Pengamanan File Video dengan algoritma *Advanced Encryption Standard (AES)*

[1]Agung Susilo Yuda Irawan, [2]Ahmad Farhan El Ramdhani, [3]Muhamad Jordi, [4]Rizal Saepul Mahdi, [5]Tohirin Al Mudzakir

[1,2,3,4]Program Studi Teknik Informatika, Universitas Singaperbangsa Karawang

[5]Program Studi Teknik Informatika, Universitas Buana Perjuangan Karawang

Email: agungsyi@staff.unsika.ac.id

Abstract

Cryptography is a method that can be used to secure data. Data that is usually secured using cryptography is text data. Text data is usually used in messages to communicate. The contents of the message are secured by cryptography. There are two main procedures in cryptography, namely encryption and decryption. Encryption is a procedure performed to encode an original data or message into a coded data or message. Instead, decryption is a procedure performed to return a message or data that is encrypted into the original message or data as before. Cryptography has a variety of algorithms, one of which is the Advanced Encryption Standard (AES) algorithm. AES is a cryptographic algorithm that has a high level of security. In this research, an AES algorithm is implemented to securing data in the form of video with mp4 format. Tests carried out using cryptographic applications, namely CrypTool. To be encrypted and decrypted, video data is converted in the form of HexDump. From this research it was produced that the AES algorithm is effective for securing video data. Encrypted video data cannot be played with the media player and does not have detailed information like the original data. However, when decrypted the data is successfully played normally with a media player and has detailed information like the original data.

Keywords: *cryptography, AES, MP4, cryptool, hexdump*

Abstraksi

Kriptografi merupakan suatu metode yang dapat digunakan untuk mengamankan data. Data yang biasanya diamankan menggunakan kriptografi adalah data teks. Data teks biasa digunakan dalam pesan untuk berkomnikasi. Isi pesan tersebutlah yang diamankan dengan kriptografi. Prosedur utama dalam kriptografi ada dua, yaitu enkripsi dan dekripsi. Enkripsi merupakan prosedur yang dilakukan untuk menyandikan suatu data atau pesan asli menjadi data atau pesan bersandi. Sebaliknya, dekripsi merupakan prosedur yang dilakukan untuk mengembalikan pesan atau data yang disandikan menjadi pesan atau data asli seperti semula. Kriptografi memiliki beragam algoritma, salah satunya yaitu algoritma *Advanced Encryption Standard* (AES). AES merupakan salah satu algoritma kriptografi yang memiliki tingkat keamanan yang tinggi. Pada penelitian ini dilakukan implementasi algoritma AES untuk mengamankan data berupa video dengan format *mp4*. Pengujian dilakukan dengan menggunakan aplikasi kriptografi yaitu *CrypTool*. Untuk dapat dienkripsi dan didekripsi, data video diubah dalam bentuk *HexDump*. Dari penelitian ini dihasilkan bahwa algoritma AES efektif untuk mengamankan data video. Data video yang terenkripsi tidak dapat diputar dengan media *player* dan tidak memilik detail informasi seperti data aslinya. Akan tetapi ketika didekripsi data tersebut berhasil diputar secara normal dengan media *player* dan memiliki detail informasi seperti data aslinya.

Kata kunci: kriptografi, AES, MP4, cryptool, hexdump

1. PENDAHULUAN

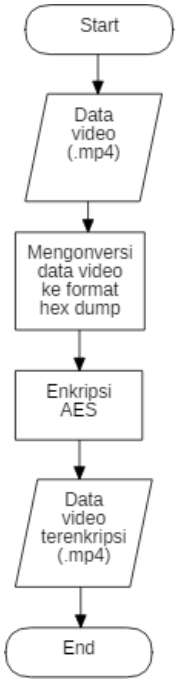
Keamanan data merupakan hal yang sangat penting untuk diperhatikan bagi setiap individu maupun organisasi. Data menjadi sangat penting [1], Hal tersebut dikarenakan ada beberapa data yang sifatnya pribadi, yang mana data tersebut dijaga kerahasiaannya dari pihak-pihak yang tidak bersangkutan ataupun tidak berkepentingan. Ancaman terjadinya serangan dari pihak-pihak yang tidak berkepentingan untuk dapat mengambil dan melihat data pribadi milik seseorang atau organisasi selalu dimungkinkan dapat terjadi kapanpun dan di manapun, apalagi di dalam suatu lalu lintas jaringan komunikasi yang semakin luas dan tak kenal ruang dan waktu pada era kemajuan teknologi saat ini.

Salah satu metode yang dapat digunakan untuk mengamankan data [2] yaitu dengan menerapkan konsep kriptografi. Kriptografi merupakan sebuah metode yang dapat mengubah data teks asli menjadi data teks baru yang tidak dapat dibaca seperti aslinya. Ada dua konsep utama dalam kriptografi yaitu enkripsi dan dekripsi. Salah satu tools kriptografi yang terkenal adalah cryptool [3] Kriptografi memiliki berbagai macam algoritma yang dapat digunakan untuk mengamankan data, salah satunya yaitu algoritma *Advanced Encryption Standard (AES)*. AES merupakan algoritma kriptografi modern yang dianggap memiliki tingkat keamanan yang tinggi [4]. AES merupakan pengembangan dari algoritma standar *DES (Data Encryption Standard)* [5]. AES memiliki blockkode simetris yang menggantikan Algoritma *DES (Data Encryption Standard).* Algoritma AES memiliki ukuran block konstan yaitu sepanjang 128bit tapi memiliki panjang kunci yang berbeda-beda[6].

