Teknik Pembangkit Kunci Algoritma RSA Menggunakan Algoritma Diffie Hellman pada Keamanan Citra

Reno Prastya[1], Akim M.H. Pardede[2], Achmad Fauzi[3]
[1,2,3]STMIK Kaputama Binjau, Jl.Veteran No.4A-9A, Binjai, Sumatra Utara

ARTICLE INFORMATION

Received: April 8, 2022
Revised: April 22, 2022
Available online: April, 2022

KEYWORDS

Citra, Algoritma RSA, Diffie Hellman, Microsoft Visual Basic 2010

CORRESPONDENCE

Phone: +62 853-6000-5202
E-mail: info@kaputama.ac.id

A B S T R A K

Kemajuan yang pesat dalam dunia teknologi memudahkan manusia dalam bertukar informasi, informasi dapat berupa teks ataupun visual. Suatu informasi visual atau citra yang dimiliki seseorang maupun instansi rentan terhadap pencurian, penyandapan dan pengubahan informasi yang dapat merugikan pihak lain. Kriptografi merupakan salah satu cara untuk mengamankan file yang berupa teks atau gambar. Pengamanan terhadap informasi dalam bentuk citra dilakukan dengan menggunakan algoritma RSA yang di perkuat dengan algoritma Difie Hellman dalam menciptakan kunci untuk mengenkripsi dan dekripsi citra. Algoritma Diiffie Hellman digunakan sebagai pembentukan kunci, yang mana kunci yang telah dibentuk akan digunakan sebagai kunci publik dan kunci private dari algoritma RSA. Hasil kombinasi kedua algoritma ini menghasilkan kunci yang kompleks yang akan sulit di tebak. Implemntasi sistem keamanan menggunakan perangkat lunak Microsoft Visual Basic 2010. Hasil dari sistem ini berupa file citra yang tidak dimengerti dan akan kembali normal setelah di dekripsi.

PENDAHULUAN

Citra atau gambar 2 dimensi merupakan salah satu bentuk multimedia yang penting. Yang menyajikan informasi secara visual dan informasi yang disajikan oleh sebuah gambar lebih kaya daripada informasi yang disajikan secara tekstual. Citra tidak hanya disimpan didalam flash disk, hard disk atau perangkat memory lainnya, tetapi juga ditransmisikan melalui saluran publik seperti internet yang rawan penyandapan atau pencurian. Untuk citra yang bersifat pribadi atau yang bersifat rahasia perlu memperhatikan aspek keamanan agar gambar tidak disalahgunakan seperti dengan cara mengganti gambar atau memodifikasi gambar untuk mempermalukan atau merugikan orang lain. Mengamankan gambar atau citra merupakan hal yang sangat penting dan harus dilakukan untuk menjaga informasi atau data agar tidak diketahui oleh pihak yang tidak berkepentingan. Salah satu cara untuk mengamankan gambar adalah dengan metode kriptografi.

Kriptografi adalah ilmu mengenai teknik enkripsi yang mana plaintext diacak menggunakan suatu kunci enkripsi menjadi ciphertext. Kriptografi mempunyai berbagai teknik, di penelitian ini penulis menggunakan algoritma Rivest Shamir Andleman (RSA) dan algoritma Diffie Hellman. Keamanan algoritma RSA sendiri terletak pada sulitnya memfaktorkan bilangan yang besar menjadi bilangan faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci private. Sedangakn algoritma Diffie Hellman memiliki keamanannya dari kesulitan menghitung algoritma diskrit. Algoritma ini dapat digunakan dalam mendistribusikan kunci publik yang dikenal dengan protokol pertukaran kunci. Proses yang akan dilakukan untuk mengamankan citra adalah dengan cara memecah citra menjadi piksel kemudian menggunakan algoritma RSA untuk mengenkripsi dan algoritma Diffie Helman sebagai pembangkit bilangan primanya. Hal tersebut tentunya akan membuat cara pemecahannya menjadi lebih kompleks..

