Buletin Sistem Informasi dan Teknologi Islam
Vol 1, No 2, Mei 2020, pp. 66-70
ISSN: 2721-0901

Implementasi Metode Enkripsi dan Deskripsi File menggunakan Algoritma Twofish

Zulihsan R[a,1,*], Tasrif Hasanuddin [a,2], Syahrul Mubarak Abdullah [a,3]

[a] *Program Studi Teknik informatika,Fakultas Ilmu Komputer,Universitas Muslim Indonesia,Jl.Urip Sumoharjo KM.05, Makassar dan 90231 ,Indonesia*
[1]*ihsanrahman144@gmail.com;* [2] *tasrif.hasanuddin@umi.ac.id;* [3]*syahrul.mubarak@umi.ac.id*
**corresponding author*

INFORMASI ARTIKEL

Diterima : 14 – 05 – 2020
Direvisi : 23 – 05 – 2020
Diterbitkan : 30 – 05 – 2020

Kata Kunci:
Kriptografi
Algoritma Twofish

ABSTRAK

Sistem keamanan data dan kerahasiaan data merupakan salah satu aspek penting dalam perkembangan dunia komunikasi, khususnya komunikasi yang menggunakan komputer dan terhubung dengan jaringan. Algoritma Twofish merupakan salah satu algoritma kriptografi yang bersifat simetris dan beroperasi dalam bentuk blok cipher, jaringan fiestel, dan s-box. Dengan ini Penelitian ini bertujuan untuk mengimplementasikan algoritma twofish dan mengujinya dengan cara membuat sebuah aplikasi berbasis web yang dapat digunakan untuk proses enkripsi dan deskripsi file. Pengujian dilakukan menggunakan file dokumen dengan extension *.doc, *.pdf, dan *.jpg pada aplikasi sistem tersebut.

I. Pendahuluan

Di era modern saat ini, menjaga kerahasiaan informasi merupakan hal yang sangat penting. Sebagai contoh bagi instansi perusahaan besar, penyimpanan dokumen serta data - data penting adalah kewajiban yang mesti dilakukan. Penyalahgunaan data-data rahasia perusahaan tersebut oleh pihak tertentu tentunya bisa saja menimbulkan kerugian yang sangat besar pada perusahaan tersebut. Contoh lainnya adalah komunikasi suara lewat jaringan internet [1]. Kemungkinan pihak lain untuk mencuri informasi yang disampaikan lewat komunikasi elektronik tersebut sangat besar mengingat belum adanya sekuritas khusus terhadap aplikasi tersebut. Karenanya, salah satu alternatif yang dapat digunakan untuk menjaga kerahasiaan informasi tersebut adalah dengan menyamarkannya menjadi bentuk tersandi yang tidak bermakna. Hal tersebut dapat dilakukan dalam kriptografi [2].

Kriptografi merupakan salah satu metode pengamanan data yang dapat digunakan untuk menjaga kerahasiaan data, keaslian data serta keaslian pengirim. Metode ini bertujuan agar informasi yang bersifat rahasia yang dikirim melalui telekomunikasi umum seperti LAN atau internet, tidak dapat diketahui atau dimanfaatkan oleh orang yang tidak berkepentingan atau yang tidak berhak menerimanya [3]. Kriptografi biasanya dalam bentuk enkripsi. Proses enkripsi merupakan proses untuk meng-*encode* dalam bentuk yang hanya dapat dibaca oleh sistem yang mempunyai kunci untuk membaca data tersebut [2]. Proses enkripsi dapat dengan menggunakan software atau hardware. Hasil enkripsi tersebut cipher. Cipher kemudian didekripsi dengan device dan kunci yang sama tipenya (sama softwarenya serta sama kuncinya).

Dengan kriptografi terdapat berbagai macam sistem sandi yang tujuan penggunaan dan tingkat kerahasiaannya berbeda sesuai dengan permintaan user, tetapi dalam prakteknya user menginginkan kemudahan-kemudahan seperti: kerahasiaan data, kecepatan maupun biaya yang murah [5]. Hal ini merupakan kendala dalam membuat suatu sistem kriptografi.

