Buletin Sistem Informasi dan Teknologi Islam
Vol 2, No 2, Mei 2021, pp. 72-77
ISSN: 2721-0901

Penerapan Enkripsi dan Dekripsi File Menggunakan Algoritma *Twofish*

Alriadi Try Putra[a,1,*], Poetri Lestari L.B[a,2], Farniwati Fattah[a,3]

[a]*Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Muslim Indonesia, Jl. Urip Sumohardjo KM.05, Makassar dan 90231, Indonesia*
[1]*alriaditryputra@gmail.com;* [2]*poetrilestari@umi.ac.id;* [3]*farniwatifattah@umi.ac.id;*
**corresponding author*

INFORMASI ARTIKEL

Diterima : 10 – 05 – 2021
Direvisi : 24 – 05 – 2021
Diterbitkan : 31 – 05 – 2021

Kata Kunci:
File MP4
Enkripsi
Dekripsi
Algoritma Twofish

ABSTRAK

Seiring dengan perkembangan teknologi, tingkat pengguna internet semakin meningkat. Survei menunjukkan bahwa kenaikan jumlah pengguna internet akan terus bertambah, semakin banyaknya pengguna internet maka semakin banyak juga kejahatan yang terjadi di dunia maya. Salah satu teknik penyembunyian informasi yang cukup terkenal yaitu steganografi. Teknik ini bekerja dengan cara menyembunyikan informasi rahasia di dalam informasi lain sehingga informasi tersebut tidak dapat diketahui oleh orang lain yang tidak bersangkutan. Teknik ini memiliki beberapa metode salah satunya ialah algoritma *twofish*. Algoritma ini sangat baik digunakan dalam proses enkripsi dan dekripsi data, dibandingkan beberapa algoritma lainnya, dikarena algoritma *twofish* merupakan algoritma kuat yang sampai saat ini dinyatakan aman karena masih belum ada serangan kriptanalisis yang benar-benar dapat mematahkan algoritma ini. Aplikasi ini dibangun agar dapat membantu pengguna dalam pengamanan data informasi yang terkandung dalam *file* MP4 yang dikirim tersebut. Setelah melakukan enkripsi/dekripsi *file* sistem juga akan menampilkan angka kecepatan proses enkripsi/dekripsi *file* yang telah diproses. Berdasarkan hasil pengujian yang dilakukan dengan menggunakan teknik *blackbox* menghasilkan *presentase* tertinggi dari kuisioner sebesar 83% menyatakan setuju dengan adanya aplikasi tersebut. Oleh karena itu dapat disimpulkan bahwa sistem yang dibangun, tidak memakan waktu yang lama dalam proses enkripsi/dekripsi file MP4 serta sangat membantu pengguna dalam proses pengamanan data informasi yang terkandung dalam file MP4 tersebut.

I. Pendahuluan

Seiring dengan perkembangan teknologi, tingkat pengguna internet semakin meningkat. Persentase pengguna internet pada daerah perkotaan pada tahun 2014 sekitar 25,84% dan meningkat pada tahun 2018 menjadi 50,92%. Sedangkan pengguna internet didaerah pedesaan pada tahun 2004 sekitar 8,37% dan meningkat menjadi 26,56% pada tahun 2018[1]. Survei menunjukkan bahwa kenaikan jumlah pengguna internet akan terus bertambah, semakin banyaknya pengguna internet maka semakin banyak juga kejahatan yang terjadi di dunia maya. Kejahatan yang paling banyak dilakukan saat ini adalah dengan melalui *website.*