METODE PENELITIAN

2.1. Pengertian Kriptografi

Kriptografi adalah ilmu mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi mendapatkan kembali data asli. Proses enkripsi dilakukan menggunakan suatu algoritma dengan beberapa parameter.

2.2. Algoritma RSA(Rivest-Shamir- Adleman)

Algoritma RSA (Rivest-Shamir-Adleman) ditemukan pertama kali pada tahun 1977 oleh Ron Rivest, Adi Shamir, dan Leonard Adlemandan RSA sendiri diambil dari nama belakang penemunya kemudian disatukan menjadi Rivest Shamir Adlema. Algoritma RSA merupakan kriptografi kunci publik yang masih sangat populer digunakan, karena kunci-kunci yang panjang dan penerapannya semakin sempurna.

Algoritma RSA (Rivest-Shamir-Adleman) ditemukan pertama kali pada tahun 1977 oleh *Ron Rivest, Adi Shamir, dan Leonard Adleman*dan RSA sendiri diambil dari nama belakang penemunya kemudian disatukan menjadi *Rivest Shamir Adlema.* Algoritma RSA merupakan kriptografi kunci publik yang masih sangat populer digunakan, karena kunci-kunci yang panjang dan penerapannya semakin sempurna.

RSA mempunyai dua kunci, yaitu kunci publik dan kunci privat yang dimana Kunci publik diketahui oleh umum dan digunakan sebagai proses enkripsi, sedangkan kunci privathanya pihak tertentu yang boleh mengetahui dan digunakan untuk proses dekripsi.

Untuk membangkitan pasangan kunci RSA, digunakan algoritma sebagai berikut:

1. Dipilih dua buah bilangan prima sembarang yang besar, p dan q. Nilai p dan q harus dirahasiakan.
2. Dihitung n = p x q. Besaran n tidak perlu dirahasiakan.

3. Dihitung fungsi Euler's totient ?(n) = (p – 1)(q –1)
4. Dipilih sebuah bilangan bulat sebagai kunci publik, disebut namanya e, yang relatif prima terhadap ?(n). e relatif prima terhadap ?(n) artinya faktor pembagi terbesar keduanya adalah 1, secara matematis disebut gcd (e, ?(n)) =1.
5. Dihitung diterminasi d dengan rumus d =e- 1(mod ?(n)), d adalah multiplikasi invers dari e mod?(n)
6. d sebagai komponen kunci private sehingga e * d mod (n) =1
7. Kunci pablik mengandung modulo n dan eksponen e, sehingga (e,n)
8. Kunci privat mengandung modulo n dan eksponen d, sehingga (d,n).

Keamanan algoritma RSA terletak pada tingkat kesulitan dalam memfaktorkan bilangan non-prima menjadi faktor primanya, yangdalam hal ini n = p x q. Jika n berhasil difaktorkan menjadi p dan q, maka m = (p – 1)(q – 1) dapat dihitung. Dan karena kunci enkripsi e telah diumumkan (tidak dirahasi- akan), maka kunci dekripsi d dapat dihitung melalui persamaan (d x e) mod n = 1. Selama belum ditemukan cara untuk memfak-torkan bilangan besar menjadi faktor-faktor primanya, maka selama itu pula keamanan algoritma RSA terjamin. Penemu algoritma RSA menyarankan nilai p dan q panjangnya lebih dari 100 digit. Dengan demikian hasil kali n = p x q akan berukuran lebih dari 200digit.

Adapun Proses Enkripsi dan dekripsi RSA antara lain sebagai berikut :

1. Proses Enkripsi:
   a. Nyatakan pesan menjadi blok-blok plainteks: m1, m2, m3, … (harus dipenuhi persyaratan bahwa nilai mi harus terletak dalam himpunan nilai 0, 1, 2, …, n – 1 untuk menjamin hasil perhitungan tidak berada di luarhimpunan)
   b. Hitung blok cipherteks ci untuk blok plainteks pi dengan persamaan ci = mie mod n dalam hal ini, e adalah kunci publik.
2. Proses Dekripsi:
   Proses dekripsi dilakukan dengan menggunakan persamaan mi = ci d mod n, yang dalam hal ini, d adalah kunci privat (Fauzi and Rahayu, 2020)

