Modifikasi Algoritma Kriptografi RSA Multiprima Menggunakan *Chinese Remainder Theorem* dan *Garner's Algorithm*

Fatimah Putri Johari[#1], Dewi Murni[*2], Hendra Syarifuddin [*3]

[#]*Student of Mathematics Department Universitas Negeri Padang, Indonesia*
[*]*Lecturers of Mathematics DepartmentUniversitas Negeri Padang, Indonesia*

[1]fatimahputry27@gmail.com
[2]dewimunp@gmail.com
[3]hendrasy@yahoo.com

Abstract–Cryptographic algorithms multiprime RSA (Rivest-Shamir-Adleman) is one of the public key cryptographic algorithms that are widely used, because the algorithm is easily applied and security is also guaranteed. But on the other hand this algorithm has drawbacks, namely the process of decryption a takes a relatively long time because using modular exponentiation. To address this, it will do modifications to the process of decrypting RSA Cryptographic algorithms multiprime by finding a method that can cut the number of modular exponentiation operation is great modular exponentiation operation into several smaller ones. This modification is only focused on the process of decryption is done by leveraging the next reminder: chinese theorem can be solved using Garner's algorithm. This modification of the results obtained a new private key used for decryption process

Keywords –Cryptography, Multiprime RSA, Chinese Remainder Theorem(CRT), Garner's Algorithm

Abstrak – Algoritma kriptografi RSA *(Rivest-Shamir-Adleman)* multiprima adalah salah satu algoritma kriptografi kunci publik yang banyak digunakan, karena algoritma ini mudah diaplikasikan dan keamanannya juga terjamin. Namun disisi lain algoritma ini memilki kelemahan yaitu proses pendekripsiannya membutuhkan waktu yang relatif lama karena menggunakan perpangkatan modular yang besar. Untuk mengatasi hal ini maka akan dilakukan modifikasi pada proses dekripsi algoritma kriptografi RSA multiprima dengan mencari suatu metode yang dapat memotong jumlah operasi perpangkatan modular yang besar menjadi beberapa operasi perpangkatan modular yang lebih kecil. Modifikasi ini hanya difokuskan pada proses dekripsi yang dilakukan dengan memanfaatkan *Chinese Reminder Theorem* yang selanjutnya dapat diselesaikan dengan menggunakan *garner's algorithm*. Dari hasil modifikasi ini diperoleh kunci privat baru yang digunakan untuk proses dekripsi.

Kata kunci – Kriptografi, RSA Multiprima, *Chinese Remainder Theorem (CRT), Garner's Algorithm*

PENDAHULUAN

Informasi merupakan suatu hal yang penting bagi sebuah organisasi maupun individual, termasuk kemampuan dalam mengakses dan menyediakan informasi secara tepat, cepat dan akurat. Pada prakteknya tidak semua informasi dapat dikomunikasikan secara bebas, karena ada beberapa informasi yang sifatnya rahasia dan hanya boleh diketahui oleh pihak – pihak tertentu saja. Informasi yang berifat rahasia harus diamankan terlebih dahulu sebelum dikirim ke penerima yang bersangkutan. Keamanan informasi adalah bagaimana kita dapat mencegah penipuan, atau paling tidak mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, untuk melindungi informasi dari pengaksesan, penggunaan, penyebaran, perusakan, perubahan, dan penghancuran tanpa otorisasi yang sah.

Semakin pesatnya perkembangan ilmu pengetahuan dan teknologi proses komunikasi dan pertukaran informasi menjadi semakin mudah. Keamanan dan kerahasiaan informasi yang dipertukarkan adalah suatu hal yang penting karena banyaknya pembajakan dan perusakan informasi oleh pihak – pihak yang tidak berwenang. Untuk mengatasi hal tersebut maka perlu dilakukan pengamanan terhadap informasi. Salah satu ilmu yang yang dikenal sebagai pengaman pesan/informasi rahasia adalah kriptografi.

