SIMULASI ALGORITMA ENKRIPSI PESAN

DENGAN METODE RIVEST SHAMIR ADLEMAN (RSA)

Ayub Kris Bobby Aritonang
Mahasiswa Program Studi D3 Teknik Telekomunikasi
Universitas Telkom Jakarta
Jl.Daan Mogot, Jakarta, Indonesia
ayubkris@student.telkomuniversity.ac.id

Nurwan Reza Fachrur Rozi ST.,MT.
Staff pengajar Program Studi D3 Teknik Telekomunikasi
Universitas Telkom Jakarta
Jl.Daan Mogot, Jakarta, Indonesia
nurwan@telkomuniversity.ac.id

Abstrak **— Keamanan dan kerahasiaan data merupakan poin penting yang perlu kita jaga keamananya. Kasus yang terjadi akibat penyisipan aplikasi pada perangkat pengguna yang dapat melihat username dan password email, data kontak, dan file pengguna. Melindungi data teks melalui enkripsi dan kompresi menggunakan algoritma RSA. Data yang digunakan bisa berupa teks atau file teks. Teks atau data berupa teks terlebih dahulu dienkripsi menggunakan algoritma RSA kemudian dikompres menggunakan algoritma lain atau bisa langsung digunakan. Kecepatan rata-rata pembangkitan kunci adalah 0,156 detik,kecepatan enkripsi 0,019 detik, kecepatan kompresi 0,019 detik, kecepatan dekompresi 0,050 detik, dan kecepatan dekripsi 0,040 detik. Mengenkripsi dan mengompresi data teks atau file teks dapat membantu Anda mengirim pesan rahasia yang tidak ingin dilihat orang lain.**

Kata Kunci: enkripsi , kompresi, RSA, teks.

I. PENDAHULUAN

Dunia digital berkembang pesat, memungkinkan komunikasi real-time dan daya saing dalam telekomunikasi. Internet telah memungkinkan orang untuk berkomunikasi tanpa penundaan, bahkan jika mereka adalah negara yang berbeda. Data, salah satu jenis subjek, adalah subjek yang berisi informasi kuantitatif atau kualitatif yang dapat dibagikan dengan cepat dan mudah. Di era digital, data dapat dibagikan melalui berbagai media, termasuk internet, radio, dan sumber lainnya. Data dapat berisi informasi berharga yang sensitif. Namun, perkembangan komunikasi data juga membawa risiko. Misalnya, jika data dibagikan, data tersebut tidak dapat diakses atau dihancurkan dengan mudah, karena dapat dengan mudah disusupi atau dicuri. Internet juga membawa ancaman baru, seperti malware, virus, dan virus yang dapat dengan mudah membahayakan data. Oleh karena itu, sistem perlindungan data harus diterapkan untuk melindungi, melindungi, dan mengelola data. Sistem ini harus melindungi informasi digital dari ancaman seperti akses tidak sah, akses tidak sah, kontrol administratif, dan akses, serta data logistik dari aplikasi cloud. Ini juga melindungi pengguna dan proses organisasi. Jenis data yang paling umum yang dibagikan dan tidak dibagikan adalah informasi pribadi.

II. KAJIAN TEORI

Data umumnya dibagi menjadi dua kategori : data rahasia dan data tidak rahasia. Data non-rahasia biasanya kurang diperhatikan. Yang benar-benar perlu pertimbangkan adalah data rahasia. Informasi yang terkandung di dalam data tersebut sangat berharga bagi mereka yang membutuhkannya, karena informasi dari data tersebut dapat dengan mudah digandakan serta dapat digunakan sebagai tindakan kriminal. Biasanya dilakukan dengan berbagai cara ilegal untuk mendapatkan informasi di dalamnya.