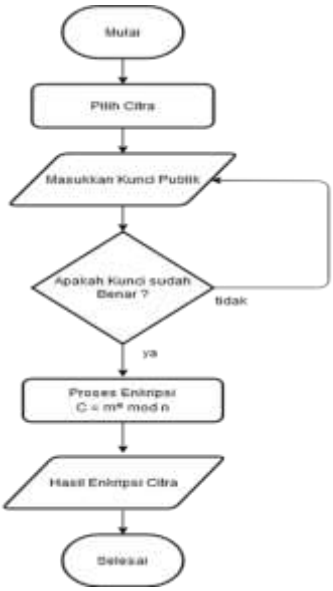
2.2. Algoritma Diffie Hellman

Algoritma pertukaran kunci Diffie- Hellman (protokol Diffie-Hellman) berguna untuk mempertukarkan kunci rahasia pada komunikasi menggunakan kriptografi simetris. Kekuatan algoritma ini adalah pada sulitnya melakukan perhitungan logaritma diskrit. Langkah-langkahnya adalah sebagai berikut,

1. Misalkan Alice dan Bob adalah pihak-pihak yang berkomunikasi. Mula-mula Alice dan Bob menyepakati 2 buah bilangan yang besar (sebaiknya prima) P dan Q, sedemikian sehingga P < Q. Nilai P dan Q tidak perlu rahasia, bahakan Alice dan Bob dapat membicarakannya melalui saluran yang tidak aman sekalipun.
2. Alice membangkitkan bilangan bulat acak x yang besar dan mengirim hasil perhitungan berikut kepada Bob :
   $X = P^x \bmod Q$.
3. Bob membangkitkan bilangan bulat acak y yang besar dan mengirim hasil perhitungan, berikut kepada Alice:
   $Y = P^y \bmod Q$.
4. Alice menghitung $K = Y^x \bmod Q$.
5. Bob menghitung $K' = X^y \bmod Q$.
   Jika perhitungan dilakukan dengan benar maka K = K'. Dengan demikian Alice dan Bob telah memiliki sebuah kunci yang sama tanpa diketahui pihak lain.

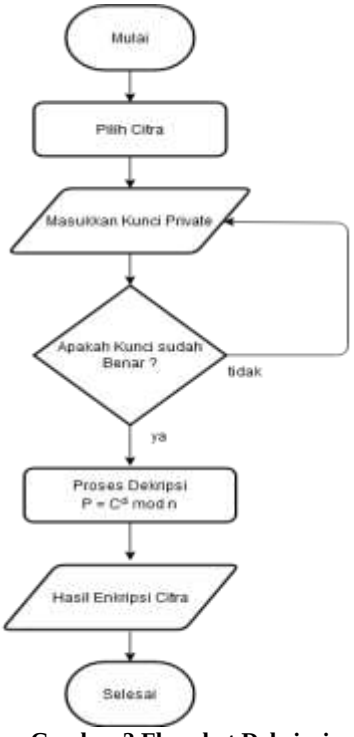
HASIL DAN PEMBAHASAN

3.1 Flowchart Enkripsi



Gambar 1.Flowchat Enkripsi

3.2 Flowchart Dekeipsi



Gambar 2 Flowchat Dekripsi

3.3 Konversi Citra

Pada proses konversi nilai citra, peneliti menggunakan citra berukuran 15x15 piksel untuk di konversi menjadi nilai RGB. Berikut adalah citra yang akan di konversi.

Gambar 3 Citra yang akan di konversi

3.4 Perhitungan Enkripsi Algoritma Diffie Hellman

Pencarian nilai Diffie Hellman 1 :

Pengirim membangkitkan bilangan bulat acak yang besar *x* dan mengirim hasil perhitungan kepada penerima. Dengan ketetapan g < n.

