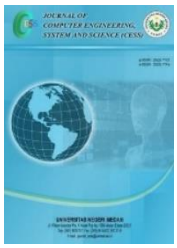
CESS
(Journal of Computing Engineering, System and Science) 8(2) July 2023 576-582

e-ISSN: 2502-714x
p-ISSN: 2502-7131

Contents list available at www.jurnal.unimed.ac.id

CESS
(Journal of Computing Engineering, System and Science)

journal homepage: https://jurnal.unimed.ac.id/2012/index.php/cess



Analisis Perbandingan Kinerja Multi Prime RSA Dan Multi Power RSA

Performance Comparison Analysis of Multi Prime RSA and Multi Power RSA

Iwada Grawilser Talunohi[1], Ibnu Jaki Lubis[2], Sutarman[3*], Ade Candra[4]

[1,2,3,4] Universitas Sumatera Utara
Jl. Dr. T. Mansur No.9, Kota Medan, Sumatera Utara 20222
email: [1]iwadagrawilser@students.usu.ac.id, [2]ibnujaki@students.usu.ac.id, [3]sutarman@usu.ac.id, [4]ade_candra@usu.ac.id

A B S T R A K

Saat ini cukup banyak algoritma yang digunakan untuk pengamanan informasi dalam sistem atau perangkat lunak. Masing-masing algoritma tersebut memiliki tingkat waktu dalam key generate, enrkripsi dan dekripsi yang berbeda-beda. Dalam menggunakan algoritma tersebut harus mempertimbangkan waktu jika ingin menerapkan dalam suatu sistem atau perangkat lunak. Dalam penelitian ini, akan melakukan perbandingan kinerja dari dua algoritma asimetris yaitu Multi Power RSA dan Multi Prime RSA yang masing-masing merupakan varian dari RSA. Algoritma ini terdiri dari 2 kunci yaitu kunci publik dan kunci privat. Pengujian algoritma tersebut akan dilakukan dalam bahasa python. Kesimpulan yang didapat adalah algoritma Multi Prime RSA lebih cepat di bandingkan dengan Multi Power RSA dalam proses enkripsi dan dekripsi. Multi Power RSA lebih cepat dari Multi Prime RSA dalam proses key generate.

Kata Kunci: *Kriptografi, RSA, Enkripsi, Dekripsi*

A B S T R A C T

Currently, quite a lot of algorithms are used to secure information in systems or software. Each of these algorithms has a different level of speed (time) in key generation, encryption and decryption. In using the algorithm must consider speed (time) if you want to implement it in a system or software. In this study, we will compare the performance of two asymmetric algorithms, namely Multi Power RSA and Multi Prime RSA, each of which is a variant of RSA. This algorithm consists of 2 keys, namely the public key and the private key. Testing the algorithm will be carried out in Python. The conclusion obtained is that the Multi Prime RSA algorithm is faster than the Multi Power RSA in the encryption and decryption process. Multi Power RSA is faster than Multi Prime RSA in the key generation process.

**Penulis Korespondensi:*
email: sutarman@usu.ac.id

Keywords: *Cryptography, RSA, Encryption, Decryption*

1. PENDAHULUAN

Pada saat ini terdapat berbagai macam algoritma Kriptografi simetri maupun asimetri. Jika suatu algoritma Kriptografi dipercaya kuat namun diketahui lamba dalam proses penyandiannya maka tidak akan dijadikan pilihan oleh pengguna. Didalam penggunaan suatu kriptografi, selain keamanan enkripsi kecepatan dari kinerja algoritma tersebut juga menjadi pertimbangan penggunaan algoritma kriptografi tersebut karena akan berpengaruh pada kinerja suatu sistem.

Serangan dari attacker pada saat ini sangatlah mengganggu keamanan suatu aplikasi atau sistem. Attacker saat ini dilakukan oleh manusia sendiri dengan seiringnya perkembangan teknologi memungkinkan attacker bukan lagi manusia melainkan teknologi itu sendiri yang dirancang untuk melakukan serangan pada keamanan suatu aplikasi atau sistem. Untuk menginimalisir tingkat serangan tersebut maka dibutuhkan sebuah tingkat keamanan yang cukup untuk menghindari hal tersebut. Hal ini juga bertujuan untuk menyamarkan informasi yang dikirim ke penerima agartidak sembarangan diakses oleh pihak lain yang tidak memiliki hak untuk menerima informasi tersebut. Ada beberapa cara yang dilakukan untuk melakukan pengamanan data ataupun pesan dari serangan attacker yaitu dengan menggunakan teknik penyamaran data atau pesan yang disebut dengan kriptografi.

