JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER

e-ISSN : 2963-7104 (Online)
p-ISSN : 2962-3022 (Print)
Volume 2 No 3 Februari 2024 - Page: 535-544

Aplikasi Enkripsi Data Video Menggunakan Metode Rsa Dan Blowfish Berbasis Web

Yusmaifany [1,*] , Tommy [2], Rosyidah Siregar[3]

[1] Teknik dan Komputer, Teknik Informatika, Universitas Harapan Medan, Medan, Indonesia
[2] Fakultas, Program Studi, Nama Institusi, Kota, Indonesia

Email: [1*] yusmaiifani2906@gmail.com, [2,] rosyidahsiregar.88@gmail.com, [3] tomshirakawa@gmail.com

Abstrak

Perkembangan teknologi pada era digital sekarang ini memiliki dampak yang begitu besar dalam kehidupan manusia, salah satunya adalah teknologi video. Video merupakan salah satu media komunikasi yang paling populer dan banyak digunakan terutama dalam hal konferensi, rekaman rapat kantor, rekaman belajar mengajar oleh guru dan lain sebagainya. Akan tetapi, karena banyak orang cenderung berbagi dan menyimpan video dalam jumlah besar di internet, keamanan data video menjadi hal yang sangat penting untuk dilindungi agar data video tidak bisa di akses oleh orang yang tidak berwenang. Dengan demikian peneliti merancang sebuah aplikasi enkripsi data video yang menggunakan metode *RSA(Rivest Shamir Adleman)* dan *blowfish* sebagai algoritma keamanan untuk meningkat tingkat keamanan dan kecepatan performa enkripsi dan dekripsi. hasil uji coba penelitian pada sistem aplikasi enkripsi data video menggunakan metode *RSA (Rivest Shamir Adleman)* dan *Blowfish* menunjukkan bahwa aplikasi ini mampu dan berhasil mengamankan data video dengan tingkat kecepatan dan keamanan yang tinggi, sehingga mengurangi resiko kebocoran dan peretasan data video.

Kata Kunci : Enkripsi Data Video, RSA, Blowfish, Keamanan Data, Aplikasi Berbasis Web.

Abstract

Technological developments in today's digital era have such a big impact on human life, one of which is video technology. Video is one of the most popular and widely used communication media, especially in terms of conferences, recording of office meetings, recording of teaching and learning by teachers and so on. However, because many people tend to share and store videos in large quantities on the internet, video data security is very important to protect so that video data cannot be accessed by unauthorized persons. Thus the researchers designed a video data encryption application that uses the *RSA* method *(Rivest Shamir Adleman)* and *blowfish* as a security algorithm to increase the level of security and speed of encryption and decryption performance. The results of research trials on video data encryption application systems using the *RSA (Rivest Shamir Adleman)* and *Blowfish* methods show that these applications are capable of completing video data security with a high level of speed and security, thereby reducing the risk of video data leakage and hacking.

Key Words : *Video Data Encryption, RSA, Blowfish, Data Security, Web-Based Applications.*

1. PENDAHULUAN

Pada era digital sekarang ini, video menjadi salah satu media komunikasi yang paling populer dan banyak digunakan terutama dalam hal konferensi, rekaman rapat kantor,rekaman belajar mengajar oleh guru dan lain sebagainya. Akan tetapi, karena banyak orang cenderung berbagi dan menyimpan video dalam jumlah besar di internet, keamanan data video menjadi hal yang sangat penting untuk dilindungi agar data video tidak bisa di akses oleh orang yang tidak berwenang[1].

Kriptografi merupakan ilmu yang mempelajari teknik matematika untuk mengamankan informasi digital, sistem dan komputasi yang terdistribusi[2]. Kriptografi bertujuan untuk menjaga keamanan dan kerahasian data agar terhindar dari pihak yang tidak berkepentingan atas akses data tersebut[3]. Enkripsi data merupakan proses mengubah pesan atau data asli menjadi bentuk yang tidak dapat dibaca atau dimengerti oleh pihak yang tidak berwenang.

Dalam lingkup perlindungan dan kerahasiaan data, salah satu keamanan yang dapat digunakan adalah metode *RSA(Rivest Shamir Adleman)* dan *Blowfish*. Enkripsi data video dengan metode *RSA(Rivest Shamir Adleman)* dan *Blowfish* termasuk salah satu teknik yang dapat digunakan untuk meningkatkan tingkat keamanan data video[4]. *RSA(Rivest Shamir Adleman)* adalah algoritma kriptografi a*simetris* yang mempunyai kunci publik dan kunci pribadi untuk mengenkripsikan dan mendekripsikan data. Sementara itu, *Blowfish* adalah algoritma kriptografi *simetris* yang menggunakan kunci yang sama untuk mengenkripsi dan mendekripsikan data[5].