G = 37

N = 70

X = 253

$X = g^x \mod n$

$X = 37^{253} \mod 70 = 37$

Penerima membangkitkan bilangan bulat acak yang besar *y* dan mengirim hasil perhitungan kepada pengirim

Y = 162

$Y = g^y \mod n$

$Y = 37^{162} \mod 70 = 29$

Pengirim menghitung kunci simetri

$K = y^x \mod n$

$K = 29^{253} \mod 70$

K = 29

Penerima menghitung kunci simetri, jika benar maka

$K = K^1$

$K^1 = x^y \mod n$

$K^1 = 37^{162} \bmod 70$
$K^1 = 29$

Pencarian nilai Diffie Hellman 2 :
Pengirim membangkitkan bilangan bulat acak yang besar *x* dan mengirim hasil perhitungan kepada penerima. Dengan ketetapan g < n.
G = 81
N = 97
X = 59
$X = g^x \bmod n$
$X = 81^{59} \bmod 97 = 6$

Penerima membangkitkan bilangan bulat acak yang besar *y* dan mengirim hasil perhitungan kepada pengirim
Y = 80
$Y = g^y \bmod n$
$Y = 81^{80} \bmod 97 = 35$

Pengirim menghitung kunci simetri
$K = y^x \bmod n$
$K = 35^{59} \bmod 97$
K = 61

Penerima menghitung kunci simetri, jika benar maka
$K = K^1$
$K^1 = x^y \bmod n$
$K^1 = 6^{80} \bmod 97$
$K^1 = 61$

3.5 Proses Enkripsi Kombinasi Diffie-Helman dengan Algoritma RSA

Nilai P pada algoritma RSA di dapat dari nilai Diffie Hellman 1 dan Nilai Q pada algoritma RSA di dapat dari nilai Diffie Hellman 2. Berikut perhitungan enkripsi dengan algoritma kombinasi :

pixel (0,0)
$Red = 89^{47} \bmod 1769 = 84$
$Green = 91^{47} \bmod 1769 = 531$
$Blue = 112^{47} \bmod 1769 = 1035$

pixel (0,1)
$Red = 119^{47} \bmod 1769 = 192$
$Green = 117^{47} \bmod 1769 = 1306$
$Blue = 138^{47} \bmod 1769 = 622$

pixel (0,2)
$Red = 167^{47} \bmod 1769 = 1086$
$Green = 155^{47} \bmod 1769 = 282$
$Blue = 159^{47} \bmod 1769 = 358$

pixel (0,3)
$Red = 179^{47} \bmod 1769 = 138$
$Green = 169^{47} \bmod 1769 = 1660$
$Blue = 168^{47} \bmod 1769 = 141$

pixel (0,4)
$Red = 189^{47} \bmod 1769 = 396$
$Green = 179^{47} \bmod 1769 = 138$
$Blue = 170^{47} \bmod 1769 = 136$

pixel (0,5)
$Red = 222^{47} \bmod 1769 = 675$
$Green = 203^{47} \bmod 1769 = 522$
$Blue = 186^{47} \bmod 1769 = 1699$

Sampai perhitungan tersebut mencapai pixel ke :
pixel (14,13)
$Red = 90^{47} \bmod 1769 = 772$
$Green = 81^{47} \bmod 1769 = 1620$
$Blue = 16^{47} \bmod 1769 = 1415$

pixel (14,14)

Red = 112^{47} mod 1769 = 1035
Green = 109^{47} mod 1769 = 1173
Blue = 14^{47} mod 1769 = 1634

3.6 Proses Dekripsi Kombinasi Diffie Hellman dengan Algoritma RSA
pixel (0,0)
Red = 84^{143} mod 1769 = 89
Green = 531^{143} mod 1769 = 91
Blue = 1035^{143} mod 1769 = 112

pixel (0,1)
Red = 192^{143} mod 1769 = 119
Green = 1306^{143} mod 1769 = 117
Blue = 622^{143} mod 1769 = 138

pixel (0,2)
Red = 1086^{143} mod 1769 = 167
Green = 282^{143} mod 1769 = 155
Blue = 358^{143} mod 1769 = 159

pixel (0,3)
Red = 138^{143} mod 1769 = 179
Green = 1660^{143} mod 1769 = 169
Blue = 141^{143} mod 1769 = 168

pixel (0,4)
Red = 396^{143} mod 1769 = 189
Green = 138^{143} mod 1769 = 179
Blue = 136^{143} mod 1769 = 170

pixel (0,5)
Red = 675^{143} mod 1769 = 222
Green = 522^{143} mod 1769 = 203
Blue = 1699^{143} mod 1769 = 186