Penelitian ini bertujuan untuk melakukan pengamanan data video berformat mp4 dengan menerapakan algoritma AES dengan menggunakan salah satu software kriptografi yaitu cryptool untuk melakukan proses enkripsi dan dekripsi.

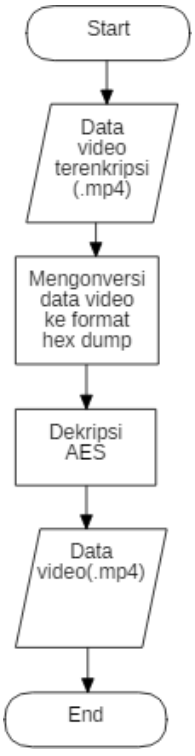
2. METODE PENELITIAN

Penelitian ini terdiri dari 2 proses utama yaitu proses enkripsi dan proses dekripsi. Adapun untuk proses enkripsi alurnya seperti pada Gambar 1 dibawah ini:



Gambar 1. Proses enkripsi data video mp4

Sedangkan untuk proses dekripsi alurnya seperti pada Gambar 2 dibawah ini:



Gambar 1. Proses dekripsi data video mp4

3. HASIL DAN PEMBAHASAN

Hasil perbandingan dari file video *mp4* yang dienkripsi dan didekripsi dengan algoritma AES dapat di lihat pada Tabel 1 berikut.

Tabel 1. Perbandingan File Asli, Enkripsi dan Dekripsi

	File Enkripsi	File Dekripsi	File Asli
Informasi Video			
Length	-	00:03:33	00:03:33
Frame width	-	1152	1152
Frame height	-	720	720
Data rate	-	191 kbps	191 kbps
Total bitrate	-	317 kbps	317 kbps
Frame rate	-	25.00 frames/second	25.00 frames/second
Informasi Audio			
Bit rate	-	125 kbps	125 kbps
Channels	-	2 (stereo)	2 (stereo)
Audio sample rate	-	44.100 kHz	44.100 kHz
Informasi File			
Size	8.16 MB	8.16 MB	8.16 MB
Dapat diputar	Tidak	Ya	Ya

Pada Tabel 1 ditunjukkan bahwa hasil enkripsi suatu file video mp4 dengan algoritma AES dengan panjang kunci 128bit telah menghasilkan suatu file terenkripsi yang tidak memiliki detail informasi seperti pada file aslinya. Selain dari pada itu file hasil enkripsi tersebut tidak dapat diputar atau dijalankan pada media player.

Sementara ketika file terenkripsi tersebut didekripsi dengan algoritma AES menggunakan kunci yang sama, hasilnya file yang telah didekripsi dapat memunculkan kembali detail informasi yang dimilikinya. Detail informasi tersebut sama dengan file aslinya dan file yang telah didekripsi dapat diputar atau dijalankan kembali pada media player.

Walaupun file hasil enkripsi tidak dapat memunculkan detail informasi seperti file asli dan tidak dapat diputar pada media player, tetapi ukuran dari ketiga file tersebut tetap sama yaitu 8.16 MB meskipun telah dilakukan enkripsi ataupun dekripsi.

4. KESIMPULAN

Dari hasil penelitian ini dapat disimpulkan bahwa, algoritma Advanced Encryption Standard (AES) dapat digunakan untuk mengamankan file video mp4 dengan ketentuan bahwa file tersebut diubah terlebih dahulu bentuknya ke bentuk hexdump untuk dapat dienkripsi dan didekripsi. File yang terenkripsi tidak dapat menampilkan detail informasi seperti file aslinya, tetapi ukurannya tetap sama dengan file aslinya. Selain daripada itu, file tersebut tidak dapat diputar menggunakan media player. Sementara ketika file yang terenkripsi didekripsi, file tersebut dapat menampilkan kembali detail informasi seperti file aslinya dan file tersebut dapat diputar menggunakan media player.

DAFTAR PUSTAKA

[1] Kurniawan, D., & Priyatna, B. (2018). Pengamanan data berbasis mobile android dengan penggabungan linear feedback shift register (lfsr) dan modifikasi matriks kunci algoritma kriptografi playfair cipher. Jurnal TELEMATIKA MKOM Vol, 10(1).

[2] Mayasari, R., & Heryana, N. (2016). Perancangan Aplikasi Penyembunyian Pesan Teks Terenkripsi pada Citra Digital Menggunakan Metode Least Significant Bit (LSB). *Syntax: Jurnal Informatika*, *5*(1), 86-92.

[3] Esslinger, Bernhard. & the CrypTool Team. (Agustus, 2017). The CrypTool Book: Learning and Experiencing Cryptography with CrypTool and SageMath. (edisi keduabelas) [Online]. Tersedia: www.cryptool.org.

[4] Farisi, A. (2018). Analisis Kinerja Algoritma Kriptografi Kandidat Advanced Encryption Standard (AES) pada Smartphone, *4*(2), 199–208.

[5] Marisman, A. F., & Hidayati, A. (2015). Pembangunan Aplikasi Pembanding Kriptografi Dengan Caesar Cipher Dan Advance Encryption Standard (Aes) Untuk File Teks. Jurnal Penelitian Komunikasi dan Opini Publik, 19(3), 123498.

[6] Wijaya, H. (2020). Implementasi Kriptografi AES-128 Untuk Mengamankan URL (Uniform Resource Locator) dari SQL Injection. Akademika Jurnal, 17(1), 8-13.