KRIPTANALISIS KUNCI PUBLIK ALGORITMA RABIN MENGGUNAKAN METODE KRAITCHIK

Drs. Swingly Purba, M.Sc

Program Studi S-1 Teknik Informatika, Institut Sains Dan Teknologi TD Pardede
Jl. DR.TD Pardede No.08, Medan 20153, Indonesia.

Email : Swinglypurba@istp.ac.id

Abstrak

Algoritma Rabin merupakan algoritma asimetris *cryptography* kunci-publik (*public-keycryptography).* Algoritma asimetris adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsi. Di mana kunci enkripsi dapat disebarkan kepada umum dan dinamakan sebagai kunci publik n (*public key*), sedangkan kunci dekripsi disimpan untuk digunakan sendiri dinamakan sebagai kunci pribadi p dan q (*private key*). Keuntungan algoritma Rabin adalah dapat memecahkan nilai- nilai yang besar sedangkan kerugiannya adalah harus mencari salah satu kunci yang benar diantara 4 (empat) kemungkinan hasil pendekripsian tersebut, sehingga didapatkan kunci yang benar. Untuk menguji keamanan algoritma Rabin penulis akan melakukan pengujian pemecah kunci publik dan untuk melihat seberapa aman algoritma Rabin untuk melakukan perhitungan bilangan prima. Pada penelitian ini, penulis menggunakan Metode Kraitchik untuk memecahkan kunci privat Algoritma Rabin. Metode Kraitchik adalah salah satu metode kriptanalisis yang digunakan untuk pemfaktoran *factoring* yaitu dengan cara memfaktorkan nilai *n* menjadi dua buah bilangan faktor prima yaitu *x* dan *y* sehingga $x^2 \equiv y^2 (mod\ n)$ menjadi faktor *n*. Hasil dari pengujian didapatkan bahwa semakin besar panjang dan nilai kunci publik *n* tidak selalu menghasilkan waktu pemfaktoran yang semakin lama. Pada proses pemecahan kunci publik 8 digit dengan kunci publik *n= 57292913* dan kunci privat yang didapatkan *p = 6719* dan *q = 8527* membutuhkan waktu proses 6 *ms (milliseconds).*

Kata Kunci : Kriptografi, Kriptanalisis, Algoritma Rabin, Metode Kraitchik.

Abstrak

Algoritma Rabin merupakan algoritma asimetris *cryptography* kunci-publik (*public-keycryptography).* Algoritma asimetris adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsi. Di mana kunci enkripsi dapat disebarkan kepada umum dan dinamakan sebagai kunci publik n (*public key*), sedangkan kunci dekripsi disimpan untuk digunakan sendiri dinamakan sebagai kunci pribadi p dan q (*private key*). Keuntungan algoritma Rabin adalah dapat memecahkan nilai- nilai yang besar sedangkan kerugiannya adalah harus mencari salah satu kunci yang benar diantara 4 (empat) kemungkinan hasil pendekripsian tersebut, sehingga didapatkan kunci yang benar. Untuk menguji keamanan algoritma Rabin penulis akan melakukan pengujian pemecah kunci publik dan untuk melihat seberapa aman algoritma Rabin untuk melakukan perhitungan bilangan prima. Pada penelitian ini, penulis menggunakan Metode Kraitchik untuk memecahkan kunci privat Algoritma Rabin. Metode Kraitchik adalah salah satu metode kriptanalisis yang digunakan untuk pemfaktoran *factoring* yaitu dengan cara memfaktorkan nilai *n* menjadi dua buah bilangan faktor prima yaitu *x* dan *y* sehingga $x^2 \equiv y^2 (mod\ n)$ menjadi faktor *n*. Hasil dari pengujian didapatkan bahwa semakin besar panjang dan nilai kunci publik *n* tidak selalu menghasilkan waktu pemfaktoran yang semakin lama. Pada proses pemecahan kunci publik 8 digit dengan kunci publik *n= 57292913* dan kunci privat yang didapatkan *p = 6719* dan *q = 8527* membutuhkan waktu proses 6 *ms (milliseconds).*

Kata Kunci : Kriptografi, Kriptanalisis, Algoritma Rabin, Metode Kraitchik.

I PENDAHULUAN

A. Latar Belakang

Kriptografi ditujukan untuk memberi layanan keamanan, salah satunya dalam aspek kerahasiaan. Kerahasiaan adalah suatu layanan yang ditujukan untuk menjaga agar pesan-pesan yang akan dikirim tidak dapat dibaca oleh pihak-pihak yang tidak berhak dengan cara menyandikan *plaintext* (pesan asli) menjadi *ciphertext* (pesan sandi) yang disebut enkripsi. Sedangkan proses pengembalian *ciphertext* menjadi *plaintext* disebut dekripsi. Proses enkripsi dan dekripsi

tersebut menggunakan algoritma kriptografi atau disebut juga *cipher*.

Algoritma Rabin merupakan algoritma asimetris. Algoritma Rabin memiliki kunci privat yang terdiri dari dua bilangan prima *p* dan *q* dan kunci publik yang terdiri dari $n = p * q$. Keamanannya didasarkan pada sulitnya faktorisasi dari *p* dan *q* yang belum diketahui. Di mana nilai *p* dan $q \pmod 4 = 3$. Di mana pada algoritma Rabin *Public Key* ini akan menghasilkan 4 (empat) kemungkinan hasil pendekripsian yang mengharuskan si penerima menentukan hasil dekripsi yang benar, si penerima harus mencari salah satu kunci yang benar diantara 4 (empat) kemungkinan hasil pendekripsian tersebut, sehingga didapatkan kunci yang benar.