Sampai perhitungan tersebut mencapai pixel ke :
pixel (14,13)
Red = 1035^{143} mod 1769 = 112
Green = 1620^{143} mod 1769 = 81
Blue = 1415^{143} mod 1769 = 16

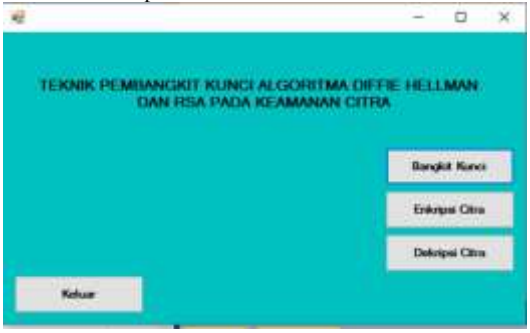
pixel (14,14)
Red = 772^{143} mod 1769 = 90
Green = 1173^{143} mod 1769 =109
Blue = 1634^{143} mod 1769 = 14

Aplikasi pengamanan citra menggunakan metode RSA dan Diffie Hellman ini di bangun dengan tujuan menjaga kepemilikan agar tetap aman dari tindakan pencurian. Hal ini di lakukan dengan cara mengenkrip data tersebut dan dapat di dekripsi sebagai pembuktian kepemilikan dari citra tersebut. Proses enkripsi dan dekripsi harus menggunakan aplikasi dan kunci yang sama.

Tampilan dari sistem perbaikan citra yang telah dirancang menggunakan aplikasi pemerograman *Visual Basic 2010*, dengan penerapan algoritma RSA dan Diffie Hellman pengamanan citra, yaitu sebagai berikut :

a.Tampilan Halaman Utama Sistem

Setelah program dijalankan maka sistem akan menampilkan halaman utama dari sistem yang telah dibangun, dalam tampilan halaman utama sistem terdapat menu yang dapat digunakan oleh pengguna yaitu menu halaman utama, proses bangkit kunci, enkripsi citra, dekripsi citra dan keluar. Tampilan halaman utama sistem tersebut adalah sebagai berikut:



Gambar 4 Tampilan antarmuka

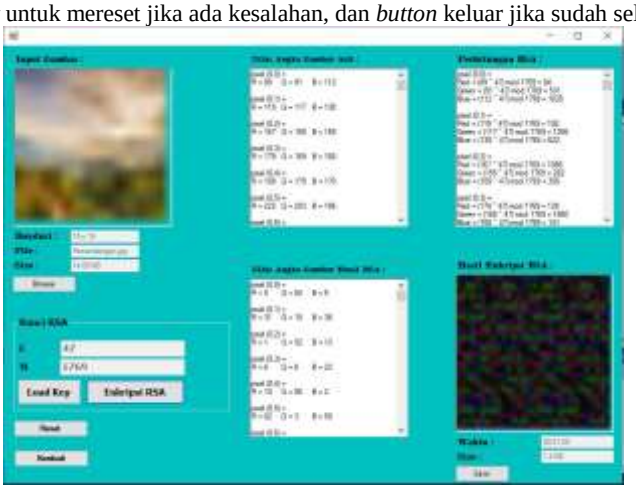
b.Tampilan Halaman Proses Bangkit Kunci

Pada tampilan bangkit kunci menampilkan beberapa baris untuk proses bangkit kunci, pada tampilan ini pengguna sistem harus menyimpan kunci yang mana nantinya untuk digunakan dalam penenkripan atau pendekripan pada citra yang akan di amankan, tampilan halaman bangkit kunci adalah sebagai berikut :

Gambar 5 Tampilan antarmuka pembangkit kunci

c. Tampilan Halaman Enkripsi Citra

Pada tampilan ini sistem akan menampilkan Input Gambar yang akan diamankan, *Form* Kunci Diffie Hellman dan RSA yang mana akan memunculkan kunci yang telah kita save dari *form* bangkit kunci, *Form* nilai angka gambar asli yang dimana akan memunculkan nilai suatu citra asli, *Form* nilai angka gambar hasil enkripsi yang dimana akan memunculkan nilai suatu citra yang telah di enkripsi, *Form* perhitungan akan memunculkan perhitungan enkripsi, *button save* untuk menyimpan enkripsi suatu citra, *button reset* untuk mereset jika ada kesalahan, dan *button* keluar jika sudah selesai.