Ancaman terhadap keamanan informasi semakin besar, terutama untuk informasi yang dirahasiakan tersebut. Berbagai ancaman di dunia maya membuat orang khawatir akan keamanan informasi yang dikirimnya. Kekhawatiran inilah yang membuat pengiriman informasi sedikit terhambat, sedangkan informasi tersebut sangat penting bagi orang-orang tertentu. Banyak cara yang dapat dilakukan untuk menyembunyikan informasi yang akan dikirim. Pertama, menggunakan teknik kriptografi, yakni dengan menyandikan informasi menggunakan algoritma tertentu [2]. Dalam penyandian tersebut, mampu mengubah tampilan pesan menjadi sebuah kode-kode aneh yang justru akan membuat penasaran bagi orang yang membacanya, sehingga orang tersebut akan berusaha untuk mengetahui kode-kode aneh yang ditemukannya. Teknik lain adalah dengan menyisipkan pesan yang akan dikirimkan ke media lain, sehingga pesan tersebut akan "tersembunyi" dan yang akan nampak ialah media lain yang digunakan untuk menyisipkan pesan. Teknik penyembunyian informasi yang cukup terkenal yaitu steganografi [3]. Teknik ini mengimbangi kekurangan dari kriptografi yang dapat dengan mudah menimbulkan kecurigaan. Steganografi menyembunyikan informasi rahasia di dalam informasi lain sehingga informasi tersebut tidak dapat diketahui oleh orang lain yang tidak bersangkutan. Teknik ini

mempunyai beberapa metode yang digunakan untuk mengenkripsinya, salah satunya dengan menggunakan algoritma *twofish* [4].

Berdasarkan permasalahan diatas peneliti berinisiatif untuk membuat penerapan enkripsi dan deskripsi *file* menggunakan algoritma *twofish*. Algoritma ini sangat baik digunakan dalam proses enkripsi dan dekripsi data, dibandingkan beberapa algoritma lainnya, dikarena algoritma *twofish* merupakan algoritma kuat yang sampai saat ini dinyatakan aman karena masih belum ada serangan kriptanalisis yang benar-benar dapat mematahkan algoritma ini [5]. Algoritma *twofish* juga merupakan salah satu dari lima finalis dalam pemilihan AES (*Advanced Encryption Standard*). Algoritma *twofish* dinilai memiliki tingkat keamanan yang tinggi dibandingkan dengan algoritma yang lainnya[6], [7].

Hasil dari penelitian ini berupa sebuah aplikasi yang mana aplikasi tersebut mampu melakukan enkripsi dan dekripsi *file* berupa *file* Mp4, file asli yang berisi informasi penting akan disisipkan kedalam *file* biasa menggunakan teknik enkripsi *file* dengan penerapan algoritma *twofish*. Kemudian ketika isi dari *file* asli, ingin diketahui maka kita menggunakan teknik dekripsi file dengan penerapan algoritma *twofish* untuk memecah kode-kode tersebut menjadi teks yang berisi informasi sebelumnya (asli). Algoritma ini tidak mengandung kunci yang lemah, sangat efisien, serta memiliki *design* yang fleksible dan *simple*[8].

II. Metode

A. Tahapan Pengumpulan Data

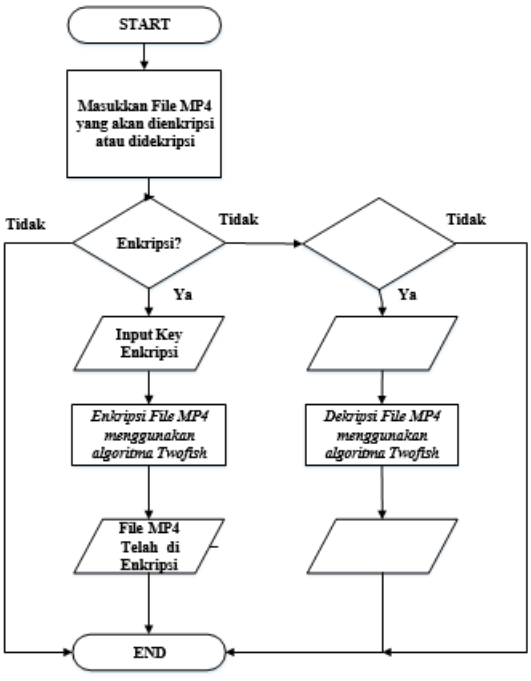
Pengumpulan data dan informasi dilakukan dengan cara observasi. Teknik pengumpulan data dengan cara tersebut bertujuan untuk mengetahui informasi yang terjadi sebenarnya. Penulis mengamati secara langsung informasi yang ada serta mengamati sistem yang berjalan sehingga memudahkan penulis untuk membuat program aplikasi enkripsi dan dekripsi dengan penerapan algoritma *twofish* pada eksistensi file Mp4.

