SNESTIK
Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informatika
https://ejurnal.itats.ac.id/snestik dan https://snestik.itats.ac.id

Informasi Pelaksanaan :
SNESTIK IV - Surabaya, 27 April 2024
Ruang Seminar Gedung A, Kampus Institut Teknologi Adhi Tama Surabaya

Informasi Artikel:
DOI : 10.31284/p.snestik.2024.5918

Prosiding ISSN 2775-5126

Fakultas Teknik Elektro dan Teknologi Informasi-Institut Teknologi Adhi Tama Surabaya
Gedung A-ITATS, Jl. Arief Rachman Hakim 100 Surabaya 60117 Telp. (031) 5945043
Email : snestik@itats.ac.id

Implementasi Kriptografi pada Email Menggunakan Metode Advanced Encryption Standard dan Rivest Code 4 Berbasis Web

Danang Haryo Sulaksono*, Juan Yoseph Oktafilia Putra
Institut Teknologi Adhi Tama Surabaya
e-mail: danang_h_s@itats.ac.id

ABSTRACT

Computer progress has had a major impact on people's lives, especially in terms of the efficient exchange of information. However, it also brings with it increased security risks, especially when using email, leading to concerns about data loss and tampering. To mitigate these risks, cryptographic security measures have been implemented. Cryptography protects the confidentiality and integrity of data. Two common cryptographic methods were used in this study: Advanced Encryption Standard (AES) and Rivest Code 4 (RC4). AES is a standard algorithm for symmetric key encryption, while RC4 is a stream cipher that processes input data simultaneously. In the study, email messages were sent in plain text, encrypted in ciphertext and decrypted back into plain text using the same algorithm. The test results showed that RC4 had the lowest average CPU load (17.3%) during encryption, while AES had the lowest average memory load (36%). The avalanche effect tests showed a high average value (94.799%) for plaintext and key tests. RC4 also showed the fastest average encryption time (0.608 seconds). These findings indicate that both the AES and RC4 methods are suitable for encrypting email content.

***Keywords**: Cryptography, Advanced Encryption Standard, Rivest Code 4,plaintext, ciphertext*

ABSTRAK

Kemajuan komputer telah memberikan dampak besar terhadap kehidupan masyarakat, terutama dalam hal efisiensi pertukaran informasi. Namun, hal ini juga membawa peningkatan risiko keamanan, terutama saat menggunakan email, sehingga menimbulkan kekhawatiran tentang kehilangan dan gangguan data. Untuk memitigasi risiko ini, langkah-langkah keamanan kriptografi telah diterapkan. Kriptografi melindungi kerahasiaan dan integritas data. Dua metode kriptografi umum digunakan dalam penelitian ini: Advanced Encryption Standard (AES) dan Rivest Code 4 (RC4). AES merupakan algoritma standar untuk enkripsi kunci simetris, sedangkan RC4 merupakan stream cipher yang memproses data masukan secara bersamaan. Dalam penelitian tersebut, pesan email dikirim dalam teks biasa, dienkripsi dalam teks tersandi, dan didekripsi kembali menjadi teks biasa menggunakan algoritma yang sama. Hasil pengujian menunjukkan bahwa RC4 memiliki rata-rata beban CPU terendah (17,3%) selama enkripsi, sedangkan AES memiliki rata-rata beban memori terendah (36%). Pengujian efek longsoran menunjukkan nilai rata-rata yang tinggi (94,799%) untuk pengujian teks biasa dan kunci. RC4 juga menunjukkan waktu enkripsi rata-rata tercepat (0,608 detik). Temuan ini menunjukkan bahwa metode AES dan RC4 cocok untuk mengenkripsi konten email.