2. DASAR/TINJAUAN TEORI

Kriptografi merupakan satu bagian dari jaringan komputer yang dapat mengubah informasi menjadi tidak terbaca atau terdefinisi [1]. Sederhananya kriptografi yaitu mengenkripsi pesan yang sebagai plaintext menjadi sebuah chipertext. Dalam proses pengubahan plaintext menjadi chipertext, kriptografi menggunakan algoritma berdasarkan dengan ilmu matematika. Sejauh ini terdapat beberapa varian kriptografi untuk mengamankan sebuah pesan atau informasi. Salah satu jenis algoritma dalam kriptografi yaitu algorita RSA cryptosystem. RSA adalah teknik kriptografi kunci publik yang sebagian besar berpusat pada kompleksitas pemfaktoran bilangan prima besar [2].RSA Cryptosystem merupakan sebuah algoritma dalam kriptografi yang menggunakan 2 kunci yang berbeda dalam mengamankan sebuah pesan atau informasi, untuk fungsi yang pertama digunakan untuk mengubah sebuah pesan atau informasi menjadi tidak dapat terdefinisi dan untuk kunci yang kedua digunakan untuk mengembalikan pesan atau informasi yang sudah diubah sebelumnya.

Dalam RSA terdapat beberapa varian seperti Multi Prime RSA dan Multi Power RSA [3]. Multi-Prime (MP)RSA adalah konstruksi RSA yang modulus publiknya merupakan produk dari lebih dari dua bilangan prima, dan operasi kunci privatnya dapat dipercepat dengan menggunakan Chinese Reminder Theorem (CRT) [4]. Multi Power RSA merupakan varian RSA yang menggunakan modulus dari rumus $N = P^m Q$ untuk mempercepat proses dekripsi dari RSA[5]. Pada penelitian ini, penulis akan melakukan analisis kinerja dari kedua varian RSA tersebut.

3. METODE

3.1. Algoritma RSA

Algoritma RSA merupakan algoritma kriptografi kunci publik yang paling sering digunakan dan Algoritma ini diciptakan oleh tiga peneliti dari MIT yaitu Ronald Rivest, Adi Shamir, dan Len Adleman, pada tahun 1976.

Dalam menggunakan algoritma RSA diawali dengan pembangkitan kunci publik dan kunci privat untuk proses enkripsi dan deksripsi dalam memberikan keamanan pada pesan [6]. Berikut adalah tahap-tahap dalam melakukan pembangkitan kunci algoritma RSA:

3.1.1. Key Generate

a. Memilih dua bilangan prima yaitu p dan q.
b. Menghitung nilai n:

$$N = p \times q$$

c. Menghitung nilai $\phi(n)$:

$$\phi(N) = (p-1)(q-1)$$

d. Memilih sebuah bilangan bulat e sebagai kunci publik, dengan syarat nilai e harus relatif prima terhadap $\phi(N)$.
e. Menghitung kunci privat d dari e.

$$d \equiv e - 1 \ mod \ (\phi(N))$$

f. Hasilnya merupakan pasangan kunci publik (e, n) dan kunci privat (d, N).

3.1.2. Enkripsi

Berikut adalah tahap-tahap untuk melakukan enkripsi pesan :

a. Menerima publik key (*N, -e*).
b. Kemudian enkripsi pesan dengan rumus :

$$C \equiv M^e \ (mod \ N)$$

c. Hasil Chipertext (*C*) dikirim ke penerima

3.1.3. Deksripsi

Untuk mengembalikan chipertext ke plaintext menggunakan proses dekripsi dengan tahap-tahap berikut:

a. Terima Chipertext (*C*)
b. Kemudian deksipsi pesan degan rumus :

$$M=C^d \ (mod \ N)$$

3.2. Algoritma RSA Multi Prime

Algoritma kriptografi Multi Prime RSA adalah algoritma kriptografi RSA yang menggunakan lebih dari dua bilangan prima sebagai kunci privat [7]. Sama halnya dengan algoritma RSA standar algoritma RSA multiprima juga terdiri dari algoritma pembangkitan kunci, algoritma enkripsi dan algoritma dekripsi.

