JTRISTE, Vol.3, No.1, Maret 2016, pp. 15~21
ISSN: 2355-3677

Sistem Proteksi Ganda Dengan Menggunakan Algoritma Rivest Shamir Adleman (RSA) dan Elgamal untuk Proses Enkripsi dan Dekripsi

Islamiyah
Program Studi Teknik Informatika Universitas Mulawarman
Islamiyah1601@yahoo.co.id

Abstrak

Keamanan dan kerahasiaan merupakan aspek penting yang dibutuhkan dalam proses pertukaran pesan melalui media jaringan/internet. Teknik kriptografi dapat digunakan untuk memberi perlindungan keamanan pada pesan rahasia. Pengembangan teknik kriptografi ganda dengan kombinasi algoritma RSA untuk proses enkripsi dan dekripsi dan algoritma ElGamal untuk proses enkripsi dan dekripsi diharapkan dapat melindungi pesan rahasia. Penelitian ini bertujuan untuk mengkombinasikan kriptografi RSA dan ElGamal yang memberikan proteksi ganda pada pesan rahasia di dalam sebuah teks. Hasil dari penelitian ini adalah sebuah aplikasi kriptografi dengan menggunakan dua algoritma yang dapat melakukan proses enkripsi dan dekripsi dengan menggunakan bahasa pemograman Visual Basic 6.0

Kata-kata kunci: Kriptografi, RSA, ElGamal, Proteki Ganda, enkripsi, deskripsi

Abstract

Security and confidentiality are important aspects needed in the exchange of messages over the network/ internet. Cryptographic techniques can be used to provide security protection to the secret message. Development of multiple cryptographic techniques in combination with RSA algorithm for encryption and decryption and ElGamal algorithm for encryption and decryption process is expected to protect the secret message. This research aims to combine RSA and ElGamal cryptography that provides double protection to the secret message in a text. The result of this study is an aplication of cryptografi by using two algorithms that can perform encryption and decryption using the programming language Visual Basic 6.0

Keywords : Cryptography, RSA, ElGamal, double protection, encryption, decryption .

1. **Pendahuluan**

Teknologi informasi dan komunikasi telah berkembang pesat, memberikan pengaruh yang besar bagi kehidupan manusia. Perkembangan teknologi jaringan dan internet memungkinkan setiap orang untuk saling bertukar data, informasi, atau pesan kepada orang lain tanpa batasan jarak dan waktu. Keamanan dan kerahasiaan merupakan aspek penting yang dibutuhkan dalam proses pertukaran pesan/informasi melalui jaringan/internet,karena turut berkembang pula kejahatan teknologi dengan berbagai teknik interupsi, penyadapan, modifikasi, maupun fabrikasi. Tanpa adanya jaminan keamanan, orang lain dapat dengan mudah mendapatkan pesan/informasi yang dikirimkan melalui jaringan/internet. Berbagai macam teknik keamanan telah dikembangkan untuk melindungi dan menjaga kerahasiaan pesan agar terhindar dari orang yang tidak berhak, salah satunya yaitu teknik kriptografi. Kriptografi adalah suatu ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya

Pada saat ini, algoritma kriptografi telah berkembang secara modern dengan bantuan teknologi komputasi digital. Kriptografi modern menggunakan gagasan yang sama seperti kriptografi klasik, namun tidak beroperasi dalam modus karakter alfabet seperti pada algoritma kriptografi klasik. Kriptografi modern beroperasi pada mode bit, yang berarti semua data dan informasi (kunci, plainteks, maupun cipherteks) dinyatakan dalam rangkaian (string) bit biner, 0 dan 1.

Kriptografi memiliki dua konsep utama, yaitu enkripsi dan dekripsi. Enkripsi adalah proses menyandikan *plaintext* menjadi *ciphertext* dengan mengubah pesan menjadi bentuk lain yang disamarkan agar tidak dikenali secara langsung, sedangkan dekripsi adalah proses

mengembalikan *ciphertext* menjadi *plaintext.* Proses enkripsi dan dekripsi membutuhkan kunci sebagai parameter yang digunakan untuk transformasi. Hasil (*output)* kriptografi adalah sebuah bentuk yang berbeda dari pesan/informasi asli, dan memiliki ciri yang seolah-olah acak/tidak teratur. Perubahan pada hasil tersebut dapat membuat kecurigaan tentang informasi apa yang terkandung didalamnya. Teknik kriptografi dapat dipecahkan dengan kemampuan teknologi komputasi.

