagi menjadi blok-blok kecil yang akan dienkripsi menggunakan kunci publik *Elgamal* yang dihasilkan dari algoritma *AES* dan akan melakukan iterasi untuk setiap blok data video.
f. Jika proses enkripsi selesai, maka video akan terdownload otomatis
g. Enkripsi data video selesai.
h. Dalam proses dekripsi, pengguna mengunggah atau mengirim data video yang sudah dienkripsi beserta *ciphertext* nya.
i. Lalu pengguna juga mengupload *private key* untuk mendekripsikan data video yang telah terenkripsi.
j. Dalam proses dekripsi data video, operasi yang dilakukan adalah membagi data video menjadi blok-blok kecil.
k. Lalu terjadi proses dekripsi menggunakan *private key* dan *ciphertext*.

l. Ketika proses dekripsi selesai, data video akan otomatis terdownload ke folder.
m. Proses dekripsi selesai.

4. HASIL DAN PEMBAHASAN

4.1. Memuat hasil, Evaluasi Keamanan Algoritma

Dalam evaluasi keamanan algoritma implementasi algoritma *AES* dan *Elgamal* untuk enkripsi dan dekripsi file video MP4 berbasis web, ada beberapa aspek yang perlu diperhatikan:

4.2. Keamanan Algoritma *AES (Advanced Encryption Standard)*

a. Kekuatan Kriptografi**:**
Algoritma *AES* dikenal sebagai salah satu algoritma simetris yang sangat aman. Dengan kunci berukuran 128-bit, 192-bit, dan 256-bit, *AES* menawarkan tingkat keamanan yang sangat tinggi karena membutuhkan waktu yang sangat lama untuk dipecahkan dengan algoritma brute force.
b. Serangan yang Mungkin Terjadi:
Meskipun *AES* sangat kuat terhadap serangan *brute force*, ada beberapa potensi serangan seperti *side-channel attacks*, di mana penyerang tidak mencoba meretas algoritma secara langsung, tetapi mengeksploitasi informasi yang diperoleh dari lingkungan perangkat keras (misalnya, waktu eksekusi, konsumsi daya, atau emisi *elektromagnetik*).

4.3. Keamanan Algoritma *Elgamal*

Keamanan Kunci Publik dan Privasi: *Elgamal* adalah algoritma kriptografi asimetris yang aman karena didasarkan pada kesulitan masalah logaritma diskret. Serangan terhadap *Elgamal*, seperti serangan discrete logarithm, memerlukan sumber daya komputasi yang sangat besar, yang pada praktiknya tidak dapat dilakukan dalam waktu singkat dengan perangkat keras modern.

4.4. Tampilan Awal

Gambar 7. Tampilan Awal

Gambar diatas merupakan tampilan awal dari sistem aplikasi berbasis web yang telah peneliti buat, pada tampilan diatas pengguna bisa memilih tiga menu yang telah dibuat dan memiliki fungsi sesuai judulnya, empat menu tersebut yaitu menu enkripsi, dekripsi, tentang aplikasi dan *about us*.

4.5. Tampilan Enkripsi

Gambar 8. Gambar Tampilan Enkripsi

Pada gambar diatas adalah tampilan enkripsi, dimana pengguna dapat memulai proses enkripsi dengan cara :

a. Mengupload file video yang akan dienkripsikan
b. Memasukkan *plaintext*
c. Mengklik tombol *generate key*, untuk mendapatkan sepasang kunci *Elgamal* yang telah terenkripsi menggunakan kunci *AES*, yang mana kunci publik untuk mengenkripsi data video dan kunci pribadi untuk mendekripsi data video.
d. Lalu klik submit.
e. Setelah itu pengguna akan mendapatkan *private key* dan *ciphertext* yang langsung terdownload otomatis, *private key* dan *ciphertext* ini harus disimpan dengan karena keduanya akan digunakan untuk mendekripsikan data video.
f. Tunggu proses enkripsi
g. Ketika proses enkripsi selesai, data video enkripsi akan langsung terdownload.
h. Proses enkripsi selesai