Kenyataan dalam proses pengamanan data dengan metode kriptografi sering kali dibutuhkan waktu yang relatif lama dibandingkan tanpa menggunakan metode kriptografi. Oleh karena itu, diusahakan membuat sistem yang sandi yang lebih cepat dalam kriptografi tanpa mengabaikan kaidah kerahasiaan yang ingin dicapai dan hanya membutuhkan biaya yang murah.

Pada tahun 1972 dan 1974 National of Standart (sekarang bernama NIST) mengumumkan adanya standar enkripsi, yaitu DES (Data Encryption Standard) [6]. Dalam proses perkembangannya ternyata kunci dalam DES dirasa terlalu pendek bagi keamanan komersial akhirnya, NIST mengumumkan AES (Advanced Encryption Standard) [7] pada tahun 1997. Salah satu kandidat AES adalah Twofish. Hal ini disebabkan

Twofish memenuhi semua kriteria yang dibutuhkan NIST, yaitu 128-bit block, 128-bit, 192-bit dan 256 bit key (kata kunci), efisien pada platform manapun.

II. Metode

Kriptografi berasal dari bahasa Yunani, crypto dan graphia. Crypto berarti secret (rahasia) dan graphia berarti writing (tulisan). Jadi kriptografi berarti secret writing (tulisan rahasia). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ketempat lain. Kriptografi pada dasarnya sudah dikenal sejak lama. Menurut catatan sejarah, kriptografi sudah digunakan oleh bangsa Mesir sejak 4000 tahun yang lalu oleh raja- raja Mesir pada saat perang untuk mengirimkan pesan rahasia kepada panglima perangnya melalui kurir-kurinya. Orang yang melakukan penyandian ini disebut kriptografer, sedangkan orang yang mendalami ilmu dan seni dalam membuka atau memecahkan suatu algoritma kriptografi tanpa harus mengetahui kuncinya disebut kriptanalis [2].

Ada empat tujuan mendasar dari ilmu kriptografi, yaitu:

1) Kerahasiaan (Confidentiality), yaitu layanan agar isi pesan yang dikirimkan tetap rahasia dan tidak diketahui oleh pihak lain (kecuali pihak pengirim, pihak penerima/pihak-pihak memiliki ijin). Layanan ini direalisasikan dengan menyandikan pesan menjadi cipherteks.
2) Integritas data (data integrity), adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain menyangkut penyisipan, penghapusan, dan pensubtitusian data lain ke dalam data yang sebenarnya.
3) Otentikasi (authentication) yaitu layanan yang berhubungan dengan identifikasi. Baik otentikasi pihak-pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data/informasi.
4) Nirpenyangkalan (non-repudiation), yaitu layanan yang dapat mencegah suatu pihak untuk menyangkal aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal dirinya).

A. Algoritma TWOFISH

Algoritma Twofish merupakan algoritma kriptografi kunci simetrik cipher blok dengan panjang setiap blok adalah tetap 128 bit [8]. Sedangkan kunci yang dapat diterima adalah: 128, 192, atau 256 bit. Algoritma Twofish memanfaatkan teknik pemanipulasian bit, kotak permutasi/pemutihan, jaringan feistel, pemutaran ulang dengan pergiliran kunci dengan jumlah perputaran dan pergiliran kunci sebanyak 16 kali, tranformasi pseudo- Hadamard, ekspansi dan filter, dan kotak MDS (*Most Distance Separable*).