Pada penelitian sebelumnya yang berjudul "Teknik Pemecah Kunci Algoritma RSA (*Rivest Shamir Adleman*) dengan Metode *Kraitchik*" bahwa kunci privat algoritma RSA dapat dipecahkan dengan memfaktorkan kunci publik *n* menggunakan metode *Kraitchik* dan ditinjau dari parameter waktu yang dilakukan.

Berdasarkan latar belakang yang telah penulis uraikan, maka dilakukan penelitian dengan judul "**Kriptanalisis Kunci Publik Algoritma RabinMenggunakan Metode *Kraitchik***".

A. Rumusan Masalah

Berdasarkan latar belakang di atas, maka dapat disimpulkan rumusan masalahnya adalah apakah kunci privat algoritma Rabin dapat dipecahkan dengan memfaktorkan kunci publik *n*.

B. Batasan Masalah

Dalam melakukan penelitian ini, peneliti membatasi ruang masalah yang akan diteliti. Batasan-batasan masalah yang digunakan adalah :

1. Pemfaktoran kunci publik *n* untuk mendapatkan nilai *p* dan *q* sehingga mendapat kunci privatnya dengan menggunakan metode *Kraitchik*.
2. Uji bilangan prima menggunakan Algoritma *Lehmann*
3. Algoritma pemecahan kunci dihitung dari lama proses waktu program
4. Aplikasi yang digunakan berbasis dekstop dan menggunakan *software C#*.

C. Tujuan Penelitian

Tujuan utama yang ingin dicapai pada penelitian ini adalah untuk memecahkan kunci publik *n* menggunakan metode *Kraitchik* serta melihat pemfaktoran kunci publik dengan metode *Kraitchik*.

D. Manfaat Penelitian

Manfaatyangdiperolehdari penelitian ini adalah mengetahui efisiensi metode *Kraitchik* dalam memecahkan kunci publik algoritma Rabin untuk mengembangkan motode kriptanalisis yang lebih efisien dan untuk mengetahui tingkat keamanan dari algoritma Rabin.

E. Metode Penelitian

Metode penelitian yang dilakukan dalam penelitian ini adalah:

1. Studi Pustaka
   Pada tahap ini penelitian dimulai dengan mecari referensi dari berbagai sumber terpercaya dan melakukan peninjauan pustaka melalui buku-buku, artikel ilmiah, dan penelitian-penelitian lainnya dalam bentuk jurnal yang berhubungan dengan Algoritma *Rabin dan Kraitchik Method.*
2. Analisa dan Perancangan.
   Berdasarkan ruang lingkup penelitian, penulis melakukan analisa terhadap apa saja yang akan dibutuhkan dalam penelitian untuk segera dirancang dalam sebuah diagram alir (*flowchart),* diagram *fishbone* dan diagram *UML.*
3. Implementasi
   Pada tahap ini, membuat sebuah sistem dengan menggunakan bahasa pemrograman C# sesuai dengan diagram alir yang telah dirancang.
4. Pengujian
   Pada tahap ini, sistem yang telah dirancang untuk melakukan kriptanalisis terhadap kunci publik untuk mendapatkan kunci privat dangan menggunakan metode faktorisasi.
5. Dokumentasi
   Pada tahap ini, penelitian yang telah dilakukan, di dokumentasikan mulai dari tahap analisa sampai kepada tahap pengujian dalam bentuk skripsi.

II. LANDASAN TEORI

A. Kriptogafi

Kriptografi sangat berkaitan sekali dengan keamanan suatu informasi. Kata kriptografi berasal dari bahasa Yunani yaitu *kryptos* (tersembunyi atau rahasia) dan *graphein* (menulis) atau *logi* (ilmu). Secara istilah kriptografi didefinisikan sebagai ilmu sekaligus seni untuk menjaga kerahasiaan pesan (data atau informasi) yang memiliki arti, dengan cara menyamarkannya (mengacak) menjadi bentuk yang tidak dapat dimengerti dengan menggunakan suatu algoritma tertentu

B. Tujuan Kriptografi

Secara garis besarnya tujuan kriptografi adalah untuk mencegah pengaksesan informasi yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab. Adapun tujuan dari kriptografi adalah sebagai berikut:

a. Kerahasian(*Confidentiality*).
   Menjaga informasi dari campur tangan pihak-pihak lain yang tidak berhak, kecuali yang memiliki hak.

b. Keutuhan Data (*Data Integrity*).
Meyakinkan tidak terjadinya pengubahan data oleh pihak yang tidak memiliki hak. Untuk meyakinkan keamanan dari suatu data tersebut, dapat dilakukan pendeteksian apakah data tersebut telah mengalami manipulasi.

c. Autentikasi (*Authentication*).
Untuk pemberian identifikasi. Autentikasi diberikan kepada penerima pesan dan pengirim pesan agar saling berhubungan dan melakukan autentikasi.

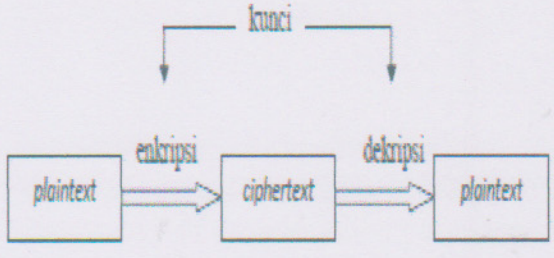
d. Nirpenyangkalan (*Non-Repudiation*).
Mencegah agar pihak yang menyangkal tidak dapat menolak pesan yang telah dikirim atau diterima.