4.6. Tampilan Dekripsi

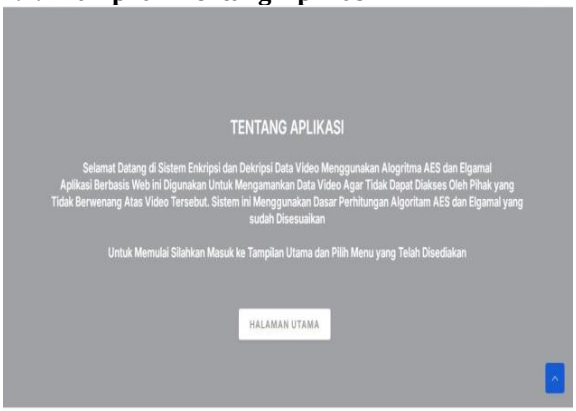
Gambar 9. Gambar Tampilan Dekripsi

Pada gambar diatas merupakan tampilan dekripsi video. Dimana pada tampilan ini pengguna

dapat mendekripsi data video yang telah terenkripsi sebelumnya. Adapun cara untuk mendekripsikan data video yang telah terenkripsi yaitu :

a. Pengguna mengupload data video yang telah terenkripsi.
b. Pengguna memasukkan *ciphertext* yang didapat dari proses enkripsi.
c. Lalu pengguna juga mengupload *private key* yang telah didapat dari proses enkripsi.
d. Klik submit dan tunggu proses dekripsi.
e. Ketika proses dekripsi selesai maka data video dekripsi akan langsung terdownload.
f. Enkripsi selesai.

4.7. Tampilan Tentang Aplikasi



Gambar 10. Gambar Tampilan Tentang Aplikasi

Pada gambar diatas merupakan tampilan dari definisi singkat mengenai sistem aplikasi yang dibuat oleh penulis dengan judul aplikasi enkripsi data video menggunakan algoritma *Elgamal* dan *AES* berbasis web.

4.8. Tampilan *About Us*

Gambar 11. Gambar Tampilan *About Us*

Gambar diatas merupakan tampilan gambar dari *about us* yang menampilkan data diri singkat pembuat aplikasi berbasis wab yang berisikan nama, npm, no hp dan email.

4.9. Tampilan View Data Video

Pada gambar 12 merupakan tampilan data video asli sebelum dilakukan proses enkripsi, dimana

Gambar 12. Gambar Tampilan View Data Video

5. KESIMPULAN DAN SARAN

Memuat Berdasarkan pada penelitian dan pembahasan penelitian mengenai implementasi algoritma *AES* dan *Elgamal* untuk enkripsi dan dekripsi file video *MP4* berbasis web, dapat diambil beberapa kesimpulan sebagai berikut:

Implementasi algoritma *AES* dan *Elgamal* memberikan keamanan yang kuat dimana algoritma *Elgamal* terbukti efisien dan aman untuk enkripsi dan dekripsi file video *MP4* dengan ukuran besar. Kecepatan enkripsi asimetris yang ditawarkan *Elgamal* sangat cocok untuk data yang berukuran besar seperti video dan algoritma AES *(Advanced Encryption Standard*), yang digunakan untuk mengenkripsi kunci *Elgamal*, menambah lapisan keamanan dengan enkripsi simetris, melindungi kunci dari potensi penyadapan selama transmisi.

Rancangan antarmuka enkripsi dan dekripsi yang efektif dan *userfrendly* dimana aplikasi berbasis web yang menggunakan protokol *HTTPS* dan autentikasi pengguna yang kuat menambah perlindungan terhadap serangan jaringan seperti *man-in-the-middle* atau penyadapan data, sedangkan algoritma enkripsi *Elgamal* dan *AES* yang digunakan pada aplikasi enkripsi data video ini bekerja dengan baik sehingga proses pengamanan data video jauh lebih aman karena algoritma *Elgamal* membantu meningkatkan tingkat keamanan dan algoritma *AES* membantu mempercepat proses enkripsi.

Berdasarkan pada hasil penelitian dan kesimpulan diatas, peneliti memberikan saran yaitu : Dalam penggunaan sistem aplikasi dengan ukuran data yang cukup besar, disarankan untuk menggunakan *hardware* dengan spesifikasi yang lebih tinggi terutama dalam hal processor dan memori komputer. Dan pengguna juga harus menjaga kunci *private key* dan *ciphertext* dengan baik, karena akan digunakan untuk dekripsi data video. Untuk menangani file video yang sangat besar (lebih dari 1 GB), diperlukan optimasi lebih lanjut dalam hal kecepatan enkripsi dan dekripsi. Salah satu solusinya adalah dengan menggunakan kompresi video sebelum proses enkripsi untuk mengurangi ukuran file dan mempercepat proses..