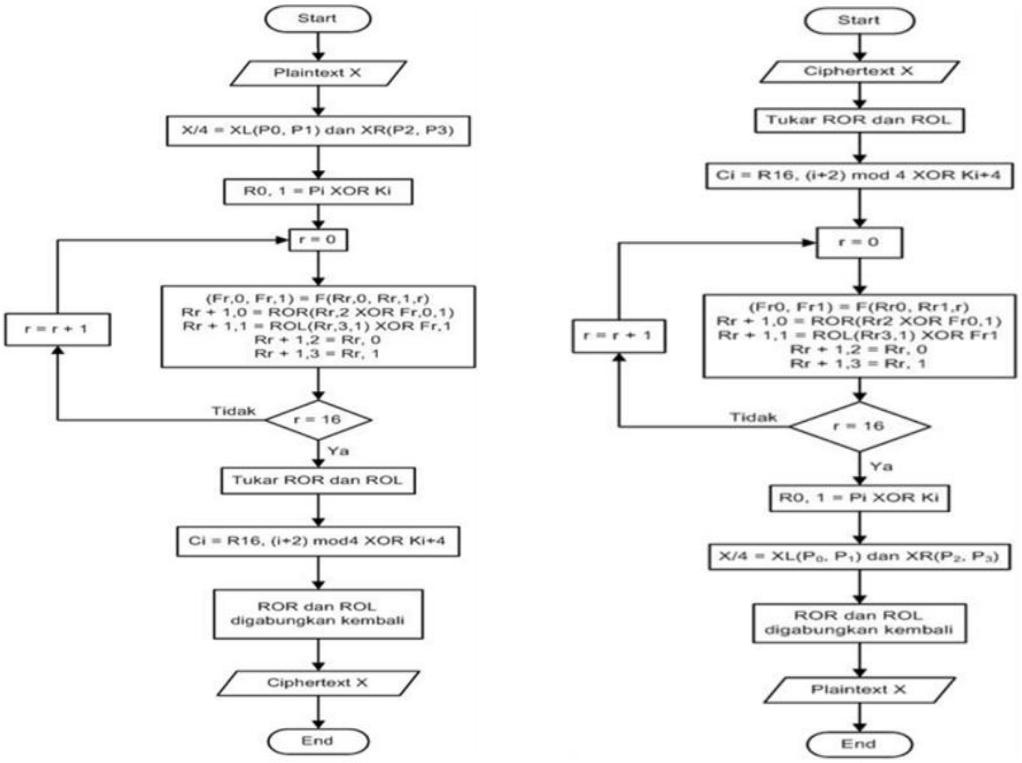
B. Blok Pembangunan TWOFISH

Secara garis besar algoritma twofish dibangun dari beberapa algoritma utama, algoritma-algoritma tersebut diambil dari prinsip pembangunan algoritma *cipher* blok:

- Kotak-S adalah matriks yang berisi substitusi non-linear yang memetakan satu atau lebih bit dengan satu atau lebih bit yang lain dan digunakan di banyak *cipher* blok. Kotak-S memiliki ukuran input dan ukuran output yang bervariasi. Ada empat pendekatan yang digunakan dalam mengisi Kotak-S: dipilih secara acak, dipilih secara acak lalu diuji, dibut oleh orang, dihitung secara matematis. Kotak-S pertama digunakan di Lucifer, lalu DES dan diikuti banyak algoritma enkripsi yang lain. Twofish menggunakan empat buah 8x8 bit Kotak-S yang berbeda, bijektif, dan bergantung pada kunci. Kotak-S ini dibuat menggunakan 8x8 bit permutasi dan material kunci.