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER

e-ISSN : 2963-7104 (Online)
p-ISSN : 2962-3022 (Print)
Volume 2 No 3 Februari 2024 - Page: 535-544

Dalam konteks aplikasi berbasis web, enkripsi data video menggunakan metode *RSA (Rivest Shamir Adleman)* dan *Blowfish* dapat dilakukan dengan mengimplementasikan algoritma enkripsi pada web server. Data video akan di enkripsi menggunakan kunci *RSA (Rivest Shamir Adleman)* dengan kunci yang telah dipilih secara acak, kunci *RSA(Rivest Shamir Adleman)* tersebut terlebih dahulu dienkripsikan dengan kunci *blowfish*, dan nantinya kunci *RSA* yang akan mengenkripsikan data video, kunci public untuk enkripsi data video dan kunci privat untuk dekripsi data video, sehingga hanya pihak yang memiliki kunci pribadi *RSA(Rivest Shamir Adleman)* yang dapat membuka data video. Dengan cara ini, data video dapat dijamin keamanan dan kerahasiaanya saat di bagikan atau disimpan dalam jaringan internet.

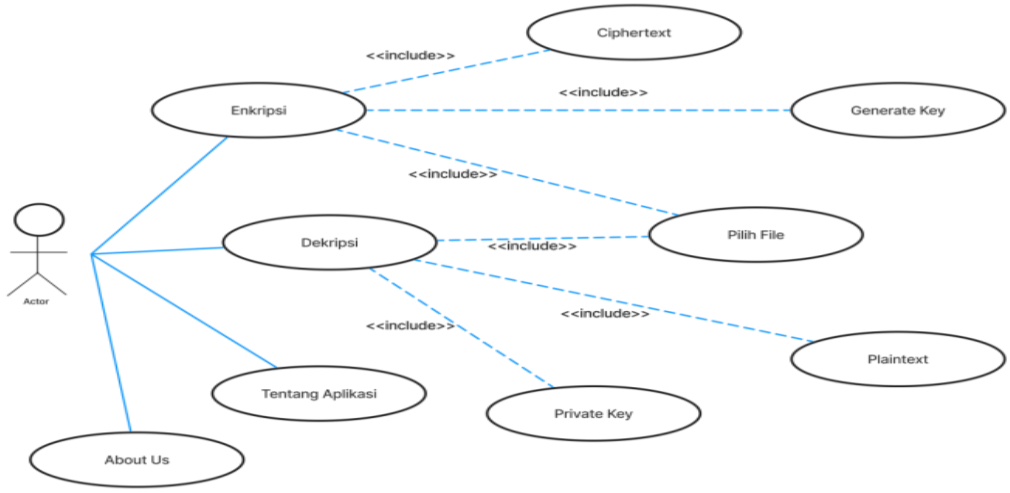
2. METODOLOGI PENELITIAN

2.1 Perancangan Sistem

Perancangan sistem merupakan suatu proses menggambar, merencanakan dan menjelaskan penjabaran secara rinci mengenai sistem yang akan dibuat, bagaimana alur kerja sistem dibangun,termasuk juga komponen-komponen, struktur, dan interaksi proses berjalannya sistem tersebut. Perancangan sistem ini memiliki tujuan untuk membuat rencana yang lebih detail dan terperinci bagaimana sistem akan beroperasi.

2.2 *Use Case* Enkripsi dan Dekripsi

Berikut ini penulis membuat rancangan dan penjelasan dari *use case* :

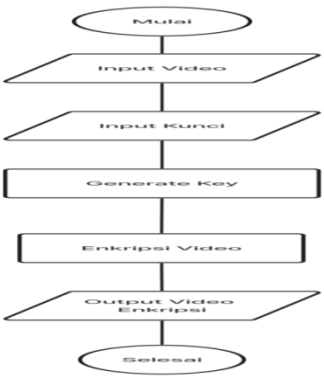


Gambar 1. *Use Case* Enkripsi dan Dekripsi

2.3 *Flowchart* Sistem

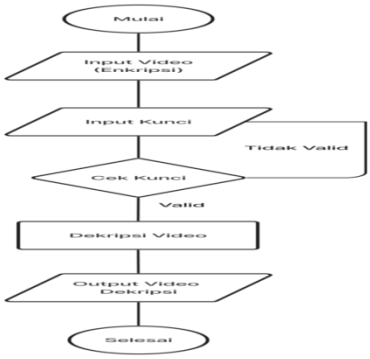
Flowchart merupakan langkah-langkah dan urutan proses yang menggambarkan alur logika dari data yang akan diproses oleh program web dari awal hingga akhir yang akan penulis buat.
Berikut adalah *flowchart* enkripsi dan dekripsi data video :

a. *Flowchart* Enkripsi



Gambar 2. *Flowchart* Enkripsi

b. *Flowchart* Dekripsi



Gambar 3. *Flowchart* Dekripsi

e-ISSN : 2963-7104 (Online)
p-ISSN : 2962-3022 (Print)
Volume 2 No 3 Februari 2024 - Page: 535-544

2.4 Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu *cryptos* yang artinya "*secret*" (yang tersembunyi) dan *graphein* yang artinya "*writting*" (tulisan). Jadi, kriptografi berarti "*secret writing*" (tulisan rahasia)[6].