C. Jenis-jenis Kriptografi

Ada 2 (dua) macam algoritma kriptografi yang berdasarkan dari kuncinya yaitu, Algoritma Simetris (kunci tunggal) dan Algoritma Asimetris (kunci publik).

1. Algoritma Simetris

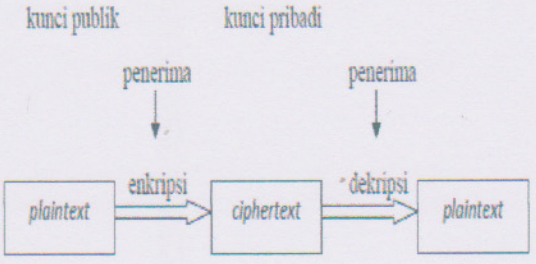
Enkripsi simetris sering disebut dengan enkripsi konvensional atau enkripsi kunci-tunggal (*single key*). Pada model enkripsi simetris digunakan algoritma yang sama untuk proses enkripsi atau dekripsi dengan memakai satu kunci yang sama seperti pada gambar 1 berikut ;



Gambar 1. Model Sederhana algoritma simetris[4].

2. Algoritma Asimetris

Algoritma Asimetris adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsi. Di mana kunci enkripsi dapat disebarkan kepada umum dan dinamakan sebagai kunci publik (*public key*), sedangkan kunci dekripsi disimpan untuk digunakan sendiri dinamakan sebagai kunci pribadi (*private key*) seperti pada gambar 2 berikut ;



Gambar 2. Model Sederhana algoritma Asimetris[4]

D. Algoritma Rabin

Algoritma Rabindiperkenalkan oleh Michael O. Rabin pada tahun 1979. Algoritma Rabin menggunakan pemfaktoran bilangan untuk melakukan pengamanan. Metode pemfaktoran bilangan secara cepat sampai saat ini belum terpecahkan. Selain itu, Rubin *Public Key* ini akan menghasilkan empat kemungkinan hasil pendekripsian yang mengharuskan si penerima menentukan hasil dekripsi yang benar[6].

1. Pembangkit Kunci

Proses pembangkitan kunci algoritma Rabin *Public Key* sebagai berikut:

1. Pilih dua buah bilangan prima yang sembarang dan berbeda (p dan q), di mana $p \equiv q \equiv 3 \pmod 4$. Dengan kata lain jika
   $p \bmod 4 = 3$ .....(1)
   $q \bmod 4 = 3$ .....(2)
2. Hitung nilai *n* yang merupakan kunci publik dengan rumus
   $n = p * q$ .....(3)
   di mana *p* dan *q* adalah kunci privat.
3. *Publish* nilai *n* (kunci publik) dan *p* dan *q* (kunci privat).
   Untuk mengenkripsi pesan hanya dibutuhkan kunci publik *n*, sedangkan untuk dekripsi dibutuhkan bilangan *p* dan *q* sebagai kunci privatnya.
   contoh : Misalkan A akan membangkitkan kunci publik dan kunci privat miliknya. A memilih nilai p = 103 dan q = 211 (keduanya bilangan prima). Kemudian A menghitung :
   n = 103 * 211
   n = 21733
   A mendapat kunci privat dan mendapat kenci publik, tetapi A harus menyimpan kunci privat *p* dan *q*.

2. Proses Enkripsi

Berikut adalah langkah–langkah proses enkripsi pesan rahasia menggunakan algoritma Rabin *Public Key* yang telah dimodifikasi adalah :

1. Dapatkan nilai *n* (kunci publik) dari *recipient*.
2. Tentukan pesan yang akan dikirim dan konversi dengan salah satu *encoding* ASCII dalam bentuk biner dan kemudian ubah dalam bentuk desimal sehingga di peroleh nilai *m*.

3. Hitung nilai *ciphertext C* dengan menggunakan rumus :
$C = m^2 \bmod n$ .....(4)
di mana :
C = *ciphertext*
n = kunci publik
m = nilai desimal dari hasil penggandaan nilai biner *plaintext*.
Contoh : A mendapatkan kunci publik yaitu: n = 21733 . Misalkan A mengirim pesan kepada B. Pesan (*plaintext*) yang akan dikirim ke B adalah
m = "D"
kemudian si B akan mengubah ke dalam *encoding* ASCII dalam bentuk biner dan kemudian ubah dalam bentuk desimal sehingga

p = 103	q = 211		
X	Y	D	K
0	1	211	
1	0	103	1
-1	1	108	0
1	0	103	1
-2	1	5	20
41	-20	3	1
-43	21	-2	1
84	-41	1	

di peroleh nilai m.
Misal m = " D " = 68
↑
ASCII
$m = 68_{10} = 0010001_2$
m = 00100010010001
sehingga di temukan nilai $m = 8772_{10}$
selanjutnya menghitung nilai *ciphertext* yaitu:
$C = m^2 \bmod n$
$C = 8772^2 \bmod 21733$
$C = 76\,947\,984 \bmod 21733$
Sehingga di dapatkan nilai C = 13164
4. Kirim nilai C ke *recipient*