- Kode MDS (Maximum Distance Separable) pada sebuah field adalah pemetaan liner dari x elemen field ke y elemen field, dan menghasilkan vektor komposit $x + y$ elemen, dengan ketentuan bahwa jumlah minimum dari elemen bukan nol pada setiap vektor bukan nol paling sedikit $y + 1$. Dengan kata lain, jumlah elemen yang berbeda diantara dua vektor berbeda yang dihasilkan oleh pemetaan MDS paling sedikit $y + 1$. Dapat dibuktikan dengan mudah bahwa tidak ada pemetaan yang dapat memiliki jarak pisah yang lebih besar diantara dua vektor yang berbeda, maka disebut jarak pisah maksimum (maximum distance separable). Pemetaan MDS dapat direpresentasikan dengan sebuah MDS matriks yang teridiri dari $x \times y$ elemen. Kode perbaikan-kesalahan Reed Solomon (RS) adalah MDS. Kondisi yang diperlukan untuk sebuah $x \times y$ matriks untuk menjadi MDS adalah semua kemungkinan submatriks kotak, yang diperoleh dengan membuang kolom atau baris, adalah tidak singular. Serge Vaudenay pertama kali mengajukan matriks MDS sebagai elemen desain kode. Shark dan Square menggunakan matrika MDS, meskipun konstruksinya pertama kali ditemukan di kode Manta yang tidak dipublikasikan. Twofish menggunakan matriks MDS tunggal 4x4.

Proses Encode algoritma twofish adalah proses enkripsi file hingga menghasilkan chipertext kunci dengan panjang 128 bit. Sedangkan proses decode algoritma twofish adalah proses deskripsi file hingga menghasilkan plaintext yang sama pada saat enkripsi file [8][9]. Perbedaan prosesn enkripsi dan deskripsi Algoritma *twofish* dapat kita lihat pada gambar 1:



Gambar 1. *flowchart* proses enkripsi dan deskripsi file algoritma *twofish*

C. Keamanan TWOFISH

Tingkat keamanan suatu algoritma kunci simetris tipe *cipher* blok dapat diukur dari tingkat kerumitan algoritma, panjang blok yang digunakan, panjang kunci yang digunakan dan tingkat pengacakan plainteks terhadap cipherteks [8]. Algoritma Twofish menggunakan jaringan Feistel dan kotak-S dalam implementasinya. Karena itu tingkat keamanan algoritma ini juga dipengaruhi oleh cara penjadwalan kunci internal dan cara pembangkitan kunci-S.

Semakin tinggi tingkat kerumitan suatu algoritma maka algoritma tersebut semakin sulit dipecahkan. Semakin besar ukuran blok yang digunakan akan mengakibatkan semakin jarangnya terdapat chiperteks berulang yang berasal dari plainteks yang sama. Hal ini menyebabkan hubungan antara plainteks dan chiperteks menjadi kabur, sehingga mempersulit kriptanalisis untuk melakukan penyerangan terhadap algoritma kriptografi yang digunakan.

Ukuran panjang suatu kunci juga berpengaruh pada kekuatan algoritma. Biasanya semakin panjang dan acak suatu kunci akan mempersulit penyerangan algoritma kriptografi. Tingkat pengacakan plainteks dan cipherteks yang tinggi mengakibatkan sulitnya mencari hubungan antara plainteks dan cipherteks. Hal ini akan mempersulit kriptanalisis untuk melakukan penyerangan.

Kotak-S digunakan algoritma *Twofish* dalam fungsi *f* pada jaringan feistel. Cara pembangkitan kotak-S ini mempengaruhi tingkat kerumitan pada fungsi *f* tersebut. Ada dua macam pendekatan dalam pembangkitan kotak-S ini. Pertama adalah pembangkitan kotak-S secara statis, pembangkitan secara statis ini berarti kotak-S yang digunakan tidak bergantung pada plainteks dan kunci yang dimasukkan. Pendekatan kedua adalah pembangkitan kotak-S secara dinamis. Pembangkit dinamis ini biasanya diimplementasikan dengan menggunakan fungsi bilangan acak [10].

III. Hasil dan Pembahasan

Pengujian ini akan dilakukan untuk mengetahui apakah sistem aplikasi sudah berjalan sesuai dengan metode enkripsi dan deskripsi menggunakan *algoritma twofish* yang telah dibuat. Pengujian dilakukan secara langsung dan teliti, agar proses pengujian berjalan dengan sesuai harapan.