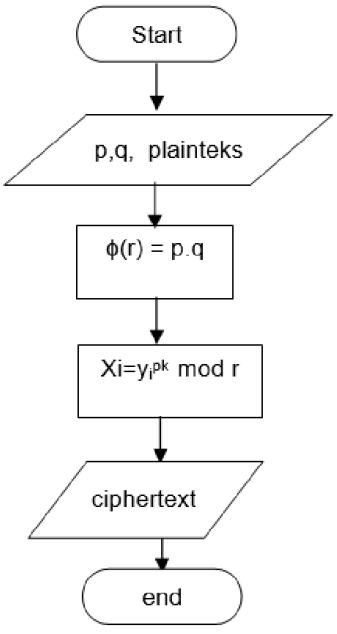
Kriptografi moderen dapat digabungkan agar mendapatkan proteksi ganda. Algoritma *Rivest Shamir Adlema*n (RSA) dan Algoritma ElGamal dapat dikombinasikan untuk membuat menghasilkan dua lapis keamanan yang dapat memberi perlindungan lebih pada pesan rahasia. Pesan rahasia dienkripsi dengan kunci lalu disembunyikan, dan pesan rahasia dapat diekstraksi dan didekripsi kembali persis sama seperti aslinya dengan menggunakan kunci yang sama. Kriptografi dapat memberikan keamanan pada pesan rahasia. Pesan rahasia terlebih dahulu dienkripsi dan didekripsi dengan algoritma *Rivest Shamir Adleman* **(**RSA) dan proses yang sama dilakukan dengan menggunakan algoritma ElGamal.

Ada beberapa penelitian sebelumnya yang mendasari adanya penelitian ini. Penelitian pertama Basuki Rahmat (2010) dengan judul Steganografi Menggunakan Metode Least Significant Bit dengan Kombinasi Algoritma Kriptografi Vigenère dan RC4. Penelitian ini bertujuan untuk mengkombinasikan kriptografi Vigenère dan RC4 yang terintegrasi dengan metode steganografi, untuk memberikan proteksi ganda pada pesan rahasiadi dalam sebuah gambar/citra digital. Hasil dari penelitian ini adalah sebuah aplikasi yang diberi nama “StegoKripto”yang telah berhasil mengkombinasikan kriptografi dan steganografi. Penelitian kedua Yudhistira Taufan (2011) dengan judul Enkripsi Email dengan Menggunakan Metode ElGamal pada Perangkat Mobile. Penelitian ini menghasilkan cipherteks yang mana ketika penerima ingin membacanya, perlu untuk melakukan proses dekripsi. Selain itu, proses enkripsi pada plainteks yang sama diperoleh cipherteks yang berbeda-beda, namun pada proses dekripsi diperoleh plainteks yang sama, sehingga membuat email menjadi lebih secure dibanding sebelumnya.

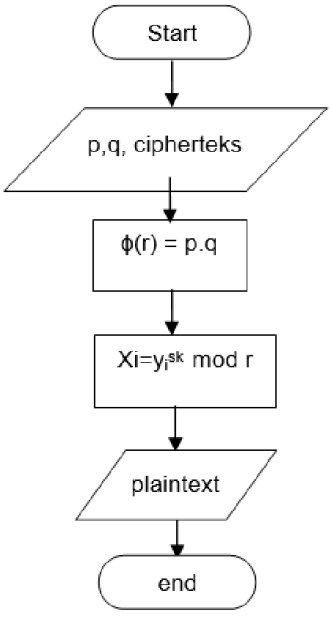
2. Metode Penelitian

Proses enkripsi dan dekripsi algoritma RSA

Proses enkripsi adalah proses untuk mengubah plainteks menjadi cipherteks sedangkan proses dekripsi adalah proses mengubah cipherteks ke planteks semula