3. Proses Dekripsi
Berikut adalah langkah–langkah proses dekripsi dengan menggunakan algoritma Rabin *Public Key* yang telah dimodifikasi:
1. Terima C dari *sender*.
2. Tentukan nilai *yp* dan *yq* yang merupakan pembagi GCD (*Greatest Common Divisor*) dari *p* dan *q* dengan menggunakan Algoritma *Extended Euclidean*. Karena GCD bilangan prima adalah 1, maka dapat ditulis sebagai berikut :
$yp * p + yq * q = gcd(p,q)$
$yp * p + yq * q = 1$ .....(5)
3. Hitunglah nilai mp dan mqdengan rumus:
$mp = C^{\frac{p+1}{4}} \bmod p$ .....(6)
$mq = C^{\frac{q+1}{4}} \bmod q$ .....(7)
4. Di mana *mp* adalah akar kuadrat dari *ciphertext* terhadap *p* dan *mq* adalah akar kuadrat dari *ciphertext* terhadap *q*.
5. Hitunglah v dan w
$v = yp * p * mq$ .....(8)
$w = yq * q * mp$ .....(9)
6. Hitung nilai *r, s, t* dan *u* dengan persamaan berikut :
$r = (v + w) \bmod n$ .....(10)
$s = (v - w) \bmod n$ .....(11)
$t = (-v + w) \bmod n$ .....(12)
$u = (-v - w) \bmod n$ .....(13)
7. Ubahlah nilai desimal *r, s, t* dan *u* diubah ke dalam bentuk biner. Kemudian nilai biner *r, s, t,* dan *u* kemudian dibagi menjadi 2 (dua) bagian. Bandingkan kedua bagian tersebut. Jika kedua bagian tersebut menghasilkan bentuk biner yang sama, maka didapatlah hasil dekripsi *ciphertext C*. Jika dibagi 2 (dua) akan menghasilkan biner yang sama dan biner antara ruas kanan dan ruas kiri juga sama. Maka didapatkan nilai *plaintext*-nya.

Contoh : si B menerima C = 13164 dari si A. Selanjutnya menetukan nilai *yp* dan *yq* dengan menggunakan GCD (*Greatest Common Divisor*) dari *p* dan *q* dengan menggunakan Algoritma *Extended Euclidean*.

Maka didapatkan nilai *yp* = 84 dan *yq* = -41
Selanjutnya mengitung nilai *mp* dan *mq* yaitu

$mp = 13164^{\frac{103+1}{4}} \bmod 103$
$mp = 13164^{\frac{104}{4}} \bmod 103$
$mp = 13164^{26} \bmod 103$
$mp = 17$

$mq = 13164^{\frac{211+1}{4}} \bmod 211$
$mq = 13164^{\frac{212}{4}} \bmod 211$
$mq = 13164^{53} \bmod 211$
$mq = 121$

setelah mendapatkan nilai *mp* dan *mq*, maka selanjutnya akan menghtung nilai *v* dan *w* yaitu:
$v = 84 * 103 * 121$ $v = 1046892$
$w = -41 * 211 * 17$ $w = -147067$
selanjutnya menghitung nilai *r, s, t* dan *u*
$r = (1046892 + (-147067)) \bmod 21733$
$= 899825 \bmod 21733$

Drs. Swingly Purba, M.Sc
KRIPTANALISIS KUNCI PUBLIK ALGORITMA RABIN MENGGUNAKAN METODE KRAITCHIK
Halaman 205-213

r = 8772
s = (1046892 – (- 147067)) *mod* 21733
= 1193959 *mod* 21733
s = 20377
t = (- 1046892+(-147067)) *mod* 21733
= -1193959 *mod* 21733
t = *1356*
u = (- 1046892 -(-147067)) *mod* 21733
= (- 1046892+147067) *mod* 21733
= -899825 *mod* 21733
u = 12961

selanjutnya nilai desimal *r, s, t* dan *u* di ubah ke dalam bentuk biner. Jika dibagi 2 (dua) akan menghasilkan biner yang sama dan biner antara ruas kanan dan ruas kiri juga sama. Maka didapatkan nilai *plaintext*-nya.

$r = 8772_{10}$ = 0010001 0010001$_2$benar
$s = 20377_{10}$ = 10011001 1111001$_2$ salah
$t = 1356_{10}$ = 001100 10101$_2$salah
$u = 12961_{10}$= 1000010 1010011$_2$ salah

maka nilai *plaintext* yang benar berada pada kunci r yaitu 8772_{10}.

E. KRIPTANALISIS

Kriptanalisis adalah sebuah ilmu mengenai *cipher, ciphertext,* atau *cryptosystems* yang bertujuan untuk menemukan kelemahan dalam sistem penyandian dan juga memecahkan *ciphertext* tanpa memiliki kunci yang sah dan biasanya mendapatkan beberapa kuncinya atau bahkan *plaintext* dan juga keseluruhan kuncinya. Tanpa perlu mengetahui kunci ataupun algoritma pembangun dari *ciphertext* tersebut.