Kriptografi adalah ilmu sekaligus seni untuk menjaga keamanan sebuah pesan rahasia. Kriptografi berasal dari bahasa Yunani: "*cryptos"* artinya rahasia, dan "*graphein"* artinya tulisan. Jadi, secara morfologi kriptografi bearti tulisan rahasia. Kriptografi adalah ilmu yang mempelajari teknik – teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasian data, keabsahan data, integritas data, serta autentikasi data. Keamanan informasi/pesan diperoleh dengan menjadikannya sebagai pesan yang tidak mempunyai makna[3].

Menurut sejarahnya kriptografi sudah lama digunakan oleh tentara sparta di Yunani pada tahun 400

SM. Di dalam kriptografi pesan yang dirahasiakan dinamakan dengan *plaintext* dan pesan hasil penyandian disebut dengan *chipertext*. Sedangkan proses menyandikan *plaintext* menjadi *chipertext* dikenal dengan istilah *enkripsi* dan sebaliknya disebut *dekripsi.*

Dalam perkembangannya kriptografi terbagi menjadi dua, yaitu kriptografi klasik dan kriptografi kunci publik. Kriptografi klasik telah dipakai sebelum era komputer yang umumnya merupakan teknik penyandian dengan kunci simetrik menggunakan metode substittusi (pergantian huruf) atau tranposisi.

Sistem kriptografi klasik selalu mengasumsikan pihak pengenkripsi dan pihak pendekripsi memiliki kunci rahasia yang disebut K (kunci simetri). Kunci rahasia K harus dibangkitkan secara rahasia dan di distribusikan ke pengenkripsi dan pendekripsi melalui saluran yang diasumsikan aman. Kebutuhan untuk mendapatkan saluran yang aman merupakan sebuah tantangan dalam sistem kriptografi simetri. Sistem kriptografi kunci publik mengatasi asumsi bahwa tidak dibutuhkan saluran aman untuk distribusi kunci.

Dari sekian banyak algoritma kriptografi kunci publik yang pernah dibuat, algoritma yang paling populer adalah algoritma *RSA (Rivest Shamir Adleman).* Algoritma *RSA* dibuat oleh 3 orang peneliti yaitu: Rivest, Shamir, dan Adleman pada tahun 1977. Algoritma ini menyediakan keamanan tingkat tinggi dan mudah diaplikasikan. Algoritma RSA merupakan algoritma asimetris yang mana pengguna memiliki sepasang kunci yaitu kunci publik dan kunci privat. Kunci publik bersifat tidak rahasia sehingga dapat di distribusikan melalui saluran tidak aman sedangkan kunci privat bersifat rahasia dan harus dijaga kerahasiaanya oleh pemegang kunci[3].

Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima[2]. Pemfaktoran dilakukan untuk memperoleh kunci privat yang digunakan untuk mendekripsi cipherteks. RSA terbukti secara matematika memiliki keamanan yang tinggi karena berstandar pada persoalan faktorisasi yang efesien. Selama belum ditemukan algoritma yang efisien untuk pemfaktoran bilangan besar menjadi faktor-faktor primanya, maka keamanan algoritma RSA tetap terjamin. Namun pada proses pendekripsiannya algoritma ini membutuhkan waktu yang relatif lama karena menggunakan perpangkatan modular yang besar.

Solusi dari permasalahan perpangkatan modular yang besar adalah dengan mencari suatu metode yang dapat memotong jumlah operasi pembagian. Salah satu hal yang dapat dilakukan untuk memotong jumlah operasi pembagian adalah dengan memanfaatkan *Chinese Remainder Theorem* (CRT). *Chinese Remainder Theorem* akan membagi operasi perpangkatan modular yang besar menjadi beberapa operasi perpangkatanmodular yang lebih kecil. Sedangkan untuk menyelesaikan *Chinese Remainder Theorem* dapat dimanfaatkan *Garner's Algorithm.Garner's Algorithm* (agoritma garner) adalah suatu metode untuk meyelesaikan *Chinese Reminder Theorem* secara optimal untuk mempercepat proses pencarian solusi[4].

Algoritma kriptografi RSA telah berkembang menjadi algoritma kriptografi RSA multiprima. Algoritma kriptografi RSA multiprima adalah algoritma kriptografi RSA yang mengunakan lebih dari dua bilangan prima[1]. Sama halnya dengan algoritma RSA standar algoritma RSA multiprima juga terdiri dari algoritma pembangkitan kunci, algoritma enkripsi dan algoritma dekripsi.