Keamanan data biasanya meliputi hal-hal berikut :

1. Fisik, dimana pihak yang tidak berwenang berusaha untuk mendapatkan data dengan cara merusak atau mensabotase tempat penyimpanan data tersebut.
2. Organisasi/human eror, dalam kasus ini pihak tidak berwenang berusaha mendapatkan data dengan cara memanfaatkan kelalaian anggota yang sedang menangani data tersebut. Dapat dengan cara physing atau scamming
3. Ancaman eksternal, disini pihak tidak bertanggung jawab berusaha mendapatkan data dengan cara menembus sistem keamanan dengan paksa kemudian mencuri data yang tersimpan pada komputer tersebut.

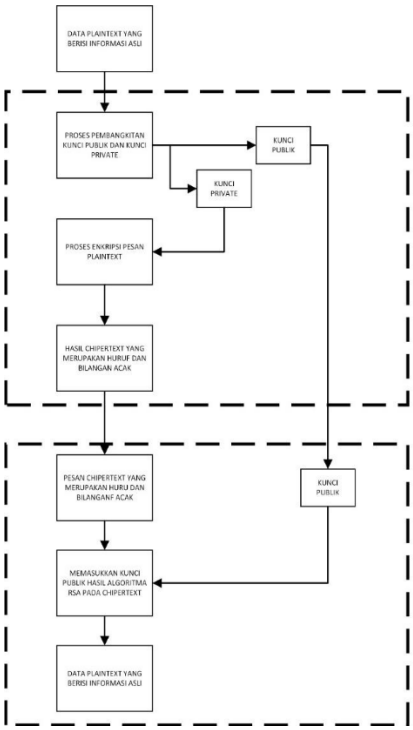
Biasanya keamanan data digunakan untuk memenuhi 3 pilar keamanan informasi, yaitu :

III. METODE

Metode yang digunakan pada penelitian kali ini akan membahas langkah-langkah yang digunakan dalam mengenkripsi data pesan menggunakan algoritma Rivest Shamir Aldeman agar merndapat pesan chiper yang baik dan aman.

Identifikasi masalah mengenai tugas ini melibatkan identifikasi dan pemahaman masalah dalam bidang kriptografi berbasis teks. Sangat penting untuk memahami masalah dalam penelitian sebelumnya tentang kriptografi dalam manipulasi teks data dan implementasinya dalam kehidupan sehari-hari. Penelitian sebelumnya berfokus pada berbagai algoritma, seperti RSA, yang memiliki beberapa perbedaan dibandingkan dengan metode lain karena dua kuncinya: publik dan pribadi. Analisis kompresi berbasis Shannon-Fano menunjukkan bahwa kompresi ini memiliki perbedaan dibandingkan dengan algoritma kompresi lainnya dan memiliki tingkat kompresi yang lebih tinggi.

Pada tahap analisis perancangan sistem dan analisis desain pada tampilan sistem dilakukan dengan cara analisis masalah yaitu sistem input dan output. Analisis cara kerja algoritma RSA dalam menentukan kunci publik dan private, mengenkripsi dan mendekripsi file teks. Dapat dilihat pada blok diagram dibawah ini



IV. HASIL DAN PEMBAHASAN

Pada penelitian enkripsi pesan dengan menggunakan algoritma RSA kali ini dilakukan uji coba sebanyak 10 kali dengan menggunakan parameter yang berbeda pada tiap uji coba mulai dari panjang pesan asli yang dimasukkan, besar bilangan prima untuk nilai p dan q sebagai acuan pembangkitan kunci serta pengamatan hasil dari semua kombinasi yang akan di uji coba.

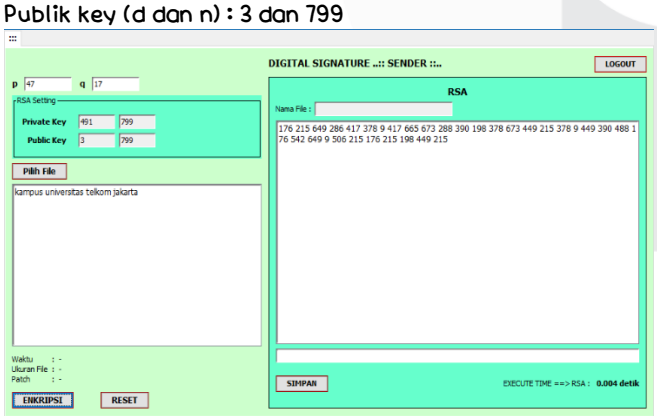
uji coba dengan pesan "kampus universitas telkom jakarta"

