**PRAKTIKUM**

**SISTEM KEAMANAN DATA**



Disusun Oleh:

Algeori Wira Wahyu Hidayat (V3920006)

Ardianita Fauziyah (V3920009)

Elya Kumala Fauziyah (V3920020)

Hemalia Aisyah Putri (V3920025)

Linda Ramawati (V3920033)

**PRODI D3 TEKNIK INFORMATIKA (MADIUN)**

**SEKOLAH VOKASI**

**UNIVERSITAS SEBELAS MARET**

**SURAKARTA**

**2021**

Implementasi Algoritma Kriptografi RSA untuk

Enkripsi dan Dekripsi Email

1. Latar Belakang

Sejalan dengan perkembangan teknologi, semakin mengubah cara masyarakat dalam berkomunikasi. Dulu komunikasi jarak jauh masih menggunakan cara yang konvensional, yaitu dengan cara saling mengirim surat, tetapi sekarang komunikasi jarak jauh dapat dilakukan dengan mudah dan cepat yaitu dengan adanya teknologi seperti email, layan pesan singkat (sms), dan Internet yang merupakan salah satu teknologi telekomunikasi yang paling banyak digunakan. Pada proses pengiriman data (pesan) terdapat beberapa hal yang harus diperhatikan, yaitu : kerahasiaan, integritas data, autentikasi dan non repudiasi. Oleh karenanya dibutuhkan suatu proses penyandian atau pengkodean pesan sebelum dilakukan proses pengiriman. Sehingga pesan yang dikirim terjaga kerahasiaannya dan tidak dapat dengan mudah diubah untuk menjaga integritas pesan tersebut. Ilmu yang mempelajari tentang cara-cara pengamanan data dikenal dengan istilah Kriptografi, sedangkan langkah-langkah dalam kriptografi disebut algoritma kriptografi. Berdasarkan dari kunci yang digunakan algoritma kriptografi dapat dibagi menjadi dua, Algoritma Simetrik dan Algoritma Asimetrik. Dimana Algoritma Simetrik menggunakan satu kunci untuk proses enkripsi dan dekripsinya. Sedangkan Algoritma Asimetrik menggunakan dua kunci berbeda untuk proses enkripsi dan dekripsinya, yaitu kunci umum (public key) yang digunakan untuk proses enkripsi yaitu perubahan data teks asli (plaintext) menjadi teks rahasia (cipher text) yang sifatnya tidak rahasia, dan kunci pribadi (private key) yang digunakan untuk proses dekripsi yaitu pengembalian data teks rahasia (ciphertext) menjadi teks asli (plain text) yang sifatnya rahasia dan masing-masing pihak memiliki kunci pribadi yang berbeda. Penggunaan kunci pribadi dapat digunakan untuk autentikasi (pengenalan identitas pengirim) dan non repudiasi (pencegahan penyangkalan pengiriman data) karena dalam proses dekripsi dapat diketahui siapa pihak pengirim dengan melihat kunci pribadi yang dipakai. Contoh algoritma kriptografi yang dapat diandalkan adalah RSA, dimana RSA merupakan proses penyandian kunci asimetris (asymmetric key). Proses perumusan RSA didasarkan pada Teorema Euler, sedemikian sehingga menghasilkan kunci umum dan kunci pribadi yang saling berkaitan. Sehingga meskipun proses enkripsi dan dekripsi menggunakan dua kunci yang berbeda hasilnya akan tetap benar. Kunci umum dan kunci pribadi yang digunakan adalah suatu bilangan prima, dan disarankan bilangan prima yang besar. Hal ini digunakan untuk pencegahan usaha pemecahan teks rahasia, karena semakin besar bilangan prima yang digunakan sebagai kunci maka semakin sulit mencari bilangan besar sebagai faktornya.

1. Tujuan penelitian

Merancang dan membangun purwarupa email client yang mampu melakukan enkripsi dan dekripsi dengan menerapkan ilmu kriptografi RSA sehingga dirasakan aman.