Kata Kunci : Kriptografi, Advanced Encryption Standard, Rivest Code 4, plainteks, chiperteks

PENDAHULUAN

Pesatnya perkembangan teknologi saat ini terjadi karena perkembangan dari teknologi Komputer yang dapat membantu manusia dalam berbagai macam kegiatan, Seperti pertukaran informasi dapat dilakukan salah satunya menggunakan E-Mail (Electronic Mail) karena kemudahan dalam penggunaan dan pengiriman pesan dapat dilakukan secara efisiensi Namun dibalik kelebihan dan keuntungan dari kemajuan teknologi yang diberikan terdapat potensi berbahaya yang muncul. Permasalahan dari penggunaan E-Mail (Electronic Mail) adalah sering terjadi suatu kebocoran informasi. hal ini dapat terjadi karena pengiriman email akan melalui proses yang panjang dan melewati banyak server. Proses Panjang itu terdapat celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab dengan mencuri atau memanipulasi informasi di dalam akun E-mail. Oleh karena itu dibutuhkan sebuah sistem teknologi keamanan dalam menggunakan sebuah media elektronik yang dapat membantu mengamankan data dan informasi dari serangan cyber salah satunya adalah dengan teknologi keamanan kriptografi yang dapat diterapkan dalam pengiriman dan pengamanan pesan dalam sebuah email.

Kriptografi sendiri secara umum dapat diartikan sebagai ilmu dan seni penyandian yang digunakan untuk menjaga keamanan dan kerahasian dari suatu data. Banyak metode yang sering digunakan dalam kriptografi Salah satu metode kriptografi yang sering digunakan adalah AES dan RC4 yang dapat melindungi dalam bentuk kerahasian pesan informasi atau data serta dapat memberi perlindungan terhadap pengubahan atau pemalsuan informasi yang tidak diinginkan. kriptografi bertujuan melindungi kerahasian dari pesan dengan cara menyamarkan isi pesan atau informasi menjadi bentuk tersandi yang tidak dapat dibaca oleh siapapun (Aditya Indra & Pramusinto, 2018a; Ukkas et al., n.d.-a)

Dalam penelitian terdahulu yang dilakukan oleh Ahmad Galih Pramudito dan Dewi Kusumaningsih pada tahun (2018) dengan judul "Implementasi Algoritma AES 128 Dan RC4 Untuk Pengamanan Email Pada PT Dinamika Hydro Engineering" hasil dari penelitiannya adalah proses pengiriman E-Mail yang menggunakan enkripsi dengan metode AES 128 dan RC4 menjadi lebih aman, sedangkan untuk pesan yang diterima menjadi tidak dapat terbaca apabila tidak menggunakan aplikasi kriptografi, untuk hasil deskripsi akan kembali seperti semula tanpa ada perubahan sedikitpun. Dalam kecepatan proses enkripsi dan dekripsi akan berbanding lurus dengan ukuran pesan dan file lampiran.

METODE

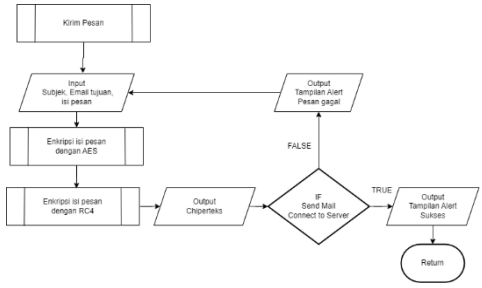
Tahapan Penelitian

Metode penelitian ini mempelajari bagaimana berbagai langkah penelitian yang dilakukan secara sistematik. Dalam hal ini perlu dijelaskan mengapa sebuah metode penelitian atau teknik tersebut dipilih

Perancangan Sistem

Pada bagian ini akan memberikan gambaran umum mengenai alur proses berjalanya enkripsi pada aplikasi email menggunakan metode Advanced Encryption Standard dan Rivest Code 4 :

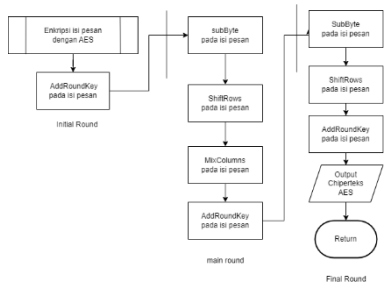
Proses Pengiriman Pesan



Gambar 1 Flowchart Proses Pengiriman Pesan

Pada menu proses kirim pesan pengguna akan menginput email tujuan, subjek pesan, isi pesan email. selanjutnya isi pesan akan di enkripsi menggunakan metode AES dan dilanjutkan enkripsi menggunakan metode RC4 yang menghasilkan output berupa chiperteks berikutnya pesan akan dikirim ke server dan apabila proses berhasil pesan email akan diteruskan kepada email tujuan dan akan muncul tampilan pesan sukses dan apabila gagal akan muncul tampilan pesan gagal dan tampilan akan Kembali ke menu untuk Input pesan.