B. Teknik Analisis Data

Teknik analisis data pada penelitian ini dengan mengumpulkan data informasi mengenai pendapat masyarakat terkait keamanan data informasi khusunya dalam bentuk file MP4 (*Video*) yang dikirim melalui media digital saat ini. Kemudian setelah mendapatkan data tersebut, peneliti mulai melakukan analisis terhadap sistem yang akan dibangun berdasarkan data yang telah diperoleh, setelah itu peneliti mulai membuat sistem enkripsi/dekripsi *file* dengan menggunakan pernerapan algoritma *twofish*.

C. Analisis Sistem Usulan

berdasarkan permasalahan yang telah diuraikan diatas, peneliti menawarkan sebuah solusi untuk pengamanan data informasi MP4 (Video) dengan membangun sistem enkripsi/dekripsi *file* dengan penerapan algoritma *twofish*.



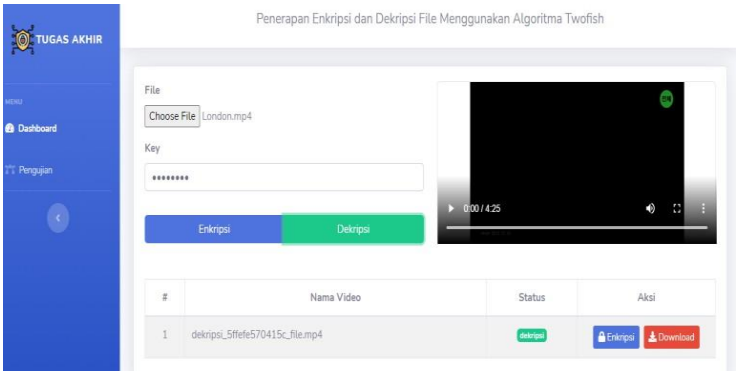
Gambar 1. Analisis Sistem Usulan

Pada gambar diatas menjelaskan mengenai usulan sistem yang akan dibangun. Yang dimana File Mp4 di masukkan ke dalam program aplikasi yang telah dibuat sebelumnya dengan penerapan algoritma *twofish*, kemudian apabila *user* ingin melakukan enkripsi *file* maka inputkan *key* enkripsi sedangkan jika user ingin melakukan dekripsi *file* maka *input key* dekripsinya. Setelah itu, sistem akan melakukan proses enkripsi/dekripsi *file* MP4 menggunakan algoritma twofish, kemudian setelah sistem telah melakukan proses enkripsi ataupun dekripsi maka sistem akan menampilkan *file* MP4 yang telah di proses tersebut.

III. Hasil dan Pembahasan

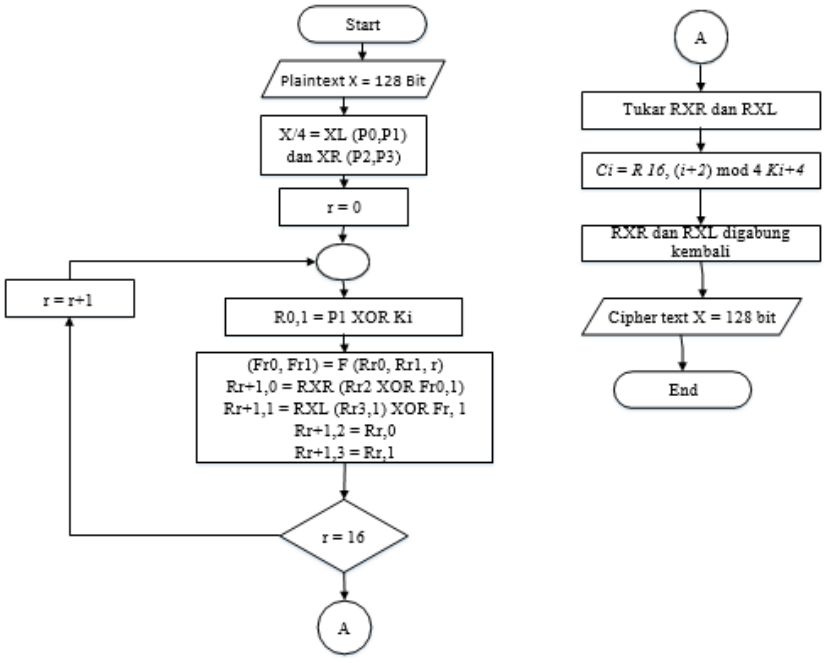
A. Penerapan Enkripsi dan Dekripsi *File* Menggunakan Algoritma *Twofish*