2.5 Algoritma *Simetris*

Algoritma *simetris* adalah metode kriptografi yang proses enkripsi dan dekripsinya menggunakan kunci rahasia tunggal, untuk mengamankan pesan pengirim dan penerima menggunakan kunci yang sama [7].

2.6 Algoritma A*simetris*

Algoritma a*simetris* dikenal dengan algoritma kunci publik, yang mana algoritma ini mempunyai kunci enkripsi dan dekripsi yang berbeda[7].

2.7 Keamanan Informasi

Keamanan informasi sangat penting dalam menjaga kerahasian data karena jika sistem komputer atau sistem informasi tidak aman, maka dapat menyebabkan terjadinya peretasan dan pencurian data oleh pihak yang tidak berwenang, hal tersebut mengakibatkan kerugian yang cukup besar bagi, organisasi maupun individu, baik secara finansial maupun reputasi[8].

2.8 Enkripsi

Enkripsi adalah proses mengubah pesan atau data asli menjadi bentuk yang tidak dapat di baca atau dimengerti, untuk menjaga kerahasiaan data tersebut sebelum dikirim melalui internet yang tidak memiliki jaminan keamanan data sama sekali[9].

2.9 Dekripsi

Dekripsi adalah proses mengubah data yang terenkripsi menjadi data asli atau disebut dengan mengubah *ciphertext* menjadi *plaintext*. Kunci hanya diberikan kepada orang yang berwenang akan akses data tersebut untuk mengubah data terenkripsi menjadi data asli yang dapat dimengerti oleh manusia[10].

2.10 RSA(Rivest Shamir Adleman)

RSA (Rivest Shamir Adleman) adalah algoritma kriptografi a*simetris* yang pertama kali ditemukan oleh Ron Rivest, Adi Shamir, dan Len Adleman pada tahun 1977[11]. *RSA (Rivest Shamir Adleman)* diambil dari nama ketiga penemu tersebut, *RSA(Rivest Shamir Adleman)* termasuk algoritma a*simetris* yang memiliki dua kunci, yaitu kunci publik dan kunci pribadi [12].

2.11 Blowfish

Pada tahun 1993 seorang *Cryptanalyst* bernama Bruce Scheneir merancang algoritma *blowfish* dan mempublikasikan algoritma *blowfish* sebagai fungsi kriptografi pada tahun 1994. *Blowfish* merupakan algoritma *simetris* 64-bit dengan panjang kunci 32-bit sampai 448-bit [3].

2.12 Data Video

video adalah media elektronik yang didalamnya terdapat gabungan teknologi audio dan visual yang menghasilkan bentuk frame atau gambar yang bergerak menjadi dinamis dan menarik[13]. Data video merupakan bentuk data yang gampang diakses oleh siapa saja.

2.13 Aplikasi Berbasis Web

Aplikasi berbasis web merupakan sebuah perangkat lunak yang diakses melalui jaringan internet menggunakan web browser pada perangkat mobile atau komputer[14].

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER

e-ISSN : 2963-7104 (Online)
p-ISSN : 2962-3022 (Print)
Volume 2 No 3 Februari 2024 - Page: 535-544

3. HASIL DAN PEMBAHASAN

Aplikasi enkripsi data video berbasis web adalah sistem berbasis web yang berfungsi untuk melindungi dan mengamankan data video agar tidak terjadi peretasan dan pencurian data oleh pihak yang tidak berwenang. Sistem aplikasi berbasis web ini menggunakan dua metode enkripsi yaitu *RSA(Rivest Shamir Adleman)* dan *Blowfish*.

3.1 Perhitungan Metode RSA

Adapun rumus dan perhitungan metode *RSA(Rivest Shamir Adleman)* untuk mendapatkaan sepasang kunci yaitu, kunci publik dan kunci pribadi[15] :

a. Inisialisasi
   1. Memilih dua bilangan prima acak :
      P = 13 dan q = 17
   2. Hitung nilai n : n = p * q
      13 * 17 = 221
   3. Lalu hitung nilai phi (n) : phi (n) = (p - 1) * (q - 1)
      12 * 16 = 192

b. Kunci publik
   Memilih bilangan acak e yang relatif dengan phi (n) = 192 dan e < phi (n), penulis memilih e =5

c. Menghitung kunci pribadi
   Menentukan bilangan d yang memenuhi syarat d * e ≡ 1 (mod phi (n)). Pada bagian ini penulis akan mencari d dengan menggunakan algoritma extended Euclidean yang berfungsi untuk menghasilkan solusi persamaan di atas :
   Menginisialisasi : phi (n) = 192, e = 5
   Langkah ke 1 : 192 = 5 * 38 + 2
   Langkah ke 2 : 5 = 2 * 2 + 1
   Langkah ke 3 : 2 = 1 * 2 + 0
   Langkah ke 4 : menerapkan subsitusi balik :
   1 = 5 – 2 * 2 = (192 – 5 * 38) * 2 = 77 * 5 – 192 * 2
   Langkah ke 5 : hasilkan d dengan memodulo phi(n) :
   d = 77 mod 192 = 77

Pada proses ini menghasilkan kunci publik yaitu (n, e) = (221, 5) dan kunci pribadi yaitu (n, d) = (221, 77). Perhitungan diatas ini menjelaskan bagaimana langkah- langkah awal untuk proses pembuatan sepasang kunci *RSA(Rivest Shamir Adleman)*, termasuk didalamnya inisialisasi, pemilihan kunci publik, dan perhitungan kunci pribadi.