Proses enkripsi : dengan input nilai bilangan prima yang kita ambil sebagai nilai p dan q adalah : p = 47 dan q = 17

Dengan input nilai bilangan prima p :47 dan q : 17 Mendapatkan hasil uji coba sebagai berikut

Private key (e dan n) : 491 dan 799

Publik key (d dan n) : 3 dan 799



Hasil Chipertext : 176 215 649 286 417 378 9 417 665 673 288 390 198 378 673 449 215 378 9 449 390 488 176 542 649 9 506 215 176 215 198 449 215

Proses generate key atau pembangkitan kunci adalah sebagai berikut.

1. Pilih dua buah bilangan prima sembarang, p dan q.
2. Hitung n = p × q (sebaiknya p ≠ q, sebab jika p = q maka n = p2 sehingga p dapat diperoleh dengan menarik akar pangkat dua dari n).
3. Hitung ø(n) = (p − 1)(q − 1).
4. Pilih kunci publik, e, yang relatif prima terhadap ø(n) yang berarti kunci publik e hanya bisa dibagi 1 dan nilainya sendiri dan bukan merupakan faktorial dari ø(n).
5. Bangkitkan kunci privat dengan menggunakan persamaan e × d = 1 (mod ø(n)).
6. Perhatikan bahwa e × d = 1 (mod ø(n)) ekivalen dengan e × d = 1 + kø(n), sehingga d dapat dihitung dengan d=(1+kø(n))/e
7. Akan terdapat bilangan bulat k yang memberikan bilangan bulat d.

Hasil dari algoritma di atas:

- Kunci publik adalah pasangan (e, n)
- Kunci privat adalah pasangan (d, n)

Catatan: n tidak bersifat rahasia, namun ia diperlukan pada perhitungan enkripsi/dekripsi

Rumus fungsi enkripsi

$C = M^e \bmod n$ (Fungsi)……(1)

Rumus fungsi dekripsi

$M = C^d \bmod n$ (Fungsi Di)……(2)

V. KESIMPULAN

Berdasarkan penelitian dan analisis sebelumnya terhadap algoritma RSA yang dikembangkan Dapat diambil kesimpulan sebagai berikut :

Hasil enkripsi RSA masih rentan untuk ditembus menggunakan mmetode brute force sehingga perlu ditambahkan sistem kompresi tambahan seperti shanon-fano atau huffman.

Data atau teks yang sudah di enkripsi hanya dapat dibuka dengan kunci private yang telah dipasangkan sebelumnya sehingga panjang kunci private juga mempengaruhi keamanan data yang di enkripsi.

Nilai p dan q memepengaruhi hasil panjang kunci private dan publik pada proses pembangkitan kunci. Nilai p dan q dapat kita ambil dari seluruh bilangan prima yang ada dan tidak diperbolehkan sama dikarenakan hasil nilai N dimana diperoleh dari perkalian nilai p x q akan menjadi N2 yang dimana nilai p dan q dapat diperoleh hanya dengan menggunakan akar N.

Semakin panjang plaintext yang dimasukkan maka juga akan mengasilkan chipertext yang semakin panjang.

Kita dapat membagi hasil chipertext yang berupa angka desimal menjadi 2 atau 3 digit angka dan mengubahnya menjadi kode ASCII untuk dapat mempersulit orang yang akan melakukan pencurian pada data tersebut dikarenakan kombinasi 2 digit dan 3 digit kode desimal menghasilkan nilai ASCII yang berbeda.