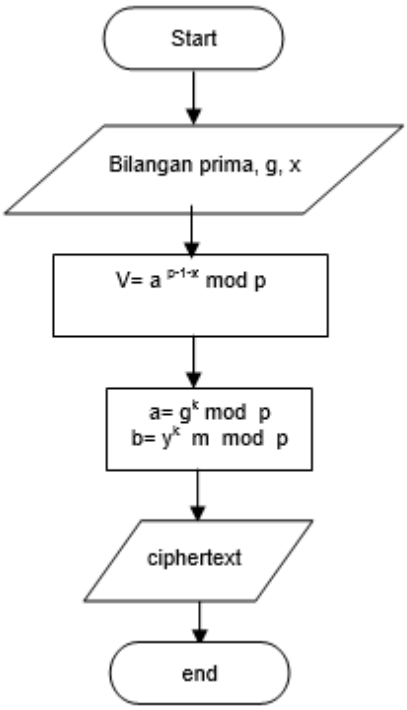


Gambar 1. Proses Enkripsi RSA

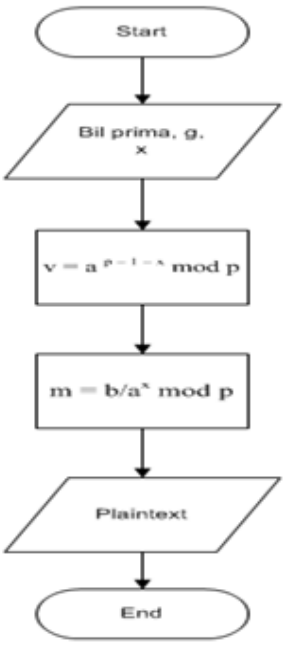


Gambar 2. Proses Dekripsi RSA

Proses enkripsi dan dekripsi algoritma ElGamal



Gambar 3. Proses Enkripsi ElGamal

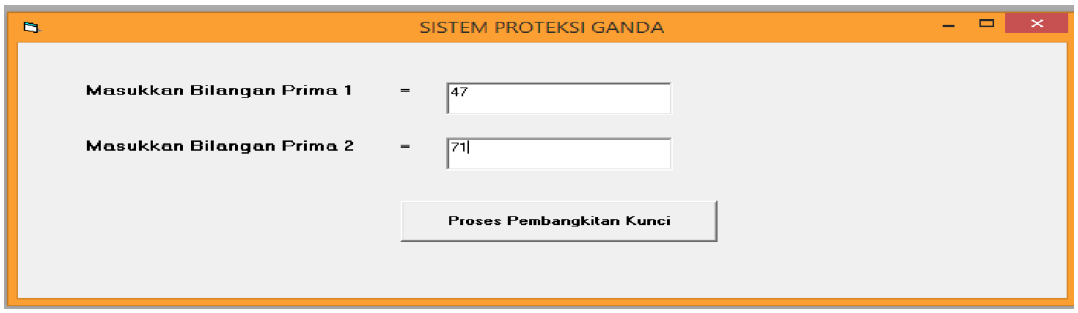


Gambar 4. Proses Dekripsi ElGamal

3. Hasil dan Pembahasan

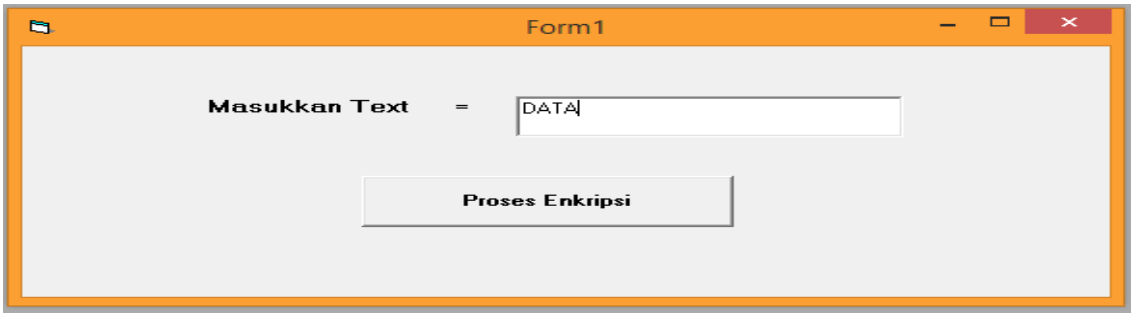
3.1 Implementasi Sistem

Gambar dibawah merupakan tampilan awal dimana akan diisikan dua bilangan prima secara acak oleh pengguna untuk membangkitkan kunci menggunakan metode Algoritma RSA.