1. algoritma yang dipakai + alur penelitian

Tahap 1. Ubah teks asli “Tes” menjadi ASCII desimal

|  |  |  |  |
| --- | --- | --- | --- |
| Karakter | T | e | s |
| ASCII(dec) | 84 | 101 | 115 |

*m* dalam desimal = 84101115

Tahap 2. Pilih nilai *P* dan *Q*

Nilai *P* dan *Q* adalah bilangan prima acak yang panjangnya 4 bit (pengujian kedua), nilai *P* ≠ *Q*. Nilai P dan *Q* yang dipakai dalam pengujian kedua *P =* 11*, Q =* 13.

Tahap 3. Tentukan nilai *r, N,* dan *E N = P . Q*

*N=* 11 *.* 13

*N =* 143

f(*r*)= (*p* – 1)(*q* – 1) = (11-1)(13-1)= 120

Nilai *E* merupakan bilangan relatif prima acak bersifat publik, Faktor Persekutuan Terbesar dari r dan nilainya < r.

*E.gdc(r)* = *E.gdc*(120)

= 59

Tahap 3. Lakukan transformasi satu ke satu untuk *m* (terletak pada rentang 0 – (*n*-1) ) hal ini dilakukan agar nilai enkripsi tidak terlampau besar.

Rentang setiap blok *m* = 0 – (*n*-1) = 0 – 142

*m* = 84101115

*m1* = 84

*m2* = 101

*m3* = 115

Tahap 4. Enkripsi Pesan

*Y = me mod NY1 = m1e* mod *N ≡* 8459 mod 143 ≡ 63 *Y2 = m2e* mod *N ≡* 10159 mod 143 ≡ 17 *Y3 = m e* mod *N ≡* 11559 mod 143 ≡ 97

*Y* (*ciphertext*)= 63 17 97, hasilnya sama dengan pengujiankedua.

Tahap 5. Dekripsi Pesan

Hitung nilai *D, D* dapat dicari dengan cara coba-coba, dengan memasukkan nilai *m* satu persatu sampai hasilnya bulat, nilai *D* bersifat rahasia.

*E .D* mod *r* = 1

*E.D* ≡ 1 mod *r*

*D =* 1 (*x . r*) = 1 (*m*. 120)

*E                59*

*Dengan mencoba nilai x = 1, 2, 3, 4, .... diperoleh nilai x yang menghasilkan D yang bulat adalah 29. Dan nilai D yang didapat adalah 59.*

*D = 1 (x . r) = 1 (29. 120)*

*E                59*

*= 3840*

*59*

*= 59*

*Setelah nilai D didapat langkah selanjutnya ialah mengubah ciphertext kembali ke teks awal.*

*Y = 63 17 97 Y1 = 63 Y2 = 17 Y3 = 97*

*m= YD mod N*

*m = Y D mod N ≡ 6359 mod 143 ≡ 84*

*m2 = Y2D mod N ≡ 1759 mod 143 ≡ 101*

*m3 = Y3D mod N ≡ 9759 mod 143 ≡ 115*

*Sehingga, nilai m = 84 101 115*

*apabila dikonversikan menjadi string kembali berdasarkan*

*tabel ASCII maka akan menghasilkan teks asli “Tes”.*

d. Hasil penelitian+kesimpulan

Hasil dari penelitian ini ada enkripsi dan deskripsi. Untuk enkripsi berupa angka 41 17 20. Untuk deskripsi akan kembali ke teks asli yaitu Tes.

Berdasarkan hasil penelitian dan pembahasan yang telah

dilakukan, dapat diambil beberapa kesimpulan sebagai

berikut.

1. Aplikasi yang menerapkan algoritma kriptografi RSA ini

berjalan dengan baik mampu mengirim dan menerima

email, dan dapat mengenkripsi dan dekripsi kotak masuk

yang diterima.

2. Dengan perangkat lunak ini, tujuan penelitian tercapai yaitu

keamanan dalam menerima email terjamin. Ada

pengamanan ganda untuk membuka pesan tersandi. Saat

mendekripsi pesan yang telah dienkripsi harus

memasukkan password terlebih dahulu, apabila masukan

password salah pesan tidak akan didekripsi.

3. Perangkat lunak ini hanya mengamankan isi pesan masuk

email bukan mengamankan jalur transfer email.

4. Pada aplikasi yang dikembangkan ini, satu pesan asli dapat

menghasilkan ciphertext yang berbeda-beda, karena proses

pembangkitan kunci RSA didasarkan oleh nilai P dan Q

yang acak.

