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.2024.5714

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 Algoritma Caesar Cipher dan Rivest Shamir Adleman Super Enkripsi Teks Pesan dengan Karakter ASCII

Andra Fahrezi Kusuma, Siti Agustini, Maftahatul Hakimah, Muchamad Kurniawan
Institut Teknologi Adhi Tama Surabaya
e-mail: sitiagustini@itats.ac.id

ABSTRACT

Humans are never separated from information needs when viewed from technology use. Data security is important because it relates to confidentiality, integrity, authentication, and privacy. Some information has privacy that the public should not share. Therefore we need a way to secure information so that the information does not spread widely to unauthorized parties. This study used Caesar Cipher and RSA Algorithms to secure a text message. So the data would not be easily hacked by irresponsible parties. The encryption process started using the Caesar Cipher Algorithm by entering a key/shift of letters to produce a ciphertext. Ciphertext Caesar is used for the encryption process for the second time using the RSA algorithm. RSA ciphertext result was converted into ASCII characters. The algorithm proposed to secure message text data using a combination of letters and numbers in each trial. The Caesar Cipher Algorithm implementation results obtained an average avalanche effect value of 35.03%. At the same time, the RSA algorithm obtained an average avalanche effect value of 55.10%. And the Caesar-RSA algorithm obtained an average avalanche effect value of 59.015%. The best test results were obtained by combining the two algorithms, Caesar Cipher and RSA, which showed that the proposed algorithm could secure message text data effectively.

Keywords: *Information, Caesar Cipher, RSA, Encryption, Avalanche Effects*

ABSTRAK

Meninjau dalam penggunaan teknologi, manusia tak pernah lepas dari kebutuhan sebuah informasi. Keamanan data merupakan suatu hal penting, karena berkaitan dengan kerahasiaan, integritas, otentikasi dan privasi. Beberapa informasi memiliki privasi yang tidak boleh tersebar oleh publik, oleh karena itu

diperlukan cara dalam mengamankan informasi agar informasi tersebut tidak tersebar luas kepada pihak yang tak berwenang. Penelitian ini menerapkan Algoritma Caesar Cipher dan RSA untuk mengamankan sebuah teks pesan agar data tidak mudah diretas oleh pihak yang tidak bertanggung jawab. Proses Enkripsi dimulai pertama kali menggunakan Algoritma Caesar Cipher dengan memasukkan kunci/pergeseran huruf agar menghasilkan sebuah ciphertext yang nantinya ciphertext Caesar ini digunakan untuk proses enkripsi kedua kalinya menggunakan algoritma RSA, yang kemudian hasil ciphertext RSA dikonversikan ke dalam karakter ASCII. Algoritma yang diusulkan digunakan untuk mengamankan data teks pesan, dengan menggunakan kombinasi huruf dan angka pada setiap percobaannya. Hasil implementasi dengan menerapkan Algoritma Caesar Cipher didapatkan nilai efek avalanche rata-rata sebesar 35,03%. Sedangkan Algoritma RSA didapatkan nilai efek avalanche rata-rata sebesar 55,10%. Dan Algoritma Caesar-RSA didapatkan nilai efek avalanche rata-rata sebesar 59,015%. Hasil pengujian terbaik didapatkan dengan menggabungkan kedua algoritma yaitu Caesar Cipher dan RSA yang menunjukkan bahwa algoritma yang diusulkan mampu mengamankan data teks pesan secara efektif.

Kata kunci: Informasi, Caesar Cipher, RSA, Enkripsi, Efek Avalanche

PENDAHULUAN

Jumlah data digital berkembang pesat setiap hari melalui Internet. Keamanan memainkan peran penting dalam kemajuan sistem komunikasi, terutama dengan materi rahasia yang dikirimkan melalui jaringan karena ketersediaan data digital yang berkelanjutan dan penyerang yang mencoba mengakses data ini [1]. Meninjau dalam penggunaan teknologi, manusia tak pernah lepas dari kebutuhan sebuah informasi. Keamanan data merupakan suatu hal penting, karena berkaitan dengan kerahasiaan, integritas, otentikasi dan privasi. Beberapa informasi memiliki privasi yang tidak boleh tersebar oleh publik, oleh karena itu diperlukan cara dalam mengamankan informasi agar informasi tersebut tidak tersebar luas kepada pihak yang tak berwenang [2].