Berdasarkan uraian di atas maka penulis tertarik untuk membahas sistem kriptografi kunci publik yang menggunakan algoritma kriptografi RSA multiprima dengan memanfaatkan *Chinese Remainder Theorem* dan *Garner's Algorithm*.

METODE

Penelitian ini adalah penelitian dasar (teoritis) dengan menggunakan teori yang relevan berdasarkan studi kepustakaan. Langkah kerja yang dilakukan adalah

1. Meninjau masalah yang terkait dengan algoritma RSA multiprima.
2. Menelaah algoritma dekripsi kriptografi RSA multiprima .
3. Mengaplikasikan *Chinese Reminder Theorem* dalam menyusun algoritma dekripsi RSA multiprima dan menyelesaikannya menggunakan *Garner's Algorithm.*
4. Membangkitkan kunci algoritma RSA multiprima yang telah memanfaatkan *Chinese Reminder Theorem* dengan *Garner's Algorithm*.
5. Menerapkan algoritma kriptografi RSA multiprima yang telah dimodifikasi menggunakan *Chinese Reminder Theorem* dan *Garner's lgoritm* pada pengaman pesan rahasia.
6. Melakukan simulasi terhadap kriptografi RSA multiprima dan kriptografi RSA multiprima yang telah dimodifikasi menggunakan *Chinese Reminder Theorem* dan *Garner's Algorithm* denganbantuan software Maple 17.
7. Penarikankesimpulan.

HASIL DAN PEMBAHASAN

1. Algoritma Kriptografi RSA Multiprima

Algoritma kriptografi RSA multiprima adalah algoritma kriptografi RSA yang mengunakan lebih dari dua bilangan prima sebagai kunci privat.

Berikut ini akan dibahas terlebih dahulu mengenai algoritma kriptografi RSA multiprima yang mennggunakan tiga bilangan prima (p,qdan r)

a. Algoritma membangkitkan pasangan kunci RSA adalah sebagai berikut:

1) Memilih tiga buah bilangan prima p, q dan r.
2) Menghitung $n = p * q * r$
3) Menghiitung $\phi(n) = (p - 1)(q - 1)(r - 1)$.

4) Memiilih kunci publik, *e*, yang relatif prima terhadap $\varphi(n)$. $GCD(e,\varphi(n)) = 1$
5) Menghitung nilai *d* dengan rumus $d \equiv e^{-1} (\text{mod } \varphi(n))$
6) Kunci umum (publik) adalah $KU = (e, n)$
7) Kunci pribadi (privat) adalah $KP = (d, n)$

Contoh:
Misalkan Aini ingin membangkitkan kunci publik dan kunci privat. Aini memilih p = 17 , q = 19 dan r = 23
Selanjutnya Aini hitung nilai
n = p.q.r = 17.19. 23 = 7429
dan $\varphi(n) = (p-1)(q-1)(r-1)$.
$= (17-1).(19-1).(23-1)$
$= 16 . 18 . 22 = 6336$
Aini memilih e = 1841 karena relatif prima terhadap $\varphi(n)$kemudian menghitng nilai d menggunakan persamaan:
$1841.d \equiv 1 \pmod{6336}$.....(1)
Selanjutnya dengan menyelesaikan persamaan (1) diperoleh d = 5393
Jadi kunci publik (e,n) = (1841 , 7429) dan kunci privat (d , n) = (5393 , 7429)

b. Algoritma Enkripsi
Algoritma untuk melakukan enkripsi kriptografi RSA Multiprima adalah sebagai berikut:
1) Nyatakan plainteks m menjadi blok-blok $m_1, m_2, ...$, sedemikian sehingga setiap blok merepresentasikan nilai di dalam selang [0, *n* – 1].
2) Setiap blok m_i dienkripsi menjadi blok c_i dengan rumus $c_i = m_i^e \text{ mod}(n)$