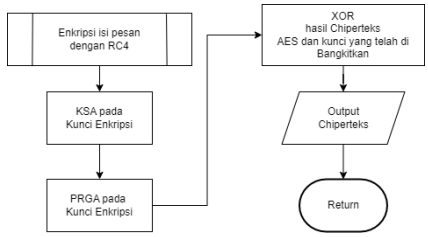
Enkripsi AES



Gambar 2 Flowchart Proses Enkripsi AES

Pada proses enkripsi menggunakan metode Advanced encryption Standard (AES) didalam proses terlebih dahulu isi pesan yang menjadi plainteks dan kunci pesan di proses dalam add round key dengan mengubah isi pesan dan kunci menjadi hexadecimal untuk initial round dan proses selanjutnya isi pesan akan di proses dalam substitusi byte dengan memetakan setiap byte dari array state dengan menggunakan tabel substitusi, ShiftRows melakukan pergeseran secara wrapping pada 3 baris terakhir dari array state, MixColumns merupakan proses mengalikan setiap kolom dari array state dengan polinomial, AddRoundKey ini melakukan operasi XOR terhadap sebuah round key dengan array state. plainteks selanjutnya akan diproses dalam final round dengan melalui subbyte, Shift rows, add round key yang sama seperti sebelumnya dan akan menghasilkan output berupa Chiperteks AES yang nantinya akan di enkripsi lagi menggunakan metode RC4.

Enkripsi RC 4



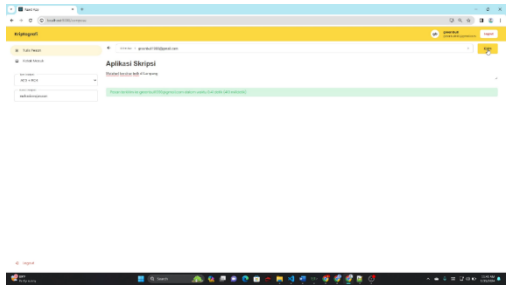
Gambar 3 Flowchart Proses Enkripsi RC4

Pada proses Enkripsi RC4 Kunci akan di ekspansi melalui proses KSA yaitu pembentukan Tabel Array S dan yang akan di permutasi dan selanjutnya akan diproses PERAGA yaitu Tabel array S akan digunakan pada proses ini untuk menghasilkan keystream yang selanjutnya hasil dari ekspansi kunci akan XOR dengan Chiperteks yang berasal dari hasil enkripsi menggunakan metode AES yang nantinya hasil dari XOR tersebut akan menghasilkan Cipherteks baru hasil penggabungan Metode AES dan RC4.

HASIL DAN PEMBAHASAN

Tampilan Hasil

Berikut ini akan dijelaskan tentang tampilan hasil dari Implementasi Aplikasi enkripsi email menggunakan metode Advanced Encryption Standard dan Rivest code 4.



Gambar 4 Tampilan Hasil Implementasi Aplikasi

merupakan tampilan untuk halaman Kirim pesan, didalamnya terdapat menu untuk memilih metode enkripsi yang akan digunakan terdapat AES, RC4, dan gabungan antara metode AES dan RC4. Selanjutnya terdapat menu untuk menulis pesan yang di dalamnya kita dapat memasukan alamat email yang dituju, Subject, dan isi dari pesan email yang akan dikirim untuk mengirim pesan yang telah ditulis terdapat menu kirim di bagian pojok kanan yang digunakan sebagai button untuk mengirim pesan.

Hasil Pengujian

pengujian pada AES, RC4, gabungan AES dan RC4 menggunakan metode Avalanche Effect dan pengujian waktu proses enkripsi

Avalanche Effect

Pada percobaan ini penulis melakukan pengujian menggunakan avalanche effect untuk melihat perubahan kecil pada input menghasilkan seberapa besar perubahan pada output dengan cara melakukan perubahan kecil terhadap plainteks dan kunci.