Pada proses pengiriman teks pesan terdapat beberapa hal yang harus diperhatikan, yaitu: kerahasiaan, integritas data, autentikasi dan non-repudiasi [3]. Oleh karena itu dibutuhkan proses penyandian atau pengkodean sebelum dilakukan proses pengiriman. Sehingga file yang dikirim terjaga kerahasiaannya dan tidak mudah diubah untuk menjaga integritas file tersebut. Ilmu yang mempelajari tentang cara pengamanan data dikenal dengan istilah Kriptografi, sedangkan langkah-langkah dalam kriptografi disebut dengan Algoritma Kriptografi. Pengguna harus selalu mengenkripsi file apa pun yang mereka kirim, idealnya menggunakan bentuk enkripsi kunci publik. Ini juga merupakan ide yang baik untuk mengenkripsi file penting atau sensitif, mulai dari kumpulan foto keluarga hingga data perusahaan seperti catatan personalia atau riwayat akuntansi [4].

Kriptografi menjadi salah satu bidang yang paling utama digunakan dan diperlukan untuk mencapai tingkat perlindungan yang tinggi antara individu yang berbeda. Kriptografi public key adalah faktor utama yang paling umum untuk keamanan dan perlindungan sistem. Ini adalah teknik yang kuat untuk mengamankan transmisi data dalam sistem. Public key menggunakan dua peran fungsi enkripsi dan dekripsi. Fungsi enkripsi berarti mengenkripsi sebuah teks pesan dan mengubahnya menjadi sandi, sedangkan fungsi dekripsi berarti mengubah sandi menjadi sebuah teks pesan [5].

Dalam banyak karya penelitian, telah ada banyak peninjauan untuk mempelajari dan mengembangkan banyak aplikasi kriptografi kunci publik untuk mengamankan data saat transmisi dalam sistem [6]. Penting memilih sebuah algoritma untuk memastikan enkripsi yang efektif dan tepat. Salah satunya adalah melakukan pendekatan baru untuk mengenkripsi dan mendekripsi teks pesan yang terkait dengan karakter ASCII menggunakan Algoritma Caesar Cipher dan RSA [7].