Aplikasi ini dibangun agar dapat membantu masyarakat dalam pengamanan data informasi yang tekandung didalam file MP4 (*Video*), dengan melalui proses enkripsi/dekripsi *file* menggunakan algoritma *twofish*, serta memberikan informasi terkait kecepatan proses enkrpsi/dekripsi yang telah diproses.



Gambar 4. Halaman Utama Aplikasi

B. Proses Enkripsi Algoritma Twofish



Gambar 2. Proses Enkripsi *Twofish*

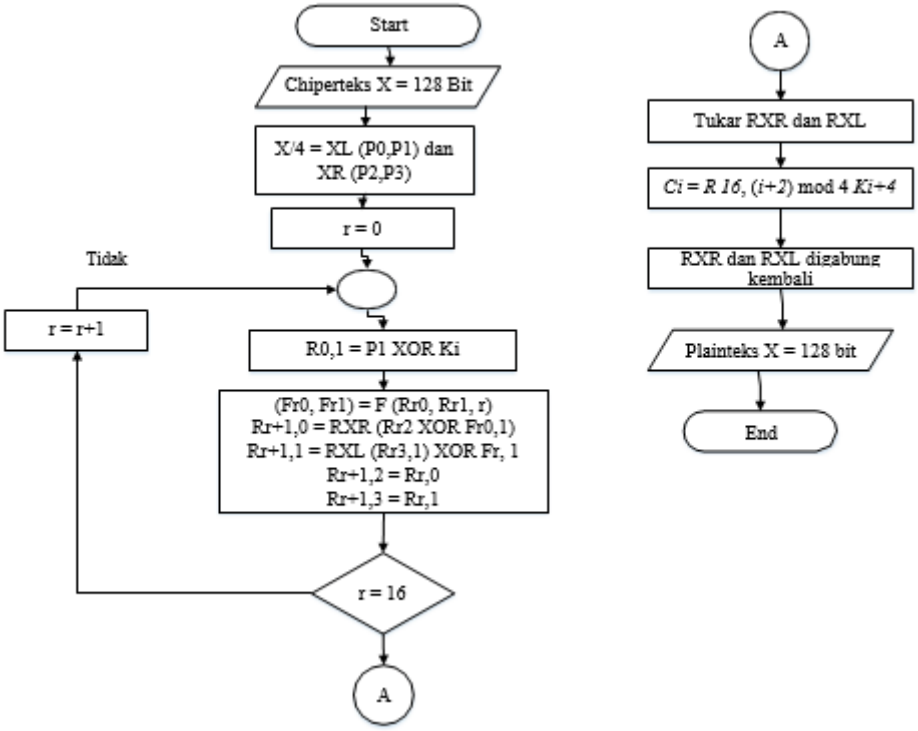
Proses Enkripsi Algoritma *Twofish*. Menjelaskan mengenai alur enkripsi algoritma *twofish*,

yaitu sebagai berikut

1) Memulai proses enkripsi (*plaintext*) dengan X = 128 bit
2) X dibagi menjadi 4 bagian. XL = P0, P1 dan XR = P2, P3
3) *Input whitening* ke-empat bagian tersebut di-XOR dengan kunci yang telah dilakukan ekspansi