Berikut adalah tahap-tahap dalam pembangkitan kunci, enkripsi dan dekripsi pada algoritma Multi Prime RSA:

3.2.1 Key Generate

a. Memilih tiga buah bilangan prima p, q dan r.
b. Menghitung N dengan rumus:
   $N = p * q * r$
c. Menghitung nilai ϕ (n)
   $\phi(N) = (p - 1)(q - 1)(r - 1)$.
d. Memilih kunci publik, e, yang relatif prima terhadap ϕ(N).
   $GCD(e, \phi(N)) = 1$
e. Menghitung kunci privat d dengan rumus
   $d \equiv e\text{-}1 \pmod{\phi(N)}$
f. Kunci publik adalah *(e, N*) dan Kunci privat adalah (*d, N*).

3.2.2. Enkripsi

Berikut adalah tahap-tahap untuk melakukan enkripsi pesan :

a. Terima nilai *N*
b. Nyatakan plainteks *M*
c. Kemudian enkripsi dengan rumus:
   $C_i = M_i \; e \bmod (N)$
d. Hasilnya dikirim ke penerima

3.2.3. Dekripsi

Untuk mengembalikan chipertext ke plaintext menggunakan proses dekripsi dengan tahap-tahap berikut:

a. Ambil kunci privat d untuk menghasilkan *M*.
b. Teks rahasia adalah *C*.
c. Teks asli didapat dari
   $M \equiv C^d \bmod (n)$

3.3. Algoritma Multi Power RSA

Multi Power RSA merupakan varian RSA yang menggunakan modulus dari rumus $N = P^m Q$ untuk mempercepat proses dekripsi dari RSA[5]. Pada enkripsi Multi Power RSA sama dengan RSA. Namun, pembangkitan kunci dalam dekripsi yang berbeda.
Berikut adalah tahap-tahap dalam pembangkitan, enkripsi dan dekripsi multi power RSA:

3.3.1 Key Generator

a. Pilih 2 bilangan prima, *p and q*
b. Tentukan nilai N dengan rumus :
   $N = pm \times q$
c. Pilih bilangan bulat e dimana:
   $GCD((n), e) = 1 \text{ and } 1 < e < (n)$
d. Tentukan nilai D dengan rumus :
   $d = e\text{-}1 \bmod (p - 1)(q - 1)$
e. Tentukan nilai dp dengan rumus :
   $dp = d \bmod (p - 1)$
   $dq = d \bmod (p - 1)$
f. Kunci publik adalah (*e, N*) and kunci privat adalah (*p, q, dp, dq*).

3.3.2 Enkripsi

Enkripsi Multi Power RSA tidak berbeda dengan enkripsi RSA.

$$Ci = Mi\ e \bmod (N)$$

3.3.3 Dekripsi

Pengembalian chipertext ke palintext menggunakan dekripsi dengan tahap-tahap berikut:

a. Tentukan Mp dan Mq dengan rumus:
   $Mp = Cdp \bmod p$
   $Mq = Cdq \bmod q$
b. Tentukan nilai M dengan:
   $M = (Mpq\ (q - 1\ modp) + Mq\ (p - 1\ modq))\ mod\ (pq)$

4. HASIL DAN PEMBAHASAN

Dalam paper ini, data yang digunakan adalah berupa data teks yang disimpan dalam file (.txt) dalam ukuran byte. Data tersebut akan dienkripsi dan didekripsi dan diukur waktunya dengan menggunakan timer yang ada di dalam operating sistem. Selanjutnya untuk mencapai tujuan tersebut maka ada beberapa hal yang harus diperhatikan dan dipersiapkan yaitu :

4.1. Data yang digunakan

Dalam mencapai hasil penelitian ini menggunakan data teks yang tersimpan dalam file dengan ekstensi (.txt) dengan pesan di dalamnya adalah TUGAS PAPER SEMINAR RESET KRIPTOGRAFI sebagai plaintextnya.