3.2 Perhitungan Metode *Blowfish*

Pada bagian ini penulis akan membuat perhitungan metode *blowfish* untuk mengenkripsi dan mendekripsi sebuah blok data video menggunakan kunci yang telah penulis tentukan sebelumnya.
Proses enkripsi :

a. Kunci *RSA(Rivest Shamir Adleman)* yang telah didapatkan data perhitungan sebelumnya yaitu, kunci publik (221, 5) dan kunci pribadi (221, 7).
b. Mengenkripsikan kunci *simetris* algoritma *blowfish* dengan kunci publik *RSA(Rivest Shamir Adleman)* kunci *simetris blowfish* yang akan dienkripsi:
   K = SECRETKEY
c. Lalu penulis mengkonversi K ke bilangan ASCII :
   83 69 67 82 69 84 75 69 89
d. Lalu mengubah setiap bilangan ASCII menjadi bilangan bulat dalam modulo n:
   P = [83, 69, 67, 82, 69, 84, 75, 69, 89]
e. Enkripsi setiap elemen blok P menggunakan *RSA(Rivest Shamir Adleman)* :
   C = [(P[]ˆe) mod n, (P[1]ˆe) mod n, (P[2]ˆe) mod n, …]
f. Hasil enkripsi *RSA(Rivest Shamir Adleman)* :
   C = [15, 156, 27, 174, 156, 183, 100, 156, 54]
g. Kunci enkripsi *simetris* yang dihasilkan dari kunci publik *RSA(Rivest Shamir Adleman)* ESK = [15, 156, 27, 174, 156, 183, 100, 156, 54]
h. Kunci *simetris* algoritma *blowfish* :
   K = ESK (hasil enkripsi *RSA*)

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
e-ISSN : 2963-7104 (Online)
p-ISSN : 2962-3022 (Print)
Volume 2 No 3 Februari 2024 - Page: 535-544

Pada tahap enkripsi selanjutnya data video akan dipecah menjadi blok-blok dengan elemen kecil dan untuk setiap blok elemen akan dienkripsi dengan algoritma *blowfish* dengan kunci *simetris* K yang sudah penulis hasilkan dari perhitungan sebelumnya.
Proses dekripsi :

a. *RSA(Rivest Shamir Adleman)* kunci pribadi (221, 77)
b. Dekripsikan kembali kunci *simetris blowfish* yang dienkripsikan sebelumnya menggunakan kunci publik *RSA(Rivest Shamir Adleman)*.
c. Kunci *simetris* hasil dekripsi *RSA(Rivest Shamir Adleman)* :
DSK = [(C[0]ˆd) mod n, (C[1]ˆd) mod n, (C[2]ˆd) mod n, …]
d. Hasil perhitungan :
DSK = [83, 69, 67, 82, 69, 84, 75, 69, 89]
e. Lalu penulis akan mengkonversi kembali DSK dari bilangan bulat menjadi karakter ASCII yaitu :
"SECRETKEY"

Pada proses selanjutnya setelah mendapatkan kunci dekripsi *simetris blowfish* "SECRETKEY" selanjutnya kunci ini yang akan digunakan untuk mendekripsikan data video.

3.3 Alur Kerja Aplikasi Berbasis Web

Adapun alur kerja aplikasi berbasis web ini, yaitu

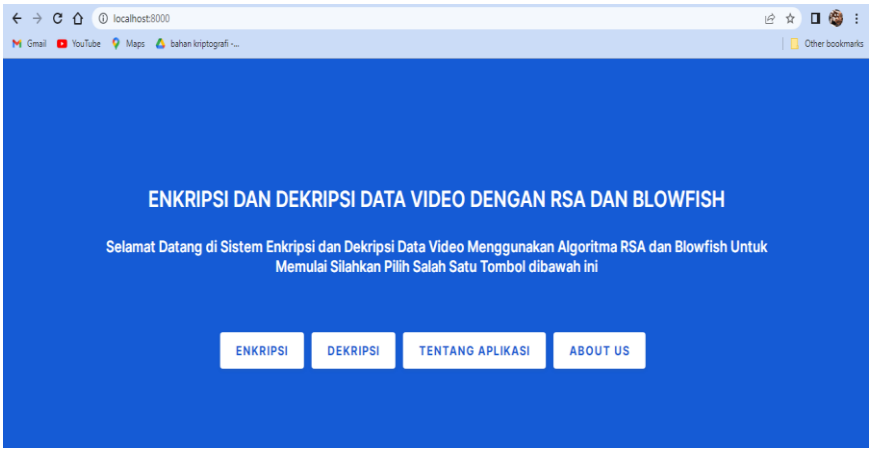
a. User mengupload data video yang akan dienkripsi melalui antarmuka user.
b. User juga memasukkan kunci *plaintext* dan melakukan *generate key*.
c. Lalu server menerima data video, setelah itu dengan menggunakan algoritma *blowfish* yang akan mengenkripsi kunci *RSA(Rivest Shamir Adleman)*, selanjutnya kunci dan data video yang telah dienkripsi akan langsung terdownload.
d. Pada saat user ingin mengakses data video yang telah dienkripsi, user bisa melihat pada folder download.
e. Selanjutnya mendekripsikan dengan *ciphertext* dan kunci pribadi *RSA(Rivest Shamir Adleman)* yang telah didekripsikan
f. Selanjutnya video yang telah didekripsi akan terdownload otomatis kepada user melalui antarmuka user.