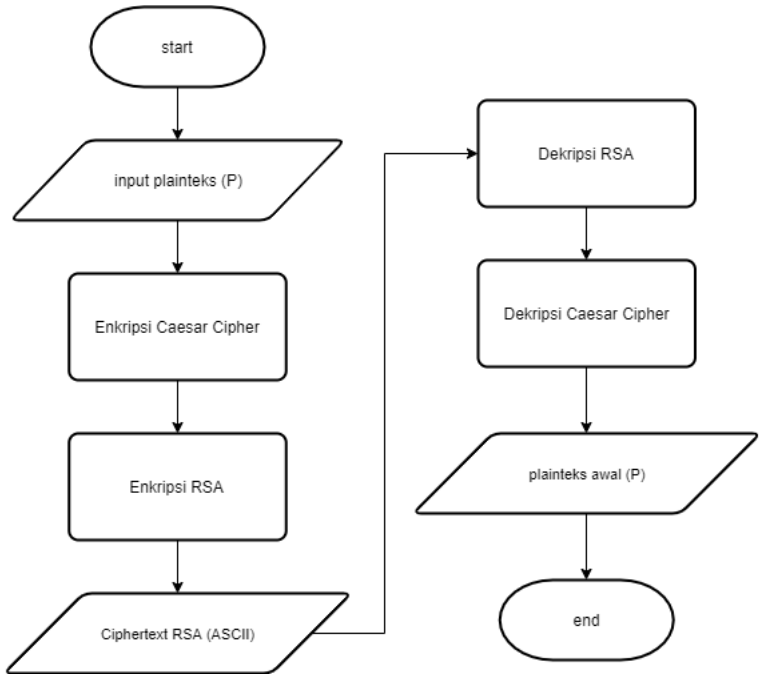
METODE

Dalam Implementasi Algoritma Caesar Cipher dan RSA Super Enkripsi Teks Pesan yang terkait dengan Karakter ASCII ini merupakan proses untuk melakukan pengamanan teks pesan dengan cara mengenkripsi teks pesan, namun dalam proses enkripsi yang pertama dilakukan dengan mengenkripsi sebuah Pesan atau Plaintext menggunakan Algoritma Caesar Cipher terlebih dahulu. Lalu hasil dari enkripsi tersebut tidak langsung di enkripsi lagi menggunakan Algoritma RSA, akan tetapi dilakukan dengan mengkonversi hasil enkripsi pertama tersebut menjadi representasi bilangan biner dan desimal terlebih dahulu.

Dalam sistem ini terdapat beberapa proses, mulai dari cara melakukan substitusi pada Plaintext menggunakan kunci yang sama hingga menghasilkan kedua kombinasi kunci yang berbeda yaitu kunci publik dan kunci pribadi, yang nantinya kombinasi ini digunakan untuk melakukan proses enkripsi maupun dekripsi dengan menggunakan Algoritma RSA.

Tahap enkripsi dengan menggunakan Algoritma Caesar Cipher ini dimulai setelah user memasukkan sebuah teks pesan yang nantinya teks pesan ini akan di enkripsi terlebih dahulu menggunakan Algoritma tersebut. Lalu hasil dari Enkripsi Caesar Cipher ini dikonversikan terlebih dahulu menjadi Representasi Bilangan Biner dan Representasi Bilangan Desimal.

Setelah mendapatkan Representasi Bilangan Desimal, selanjutnya proses enkripsi yang kedua akan dilakukan menggunakan Algoritma RSA. Lalu hasil dari Enkripsi RSA dikonversikan lagi menjadi Representasi Bilangan Biner lalu dilanjutkan dengan mengkonversi Representasi Bilangan Biner tersebut menjadi Karakter yang terkait dengan ASCII. Setelah melewati tahap tersebut, sebuah teks tersandi yang terkait karakter ASCII akan muncul didalam sistem. Untuk melakukan dekripsi dapat menggunakan fungsi invers dari enkripsi.



Gambar 1. Flowchart Algoritma Caesar - RSA

Pada Gambar 1 dijelaskan bahwa, Pertama pengguna memasukkan plaintext dan pergeseran kunci untuk melakukan enkripsi menggunakan Caesar Cipher. Hasil enkripsi (ciphertext) dari Caesar Cipher akan dijadikan sebagai input untuk proses selanjutnya, yaitu

enkripsi menggunakan RSA. Pengguna diminta memasukkan dua bilangan prima besar (p dan q) untuk membangkitkan sepasang kunci RSA. Kemudian, program akan menghasilkan kunci publik dan kunci pribadi berdasarkan nilai p dan q yang diberikan. Selanjutnya, ciphertext dari Caesar Cipher dienkripsi menggunakan kunci publik RSA. Hasil enkripsi RSA dalam bentuk angka bulat kemudian dikonversikan ke karakter ASCII. Untuk proses dekripsi dapat menerapkan fungsi invers dari kedua algoritma diatas. Pengguna juga bisa memasukkan pergeseran kunci untuk mendekripsi pesan yang dienkripsi dengan Caesar Cipher, dan akan mengembalikan plaintext awal.

HASIL DAN PEMBAHASAN

Analisa Sistem

Terdapat uraian dari hasil pengujian dan pembahasan dari proses Enkripsi Caesar Cipher dan Enkripsi Rivest Shamir Adleman.

Hasil Pengujian

Untuk pengujian ini menggunakan Algoritma Caesar Cipher – RSA menggunakan teks pesan / kalimat, dengan pergeseran kunci 13 untuk Caesar Cipher, dan Kunci Publik (65537, 2231), Kunci Pribadi (65, 2231) untuk RSA.

Plaintext: "**And let's not forget the endless joy of sharing your newfound misery with your friends There's nothing quite like sending them a playlist of melancholic melodies complete with an attached message that reads "Listen to this and reflect on the futility of existence" You're essentially a one-person support group for emotional distress and your friends will surely appreciate the chance to contemplate their life choices**".

