Jurnal Mahasiswa Ilmu Komputer (JMIK)
Vol. 03, No. 01, Maret 2022

ANALISIS PERBANDINGAN HASIL ENKRIPSI DAN DEKRIPSI ALGORITMA KRIPTOGRAFI RIJNDAEL DAN TWOFISH UNTUK PENYANDIAN DATA

Elsa Elvira Awal[1)], E. Haodudin Nurkifli[2)], Tesa Nur Padilah[3)]
[1)] Program Studi Teknik Informatika, Universitas Buana Perjuangan Karawang
[2-3*)]Program Studi Teknik Informatika, Universitas Singaperbangsa Karawang

Jalan Ronggo Waluyo Sirnabaya, Karawang
Email: elsaelvira@ubpkarawang.ac.id [1)] dudi.nurkifli@staff.unsika.ac.id [2)]
tesa.nurpadilah@staff.unsika.ac.id [3)]

Abstrak - Pada zaman modern ini, kemajuan teknologi sudah sangat pesat sehingga data atau informasi perlu diamankan secara ketat untuk menjaga kerahasiaannya. Kriptografi sendiri merupakan salah satu ilmu untuk mengamankan data atau informasi dari pihak lain yang mencoba meretas informasi tersebut. Dengan kriptografi data atau informasi bisa sampai kepada pihak yang dituju tanpa diretas oleh pihak lain yang tidak mengetahui kuncinya. Maka di penelitian ini akan dilakukan perbandingan algoritma kriptografi Rijndael dan algoritma Twofish, untuk mengetahui kecepatan waktu proses enkripsi dan dekripsi menggunakan panjang kunci yang berbeda, 128 bit dan 256 bit juga untuk mengetahui apakah ada perubahan ukuran file sebelum dan sesudah di enkripsi menggunakan algoritma kriptografi Rijndael dan algoritma Twofish. Dipilihnya algoritma kriptografi Rijndael dan algoritma Twofish karena ingin membandingkan kecepatan waktu enkripsi dan dekripsi juga ukuran *file* setelah di enkripsi menggunakan dua algoritma yang dinyatakan lemah pada penelitian sebelumnya. Penelitian ini menggunakan metodologi kuantitatif dikarenakan hasil yang didapat merupakan angka atau numerik. Penelitian ini pun menggunakan metode pendekatan kausal komparatif karena membandingkan dua objek untuk mengetahui mana yang lebih baik. Diuji menggunakan uji t 2 populasi. Hasil yang didapat pada penelitian ini yaitu untuk kecepatan waktu enkripsi menggunakan kunci 128 bit dan 256 bit, algoritma Rijndael lebih cepat dari algoritma Twofish. Untuk kecepatan waktu dekripsi menggunakan kunci 128 bit dan 256 bit, algoritma Rijndael lebih cepat dari algoritma Twofish. Dan terakhir untuk ukuran file setelah di enkripsi menggunakan kunci 128 bit dan 256 bit, tidak ada perubahan yang signifikan antara algoritma Rijndael dan algoritma Twofish.

Kata Kunci : Kriptografi, Rijndael, Twofish, uji t 2 populasi

Abstract - : *In modern times, has been very rapid advances in technology so that the data or information needs to be secured tightly to keep it confidential. Cryptography itself is one of the sciences to secure data or information from others who try to hack the information. Cryptographic data or information can be up to the addressee without being mapped out by others who do not know the key. So in this study will be a comparison of cryptographic algorithms Rijndael and algorithm Twofish, to determine the speed of encryption and decryption using key length is different, 128 bit and 256 bit also to find out if there are*

changes in the size of files before and after encryption using a cryptographic algorithm Rijndael and Twofish algorithms. Chosen the cryptographic algorithm Rijndael and Twofish algorithms for wanting to compare the speed of encryption and decryption time is also the size of the files after encryption using two algorithms are expressed weakly in previous research. This study uses a quantitative methodology because the results obtained are a number or numerical. This research was using the method of causal comparative approach for comparing two objects to determine which one is better. Tested using t-test two populations. The results obtained in this study is to speed time encryption using 128-bit key, and 256 bits, the Rijndael algorithm is faster than the algorithm Twofish. To speed time decryption using a key of 128 bits and 256 bits, the Rijndael algorithm is faster than the algorithm Twofish. And lastly to the size of the files after encryption using a key of 128 bits and 256 bits, no significant changes between the algorithm Rijndael and Twofish algorithms.