3.4 Hasil Sistem

Berikut adalah hasil dari antarmuka sistem berbasis web yang telah peneliti buat, antara lain :

a. Tampilan Awal

Gambar dibawah 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*.



Gambar 4. Gambar Tampilan Awal

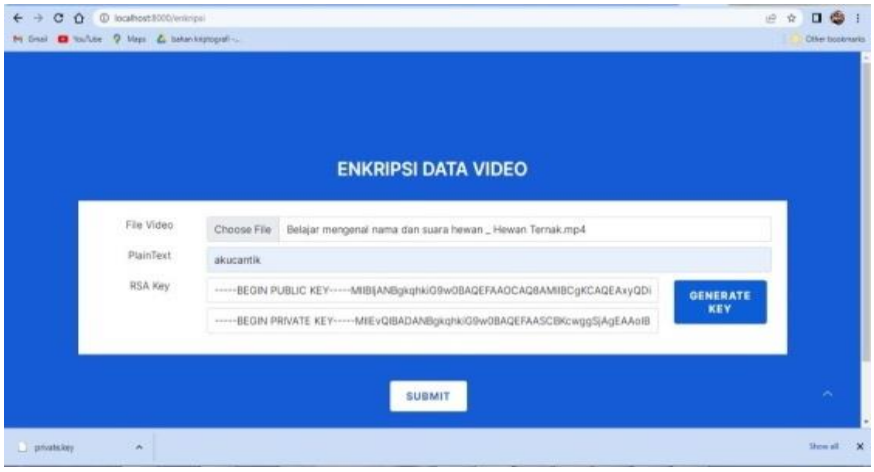
b. Tampilan Enkripsi

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

1. Mengupload file video yang akan dienkripsikan
2. Memasukkan *plaintext*

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
e-ISSN : 2963-7104 (Online)
p-ISSN : 2962-3022 (Print)
Volume 2 No 3 Februari 2024 - Page: 535-544

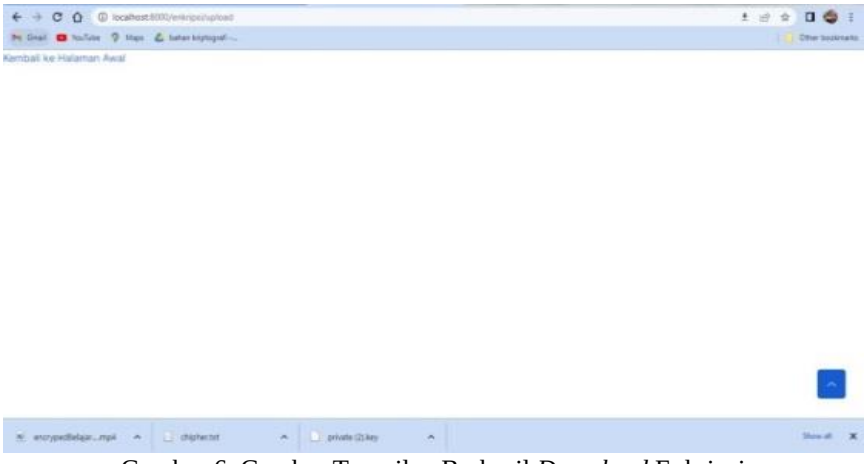
3. Mengklik tombol *generate key*, untuk mendapatkan sepasang kunci *RSA(Rivest Shamir Adleman)* yang telah terenkripsi menggunakan kunci *blowfish*, yang mana kunci publik untuk mengenkripsi data video dan kunci pribadi untuk mendekripsi data video.
4. Lalu klik submit.
5. Setelah itu pengguna akan 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.
6. Tunggu proses enkripsi
7. Ketika proses enkripsi selesai, data video enkripsi akan langsung terdownload.
8. Proses enkripsi selesai.



Gambar 5. Gambar Tampilan Enkripsi

c. Tampilan Berhasil Proses Enkripsi

Gambar dibawah merupakan tampilan dari berhasilnya proses enkripsi, untuk melihat berhasilnya proses enkripsi pengguna akan masuk ke form “kembali ke halaman awal” dan akan ada folder yang telah terdownload otomatis dari proses enkripsi data video, yaitu folder *private key*, *ciphertext* dan file enkripsi.