Berikut adalah skenario sebelum melakukan pengujian terhadap sistem:

- Menjalankan aplikasi XAMPP dengan cara mengklik *start* pada *module apache.*
- Menjalankan sistem aplikasi melalui salah satu aplikasi web browser yaitu google chrome.

- Setelah sistem terbuka selanjutnya klik tombol *choose file* yang berfungsi sebagai pilih file yang akan di proses dalam pengujian pada sistem tersebut.

Tabel 1. Tabel Skenario Pengujian

No	Skenario	Hasil Pengujian
1	Aplikasi XAMP sudah dijalankan	Sistem aplikasi terbuka di web browser
2	Pilih file pengujian	File telah dipilih ke dalam sistem
3	Proses enkripsi file	File telah terenkripsi dengan menghasilkan kode chipertext
4	Proses deskripsi file	File telah terdeskripsi dengan menghasilkan file asli sebelum enkripsi file

Pengujian ini akan dilakukan untuk mengetahui apakah sistem aplikasi sudah berjalan sesuai dengan metode enkripsi dan deskripsi menggunakan *algoritma twofish* yang telah dibuat. Pengujian dilakukan secara lansung dan teliti, agar proses pengujian berjalan dan sesuai harapan. Hasil pengujian enkripsi dan deskripsi file dokumen dapat dilihat pada tabel 2.

Tabel 2. Hasil Enkripsi dan Deskripsi File

No	Nama File	Hasil Proses	
		enkripsi	deskripsi
1	Docx 1	vj0TTbeFTJvXlwSK5NxKd0O2o+JUAXRbmQlR+7vtYG8=	C:\fakepath\Docx l.docx
2	Docx 2	vj0TTbeFTJvXlwSK5NxKd8YlXglOsEv1UQ3JZlAhlYw=	C:\fakepath\Docx 2.docx
3	Docx 3	vj0TTbeFTJvXlwSK5NxKd4oYdEOvtHXDA+nl0PYvh2I=	C:\fakepath\Docx 3.docx
4	Docx 4	vj0TTbeFTJvXlwSK5NxKdzeEitMzosqEpTTbZCgOpy4=	C:\fakepath\Docx 4.docx
5	Docx 5	vj0TTbeFTJvXlwSK5NxKd54nAh9JZej2mUdUWBEcE+c=	C:\fakepath\Docx 5.docx
6	pdf 1	2N0pW4rdx3hhi136nqMdT3gE6xQbDmXPyINN2M+wVck=	C:\fakepath\pdf l.pdf
7	pdf 2	2N0pW4rdx3hhi136nqMdT3XPg3iJhaQ2J8Ahc5UVlD8=	C:\fakepath\pdf 2.pdf
8	pdf 3	2N0pW4rdx3hhi136nqMdT3k4s/GU3hKcTGuO76U+VM8=	C:\fakepath\pdf 3.pdf
9	pdf 4	2N0pW4rdx3hhi136nqMdT1luqfSup8FrbYjsKtG2iy0=	C:\fakepath\pdf 4.pdf
10	pdf 5	2N0pW4rdx3hhi136nqMdTwQ0qD9Voo8RfjRhMYkPs9E=	C:\fakepath\pdf 5.pdf
11	Jpg 1	POiXbyLqRAzs5gwzKSMgLBCu4LizLgzL9wVsTp+hmUE=	C:\fakepath\Jpg 1.jpg
12	Jpg 2	POiXbyLqRAzs5gwzKSMgLDiH/rXXx1g7k3782mQ0AFA=	C:\fakepath\Jpg 2.jpg
13	Jpg 3	POiXbyLqRAzs5gwzKSMgLJ+rZXXMrGh1UXEsq9K85L0=	C:\fakepath\Jpg 3.jpg
14	Jpg 4	POiXbyLqRAzs5gwzKSMgLGpHK5adr4909eUyA1iWhvY=	C:\fakepath\Jpg 4.jpg
15	Jpg 5	POiXbyLqRAzs5gwzKSMgLMz4J8sDTDT87tOvXyNm120=	C:\fakepath\Jpg 5.jpg

Dari hasil implementasi proses enkripsi dan deskripsi file menggunakan *algoritma twofish* pada tabel 2, pengujian file dokumen dilakukan sebanyak 15 kali percobaan dengan file yang berbeda dimana menghasilkan masing-masing kode *chipertext* sesuai dengan kaidah prinsip algoritma twofish dengan *block chiper simetris* dengan panjang kunci 128 bit.