Keywords: *Cryptography, Rijndael, t test 2 population , Twofish*

PENDAHULUAN

Kriptografi adalah bidang pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi dan dekripsi. Teknik ini untuk mengkonversi data ke bentuk kode-kode tertentu agar informasi tidak dapat terbaca oleh siapapun kecuali pihak yang berhak. Salah satu metode kriptografi yang biasa digunakan adalah algoritma simetris yang menggunakan kunci yang sama saat melakukan enkripsi dan dekripsi sehingga informasi sulit dipahami maknanya [1].

Algoritma kriptografi terbagi dalam algoritma klasik dan modern. Contoh algoritma klasik adalah *Caesar Cipher*, sedangkan contoh dari algoritma modern adalah algoritma *Twofish* dan *Rijndael*. Kedua algoritma tersebut memiliki beberapa kesamaan yaitu, sama-sama menggunakan kunci simetris dan Cipher Blok. Namun kesamaan ini hanya struktural, karena operasi matematika yang dilakukan di dalamnya berbeda.

Kelebihan yang dimiliki algoritma *Rijndael* yaitu *Rijndael* merupakan algoritma *block cipher* dengan menggunakan sistem permutasi dan substitusi (P-Box dan S-Box) bukan dengan jaringan Feistel sebagaimana *block cipher* pada umumnya. Sedangkan kelebihan algoritma *Twofish* yaitu memiliki varian dengan sebuah nomor variabel dari setiap *round*, cocok sebagai *stream cipher* fungsi *hash* satu arah, MAC dan *pseudo random number generator*, dengan menggunakan metode konstruksi yang dapat dimengerti, memiliki varian *famili-key* untuk memungkinkan versi cipher yang berbeda dan *non interruptible*.

Penelitian ini akan membandingkan dua algoritma *Rijndael* dan *Twofish*, dengan menggunakan parameter kecepatan waktu enkripsi, kecepatan waktu dekripsi dan ukuran *file* setelah dilakukan proses enkripsi. Pemilihan *file* yang akan dienkripsi pun mengikuti penelitian sebelumnya yaitu menggunakan *file* teks yang berformat *.pdf, *.doc, dan *.txt. Namun pada penelitian ini panjang kunci diperpanjang menjadi 256 bit atau 32 byte.

KAJIAN PUSTAKA DAN LANDASAN TEORI

Kriptografi

Kriptografi adalah ilmu untuk mengurangi resiko ancaman keamanan dengan melakukan proses enkripsi dan dekripsi pada data dan informasi [2].

Algoritma Rijndael

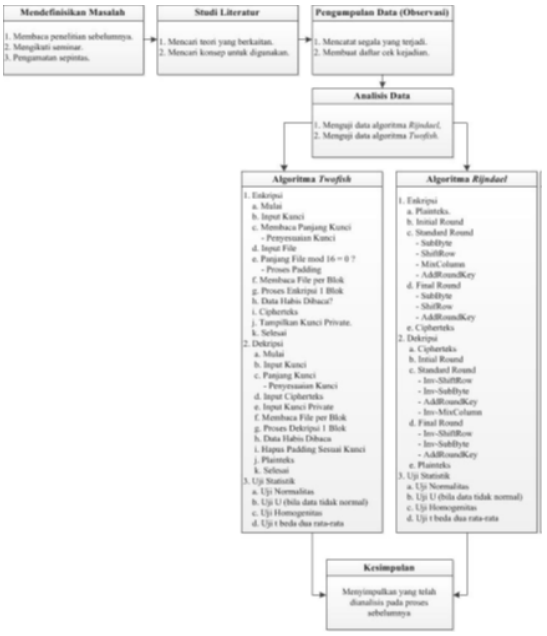
Algoritma Rijndael didesain untuk mengganti algoritma DES yang sudah cukup lama. Algoritma ini menggunakan kunci 128-bit, 192-bit atau 256 bit. Algoritma ini dibuat oleh dua orang periset yaitu Joan Daemen dan Vincent Rijmen. Rijndael telah dipilih oleh NIST (*National Institute of Standards and Technology*) sebagai proposal yang paling cocok dengan kriteria keamanan, efisiensi dalam implementasi, sifat yang berubah-ubah dan kesederhanaan [3].

Algoritma Twofish

Algoritma Twofish merupakan algoritma yang diciptakan oleh Bruce Scheiner, sebelumnya beliau menciptakan Algoritma Blowfish. Algoritma Twofish merupakan salah satu kandidat AES disebabkan Twofish memenuhi semua kriteria NIST, yaitu 128-bit block, 192 bit dan 256 bit key atau kata kunci [4].