Gambar 6. Gambar Tampilan Berhasil *Download* Enkripsi

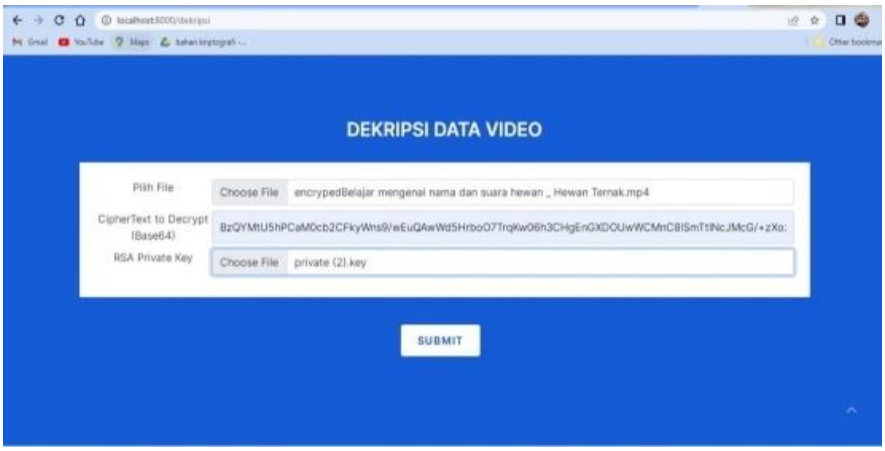
d. Tampilan Dekripsi

Pada gambar dibawah 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 :

1. Pengguna mengupload data video yang telah terenkripsi.
2. Pengguna memasukkan *ciphertext* yang didapat dari proses enkripsi.
3. Lalu pengguna juga mengupload *private key* yang telah didapat dari proses enkripsi.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
e-ISSN : 2963-7104 (Online)
p-ISSN : 2962-3022 (Print)
Volume 2 No 3 Februari 2024 - Page: 535-544

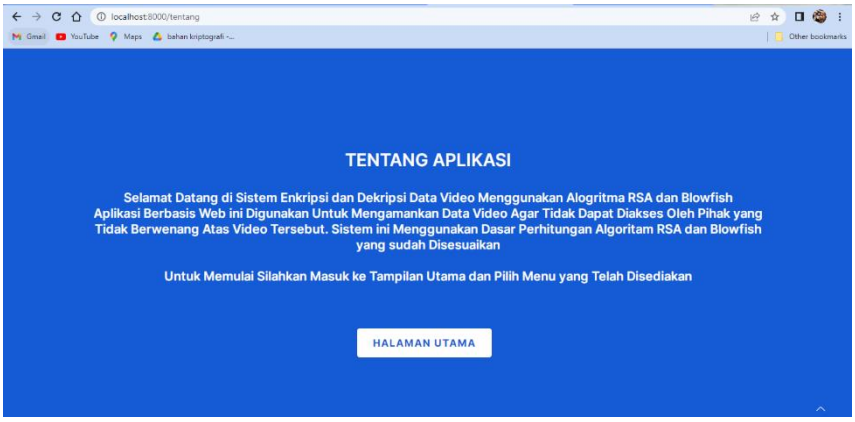
4. Klik submit dan tunggu proses dekripsi.
5. Ketika proses dekripsi selesai maka data video dekripsi akan langsung terdownload.
6. Enkripsi selesai.



Gambar 7. Gambar Tampilan Berhasil Proses Enkripsi

e. Tampilan Tentang Aplikasi

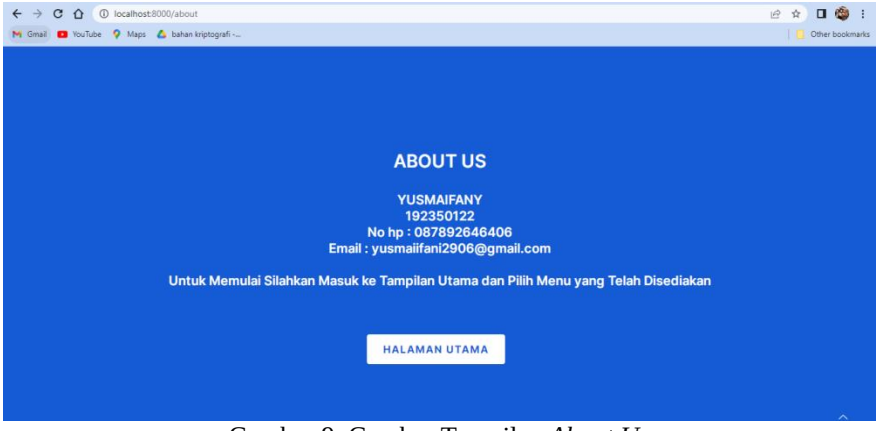
Pada gambar diatas merupakan tampilan dari definisi singkat mengenai sistem aplikasi yang dibuat oleh penulis dengan judul aplikasi enkripsi data video menggunakan metode *RSA(Rivest Shamir Adleman)* dan *Blowfish* berbasis web.