Tabel 1 Hasil Pengujian Avalanche effect

No	Plainteks	Kunci	Metode	Avalanche effect
1	Sebuah Pesan Pendek	Kampus Itats Jaya	AES	97,72%
2	Sebuah Pesan Pendek	Kampus Itats Jaya	RC4	87,5%
3	Sebuah Pesan Pendek	Kampus Itats Jaya	AES dan RC4	96,6%
4	sepulang dari SEKOLAH	ITATS kampus aku	AES	93,18%
5	sepulang dari SEKOLAH	ITATS kampus aku	RC4	100%
6	sepulang dari SEKOLAH	ITATS kampus aku	AES dan RC4	95%
7	KELINCI asyik bermain	bunga MAWAR 1234	AES	93,18%
8	KELINCI asyik bermain	bunga MAWAR 1234	RC4	100%
9	KELINCI asyik bermain	bunga MAWAR 1234	AES dan RC4	96,6%
10	RIMBUNNYA PEPOHONAN	BUNGA melati 123	AES	97,72%
11	RIMBUNNYA PEPOHONAN	BUNGA melati 123	RC4	93,75%
12	RIMBUNNYA PEPOHONAN	BUNGA melati 123	AES dan RC4	86,36%
13	Matahari Bersinar Terik	ROSEMARY flower 123	AES	90,90%
14	Matahari Bersinar Terik	ROSEMARY flower 123	RC4	96,875%
15	Matahari Bersinar Terik	ROSEMARY flower 123	AES dan RC4	96,6%

Pada hasil percobaan yang dilakukan penulis pada pengujian menggunakan avalanche effect menunjukan bahwa metode AES memiliki nilai rata-rata avalanche effect sebesar 94,54%, dan metode RC4 memiliki nilai rata-rata avalanche effect sebesar 95,625%, dan gabungan metode AES dan RC4 memiliki nilai rata-rata avalanche effect sebesar 93,632%, dan pada pengujian avalanche effect menggunakan perubahan kecil pada plainteks dan kunci menghasilkan nilai rata-rata avalanche effect sebesar 94,799% .

Waktu Proses Enkripsi

Pada percobaan ini penulis melakukan pengujian untuk mengirim pesan yang di Enkripsi Pada Setiap masing-masing metode akan dilihat seberapa lama waktu yang dibutuhkan dalam proses enkripsinya.

Tabel 2 Hasil Pengujian Waktu Proses Enkripsi

NO	Plainteks	key	AES	RC4	AES dan RC4
1	Matahari bersinar terik di Surabaya	Mahasiswa JR INFOR	0,756s	0,411s	1,091s
2	Sinarnya terhalang rimbunnya pepohonan	mahasiswa jurusan	0,449s	0,426s	0,824s
3	Burung-burung berkicau seolah sedang menyanyi	mahasiswa ITATS	1,075s	1,012s	1,403s
4	Bunyi riak jernih sungai beradu dengan batu	ITATS JAYA 12345	1,075s	1,023s	1,089s
5	si anak gajah yang sekarang tengah asyik bermain	TEKNIK INFORMATIK	1,213s	1,013s	2,226s
6	Seorang anak laki-laki bernama Andi sedang bermain	informatika itats	0,585s	0,476s	0,926s
7	Sepulang dari sekolah andi makan kue ulang tahun	ITATSJaya_if_123	0,466s	0,401s	0,763s
8	Dewi ingin ayah sehat dan berbahagia	mahasiswa jarkom	0,584s	0,452s	0,704s
9	Perkenalkan namaku Gwen Amanda aku merupakan anak pintar	program studi if	0,553s	0,418s	0,769s
10	Bolehkah aku meminjam bukumu ensiklopedia tentang hewan	jurusan infor IT	0,516s	0,454s	0,886s

Pada hasil percobaan yang dilakukan penulis pada pengujian menggunakan metode menghitung waktu proses saat enkripsi menunjukan bahwa metode AES memiliki rata-rata waktu proses enkripsi sebesar 0,618s, dan metode RC4 memiliki rata-rata waktu proses enkripsi sebesar 0,608s, dan terakhir metode gabungan AES dan RC4 memiliki rata-rata waktu proses enkripsi sebesar 1,068s.