Gambar 6 Tampilan enkripsi

d. Tampilan Halaman Dekripsi Citra

Pada tampilan ini sistem akan menampilkan input citra enkripsi yang telah di simpan sebelumnya, *Form* kunci RSA dan Diffie Hellman yang mana kuncinya yang telah kita simpan sebelumnya, *Form* nilai angka gambar dekripsi yang dimana akan memunculkan nilai suatu citra dekripsi, *Form* perhitungan akan memunculkan perhitungan dekripsi, *button save* untuk menyimpan dekripsi suatu citra, *button reset* untuk mereset jika ada kesalahan, dan *button* keluar jika sudah selesai.

Gambar 7 Tampilan dekripsi

KESIMPULAN

Berdasarkan hasil perancangan dan pembuatan program aplikasi kriptografi menggunakan metode RSA dan Diffie Hellman ini dapat di ambil kesimpulan sebagai berikut:

1. Dalam citra berhasil di terapkan dan mampu melakukan proses enkripsi dan dekripsi Semakin besar ukuran citra maka

waktu proses enkripsi dan proses dekripsi akan membutuhkan waktu yang lebih lama, Hasil pengujian pada sistem di dapatkan bahwa citra yang telah mengalami proses enkripsi dan proses dekripsi dengan algoritma RSA dan Diffie Hellman memiliki isi informasi yang sama dengan citra yang asli.

2. Pengamanan citra dengan menggunakan algoritma RSA dan Diffie Hellman untuk merahasiakan citra berjalan dengan baik. citra berhasil di enkripsi dan di dekripsi, percobaan yang dilakukan pada algoritma RSA dan Diffie Hellman, waktu proses yang di hasilkan dekripsi lebih cepat dibandingkan hasil enkripsi.
3. Untuk setiap kunci telah dibuat secara acak, Setiap nilai warna dalam piksel dienkripsi dengan kunci yang berbeda-beda menyebabkan penyerang harus mencoba segala kemungkinan kunci yang ada, Sehingga sulit untuk membobol atau menebak citra yang telah terenkrip tersebut.

DAFTAR PUSTAKA

[1] Ariyus Doni. 2008. Pengantar Ilmu Kriptografi. CV Andi Offset, Yogyakarta.
[2] Hidayatullah, Priyanto. 2017. Pengolahan Citra Digital. Informatika Bandung, Bandung.
[3] Kurniawan Erick. 2011. Cepat Mahir Visual Basic 2010. CV Andi Offset. Yogyakarta.
[4] Sadikin Rifki, 2012. Kriptografi Untuk Keamanan Jaringan dan Implementasi dalam Bahasa Java. CV Andi Offset, Yogyakarta.
[5] Setiawan. 2009. Flowchart Algoritma Dan Pemrograman Menggunakan Bahasa C++ Bulder. Graha Ilmu. Yogyakarta.
[6] Sugiarti Yuni. 2013. Analisis Dan Perancangan UML. Graha Ilmu. Yogyakarta
[7] https://www.unaki.ac.id/ejournal/index.php/majalah-ilmiah-informatika/article/view/36 (Di akses tanggal 15 Juni 2020 pukul 20.00 Wib)
[8] https://www.researchgate.net/publication/303382290_Implementasi_Algoritma_Chiper_Caesar_Untuk_Enkripsi_dan_Dekripsi_pada_tabel_ascii_Menggunakan_Bahasa_Java (Diakses pada tanggal 20 juni 2020 pukul 13.00 wib