METODE

Metode yang digunakan dalam penelitian ini adalah metodologi penelitian kuantitatif dengan pendekatan metode komparatif. Penelitian ini akan menguji kecepatan waktu proses (enkripsi dan dekripsi) dan memori yang digunakan oleh algoritma Rijndael dan algoritma Twofish. Terdapat lima tahapan di dalam metode komparatif, yaitu mendefinisikan masalah, studi literatur, pengumpulan data, analisis, dan kesimpulan. Metode pendekatan komparatif, memiliki tahapan sebagai begitu:



Gambar 1 Alur Penelitian

HASIL DAN PEMBAHASAN

Mendefinisikan Masalah

Masalah yang ditemukan pada penelitian ini adalah perubahan ukuran file setelah proses enkripsi, apakah semakin besar file maka akan semakin lama juga proses untuk mengenkripsi dan dekripsi file tersebut.

Studi Literatur

Dari beberapa referensi atau literatur yang telah dibaca, maka hasil yang didapat adalah referensi metode yang digunakan, referensi objek penelitian, referensi konsep-konsep atau kerangka dalam penelitian.

Pengumpulan Data

Pada penelitian ini populasi yang ada akan dijadikan sampel juga, dan data waktu kecepatan proses enkripsi dan dekripsi dilakukan dengan observasi, yaitu diamati secara langsung ketika proses enkripsi dan proses dekripsi. Dan untuk data ukuran file didapat secara random dari file novel yang telah dikumpulkan dalam format *.pdf, *.doc dan *.txt. Adapun untuk beberapa data kecepatan waktu proses enkripsi, waktu dekripsi dan

ukuran file sebelum dan sesudah di enkripsi, dapat dilihat oleh Gambar berikut:

No.	Ukuran *File Input*	Ukuran *File Output*	Waktu Proses Enkripsi (detik)	Waktu Proses Dekripsi (detik)
1	1.214.021	1.214.032	2	3
2	2.845.999	2.846.000	3	3
3	4.396.828	4.396.832	4	4
4	1.061.494	1.061.504	2	3
5	1.327.667	1.327.680	2	3
6	1.041.297	1.041.312	2	2
7	2.078.938	2.078.944	3	3
8	1.430.450	1.430.464	2	2
9	2.689.209	2.689.216	3	3
10	1.108.281	1.108.288	2	2

Gambar 2 File Novel *.pdf Kunci 128 bit Rijndael

No.	Ukuran *File Input*	Ukuran *File Output*	Waktu Proses Enkripsi (detik)	Waktu Proses Dekripsi (detik)
1	39.721.693	39.721.696	14	26
2	1.920.673	1.920.688	3	3
3	2.698.625	2.698.640	4	3
4	2.055.854	2.055.856	3	3
5	1.736.343	1.736.352	3	3
6	2.252.724	2.252.736	3	3
7	1.772.569	1.772.576	3	2
8	1.199.104	1.199.104	2	2
9	1.197.396	1.197.408	2	2
10	54.660.112	54.660.112	20	29

Gambar 3 File Novel *.doc Kunci 128 bit Rijndael

No.	Ukuran *File Input*	Ukuran *File Output*	Waktu Proses Enkripsi (detik)	Waktu Proses Dekripsi (detik)
1	205.779	205.792	2	2
2	241.827	241.840	2	2
3	460.879	460.880	1	2
4	294.423	294.432	2	2
5	235.946	235.952	2	2
6	319.155	319.168	2	2
7	345.343	345.344	2	2
8	529.600	529.600	2	2
9	561.795	561.808	2	1
10	619.607	619.616	2	2

Gambar 4 File Novel *.txt Kunci 256 bit Rijndael

No.	Ukuran *File Input*	Ukuran *File Output*	Waktu Proses Enkripsi (detik)	Waktu Proses Dekripsi (detik)
1	1.214.021	1.214.032	4	3
2	2.845.999	2.846.000	5	5
3	4.396.828	4.396.832	7	6
4	1.061.494	1.061.504	3	3
5	1.327.667	1.327.680	4	4
6	1.041.297	1.041.312	3	3
7	2.078.938	2.078.944	4	5
8	1.430.450	1.430.464	4	4
9	2.689.209	2.689.216	6	6
10	1.108.281	1.108.288	4	3

Gambar 5 File Novel *.pdf Kunci 128 bit Twofish

No.	Ukuran *File Input*	Ukuran *File Output*	Waktu Proses Enkripsi (detik)	Waktu Proses Dekripsi (detik)
1	39.721.693	39.721.696	60	75
2	1.920.673	1.920.688	5	5
3	2.698.625	2.698.640	6	5
4	2.055.854	2.055.856	5	4
5	1.736.343	1.736.352	5	5
6	2.252.724	2.252.736	5	5
7	1.772.569	1.772.576	5	4
8	1.199.104	1.199.104	3	3
9	1.197.396	1.197.408	4	4
10	54.660.112	54.660.112	71	69