Contoh:
Misalkan Ana ingin mengirim pesan kepada Aini. Pesan (*plaintext*) yang akan dikirim adalah
M = "Jurusan Matematika Universitas Negeri Padang"
Berdasarkan tabel desimal ASCII yang terdapat dalam lampiran, maka plainteks dapat dinyatakan sebagai berikut:
M =74, 117, 114, 117, 115, 97, 110, 32, 77, 97, 116, 101, 109, 97, 116, 105, 107, 97, 32, 85, 110, 105, 118, 101, 114, 115, 105, 116, 97, 115, 32, 78, 101, 103, 101, 114, 105, 32, 80, 97, 100, 97, 110, 103
Selanjutnya plainteks M dienkripsi menggunakan kunci publik(e,n)=(1841, 7429) dengan rumus $C \equiv M^e \pmod n$ atau $c_i \equiv m_i^e \pmod n$ dimana c_i adalah masing – masing karakter yang bersesuaian dengan tabel ASCII. Sehingga,

$c_1 \equiv 74^{1841} \pmod{7429}$
$\equiv (74^{460})^4 .74 \pmod{7429}$
$\equiv ((74^{92})^5)^4 .74 \pmod{7429}$
$\equiv (2189^5)^4 .74 \pmod{7429}$
$\equiv 3209^4 .74 \pmod{7429}$
$\equiv 358 .74 \pmod{7429}$
$\equiv 4205$

Dengan menggunakan cara yang sama dengan c_1 maka pesan yang akan dikirim Ana (*ciphertext*) untuk "Jurusan Matematika Universitas Negeri Padang" yaitu:
C = "4205, 338, 114, 338, 115, 5010, 4581, 1800, 5568, 5010, 507, 3824, 3373,5010,507, 4848, 5955, 5010, 1800, 2125, 4581, 4848, 1461, 3824, 114, 115, 4848, 507, 5010, 115, 1800, 6929, 3824, 3299, 3824, 114, 4848, 1800, 5622, 5010, 1681, 5010, 4581, 3299"

c. Algoritma Dekripsi
Algoritma untuk melakukan dekripsi kriptografi RSA Multiprima adalah sebagai berikut:
1) Ambil kunci privat d untukmenghasilkan M.
2) Teks rahasia adalah C.
3) Teks asli didapat dari $M \equiv C^d \text{ mod}(n)$

Contoh
Misalkan Aini menerima sebuah pesan dari Ana dengan *chipertext* sebagai berikut:
C = "4205, 338, 114, 338, 115, 5010, 4581, 1800, 5568, 5010, 507, 3824, 3373,5010,507, 4848, 5955, 5010, 1800, 2125, 4581, 4848, 1461, 3824, 114, 115, 4848, 507, 5010, 115, 1800, 6929, 3824, 3299, 3824, 114, 4848, 1800, 5622, 5010, 1681, 5010, 4581, 3299
Untuk mengetahui isi pesan yang dikirim oleh Ana maka Aini harus melakukan dekripsi terhadap pesan yang telah diterima dengan menggunakan kunci privat (d,n)= (5393 , 7429)
Selanjutnya *chipertext* yang telah diterima didekripsi menggunakan rumus $m_i = c_i^d \text{mod}(n)$ untuk masing – masing blok .
Untuk blok $m_1 \equiv 4205^{5393} \pmod{7429}$
$\equiv 4205^{5390+3} \pmod{7429}$
$\equiv (4205^5)^{1078} . 4205^3 \pmod{7429}$
$\equiv 3254^{1078} . 6353 \pmod{7429} \equiv (3254^2)^{539} . 6353 \pmod{7429}$
$\equiv 2191^{539} .6353 \pmod{7429}$
$\equiv (2191^7)^{77} .6353 \pmod{7429}$
$\equiv \left((2191^7)^7\right)^{11} .6353 \pmod{7429}$
$\equiv (1130^7)^{11} .6353 \pmod{7429}$
$\equiv 2854^{2*5+1} .6353 \pmod{7429}$
$\equiv (2854^2)^5 . 2854 . 6335 \pmod{7429}$
$\equiv 3132^5 . 4702 \pmod{7429}$
$\equiv 2588 . 4702 \pmod{7429}$
$= 74$