Tabel 1 Hasil Enkripsi Teks Pesan Dengan Caesar Cipher

Hasil Enkripsi Caesar Cipher: Naq#yrgf#abg#sbetrg#gur#raqyrff#wbl#bs#funevat#lbhe#arjsbhaq#zvfrel#jvgu#lbhe#sevraqf #Gurerf#abguvat#dhvgr#yvxr#fraqvat#gurz#n#cynlyvfg#bs#zrynapubyvp#zrybqvrf#pbzcyrgr #jvgu#na#nggnpurq#zrffntr#gung#ernqf#%Yvfgra#gb#guvf#naq#ersyrpg#ba#gur#shgvyvgl#b s#rkvfgrapr%#Lbher#rffragvnyyl#n#bar&crefba#fhccbeg#tebhc#sbe#rzbgvbany#qvfgerff#na q#lbhe#sevraqf#jvyy#fheryl#nccerpvngr#gur#punapr#gb#pbagrzcyngr#gurve#yvsr#pubvprf
Avalanche Effects: 41,69%
Encryption Time Caesar: 0.632197 seconds

Hasil pengujian Pada Tabel 1 terlihat bahwa plainteks berhasil di enkripsi pertama kali dengan Algoritma Caesar Cipher menggunakan pergeseran kunci sebanyak 13 dan menghasilkan nilai efek avalanche sebesar 41,69%, dan dengan durasi enkripsi selama 0.632197 detik.

Pada Tabel 2**,** terlihat bahwa sebuah kalimat hasil dari enkripsi Caesar berhasil di enkripsi kedua kali menggunakan Algoritma RSA dan menghasilkan sebuah kalimat dengan Karakter ASCII yang tidak dapat dibaca sama sekali. Proses Enkripsi dilakukan menggunakan Kunci Publik (65537, 2231). Hasil enkripsi tersebut menghasilkan nilai efek avalanche sebesar 60.32%, dan dengan durasi enkripsi selama 0.381873 detik.

Tabel 2 Hasil Enkripsi Teks Pesan dengan RSA

Hasil Enkripsi RSA (ASCII): oyĐgÿ□иqڠمÿĐqÿsٜtиqÿqķиÿиĐg□иڠڠÿзٻÿşÿڠķĴ÷ٜĐtÿٻђٜÿĐиЩsђĐgÿڠ÷ےиٮٜÿЩ÷qķÿٻђٜ ÿs÷ٜиĐgڠÿ□ķиٜиڠمÿĐqķ÷Đtÿçђ÷qиÿ□÷□иÿڠиĐg÷Đtÿqķиےÿ Ĵÿ ٛ□Ĵڠ÷□ٮqÿşÿےи□ĴĐڜķ÷□ ڜÿےи□g÷иڠÿ□ٞڜиqиÿЩ÷qķÿĴĐÿĴqqĴڜķиgÿےиڠڠĴtиÿqķĴqÿٜиĴgڠÿøڠ÷□qиĐÿqÿqķڠ÷ÿĴĐ gÿٜиs□иڜqÿĐÿqķиÿsђq÷□÷qٮÿşÿивڠ÷qиĐڜиøÿŌђٜمиÿиڠڠиĐq÷Ĵٮ□□ÿĴÿĐи¢ٜٞٞĐÿڠђٞ qÿtٜђٞsٜÿиٜq÷ĐĴ□ÿgڠ÷qٜиڠڠÿĴĐgÿٻђٜÿs÷ٜиĐgڠÿЩ□□÷ÿڠђٜиٮ□ÿĴٞи÷ڜĴqиÿqķиÿڜķĴĐ ڜиÿqÿڜĐqи□ٞĴqиÿqķиٜ÷ÿ÷□sиÿڜڜķ÷иڠ
Avalanche Effects: 60.32%
Encryption Time RSA: 0.381873 seconds