DAFTAR PUSTAKA

[1] M. H. T. A. Thoriq, A. I. H. Asep, and P. N. S. Puspita, "Data Encryption Pada File Video Menggunakan Algoritma Blowfish Berbasis Android," *Informatics Digit. Expert*, vol. 4, no. 1, pp. 33–39, 2022, doi: 10.36423/index.v4i1.880.

[2] D. Yudistira, "Perancangan Aplikasi Penyandian Agenda Pribadi Menggunakan Algoritma Kunci Public Elgamal," vol. 2, no. 1, pp. 17–21, 2022.

[3] K. Khairani and M. Z. Siambaton, "Pengamanan Data Teks Menggunakan Algoritma Kriptografi Elgamal dan XOR dari Serangan Hacker," *sudo J. Tek. Inform.*, vol. 2, no. 4, pp. 176–187, 2023, doi: 10.56211/sudo.v2i4.401.

[4] A. Syahputra and J. Prayudha, "Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Mengamankan File Soal Ujian Sekolah Dengan Kunci Algoritma 3Des (Triple DES)," *J. CyberTech*, vol. 3, no. 11, pp. 1673–1681, 2020.

[5] M. Ipdal, "Analisa Metode SHA-512 Untuk Tanda Tangan Digital Pada File Video," *J. Informatics Manag. Inf. Technol.*, vol. 1, no. 1, pp. 23–29, 2021.

[6] K. J. Nadia, A. T. Toko, and K. Jati, "Penerapan Algoritme Advanced Encryption Standard (Aes-128) Untuk Mengamankan File Dokumen Di Toko Implementation of the Advanced Encryption Standard (Aes-128) Algorithm for Document File Security," vol. 2, no. September, pp. 103–112, 2023.

[7] A. Randi, K. Lazuardy, S. Chandra, and A. Dharma, "Implementasi Algoritma Advanced Encryption Standard pada Aplikasi Chatting berbasis Android," *J. Ilmu Komput. dan Sist. Inf.*, vol. 3, no. 2, pp. 1–10, 2020.

[8] L. Clara and A. Budi, "Implementasi Metode Algoritma AES Pada Perlindungan Data Sistem Login," *J. Inform. dan Bisnis*, vol. 10, no. 2, pp. 1–14, 2021.

[9] D. Hulu, B. Nadeak, and S. Aripin, "Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan File Hasil Radiologi di RSU Imelda Medan," *KOMIK (Konferensi …*, vol. 4, pp. 78–86, 2020, doi: 10.30865/komik.v4i1.2590.

[10] D. Yudistira, "Perancangan Aplikasi Penyandian Agenda Pribadi Menggunakan Algoritma Kunci Public Elgamal," *J. Comput. Informatics Res.*, vol. 2, no. 1, pp. 17–21, 2022, doi: 10.47065/comforch.v2i1.349.

[11] A. H. Hasugian, R. A. Putri, and A. S. Zuhri, "Penerapan Metode Elgamal Untuk Mengamankan Teks Pada File Dokumen Word," *KLIK Kaji. Ilm. Inform. dan Komput.*, vol. 4, no. 2, pp. 1143–1153, 2023, doi: 10.30865/klik.v4i2.1277.

[12] I. Putra Sinaga, "Implementasi Kriptografi Hybrid Algoritma Elgamal Dan Double Playfair Cipher Dalam Pengamanan File Jpeg Berbasis Dekstop," *J. Informatics, Electr. Electron. Eng.*, vol. 1, no. 2, pp. 67–74, 2021.

[13] D. W. T. Putra and R. Andriani, "Unified Modelling Language (UML) dalam Perancangan Sistem Informasi Permohonan Pembayaran Restitusi SPPD," *J. TeknoIf*, vol. 7, no. 1, p. 32, 2019, doi: 10.21063/jtif.2019.v7.1.32-39.