4.2. *Requirement* Perangkat Lunak Pengujian

Requirement perangkat lunak yang digunakan dalam pengujian penelitian ini meliputi *requirement* perangkat keras dan perangkat lunak dengan spesifikasi sebagai berikut:

1. Perangkat Keras
   - Processor Intel Core i7 2,60GHz
   - RAM 16 GB
   - SSD 1 TB
   - VGA GTX 50
2. Perangkat Lunak
   - Windows 11
   - Python versi 3.8
   - Visual code studio

4.3. Hasil Pengujian

Dalam pengujian yang dilakukan dengan menggunakan *requirement* perangkat keras dan perangkat lunak diatas, maka di peroleh hasil pengujian nya yaitu:

Tabel 1. Tabel data waktu Key Generate, Enkripsi dan Dekripsi Algoritma Multi Power RSA

Panjang Bit	Indicator Value		
	Key Generate	**Enkripsi**	**Dekripsi**
256	43.886423110961924	0.9953975677290234	19.94776725769043
512	236.3679090270996	2.996206283569336	150.94900131225586
768	563.621997833252	6.979942321777344	370.3796863555908
1024	1429.4898509979248	9.973526000976562	810.849666595459
2048	3127.6655197143555	29.918670654296875	4445.630788803101

Tabel 2. . Tabel data waktu Key Generate, Enkripsi dan Dekripsi Algoritma Multi Prime RSA

Panjang Bit	Indicator Value		
	Key Generate	**Enkripsi**	**Dekripsi**
256	62.5	0.9944438934326172	7.981777191162109
512	125.0	2.9935836791992188	62.83235549926758
768	687.5	3.9832592010498047	169.54946517944336
1024	578.125	6.980657577514648	387.7570629119873
2048	3687.5	18.943071365356445	2485.269546508789

Dari kedua tabel diatas diperoleh hasil bahwa kecepatan waktu key generate, enkripsi dan dekripsi meningkat sesuai dengan ukuran data (bit). Dalam Multi Prime RSA lebih cepat dalam melakukan enkripsi dan dekripsi sedangkan Multi Power RSA lebih cepat dalam melakukan Key Generate.

5. KESIMPULAN

Dalam paper ini, telah dilakukan perbandingan kinerja dari dua algoritma asimetris yaitu Multi Power RSA dan Multi Prime RSA yang masing-masing merupakan varian dari RSA. Data yang digunakan dalam penelitian ini terdiri dari jumlah bit yang berbeda-beda mulai dari 256 bit sampai 3072 bit. Algoritma ini terdiri dari 2 kunci yaitu kunci publik dan kunci privat. Pengujian algoritma tersebut akan dilakukan dalam bahasa python. Kesimpulan yang didapat adalah algoritma Multi Prime RSA lebih cepat di bandingkan dengan Multi Power RSA dalam proses enkripsi dan dekripsi. Multi Power RSA lebih cepat dari Multi Prime RSA dalam proses key generate.

REFERENSI

[1] M. G. Kamardan, N. Aminudin, N. Che-Him, S. Sufahani, K. Khalid, and R. Roslan, “Modified Multi Prime RSA Cryptosystem,” *J. Phys. Conf. Ser.*, vol. 995, no. 1, 2018, doi: 10.1088/1742-6596/995/1/012030.

[2] A. A. Emmanuel, O. A. E, A. M. O, and A. E. O, “A Note on Time and Space Complexity of RSA and ElGamal Cryptographic Algorithms,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 7, pp. 143–147, 2021, doi: 10.14569/IJACSA.2021.0120716.

[3] D. Z. K. Nibir, S. Nasrin, and S. M. S. Rana, "A Variant of the RSA Cryptosystem with Smaller Keys," *Dhaka Univ. J. Sci.*, vol. 70, no. 2, pp. 15–17, 2022, doi: 10.3329/dujs.v70i2.62600.

[4] S. Gueron and N. Drucker, "Cryptosystems with a multi prime composite modulus," *CCNC 2018 - 2018 15th IEEE Annu. Consum. Commun. Netw. Conf.*, vol. 2018-January, no. 5, pp. 1–7, 2018, doi: 10.1109/CCNC.2018.8319159.

[5] U. Erdiansyah, M. K. M. Nasution, and Sawaluddin, "Hybrid cryptosystem multi-power RSA with N=PmQ and VMPC," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 725, no. 1, 2020, doi: 10.1088/1757-899X/725/1/012129.

[6] J. Felisha, "Analisis Perbandingan Algoritma RSA dengan ElGamal pada Tanda Tangan Digital," 2022.

[7] F. P. Johari, D. Murni, and H. Syarifuddin, "Modifikasi Algoritma Kriptografi RSA Multiprima Menggunakan Chinese Remainder Theorem dan Garner ' s Algorithm," *UNP J. Math.*, vol. 2, no. 2, pp. 36–41, 2019, [Online]. Available: http://ejournal.unp.ac.id/students/index.php/mat/article/view/6311