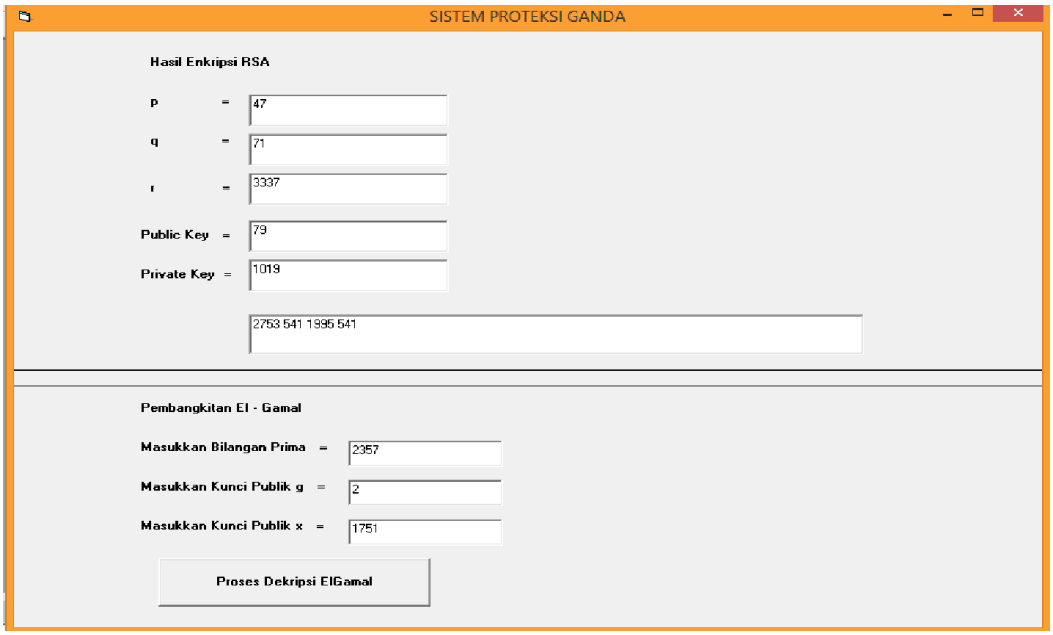
Gambar 5. Form Input Pembangkitan Kunci

Selanjutnya, setelah menginputkan dua bilangan prima sebagai pembangkit kunci, akan dilakukan proses enkripsi menggunakan metode Algoritma RSA dimana sebelumnya telah diinputkan pesan (pla), kata atau kalimat yang akan dienkripsi.



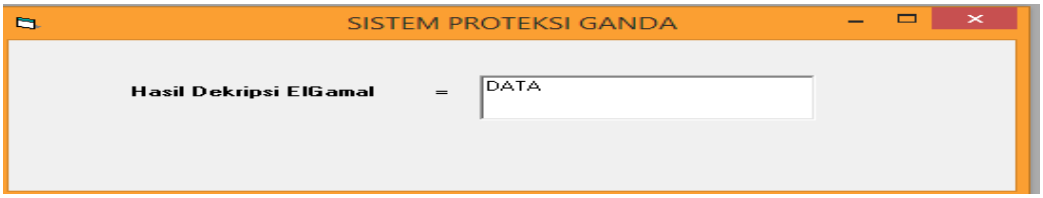
Gambar 6. Form Enkripsi Plaintext

Setelah melalui proses enkripsi dengan metode RSA, maka ditampilkan kunci private dan kunci publik yang digunakan bersama dengan hasil enkripsi yang selanjutnya akan didekripsi menggunakan metode kedua yaitu metode Algoritma ElGamal. Pada form bagian kedua yang ada di bawah, perlu diisikan bilangan prima acak serta kunci publik terbaru untuk keperluan dekripsi menggunakan Algoritma ElGamal.