Gambar 8. Gambar Tampilan Tentang Aplikasi

f. Tampilan *About Us*

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



Gambar 9. Gambar Tampilan *About Us*

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
e-ISSN : 2963-7104 (Online)
p-ISSN : 2962-3022 (Print)
Volume 2 No 3 Februari 2024 - Page: 535-544

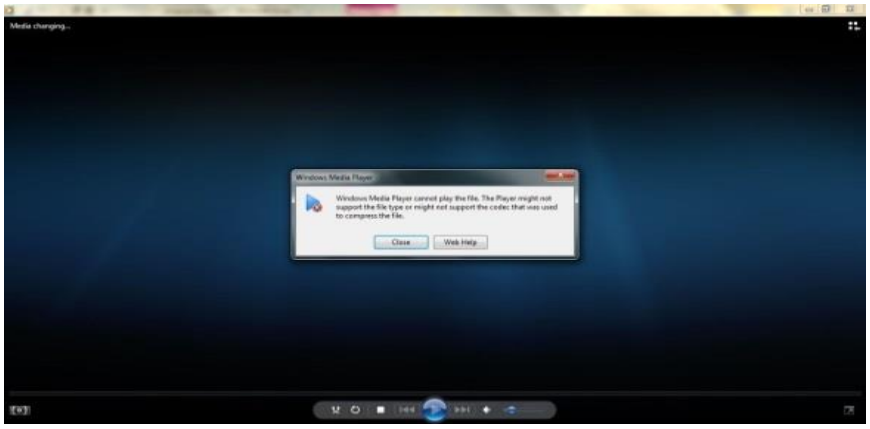
g. Tampilan View Data Video

Pada gambar dibawah ini merupakan tampilan data video asli sebelum dilakukan proses enkripsi, dimana data video tersebut dapat dibuka dan diputar sehingga dapat dilihat isi dari data video tersebut.

Gambar 10. Gambar Tampilan View Data Video

h. Tampilan View Data Video Enkripsi

Berikut merupakan tampilan dari data video yang telah berhasil dienkripsi, sehingga ketika video tersebut dibuka maka hanya menampilkan layar hitam yang tidak bisa diputar sama sekali dan menampilkan sebuah pop up yang menyatakan data video tersebut tidak bisa diputar.



Gambar 11. Gambar Tampilan View Data Video Enkripsi

i. Tampilan View Video Dekripsi

Gambar dibawah merupakan gambar dari data video yang telah berhasil didekripsikan kembali seperti semula, sehingga data video dapat dibuka dan diputar untuk melihat isi dari data tersebut.

Gambar 12. Gambar Tampilan Data Video Dekripsi

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER

e-ISSN : 2963-7104 (Online)
p-ISSN : 2962-3022 (Print)
Volume 2 No 3 Februari 2024 - Page: 535-544

3.5 Pengujian Enkripsi Video

Tabel 1. Pengujian Enkripsi Video

No	Bulir Pengujian	Output yang diinginkan	Output yang keluar	Keterangan
1	Pilih file data video	Sistem dapat memilih file data video dari file explorer.	Sistem berhasil memilih file data video dari file explorer.	Sesuai
2	*Plaintext* ke Ciphertext	Sistem dapat membaca *plaintext* dan mengubahnya dalam bentuk *ciphertext* untuk membuat eror isi data video.	Sistem berhasil membaca *plaintext* dan mengubahnya dalam bentuk *ciphertext* untuk membuat eror isi data video.	Sesuai
3	Generate key	Sistem mampu mendapatkan sepasang kunci *RSA(Rivest Shamir Adleman)* yaitu public key dan *private key* .	Sistem berhasil mendapatkan sepasang kunci *RSA(Rivest Shamir Adleman)* yaitu public key dan *private key*.	Sesuai
4	Enkripsi data video	Sistem mampu mengenkripsi data video sesuai dengan perhitungan algoritma *RSA(Rivest Shamir Adleman)* dan *Blowfish* dimana kunci *RSA(Rivest Shamir Adleman)* akan di enkripsi terlebih dahulu menggunakan kunci *blowfish*	Sistem berhasil mengenkripsi data video sesuai dengan perhitungan algoritma *RSA(Rivest Shamir Adleman)* dan *Blowfish*.	Sesuai
5	Dekripsi data video	Sistem dapat mendeteksi data video yang telah terenkripsi untuk mendekripsikan kembali menggunakan *private key* dan *ciphertext*	Sistem berhasil mendeteksi data video yang telah terenkripsi untuk mendekripsikan kembali menggunakan *private key* dan *ciphertext*	Sesuai
6	Deteksi kesalahan sistem	Sistem dapat mendeteksi kesalahan pengguna seperti pengguna tidak memasukkan file video, kunci *plaintext* dan melakukan *generate key* terlebih dahulu sebelum melanjutkan proses submit	Sistem berhasil mendeteksi kesalahan pengguna seperti pengguna tidak memasukkan file video, kunci *plaintext* dan melakukan *generate key* terlebih dahulu sebelum melanjutkan proses submit	Sesuai

e-ISSN : 2963-7104 (Online)
p-ISSN : 2962-3022 (Print)
Volume 2 No 3 Februari 2024 - Page: 535-544