4) Melakukan perulangan hingga 16 kali putaran (r = r+1), pada setiap putaran P0 dan P1 sebagai masukan dari fungsi F, P2 dilakukan operasi XOR dan dilakukan rotasi ke kanan sebanyak 1 bit, P3 dirotasikan ke kanan 1 bit dan dilakukan rotasi XOR pada keluaran fungsi F
5) Menukarkan hasil RXR dan RXL
6) *Output whitening* hasil keluaran dan melakukan operasi XOR dengan 4 buah kata dari kunci yang diekspansi
7) Menggabungkan hasil RXR dan RXL.
8) Menghasilkan *cipher text* X
9) Selesai

C. Proses Dekripsi Algoritma Twofish



Gambar 3. Proses Dekripsi

Proses Dekripsi Algoritma *Twofish*. Menjelaskan mengenai alur dekripsi algoritma twofish,

yaitu sebagai berikut

1) Memulai proses dekripsi (*cipher text*) dengan X = 128 bit.
2) X dibagi menjadi 4 bagian. XL = P0, P1 dan XR = P2, P3
3) *Input whitening* ke-empat bagian tersebut di-XOR dengan kunci yang telah diekspansi
4) Melakukan perulangan hingga 16 kali putaran dimulai dengan i = 0, pada setiap putaran P0 dan P1 sebagai masukan dari fungsi F, P2 dilakukan operasi XOR dan dirotasikan ke kanan sebanyak 1 bit, P3 dirotasikan ke kanan 1 bit dan dilakukan rotasi XOR pada keluaran fungsi
5) Menukarkan hasil RXR dan RXL
6) Output whitening hasil keluaran dan melakukan operasi XOR dengan 4 buah kata dari kunci yang diekspansi
7) Menggabungkan hasil RXR dan RXL.
8) Menghasilkan *plaintext* X
9) Selesai.

D. Pengujian Sistem

Pengujian sistem pada penelitian ini dilakukan dengan menggunkan pengujian *blackbox*, yang dilakukan secara objektif dimana aplikasi diuji secara langsung dengan menyebarkan kuisioner yang ditujukan pada

pengguna aplikasi sebanyak 14 koresponden dengan 8 pertanyaan dan 3 pilihan yang akan mewakili dari tujuan akhir penelitian.

Adapun Rekapitulasi perhitungan kuisioner pada penilitian ini sebagai berikut:

Table 1. Tabel rekapitulasi kuisioner

No	Pertanyaan	Keterangan		
		Ya	Tidak	Mungkin
1	Seringkah anda membagikan video(MP4) ?	6	3	5
2	Seringkah anda mengirim video(MP4) melalui email ?	2	10	2
3	Amankah sistem aplikasi ini untuk kerahasiaan file video (MP4) anda?	7	1	6
4	Apakah anda berminat menggunakansistem ini seterusnya ?	8	1	5
5	Apakah proses enkripsi/dekripsi fileMP4 pada sistem tidak membutuhkan waktu yang lama?	4	3	7
6	Apakah sistem yang dibangun (enkripsi/dekripsi file MP4 dengan penerapan algoritma *twofish*) dapat membantu penggunanya dalam hal keamanan serta menjaga kerahasiaandata informasi yang terkandung pada file MP4?	10	0	4
7	Apakah Metode *Twofish* cocok diimplementasikan pada sistem enkripsi/dekripsi file MP4?	9	0	5
8	Apakah aplikasi ini cocok digunakansecara umum oleh masyarakat?	9	0	5
TOTAL :		**55**	**18**	**39**

Perhitungan persentase rekapitulasi kuesioner:

Ya = (5*55)/8 = 34,37

Tidak = (4*18)/8 = 9

Mungkin = (3*39)/8 = 14,62

Total Skor : (34,37+9+14,62) = 58

Penilaian interprestasi responden kuesioner dengan menggunakan rumus index %.