Gambar 6 File Novel *.doc Kunci 128 bit Twofish

No.	Ukuran *File Input*	Ukuran *File Output*	Waktu Proses Enkripsi (detik)	Waktu Proses Dekripsi (detik)
1	205.779	205.792	2	2
2	241.827	241.840	3	2
3	460.879	460.880	3	2
4	294.423	294.432	1	2
5	235.946	235.952	2	2
6	319.155	319.168	2	2
7	345.343	345.344	2	1
8	529.600	529.600	3	5
9	561.795	561.808	3	3
10	619.607	619.616	3	3

Gambar 7 File Novel *.txt Kunci 256 bit Twofish

Analisis Data

Analisis data atau pengujian data yang digunakan ada beberapa uji, yaitu uji normalitas data untuk mengetahui apakah data tersebut berdistribusi normal atau tidak. Jika data tidak berdistribusi normal maka langkah selanjutnya adalah uji U, tapi jika data berdistribusi normal maka langkah selanjutnya adalah uji homogenitas untuk mengetahui apakah data yang akan diteliti memiliki varian yang sama atau tidak. Terakhir adalah uji t independent dua populasi. Berikut adalah hasil analisis:

Pengujian Ukuran File Setelah dienkripsi (*.pdf kunci 128 bit)

a. Uji Normalitas Data

Uji normalitas menggunakan uji Kolmogorov-Smirnow dan Shapiro-Wilk

Jika jumlah sampel > 50 → Kolmogorov-Smirnov

Jika jumlah sampel ≤ 50 → Shapiro-Wilk

Kriteria pengujian:

Jika nilai probabilitas < 0,05, maka data berdistribusi tidak normal.

Jika nilai probabilitas > 0,05, maka data berdistribusi normal.

Tests of Normality

	NamaAlgoritma	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
		Statistic	df	Sig.	Statistic	df	Sig.
Ukuran File dalam Satuan Byte	Algoritma Rijndael	,222	30	,001	,731	30	,000
	Algoritma Twofish	,222	30	,001	,731	30	,000

a. Lilliefors Significance Correction

Gambar 8 Output Uji Normalitas

Kesimpulan:

Karena nilai probabilitas untuk algoritma Rijndael dan algoritma Twofish

sama-sama dibawah 0,05, yaitu 0,000. Maka dapat disimpulkan bahwa data tidak berdistribusi dengan normal. Karena data tidak berdistribusi dengan normal, maka langkah selanjutnya yaitu melakukan uji U (Mann-Whitney).

b. Uji U (Mann-Whitney)

Setelah melakukan uji normalitas data dengan pengujian Shapiro- Wilk, langkah selanjutnya yaitu menguji perbedaan rata-rata data dengan uji U (Mann-Whitney).

Hipotesis pengujian:

H0 Asymp. Sig > Sig. : Ukuran file setelah proses enkripsi antara algoritma Rijndael sama dengan algoritma Twofish.

H1 Asymp. Sig < Sig: Ukuran file setelah proses enkripsi antara algoritma Rijndael tidak sama dengan algoritma Twofish.

Test Statistics[a]

	Ukuran File dalam Satuan Byte
Mann-Whitney U	450,000
Wilcoxon W	915,000
Z	,000
Asymp. Sig. (2-tailed)	1,000

a. Grouping Variable: NamaAlgoritma

Gambar 9 Output Uji U

Kesimpulan:

Dari output di atas diketahui nilai Asymp. Sig. sebesar 1,000, karena nilai Asymp. Sig. 1,000 > 0,05, maka sesuai dengan dasar pengambilan Keputusan dalam uji Mann-Whitney dapat disimpulkan bahwa H0 diterima. Penerimaan terhadap H0 mengandung pengertian bahwa tidak ada perbedaan yang signifikan pada ukuran file (*.pdf kunci 128 bit) yang telah dienkripsi dengan algoritma Rijndael dan algoritma Twofish.

Kesimpulan Hasil Analisis

Pada tahap terakhir yaitu kesimpulan, akan menampilkan hasil atau simpulan dari data yang telah diolah atau dianalisis, berikut tabel kesimpulan dari seluruh perhitungan yang telah dilakukan. Pada tabel pertama berisi tentang perbedaan ukuran file setelah melakukan proses enkripsi antara algoritma Rijndael dan algoritma Twofish. Pada tabel kedua berisi tentang lama waktu proses enkripsi antara algoritma Rijndael dan algoritma Twofish. Dan tabel terakhir berisi tentang lama waktu proses dekripsi antara algoritma Rijndael dan algoritma Twofish.