IV. Kesimpulan dan saran

Proses enkripsi dan deskripsi dapat diterapkan dengan baik di berbagai jenis format file docx, pdf, dan jpg. Berdasarkan hasil implementasi metode enkripsi dan deskripsi *file* menggunakan *algoritma twofish* yang telah dilakukan, algoritma Twofish adalah cipher blok yang menerima *key* dengan panjang variabel 128bit dan tidak memiliki *key* yang lemah dan perbandingan waktu proses yang diperlukan untuk enkripsi dan dekripsi dalam pembentukan *key* adalah hampir sama. Twofish memiliki kehandalan dalam implementasinya

diatas berbagai *platform microprocessor, smart card* dan *hardware* yang dibuat sebagai perangkat enkripsi data.

Daftar Pustaka

[1] O. O. Ayokunle, "Implementing Security on a Voice over Internet Protocol (VoIP) Network: A Practical Approach," *IOSR J. Comput. Eng.*, vol. 7, no. 4, pp. 24–30, 2012, doi: 10.9790/0661-0742430.

[2] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," *Inform. Mulawarman J. Ilm. Ilmu Komput.*, vol. 10, no. 1, p. 20, 2016, doi: 10.30872/jim.v10i1.23.

[3] O. K. Sulaiman, "Analisis sistem keamanan jaringan dengan Menggunakan Switch Port Security," *Comput. Eng. Syst. Sci.*, vol. 1, no. 1, pp. 9–14, 2016.

[4] E. R. Syahputra, "Analisa Pengujian Estimasi Waktu Dan Besar Ukuran File Menggunakan Algoritma Twofish Pada Proses Enkripsi Dan Dekripsi," *Times*, vol. IV, no. 2. pp. 14–19, 2015.

[5] C. Laybats and L. Tredinnick, "Information security," *Bus. Inf. Rev.*, vol. 33, no. 2, pp. 76–80, 2016, doi: 10.1177/0266382116653061.

[6] K. Rabah, "Theory and Implementation of Data Encryption Standard: A Review," *Information Technology Journal*, vol. 4, no. 4. pp. 307–325, 2005, doi: 10.3923/itj.2005.307.325.

[7] K. P. Choudhury and S. Kakoty, "Comparative Analysis of Different Modified Advanced Encryption Standard Algorithms over Conventional Advanced Encryption Standard Algorithm," *Int. J. Curr. Res. Rev.*, vol. 9, no. 22, pp. 31–34, 2017, doi: 10.7324/ijcrr.2017.9227.

[8] D. A. Trianggana and H. Latipa Sari, "Analisis Perbandingan Kinerja Algoritma Blowfish Dan Algoritma Twofish Pada Proses Enkripsi Dan Dekripsi," *Pseudocode*, vol. 2, no. 1, pp. 37–44, 2015, doi: 10.33369/pseudocode.2.1.37-44.

[9] M. Muhathir, "Perbandingan Algoritma Blowfish Dan Twofish Untuk Kriptografi File Gambar," *J. Informatics Telecommun. Eng.*, vol. 2, no. 1, p. 23, 2018, doi: 10.31289/jite.v2i1.1673.

[10] A. Devi and B. S. Ramya, "Two fish Algorithm Implementation for lab to provide data security with predictive analysis," *Int. Res. J. Eng. Technol.*, vol. 04, no. 05, pp. 3033–3036, 2017.