$$Rumus\ Index\ \% = \frac{Total\ Skor}{Y}\ x\ 100 \ldots (1)$$

Keterangan :

Y = (bobot tertinggi) x (Jumlah responden)

Maka penyelesaian akhir dari kasus diatas ialah :

= Total Skor / Y x 100

= 58/70 x 100

= 83%

Berdasarkan hasil pengujian diatas dengan memperoleh nilai 83%, maka dapat di tarik kesimpulan bahwa aplikasi ini memang membantu pengguna dalam melakukan pengamanan data informasi yang terkandung dalam file MP4 tersebut serta tidak memakan waktu yang lama untuk melakukan proses enkripsi/dekripsi file MP4 tersebut.

IV. Kesimpulan

Berdasarkan hasil penelitian diatas, dimana pada sistem enkripsi dan dekripsi *file* MP4 menggunakan penerapan algoritma *twofish* dapat memperoleh kesimpulan bahwa sistem sangat membantu pengguna dalam melakukan pengamanan data informasi *file* MP4 dengan melakukan proses enkripsi/dekripsi *file* MP4 menggunakan algoritma *twofish.* Serta proses enkripsi/dekripsi *file* MP4 yang tidak memakan waktu yang lama dalam hal ini hanya memakan waktu sekitar 0,0299 detik untuk proses enkripsi *file* dan 0,0337

detik untuk proses dekripsi *file* dengan besar ukuran *file* 3,20 Mb. Berdasarkan hasil pengujian diatas dengan memperoleh nilai 83%, maka dapat ditarik kesimpulan bahwa aplikasi ini memang membantu pengguna dalam melakukan pengamanan data informasi yang terkandung dalam *file* MP4 tersebut serta tidak memakan waktu yang lama untuk melakukan proses enkripsi/dekripsi *file* MP4 tersebut.

Daftar Pustaka

[1] Badan Pusat Statistik, "Jumlah Penduduk Perempuan Indonesia pada tahun 2018." 2015.

[2] M. Natsir, "Pengembangan Prototype Sistem Kriptografi Untuk Enkripsi Dan Dekripsi Data Office," *Jurnal*, vol. 6, pp. 2089–5615, 2016.

[3] N. Anwar, "Perancangan Steganografi Hidden Message Dengan Metode Least Significant Bit Insertion (Lsb) Berbasis Matlab," *J. Algoritm. Log. dan Komputasi*, vol. 1, no. 1, pp. 25–30, 2018, doi: 10.30813/j-alu.v1i1.1107.

[4] S. L. Allo, "Perbandingan Konsumsi Energi Algoritma Aes (256 Bit) Dan Twofish (256 Bit) Pada Ponsel Berbasis Android," *Electro Luceat*, pp. 37–51, 2015, doi: Https://Doi.Org/10.32531/Jelekn.V1i1.13.

[5] D. A. Novitasari, R. Rumani, R. Magdalena, P. S. Komputer, and U. Telkom, "Algoritma Twofish Pada Data Teks (Design and Analysis of Twofish Algorithm Cryptography Key Modification on Text Data)," vol. 2, no. 3, pp. 7412–7421, 2015.

[6] Z. Rahman, T. Hasanuddin, and S. Mubarak Abdullah, "Buletin Sistem Informasi dan Teknologi Islam Implementasi Metode Enkripsi dan Deskripsi File menggunakan Algoritma Twofish INFORMASI ARTIKEL ABSTRAK," vol. 1, no. 2, pp. 66–70, 2020.

[7] E. Hasmin, "Implementasi Algoritma Twofish Pada Keamanan Data Berbasis Aplikasi Android," *SENSITIf Semin. Nas. Sist. Inf. …*, 2019.

[8] R. S. Puji Sutan, A. C. Prihandoko, and D. M. Firmansyah, "Analisis Perbandingan Kinerja Algoritma Kriptografi Serpent dan Twofish pada Dataset 'World Bank Projects and Operations,'" *Berk. Sainstek*, vol. 8, no. 3, p. 65, 2020, doi: 10.19184/bst.v8i3.15805.