REFERENSI

Direkomendasikan menggunakan *reference Fairuzabadi, Muhammad. "Implemetasi Kriptografi Klasik menggunakan Borland Delphi," Jurnal Dinamika Informatika, 2010.*

Yuniati, Voni, et al. "Enkripsi Dan Dekripsi Dengan Algoritma Aes 256 Untuk Semua Jenis File." Informatika: Jurnal Teknologi Komputer dan Informatika, vol. 5, no. 1, doi:10.21460/inf.2009.51.69. 2009.

Mufadhol, M. "Kerahasiaan Dan Keutuhan Keamanan Data Dalam Menjaga Integritas Dan Keberadaan Informasi Data." Jurnal Transformatika Universitas Semarang, vol. 6, no. 2, 2009.

Kromodiemoeljo sentot, "Teori dan Aplikasi Kriptografi" jakarta. SPK IT Consulting, 2009 .

Hasugian, Buyung Solihin. "PERANAN KRIPTOGRAFI SEBAGAI KEAMANAN SISTEM INFORMASI PADA USAHA KECIL DAN MENENGAH" Jurnal Warta. 2017

Suryadi, Agus sumin "Pengantar Algoritma dan pemrograman teknik diagram alur ban bahasa basic dasar" edisi pertama cetakan keenam. Jakarta : Gunadarma. 1997.

Hasugian, Buyung Solihin. "PERANAN KRIPTOGRAFI SEBAGAI KEAMANAN SISTEM INFORMASI PADA USAHA KECIL DAN MENENGAH" Jurnal Warta Edisi : 53, 2017.

Suryadi, Agus sumin "Pengantar Algoritma dan pemrograman teknik diagram alur ban bahasa basic dasar" edisi pertama cetakan keenam. Jakarta : Gunadarma. 1997.

Fresly Nandar Pabokory, et al. "IMPLEMENTASI KRIPTOGRAFI PENGAMANAN DATA PADA PESAN TEKS, ISI FILE DOKUMEN, DAN FILE DOKUMEN MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD" Jurnal Informatika Mulawarman Vol. 10 No. 1 Februari 2015.

Voni Yuniati, et al. "ENKRIPSI DAN DEKRIPSI DENGAN ALGORITMA AES 256 UNTUK SEMUA JENIS FILE" 23 jurnal informatika, volume 5 nomor 1, 2009

Yudi Wiharto, Ari Irawan. "ENKRIPSI DATA MENGGUNAKAN ADVANCED ENCRYPTION STANDARD 256" JURNAL KILAT Vol. 7, No. 2, 2018

Aditia Rahmat Tulloh, et al. "Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen" Jurnal Matematika UNISBA Vol 15 No 1, 2016

Febriansyah. "ANALISIS DAN PERANCANGAN KEAMANAN DATA MENGGUNAKAN ALGORITMA KRIPTOGRAFI DES (DATA ENCYPTION STANDARD)" skripsi. Informatika. UBINUS. 2012

Fachrurozi, Muhammad Farid "enkripsi pesan rahasia menggunakan algoritma (advanced encryption standart) AES : RIJNDAEL" Skripsi. Saintek. UIN Syarif Hidayatullah. 2006.

Jeprianto, "Implementasienkripsi Dan Dekripsialgoritma Rsa Dan Kompresishannon –Fanodalam Pengamanan Data Teks," 2019

A. Ginting, R. R. Isnanto, and I. P. Windasari, "Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email," Jurnal Teknologi dan Sistem Komputer, vol. 3, no. 2, pp. 253–258, Apr. 2015

Stallings, William, "Cryptography and network security : principles and practiceBibliografi", Prentice Hall, Vol 3, 2003

Rinaldi Munir, "Algoritma & Pemrograman", Informatika, vol 4, 2002

C. Lamorahan, B. Pinontoan, and N. Nainggolan, "Data Compression Using Shannon-Fano Algorithm", dCJMA, vol. 2, no. 2, pp. 10–17, Oct. 2013.

[1] G. Pevere. "*Infrared Nation.*" *The International Journal of Infrared Design*, vol. 33, pp. 56–99, Jan. 1979.