4. KESIMPULAN

Berdasarkan pada penelitian dan pembahasan diatas peneliti menyimpulkan bahwa aplikasi enkripsi data video menggunakan metode *RSA(Rivest Shamir Adleman)* dan *Blowfish* berbasis web merupakan solusi yang baik untuk melindungi kerahasiaan data video dari pihak yang tidak berwenang. Metode enkripsi *RSA(Rivest Shamir Adleman)* dan *Blowfish* yang digunakan pada aplikasi enkripsi data video ini bekerja dengan baik sehingga proses pengamanan data video jauh lebih aman karena metode *RSA(Rivest Shamir Adleman)* membantu meningkatkan tingkat keamanan yang lebih tinggi dan metode *blowfish* membantu mempercepat proses enkripsi. Sistem enkripsi dan dekripsi data video dengan menggunakan algoritma *RSA(Rivest Shamir Adleman)* dan *blowfish* berbasis web ini dapat diakses secara offline. Hasil proses enkripsi pada sistem ini dapat mengubah isi data video tanpa merubah ekstensi dari data video aslinya, sehingga data video tersebut tidak dapat dibuka. Sedangkan hasil proses dekripsi pada sistem ini yaitu mempertahankan ekstensi asli dan merubah isi data video kedalam bentuk semula, sehingga data video dapat dibuka dan bisa diputar kembali.

REFERENCES

[1] A. Ginting, R. R. Isnanto, and I. P. Windasari, "Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email," *J. Teknol. dan Sist. Komput.*, vol. 3, no. 2, p. 253, 2015, doi: 10.14710/jtsiskom.3.2.2015.253-258.

[2] J. Katz and Y. Lindell, *INTRODUCTION TO MODERN CRYPTOGRAPHY: Second Edition*. 2014. doi: 10.1201/b17668.

[3] S. Suhandinata, R. A. Rizal, D. O. Wijaya, P. Warren, and Srinjiwi, "Analisis Performa Kriptografi Hybrid Algoritma RSA," *Jurteksi*, vol. VI, no. 1, pp. 1–10, 2019.

[4] B. K. Hutasuhut, S. Efendi, and Z. Situmorang, "Digital Signature untuk Menjaga Keaslian Data dengan Algoritma MD5 dan Algoritma RSA," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 3, no. 2, pp. 164–169, 2019, doi: 10.30743/infotekjar.v3i2.1019.

[5] I. Gunawan, "Kombinasi Algoritma Caesar Cipher dan Algoritma RSA untuk pengamanan File Dokumen dan Pesan Teks," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 2, no. 2, pp. 124–129, 2018, doi: 10.30743/infotekjar.v2i2.266.

[6] N. Fahriani and H. Rosyid, "Implementasi Teknik Enkripsi dan Dekripsi dI File Video Menggunakan Algoritma Blowfish," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 6, no. 6, p. 697, 2019, doi: 10.25126/jtiik.2019661465.

[7] N. Sakti, "Sistem Kemanan Data Menggunakan Algoritma," vol. 1, no. April, pp. 20–29, 2018.

[8] D. A. Meko, "Jurnal Teknologi Terpadu Perbandingan Algoritma DES , AES , IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data Donzilio Antonio Meko Program Studi Teknik Informatika , STIMIK Kupang Jurnal Teknologi Terpadu," *J. Teknol. Terpadu*, vol. 4, no. 1, pp. 8–15, 2018.

[9] M. H. T. Almuwaffaq, A. I. Hadiana, and P. N. Sabrina, "Data Encryption Pada File Video Menggunakan Algoritma Blowfish Berbasis Android," vol. 1, pp. 33–39, 2022.

[10] R. S. Lubis, Tulus, and E. B. Nababan, "Pengamanan File Teks Menggunakan Algoritma RSA – LUC dan Algoritma Zig-Zag dalam Hybrid Crypto Sistem," *InfoTekJar J. Nas. Inform. dan Teknol. Jar.*, vol. 6, no. 2, pp. 185–189, 2022.

[11] M. Shankar and A. P, "Hybrid Cryptographic Technique Using RSA Algorithm and Scheduling Concepts," *Int. J. Netw. Secur. Its Appl.*, vol. 6, no. 6, pp. 39–48, 2014, doi: 10.5121/ijnsa.2014.6604.

[12] M. Rsa, R. Shamir, M. Aditia, and D. Setiawan, "Penerapan Security Sistem Untuk Keamanan Data Penjualan Kopi Di Cv . Naga Sanghie Dengan," vol. 4, no. 9, 2021.

[13] A. Yudianto, "Penerapan Video Sebagai Media Pembelajaran," *Semin. Nas. Pendidik. 2017*, pp. 234–237, 2017.

[14] S. R. U. A. S. Andy Antonius Setiawan, Arie S.M. Lumenta, "Rancang Bangun Aplikasi Unsrat E-Catalog," *J. Tek. Inform.*, vol. 14, no. 4, pp. 1–9, 2019.

[15] R. N. Fuad and H. N. Winata, "Aplikasi Keamanan File Audio Wav (Waveform) Dengan Terapan Algoritma Rsa," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 1, no. 2, pp. 113–119, 2017, doi: 10.30743/infotekjar.v1i2.72.