Jenis *File*	Panjang Kunci	Algoritma *Rijndael*	Algoritma *Twofish*	Kesimpulan
pdf	128	2.049.452	2.049.452	Tidak ada perbedaan dari kedua algoritma
doc	128	13.735.658	13.735.658	Tidak ada perbedaan dari kedua algoritma
txt	128	421.810,70	421.810,70	Tidak ada perbedaan dari kedua algoritma
pdf	256	2.049.452	2.049.452	Tidak ada perbedaan dari kedua algoritma
doc	256	13.735.658	13.735.658	Tidak ada perbedaan dari kedua algoritma
txt	256	421.810,70	421.810,70	Tidak ada perbedaan dari kedua algoritma

Gambar 10 Ukuran File Setelah di enkripsi (byte)

Jenis *File*	Panjang Kunci	Algoritma *Rijndael*	Algoritma *Twofish*	Kesimpulan
pdf	128	2,47	4,33	*Rindael* lebih cepat
doc	128	7,67	20,03	*Rindael* lebih cepat
txt	128	2,03	2,3	*Rindael* lebih cepat
pdf	256	2,07	4,87	*Rindael* lebih cepat
doc	256	7,67	18,13	*Rindael* lebih cepat
txt	256	1,73	2,37	*Rindael* lebih cepat

Gambar 11 Kecepatan Waktu Enkripsi (detik)

Jenis *File*	Panjang Kunci	Algoritma *Rijndael*	Algoritma *Twofish*	Kesimpulan
pdf	128	2,73	4,2	*Rindael* lebih cepat
doc	128	8,67	20,07	*Rindael* lebih cepat
txt	128	2	2,23	*Rindael* lebih cepat
pdf	256	2,03	4,93	*Rindael* lebih cepat
doc	256	6,67	20,37	*Rindael* lebih cepat
txt	256	1,83	2,33	*Rindael* lebih cepat

Gambar 12 Kecepatan Waktu (detik)

KESIMPULAN

Dari tahap-tahap penelitian yang telah dilakukan, mulai dari perumusan masalah, pengumpulan data hingga analisis data, kesimpulan yang didapat adalah sebagai berikut:

1. Waktu proses enkripsi berpengaruh dengan besarnya ukuran file, dengan contoh file yang berukuran rata-rata 25.991.456 byte memerlukan waktu enkripsi selama 14,67 detik dan waktu dekripsi selama 14,33 detik. Sedangkan file yang berukuran rata-rata 746,760 byte memerlukan waktu enkripsi selama 2 detik dan waktu dekripsi selama 2 detik.
2. Perbedaan lamanya waktu proses enkripsi menunjukan bahwa algoritma Rijndael lebih cepat dengan rata-rata 3,94 detik pada setiap proses enkripsi, sedangkan algoritma Twofish mempunyai rata-rata 8,67 detik pada setiap proses enkripsi.
3. Perbedaan lamanya waktu proses dekripsi menunjukan bahwa algoritma Rijndael lebih cepat dengan rata-rata 3,99 detik pada setiap proses dekripsi, sedangkan algoritma Twofish mempunyai rata-rata 9,02 detik pada setiap proses dekripsi.
4. Perubahan ukuran file setelah dilakukan proses enkripsi tidak mengalami perubahan antara algoritma Rijndael dan algoritma Twofish. Keduanya memiliki rata-rata ukuran file yang sama setelah melakukan proses enkripsi, yaitu 5.402.305 byte.

REFERENSI

[1] Zulfikar, M. I., Abdillah, G., & Komarudin, A. (2019). Kriptografi untuk Keamanan Pengiriman Email Menggunakan Blowfish dan Rivest Shamir Adleman (RSA). Seminar

[2] Siringoringo, R. (2020). Analisis dan Implementasi Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File. Kumpulan Artikel Karya Ilmiah Fakultas Ilmu Komputer, 31-42.

[3] Prayitno, A., & Nurdin, N. (2017). Analisa dan Implementasi Kriptografi pada Pesan Rahasia Menggunakan Algoritma Cipher Transposition. Jurnal Elektronik Sistem Informasi dan Komputer, 1-10.

[4] Laylim, F., & Khairuzzaman, M. Q. (2019). Penerapan Algoritma Twofish dalam Perancangan Aplikasi Chat Berbasis Android. Jurnal ENTER, 76-87.