KESIMPULAN

Berdasarkan hasil pengujian yang telah dilakukan pada AES, RC4, gabungan AES dan RC4 menggunakan Pengujian metode Avalanche Effect dan Pengujian Waktu Proses Enkripsi maka penulis mendapatkan kesimpulan sebagai berikut :

1. Pada hasil percobaan yang dilakukan penulis menyatakan bahwa hasil pengujian avalanche effect dengan plainteks dan kunci diubah memiliki nilai rata-rata sebesar 94,799% dan pada hasil pengujian di setiap metode yang digunakan menunjukan bahwa metode AES memiliki nilai rata-rata avalanche effect sebesar 94,54%, dan metode RC4 memiliki nilai rata-rata avalanche effect sebesar 95,625%, dan gabungan metode AES dan RC4 memiliki nilai rata-rata avalanche effect sebesar 93,632%. dari pengujiaan ini dapat disimpulkan bahwa pada pengujian dengan plainteks dan kunci diubah memiliki nilai rata-rata yang tinggi.

2. Pada hasil percobaan yang dilakukan penulis menyatakan bahwa metode RC4 memiliki waktu rata-rata sebesar 0,608s, selanjutnya metode AES memiliki waktu rata-rata sebesar 0,618s, dan terakhir metode gabungan RC4 dan AES memiliki waktu rata-rata sebesar 1,068s. dari pengujiaan ini dapat disimpulkan bahwa hasil pengujian dari ketiga metode menunjukan bahwa metode RC4 memiliki waktu untuk proses enkripsi tercepat dan Metode gabungan AES dan RC4 memiliki waktu proses enkripsi terlama dibandingkan metode lainnya.

DAFTAR PUSTAKA

1. Aditya Indra, R., & Pramusinto, W. (2018). *APLIKASI EMAIL(Electronic Mail)MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD(AES-128) DAN ALGORITMA RIVEST CIPHER 4(RC4) BERBASIS WEB*.
2. Budi Handoko, L., & Muslih. (2022). PENGUJIAN AVALANCHE EFFECT PADA KRIPTOGRAFI TEKS MENGGUNAKAN AUTOKEY CIPHER. *2 St Proceeding STEKOM*, *2022*.
3. Daniel Zain Rohman, F., & Mufti. (2018). *IMPLEMENTASI KRIPTOGRAFI PADA PENGIRIMAN PESANEMAILDENGAN MENGGUNAKAN METODE RC4 DAN BLOWFISH BERBASIS WEB PADA PT.DASCOM JAYA SAKTI*.
4. Handoyo, J., & Subakti, Y. M. (n.d.). *KEAMANAN DOKUMEN MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD (AES)*. http://www.jurnal.umk.ac.id/sitech
5. Kusniyati, H., Diansyah, S., & Yusuf, R. (2018a). PENERAPAN ALGORITMA RIVERT CODE 4 (RC4) PADA APLIKASI KRIPTOGRAFI DOKUMEN. In */ Jurnal PETIR* (Vol. 11, Issue 1).
6. Riyantono, R., & Pramusinto, W. (2018). *APLIKASI PENGAMANAN SURAT ELEKTRONIK (EMAIL) MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD 128 (AES-128) DAN RIVEST CIPHER CODE 4 (RC4) BERBASIS WEB* (Vol. 1, Issue 2).
7. Saragi, D. R., Gultom, J. M., Tampubolon, J. A., & Gunawan, I. (2020). Pengamanan Data File Teks (Word) Menggunakan Algoritma RC4. *Jurnal Sistem Komputer Dan Informatika (JSON)*, *1*(2), 114. https://doi.org/10.30865/json.v1i2.1745
8. Tahara Shita, R., & Li Hin, L. (n.d.-a). *IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES 128BIT DAN ELGAMAL UNTUK PENGAMANAN E-MAIL PADA BANDARA INTERNASIONAL SULTAN MAHMUD BADARUDDIN II PALEMBANG*.
9. Tulloh, A. R., Permanasari, Y., & Harahap, E. (2016). Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen. *Jurnal Matematika UNISBA*, *15*(1). http://ejournal.unisba.ac.id
10. Ukkas, M. I., Arriyanti, E., Hanggara, R. T., Informatika, T., Widya, S., & Dharma, C. (n.d.-a). *IMPLEMENTASI ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) 128 BIT UNTUK PENGAMANAN PESAN TEXT DALAM EMAIL*.