Gambar 7. Form Tampilan Hasil Enkripsi RSA dan Proses Dekripsi ElGamal

Form terakhir ini menunjukkan hasil dekripsi menggunakan metode Algoritma ElGamal sesuai dengan bilangan prima serta kunci yang diinputkan pada form sebelumnya.



Gambar 8. Form Hasil Dekripsi

3.2 Uji Coba Enkripsi dan Dekripsi Algoritma RSA

Misalkan p = 47 dan *q* = 71 (keduanya prima). Selanjutnya, hitung nilai

$$\phi(r) = p \,.\, q = 3337$$

dan

$$\phi(r) = (p - 1)(q - 1) = 3220.$$

Pilih kunci publik *SK* = 79, karena 79 relatif prima dengan 3220. *PK* dan *r* sifatnya tidak rahasia.

Misal plainteks yang akan dienkripsikan adalah

X= DATA

atau dalam sistem desimal (pengkodean sesuai dengan tabel konversi ASCII) adalah

68658465

Pecah *X* menjadi blok yang lebih kecil, misalnya *X* dipecah menjadi enam blok yang berukuran 3 digit:

$x_1 = 68$
$x_2 = 65$
$x_3 = 84$
$x_4 = 65$

Enkripsi

Langkah enkripsi dari blok-blok plainteks diatas adalah sebagai berikut:

$68^{79} \bmod 3337 = 2753 = y_1$
$65^{79} \bmod 3337 = 541 = y_2$
$84^{79} \bmod 3337 = 1995 = y_3$
$65^{79} \bmod 3337 = 541 = y_4$

Jadi, cipherteks yang dihasilkan adalah

Y = 2753 541 1995 541

Dekripsi

Dekripsi dilakukan dengan menggunakan kunci rahasia

SK= 1019

Blok-blok cipherteks didekripsikan sebagai berikut:

$2753^{1019} \bmod 3337 = 68 = x_1$
$541^{1019} \bmod 3337 = 65 = x_2$
$1995^{1019} \bmod 3337 = 84 = x_3$
$541^{1019} \bmod 3337 = 65 = x_3$

Blok plainteks yang lain dikembalikan dengan cara yang serupa. Akhirnya kita memperoleh kembali plainteks semula

P= 68658465

yang dalam karakter ASCII adalah

P= DATA

Algoritma ElGamal

Misalkan A ingin membangkitkan pasangan kuncinya. A memilih p = 2357, g = 2, dan x = 1751.

A menghitung
$y = g^x \bmod p$
$y = 2^{1751} \bmod 2357 = 1185$

Jadi, kunci publik A adalah (y = 1185, g = 2, p = 2357) dan; Kunci privatnya adalah (x = 1751, p = 2357).

Enkripsi ElGamal

Misalkan B ingin mengirim plainteks DATA kepada A (nilai m masih berada di dalam selang [0, 2357 – 1]

Ubah DATA ke dalam bentuk ASCII (sesuai dengan tabel ASCII)

D = 68
A = 65
T = 84
A = 65

B memilih bilangan acak k = 10 (nilai k masih berada di dalam selang [0, 2357 – 1]). B menghitung untuk masing-masing kode ASCII:

Untuk D:

$a = g^k \bmod p = 2^{10} \bmod 2357 = 1024$
$b = y^k m \bmod p = 1185^{10} \times 68 \bmod 2357 = 1857$

Jadi, cipherteks yang dihasilkan untuk kode D adalah (1024, 1857).

Untuk A:

$a = g^k \bmod p = 2^{10} \bmod 2357 = 1024$
$b = y^k m \bmod p = 1185^{10} \times 65 \bmod 2357 = 2295$

Jadi, cipherteks yang dihasilkan untuk kode D adalah (1024, 2295).