F. METODE KRAITCHIK

Metode *Kraitchik* adalah salah satu metode kriptanalisis yang digunakan untuk pemfaktoran *factoring* yaitu dengan cara memfaktorkan nilai *n* menjadi dua buah bilangan faktor prima. Pada tahun1945, Maurice Kraitchik menemukan metode untuk memfaktorkan *n* menjadi *x* dan *y*. Metode *Kraitchik* digunakan untuk menemukan nilai *x* dan *y* sehingga $x^2 \equiv y^2 (mod\ n)$ menjadi faktor *n*. Kraitchik mengamati bahwa x^2-y^2 adalah kelipatan dari *n* dan untuk faktor *n*. Kraitchik menggunakan persamaan bentuk kn = x^2-y^2 untuk *k* adalah bilangan bulat positif, kemudian $kn = (x - y) * (x + y)$. Untuk menghitung faktor dari *n* Kratchik menggunakan persamaan

$$kn = x^2 - y^2 \quad \text{.....(14)}$$

di mana *k* adalah bilangan bulat positif (diasumsikan $x > y$. Sehingga $n = (x - y) * (x + y) / k$.

Contoh : Faktorkan 323 menggunakan metode *Kraitchik* dengan *k* adalah sebuah bilangan prima ganjil.

1. Hitung nilai x_0 dengan mengakarkan $n = 323$
$x_0 = \sqrt{n} = \sqrt{323} = 17{,}97... = 17$
2. Tentukan $k = 3$ dan hitung y^2 dengan persamaan (14) (m=1, 2, 3,...):

$$x^2 - k.n = y^2 \rightarrow (x_0 + m)^2 - k.n = y^2$$
$$(17+1)^2 - 3 * 323 = 324 - 969 = -645$$

Karena hasilnya negatif dan tidak bisa diakarkan, maka hitung y^2 dengan menaikkan nilai *m* sampai memberikan hasil yang positif dan menghasilkan akar yang sempurna:

$$(17+14)^2 - 3 * 323 = 961 - 969 = -7$$
$$(17+15)^2 - 3 * 323 = 1024 - 969 = 55$$
$$(17+16)^2 - 3 * 323 = 1089 - 969 = 120$$
$$(17+17)^2 - 3 * 323 = 1156 - 969 = 187$$
$$(17+18)^2 - 3 * 323 = 1225 - 969 = 256 = 16^2$$

Sehingga $kn = (x + y) * (x - y)$ adalah 3 * 323 = (35 + 16)*(35 - 16) = 51 * 19. Sehingga n = (51)/ 3 * 19 = 17 * 19. Sehingga didapat nilai x = 17 dan y = 19.

G. UJI BILANGAN PRIMA ALGORITMA LEHMANN

Algoritma Lehmann adalah salah satu cara untuk mencari bilangan prima dan masih ada beberapa agoritma lain yang juga digunakan untuk mencari bilangan prima. Kevalidan Algoritma *Lehmann* masih diragukan karena untuk menentukan suatu bilangan primanya yang masih sederhana[9]. Syarat-syarat pembangkit bilangan prima Algoritma *Lehmann* :

1. Tentukan bilangan a dengan syarat 1< a < p, di mana p adalah bilangan prima
2. Tentukan nilai L (Legendre)
$L = a^{(p-1)/2} \bmod p$
3. Jika nilai $L \neq 1$ atau $L - p \neq -1$ maka p bukan bilangan prima
4. Jika nilai L = 1 atau L - p = - 1, maka p kemungkinan bilangan prima lebih besar dari 50%

Contoh :

1. Bangkitkan bilangan acak a,1<a<p ; di mana nilai a = 4 dan p = 103
2. Hitunglah nilai L (Legendre)
$L = a^{(p-1)/2} \bmod p$
$= 4^{(103-1)/2} \bmod 103$
$= 4^{51} \bmod 103$
L= 1

Kemudian bangkitkan nilai a mencari kepastian dari bilangan tersebut

Misal a = 6
$L = a^{(p-1)/2} \bmod p$
$= 6^{(103-1)/2} \bmod 103$
$= 6^{51} \bmod 103$
L= 102

Kemudian cari apakah nilai L = -1 dengan cara L-p = - 1, L- p = 102 – 103, maka nilai L = -1 dan dapat dibuktikan bahwa p adalah bilangna prima.

H. PENELITIAN TERDAHULU

Berikut ini beberapa penelitian yang berkaitan Kriptanalisis Algoritma Kunci Publik Rabin menggunakan Metode *Kraitchik* :

1. Penelitian yang telah dilakukan sebelumnya oleh Widiarti Rista Maya, 2015 yang berjudul

"Analisis Kinerja Algoritma Rabin dan RSA (*Rivest Shamir Adleman*)" bahwa perbandingan kinerja Algoritma Rabin dan RSA memiliki kecepatan yang berbeda-beda, dengan menganalisis tingkat keamanannya dan tingkat kecepatan dalam memproses data.

2. Penelitian yang telah dilakukan sebelumnya oleh Budi Satria Muchlis, 2014 yang berjudul "Teknik Pemecah Kunci Algoritma RSA *(Rivest Shamir Adleman*) dengan Metode *Kraitchik*" bahwa kunci privat algoritma RSA dapat dipecahkan dengan memfaktorkan kunci publik *n* menggunakan metode *Kraitchik* dan ditinjau dari parameter waktu yang dilakukan.
3. Penelitian yang telah dilakukan sebelumnya oleh Kefa Rabah, 2006 yang berjudul "*Review of Methods for Integer Factorization Applied to Cryptography*" Keamanan RSA bergantung pada sulitnya faktorisasi n ke bilangan prima yaitu p dan q. Dengan memilih kunci yang lebih panjang itu sangat penting agar data yang akan kita kirim tidak mudah diketahui orang lain.sehingga kriptografi digunakan untuk mengamankan data dengan metode faktorisasi.