Tabel 3 Hasil Dekripsi Teks Pesan dengan RSA dan Caesar Cipher

Hasil Dekripsi RSA : Naq#yrgf#abg#sbetrg#gur#raqyrff#wbl#bs#funevat#lbhe#arjsbhaq#zvfrel#jvgu#lbhe#sevraqf #Gurerf#abguvat#dhvgr#yvxr#fraqvat#gurz#n#cynlyvfg#bs#zrynapubyvp#zrybqvrf#pbzcyrgr #jvgu#na#nggnpurq#zrffntr#gung#ernqf#%Yvfgra#gb#guvf#naq#ersyrpg#ba#gur#shgvyvgl#b s#rkvfgrapr%#Lbher#rffragvnyyl#n#bar&crefba#fhccbeg#tebhc#sbe#rzbgvbany#qvfgerff#na q#lbhe#sevraqf#jvyy#fheryl#nccerpvngr#gur#punapr#gb#pbagrzcyngr#gurve#yvsr#pubvprf
Decryption Time RSA: 0.312342 seconds
Hasil Dekripsi Caesar Cipher: And let's not forget the endless joy of sharing your newfound misery with your friends There's nothing quite like sending them a playlist of melancholic melodies complete with an attached message that reads "Listen to this and reflect on the futility of existence" You're essentially a one-person support group for emotional distress and your friends will surely appreciate the chance to contemplate their life choices
Decryption Time Caesar: 0.627606 seconds

Pada Tabel 3, Hasil Enkripsi dari RSA berhasil di dekripsi menggunakan pasangan Kunci Pribadi (65, 2231), dengan durasi dekripsi selama 0.312342 detik. Kemudian di dekripsi kedua kalinya menggunakan Algoritma Caesar Cipher dengan kunci atau pergeseran sebanyak 13 dan dengan durasi dekripsi selama 0.627606 detik.

KESIMPULAN

Berdasarkan hasil implementasi dan analisa aplikasi yang dilakukan, didapatkan beberapa kesimpulan sebagai berikut :

1. Aplikasi Algoritma Caesar – RSA menunjukkan tingkat keamanan yang tinggi dengan nilai Avalanche Effects 60,32% pada percobaan enkripsi pesan tersebut. Hal ini menandakan bahwa Algoritma Caesar - RSA mampu memberikan perlindungan yang lebih baik terhadap serangan kriptoanalisis dan cocok digunakan untuk pengamanan data yang kritis.
2. Penggunaan bilangan prima yang berbeda pada algoritma RSA cukup signifikan dalam mengubah tingkat keamanannya. Meskipun demikian, disarankan untuk menggunakan bilangan prima yang besar untuk meningkatkan tingkat keamanan algoritma RSA.

DAFTAR PUSTAKA

[1] Hoobi, M. M., Sulaiman, S. S., & Abdulmunem, I. A. (2020a). Enhanced Multistage RSA Encryption Model. IOP Conference Series: Materials Science and Engineering, 928(3). https://doi.org/10.1088/1757-899X/928/3/032068

[2] Malvi, A. (2020). Pengamanan File Gambar pada Media Video dengan Kriptografi Algoritma RSA dan Steganografi Algoritma End of File (EOF).

[3] Albert Ginting, R. R. I. I. P. W. (2015). Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email. Jurnal Teknologi Dan Sistem Komputer, 3

[4] Steef, A., A, A., & M. N, S. (2015). RSA Algorithm With a New Approach Encryption and Decryption Message Text by ASCII. International Journal on Cryptography and Information Security, 5(3/4), 23–32. https://doi.org/10.5121/ijcis.2015.5403

[5] Khairil Azhar, J., & Yuliany, S. (2019). Implementasi Algoritma RSA (Rivest, Shamir dan Adleman) untuk Enkripsi dan Dekripsi File .pdf. https://www.researchgate.net/publication/338175310

[6] Pramuditha Yenadi, R., & Hidayatullah, D. (2020). STRING (Satuan Tulisan Riset dan Inovasi Teknologi) IMPLEMENTASI METODE CAESAR CIPHER DALAM PENERAPAN SISTEM E-VOTING BERBASIS WEB PADA PEMILIHAN ABANG NONE JAKARTA.

[7] Albert Ginting, R. R. I. I. P. W. (2015). Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email. Jurnal Teknologi Dan Sistem Komputer, 3