5. Pesan kesalahan akan ditampilkan apabila terjadi kesalahan

saat memasukkan suatu nilai yang salah saat enkripsi atau

dekripsi pesan. Saat enkripsi masukan bit bernai kosong

dan saat dekripsi masukan password salah.

e. Kelebihan dan kekurangan jurnal

Kelebihan Jurnal

Kelebihan dari jurnal ini yaitu memiliki landasan teori yang terperinci dan lengkap yang mampu mencangkup beberapa hal didalamnya salah satunya saat mengirim satu pesan asli dapat menghasilkan ciphertext yang berbeda-beda, karena proses pembangkitan kunci RSA didasarkan oleh nilai P dan Q yang acak.

Kekurangan Jurnal

Kekurangan dari jurnal ini tidak banyak data yang dilampirkan dijurnal dan ada yang perlu dilakukan penelitian lebih lanjut untuk enkripsi dan dekripsi email menggunakan algoritma kriptografi yang lain.

Implementasi Algoritma RSA Pada Sistem Pendukung

Keputusan Pengalokasian Dana Bantuan Langsung

Masyarakat Dengan Metode Weighted Product

1. Judul dan latar belakang

Bantuan langsung masyarakat merupakan program pemerintah untuk mengurangi tingkat kemiskinan masyarakat indonesia, dengan menyediakan dana kepada masyarakat miskin. Namun, sering kali bantuan yang diberikan oleh pemerintah tersebut tidak tepat sasaran dimana bantuan yang seharusnya dikhususkan untuk masyarakat yang kurang mampu, tetapi masyarakat yang mampu dalam hal materi pun malah mendapatkan dana tersebut selain itu proses pelaksanaan bantuan masih bersifat manual sehingga membutuhkan waktu yang cukup lama dan tujuan pemerintah dalam mengurangi tingkat kemiskinan tidak terlaksana dengan baik. Berdasarkan studi literatur yang dilakukan didapatkan bahwa sistem pendukung keputusan dapat mengatasi permasalah pemberian bantuan langsung masyarakat dan metode yang digunakan adalah metode Weighted Product karena dapat bekerja lebih efektif dan efesien dibanding metode yang lain. Hasil penelitian ini menunjukkan bahwa sistem pendukung keputusan dapat mengatasi masalah penerima bantuan langsung masyarakat yang masih dilakukan secara manual dan subyektif di Desa Beka Kecamatan Marawola Kabupaten Sigi sehingga proses penyaluran bisa lebih cepat dan proposisi dan algoritma RSA yang digunakan mampu memberikan keamanan data kuat.

1. tujuan penelitian

Tujuan dari penelitian ini adalah mengimplementasikan sistem pendukung keputusan pengalokasian dana bantuan langsung masyarakat menggunakan metode weighted product berbasis web untuk membantu pemerintah dalam menyeleksi masyarakat yang lebih layak mendapatkan dana bantuan dan Mengunci data hasil keputusan sistem menggunakan algoritma RSA.

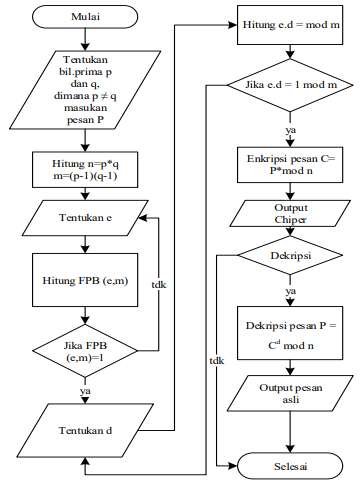
1. algoritma yang dipakai + alur penelitian

Algoritma RSA

Sistem kriptografi RSA adalah salah satu sistem kriptografi kunci publik yang ditemukan oleh Rivest, Shamir and Adleman dari Massachusett Institute of Technology (MIT) pada tahun 1976. Sejak skema sistem ini ditemukan, sistem ini menguasai sebagai satu-satunya sistem yang diterima dan diterapkan secara luas sebagai sistem kriptografi kunci publik. Sistem ini termasuk sistem enkripsi blok, karena data asli dan data sandi adalah bilangan integer antara 0 sampai (n -1), untuk semua nilai n positif. Keamanan sistem kriptografi ini bergantung kondisi tertentu. Seperti kebanyakan sistem kriptografi kunci publik lainnya, harus ada cara yang mudah diterapkan untuk membangkitkan pasangan kunci enkripsi dan dekripsinya, sehingga setiap pemakai dapat membangkitkan sebuah pasangan tanpa perlu mempersoalkan kemampuan matematikanya. Algoritma RSA memiliki besaran seperti berikut :