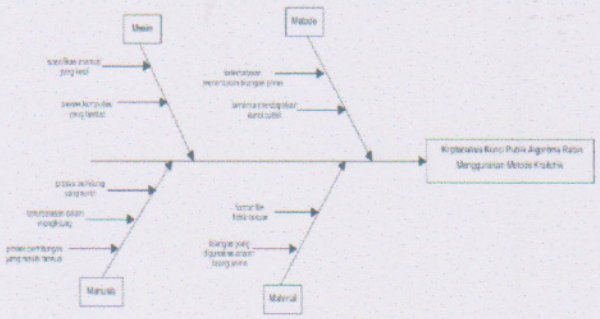
IV. ANALISIS DAN PERANCANGAN SISTEM

A. Analisis Sistem

Analisis sistem adalah sebuah proses untuk mendapatkan informasi, model, spesifikasi tentang perangkat lunak yang diinginkan.

1. Analisis Masalah

Pada penelitian ini, masalah yang akan diidentifikasi dilihat dalam diagram *Ishikawa.* Diagram *Ishikawa* merupakan diagram sebab akibat berbentuk seperti rangka ikan yang menunjukkan sebab akibat yang terjadi pada penelitian tersebut. Adapun diagram *Ishikawa* dapat dilihat pada gambar 3 berikut .



Gambar 3. Diagram *Ishikawa*

Pada gambar 3 dijelaskan tiap-tiap permasalahan yang mungkin akan terjadi dan dikelompokkan menjadi 4 kategori yaitu kategori mesin menjelaskan tentang apa-apa saja sebab akibat yang ada pada perangkat keras atau *hardware.* Kategori material menjelaskan tentang pemakaian data pada saat proses sistem. Kategori manusia menjelaskan permasalahan apa saja yang di hadapi dalam suatu proses. Kategori Metode menjelaskan apa masalah yang akan dihadapi.

2. Analisis Kebutuhan

Ada dua tipe kebutuhan yaitu:

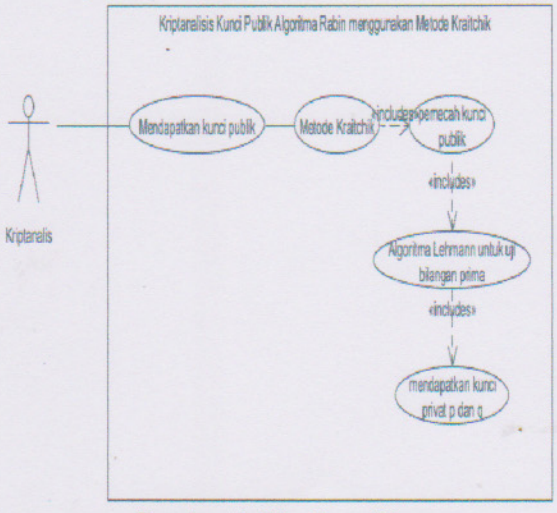
a. Kebutuhan Fungsional adalah kebutuhan apa saja yang diperlukan pada sistem dan apa-apa saja yang akan dilakukan oleh sistem tersebut.
b. Kebutuhan Non-Fungsional adalah suatu batasan-barasan yang akan menjadi tolak ukut dan melihat kepuasan terhadap sistem tersebut.

B. Analisis Proses

Analisis proses bertujuan untuk memberikan gambaran gambaran umum terhadap proses-proses yang terjadi serta memberikan gambaran-gambaran sistem yang akan dirancang.

1. Use Case Diagram

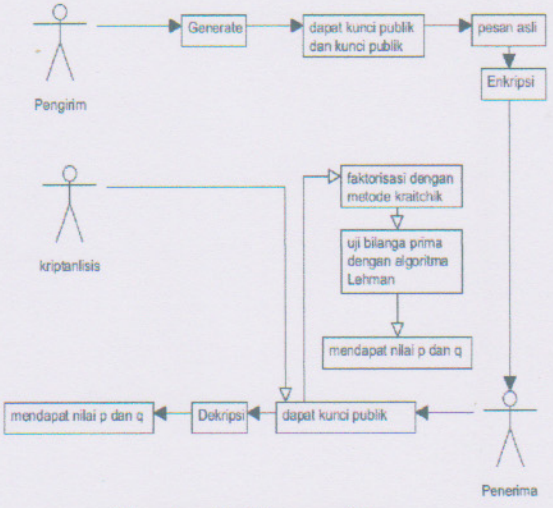
Use Case Diagram berfungsi untuk menggambarkan suatu interaksi antara pengguna dan sistem yang akan dibuat. Dengan kata lain menggambambarkan bagaimana cara berinteraksi pada sistem dan apa-apa saja yang dapat dilakukan dan bagaimana pengguna tersebut dapat menggunakan sistemnya. Seperti pada gambar 4.