Untuk T:

$a = g^k \bmod p = 2^{10} \bmod 2357 = 1024$
$b = y^k m \bmod p = 1185^{10} \times 84 \bmod 2357 = 1878$

Jadi, cipherteks yang dihasilkan untuk kode D adalah (1024, 1878).

Untuk A:

$a = g^k \bmod p = 2^{10} \bmod 2357 = 1024$
$b = y^k m \bmod p = 1185^{10} \times 65 \bmod 2357 = 2295$

Jadi, cipherteks yang dihasilkan untuk kode D adalah (1024, 2295).

Dekripsi ElGamal

A mendekripsi cipherteks dari B dengan melakukan perhitungan sebagai berikut:
Dekripsi cipherteks menggunakan persamaan dibawah:

Untuk Cipherteks (1024, 1857):

$(a^x) - 1 = a^{p-1-x} \bmod p = 1024^{605} \bmod 2357 = 113$
$m = b/a^x \bmod p = 113 \times 1857 \bmod 2357 = 68$

Jadi plaintext dari 68 sesuai dengan kode ASCII adalah D

Untuk Cipherteks (1024, 2295):

$(a^x) - 1 = a^{p-1-x} \bmod p = 1024^{605} \bmod 2357 = 113$
$m = b/a^x \bmod p = 113 \times 2295 \bmod 2357 = 65$

Jadi plaintext dari 65 sesuai dengan kode ASCII adalah A

Untuk Cipherteks (1024, 1878):

$(a^x) - 1 = a^{p-1-x} \bmod p = 1024^{605} \bmod 2357 = 113$
$m = b/a^x \bmod p = 113 \times 1878 \bmod 2357 = 84$

Jadi plaintext dari 84 sesuai dengan kode ASCII adalah T

Untuk Cipherteks (1024, 2295):

$(a^x) - 1 = a^{p-1-x} \bmod p = 1024^{605} \bmod 2357 = 113$
$m = b/a^x \bmod p = 113 \times 2295 \bmod 2357 = 65$

Jadi plaintext dari 65 sesuai dengan kode ASCII adalah A
Maka hasil dekripsi dari cipherteks diatas adalah **DATA**

4. Kesimpulan

Berikut adalah kesimpulan yang dapat ditarik dari penelitian ini adalah

1. Algoritma RSA adalah salah satu metode/algoritma enkripsi yang banyak digunakan dalam berbagai macam perangkat
2. RSA memiliki dua buah kunci, yaitu kunci privat dan kunci publik. Kunci publik adalah kunci yang dipublikasikan sedangkan kunci privat adalah kunci yang tidak boleh diberitahukan kepada siapapun
3. Elgamal ternyata dapat juga digunakan untuk dekripsi dan enkripsi pada mulanya hanya digunakan untuk *digital signature*
4. Keamanan ElGamal ini terletak pada sulitnya menghitung logaritma diskrit
5. Algoritma RSA dapat dikombinasikan dengan Algoritma ElGamal untuk sistem proteksi ganda. Pada penelitian ini algoritma kedua algoritma dapat melakukan proses enkripsi dan dekripsi

DAFTAR PUSTAKA

[1] Kramer, P. 2002. Encryption and Decryption with RSA Algorithm Mathematics and The Computer. Jakarta: Informatika.
[2] Kurniawan, Y. 2004. Kriptografi: Keamanan Internet dan Jaringan Komunikasi. Bandung: Informatika.
[3] Mao, W. 2004. Modern Cryptography. New Jersey: Prentice-Hall.
[4] Munir, R. 2006. Kriptografi. Bandung: Informatika.
[5] Short, S. 2003. Building XML Web Services For The Microsoft .Net Platform. Jakarta: PT Elex Media Komputindo.
[6] Rahmat, Basuki, dkk. 2010. Steganografi Menggunakan Metode Least Significant Bit dengan Kombinasi Algoritma Kriptografi Vigenère dan RC4
[7] Taufan, Yudistira. 2011. Enkripsi Email dengan Menggunakan Metode ElGamal pada Perangkat Mobile.
[8] Tjoenedi, FK. 2004. Pembuatan Program Digital Signature Authentication File dengan ECDSA.