1. p dan q bilangan prima (rahasia)
2. n = p.q (tidak rahasia)
3. m = (p-1)(q-1) (rahasia)
4. e = kunci enkripsi (tidak rahasia)
5. d = kunci dekripsi (rahasia)
6. P = plaintext (rahasia)
7. C = ciphertext (tidak rahasia)

Flowchart proses algoritma RSA dapat dilihat pada gambar berikut



Keamanan algoritma RSA terletak pada tingkat kesulitan dalam memfaktorkan bilangan non prima menjadi bilangan faktor primanya, yang dalam hal ini n = p x q. Sekali n berhasil difaktorkan menjadi p dan q, maka m =(p-1) (q-1) dapat dihitung. Selanjutnya karena kunci enkripsi e diumumkan (tidak rahasia), maka kunci dekripsi d dapat dihitung dari persamaan e=1(mod m). Penemu algoritma RSA menyatakan nilai p dan q panjang lebih dari 100 digit. Dengan demikian hasil kali n = p x q akan berukuran lebih dari 200 digit. Menurut Rivers dan kawan-kawan, usaha untuk mencari faktor bilangan 200 digit membutuhkan waktu komputasi selama 4 miliar tahun

1. Hasil penelitian+kesimpulan

Menghasilakan Vektor\_S dan menghitung nilai vektor\_V yang diambil dari nilai vektor\_S lalu di bagi untuk setiap atribut, dan tahap terakhir yaitu mengurutkan pilihan. Dari tahapan yang telah dilakukan maka nilai akhir tertinggi didapatkan oleh masyarakat yang mempunyai NIK 7210140107590009 dengan nilai 0.2483 dan nilai terendah didapatkan oleh masyarakat yang mempunyai NIK 7210140107620037 dengan nilai akhir 0.1089

Berdasarkan hasil pengujian dan analisis sistem pendukung keputusan pengalokasian dana bantuan langsung masyarakat menggunakan metode Weighted Product (WP) yang diimplementasikan dengan algoritma RSA dapat diambil kesimpulan:

1. Proses perhitungan dengan metode WP pada sistem pendukung keputusan ini dapat dilakukan dengan memasukkan nilai bobot kriteria dan penilaian yang diberikan kepada masyarakat

2. Terdapat 3 langkah yang harus diperhatikan dalam penyelesaian menggunakan metode WP yaitu melakukan normalisasi bobot kriteria, melakukan perhitungan pemangkatan vektor S terhadap bobot kriteria, melakukan proses alternatif keputusan vektor S sehingga menghasilkan nilai vektor V dan langkah terakhir yaitu mengurutkan pilihan.

3. Terdapat 3 langkah yang harus dilakukan dalam penyelesaian menggunakan metode algoritma RSA yaitu Pembuatan Kunci private dan public, melakukuan enkripsi terhadap data dan yang terakhir yaitu mendeskripsikan data yang terenkripsi

4. Sistem pendukung keputusan ini dibangun menggunakan bahasa pemrograman Preprocessor HyperText (PHP) berbasis website dan sistem ini dapat membantu pegawai balai Desa Beka dalam menentukan masyarakat yang akanmendapatkan rekomendasi mendapatkan bantuan dan sistem dapat mengurutkan data masyarakat yang mendapatkan rekomendasi.

5. Tingkat keakurasi perhitungan manual metode WP dengan sistem yang dibangun 98% hasilnya adalah sama

1. Kelebihan dan kekurangan jurnal

Kelebihan

Kelebihan dari jurnal ini memiliki isi yang sangat lengkap sehingga memudahkan para pembaca seperti pada bagian hasil menjelaskan bagaimana sistem berjalan dan juga bagaimana implementasi sistemnya

Kekurangan

Kekurangan dari jurnal ini perlu ditambahkan suatu metode atau algoritma yang dapat membandingkan nilai akhir apabila terjadi kesamaan nilai akhir agar dapat menentukan urutan peringkat terbaik