Gambar 4. *Use Case Diagram*

2. Diagram Umum

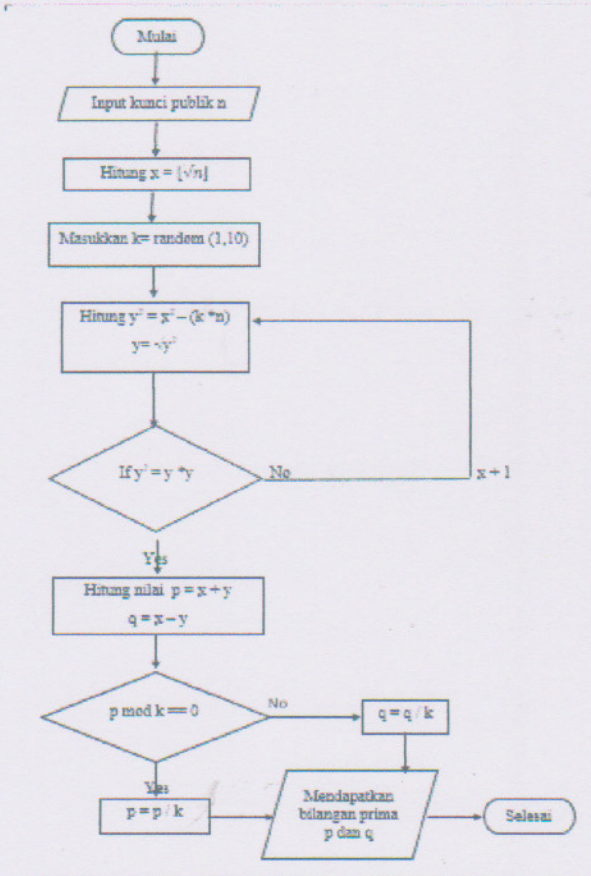
Diagram umum adalah gambaran umum dari sistem yang akan dibuat, di mana pada diargam umum ini menjelaskan cara kerja dari sistem tersebut. Pengirim akan mengacak nilai sehingga ditemukan nilai kunci publik dan kunci privat, kemudian memasukkan pesan asli dan pesan asli yang akan dikirim akan di enkripsi dimana kunci publiklah yang dikirim seperti pada gambar 5 berikut:



Gambar 5. *Diagram* Umum

3. Flowchart

Flowchart atau disebut dengan diagram alir adalah suatu jenis diagram yang menggambarkan alir kerja atau alir proses dan menampilkan langkah-langkah yang dalam bentuk suatu simbol-simbol atau gambar-gambar dan merupakan gambaran penyelesaian suatu masalah. Proses kriptanalisis dilihat pada gambar 6 berikut

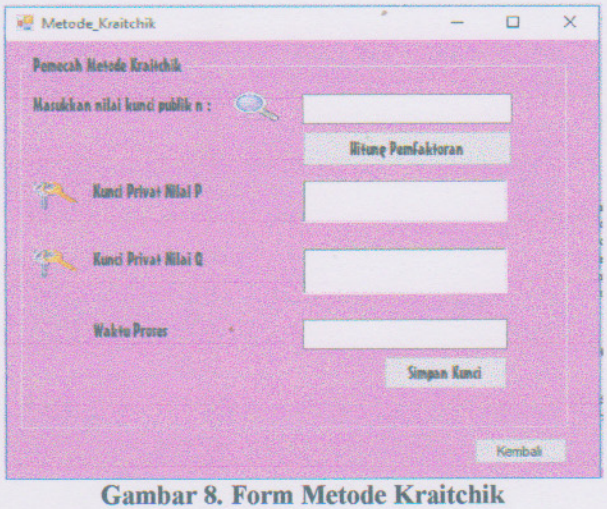


Gambar 6. Flowchart Metode Kraitchik pemecah Algoritma Rabin

V. HASIL DAN DISKUSI

A. Implementasi

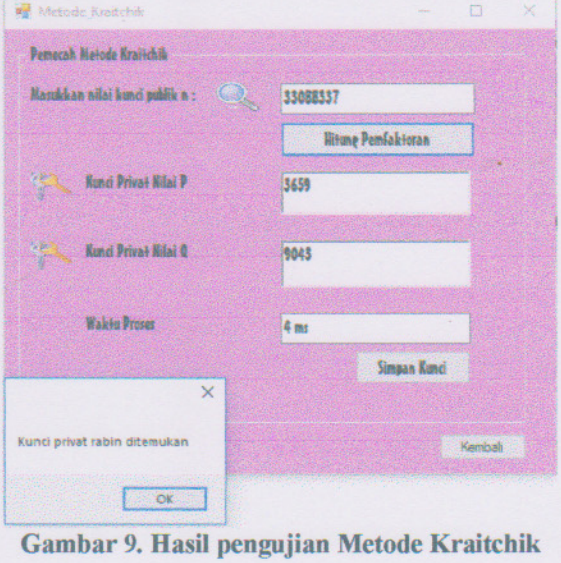
Pada penelitian ini, aplikasi yang digunakan adalah bahasa pemrograman C# (SharpDevelopment) seperti pada gambar 8 berikut :



Gambar 8. Form Metode Kraitchik

B. Pengujian

Pada penelitian ini, pengujian dilakukan sebanyak 16 kali percobaan untuk melihat hasil apakah metode Kraitchik dapat memecahkan kunci publik Algoritma Rabin. Setelah pengujian dilakukan maka hasil yang didapatkan sesuai dan metode Kraitchik dapat memecahkan kunci publik algoritma Rabin seperti pada gambar 9 berikut:



Gambar 9. Hasil pengujian Metode Kraitchik

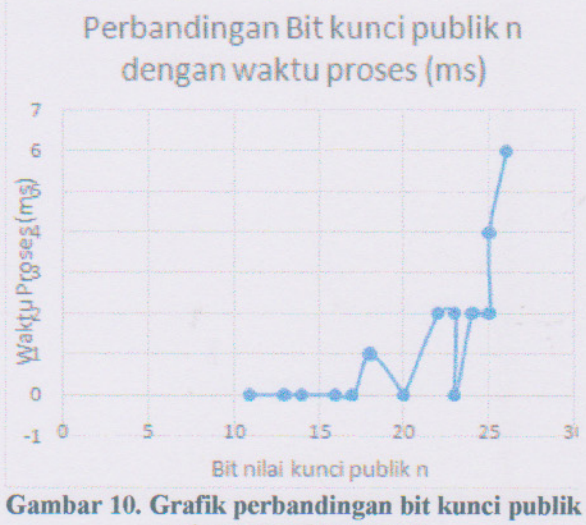
C. Pengujian Beberapa Nilai Kunci Publik n terhadap Waktu Proses

Berdasarkan pengujian kunci publik n yang dilakukan dengan cara mengurutkan bilangan terkecil sampai ke yang terbesar, maka didapatkan hasil seperti pada tabel 1. berikut :

Tabel 1. Perbandingan Kunci Public n dalam Bit terhadap Waktu Proses

No	n (digit)	Kunci Publik	n (bit)	Kunci Privat		p & q (digit)	Waktu Proses (ms)
		Nilai n		Nilai p	Nilai q		
1	4	1133	11	103	11	2 & 3	0
2		4429	13	43	103		0
3		9073	14	43	211		0
4	5	21733	14	103	211	3	0
5		62113	16	179	347		0
6		99941	17	139	719		0
7	6	176269	18	359	491		1
8		557993	20	743	751		0
9		710393	20	827	859		0
10	7	2761321	22	1091	2531	4	2
11		4214533	23	3863	1091		2
12		6881789	23	2531	2719		0
13	8	14798617	24	2699	5483		2
14		20311537	25	3023	6719		2
15		33088337	25	3659	9043		4
16		57292913	26	6719	8527		6

Maka diperoleh grafik seperti pada gambar 10 berikut :



Gambar 10. Grafik perbandingan bit kunci publik n dengan waktu proses

Dilihat bahwa waktu proses pemecahan kunci publik n tidak selalu stabil, semakin panjang bit digit kunci publik n yang digunakan maka tidak selamanya waktu proses yang dibutuhkan lama ataupun sebaliknya tidak selalu menghasikan waktu yang cepat.

VI. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan pengujian yang dilakukan pada Kriptanalisis Algoritma Rabin menggunakan metode Kraitchik maka penulis dapat menyimpulkan sebagai berikut ;

1. Telah berhasil metode *Kraitchik* untuk memecahkan kunvi publik *n* algoritma Rabin sehingga ditemukan hasil kunci privatnya yaitu nilai *p* dan *q*.
2. Pada proses algoritma Rabin menggunakan metode Kratichik, panjang kunci publik yang semakin panjang tidak menentukan lamanya waktu yang dibutuhkan untuk proses pemecahan atau semakin panjang dan besar nilai kunci publik n yang di faktorkan tidak selalu menghasilkan waktu proses yang lama ataupun sebaliknya tidak selalu menghasikan waktu yang cepat.

B. Saran

Adapun saran yang diberikan penulis terkait perbaikan dan pengembangan ke depannya adalah

1. Untuk penelitian yang selanjutnya, pemecahan kunci publik algoritma Rabin dapat dilakukan menggunakan metode yang lainnya selain menggunakan metode Kraitchik untuk melihat perbandingan dari kompleksitas waktunya dan melihat kelemahan dan kekuatan dari metode-metode yang lainnya.
2. Untuk penelitian yang selanjutnya, pemecahan kunci publik algoritma Rabin menggunakan metode Kraitchik dapat menggunakan BigInteger untuk memecahkan kunci yang panjang sehingga dapat dilihat perbandingan waktu yang dibutuhkan dalam memecahkan kunci yang panjang dan dapat menggunakan uji bilangan prima selain uji bilangan prima Lehmann.
3. Untuk penelitian selanjutnya, Pemecah metode Kraitchik dapat digunakan untuk memecahkan enkripsi algoritma pemfaktoran faktorisasi yang lainnya tidak hanya digunakan untuk pemecah algoritma Rabin saja.

DAFTAR PUSTAKA

Muchlis, Budi Satria. 2014. " *Tehnik pemecah kunci Algoritma RSA (Rivest Shamir Adleman) menggunakan metode Kraitchik's)*". Skripsi. Universitas Sumatera Utara.

Richard, Mollin . A. 2007, *An Introduction to Cryptography 2nd Edition*, Chapman & Hall.

Menezes, Man Young, 1996,*Handbook of Applied Criptography, CRC* Press.

Munir, Rinaldi. 2006. "Kriptografi". Informatika. Bandung.

Sadikin, Rifki. 2012."Kriptografi Untuk Keamanan Jaringan". Yogyakarta.

Utami, Chitra Meidhantie. 2016. "*Implementasi Algoritma Kunci Publik Rabin Cryptosystem dan Ecxtended Polybius Square dalam Pengamanan PDF*". Skripsi. Universitas Sumatera Utara.

Tilborg, H.C.A. van & Jajodi, S. 2011. Encyclopedia of Cryptography and Security. Springer Science+Business Media, LLC: New York.

Batten, Lynn Margaret. 2013. " *Public Key Cryptography Applications and attacks*". IEEE.

Schneier, B.1996. *Applied Cryptography:Protocols, Algorithms, and Source Code in C.*2nd Edition.