Dengan menggunakan cara yang sama dengan m_1, maka diperoleh *plaintext* dalam bentuk decimal ASCII. yaitu:
M = 74, 117, 114, 117, 115, 97, 110, 32, 77, 97, 116, 101, 109, 97, 116, 105,
107, 97, 32, 85, 110, 105, 118, 101, 114, 115, 105, 116, 97, 115, 32, 78, 101, 103, 101, 114, 105, 32, 80, 97, 100, 97, 110, 103
Selanjutnya plainteks yang berbentuk decimal ASCII dikonversikan kedalam nilai ASCII sehingga diperoleh

plainteks yang dimaksud, yaitu: "Jurusan Matematika Universitas Negeri Padang"

2. Mengaplikasikan Chinese Remainder Theorem Dengan Garner's Algorithm Dalam Mennyusun Algoritma Kriptografi RSA

Pengaplikasian *Chinese Remainder Theorem* dalam algoritma kriptografi RSA multiprima akan difokuskan pada proses dekripsi yang bertujuan untuk mempercepat proses dekripsi. Sedangakan untuk proses enkripsi tetap sama dengan algoritma RSA multiprima standar.

Jika M adalah plainteks dan C adalah cipherteks, maka pernyataan berikut setara dengan akibat dari teorema fermat,yaitu:

Jika C tidak habis dibagi oleh p dan $d_p \equiv d(\text{mod } (p-1))$ maka $C^{d_p} \equiv C^d \pmod p$

Karena p, q dan r adalah bilangan prima, maka pesan apapun akan dapat direpresentasikan secara unik dengan $M \equiv M_P \bmod p$, $M \equiv M_q \bmod q$ dan $M \equiv M_r \bmod r$ perhitungan ini akan lebih cepat dengan dari pada menggunakan $M \equiv C^d \pmod n$

$M_p \equiv M \pmod p$

$\equiv (C^d \bmod n) \bmod p$

$\equiv C^d \pmod p$, (karena n=pqr)

Karena $C^{d_p} \equiv C^d \pmod p$

Maka $C^d \equiv C^{d_p} \pmod p$

sehingga

$M_p \equiv C^{d_p} (\text{mod } p)$ dengan $d_p \equiv d(\text{mod}(p-1))$

Dengan cara yang sama didapatkan:

$M_q \equiv C^{d_q} (\text{mod } q)$ dengan $d_q \equiv d(\text{mod}(q-1))$

$M_r \equiv C^{d_r} (\text{mod } r)$ dengan $d_r \equiv d(\text{mod}(r-1))$

Diperoleh sistem kekongkuenan dalam bentuk *Chinese Remiander Theorem* yaitu

$M \equiv M_p \equiv C^{d_p} \pmod p$

$M \equiv M_q \equiv C^{d_q} \pmod q$

$M \equiv M_r \equiv C^{d_r} \pmod r$

Setelah diperoleh sistem kekongruenan dalam bentuk *Chinese Remainder Theorem* maka selanjutnya akan dicari solusi yang memenuhi sistem kekongruenan dengan menggunakan *Garner's Algorithm* (algoritma garner). *Garner's algorithm* adalah suatu metode untuk meyelesaikan *Chinese Remainder Theorem* secara optimal untuk mempercepat proses pencarian solusi.

Apabila diberikan sistem kekongruenan:

$M \equiv M_p \pmod p$

$M \equiv M_q \pmod q$

$M \equiv M_r \pmod r$

Sistem kekongruenan diatas dapat diselesaikan menggunakan *Garner's Algorithm* dengan prosedur sebagai berikut:

a. $V \leftarrow M_q - M_p \bmod (q)$
b. $V \leftarrow V*(p_{inv}\ q) \pmod q$, dimana $p_{inv}\ q = p^{-1} \bmod 1$
c. $M_{pq} \leftarrow V*p \pmod{pq}$
d. $M_{pq} \leftarrow M_{pq} + M_p \pmod{pq}$
e. $V \leftarrow M_r - M_{pq} \pmod r$
f. $V \leftarrow V*(pq_{inv}\ r) \pmod r$, dimana $pq_{inv}\ r = (pq)^{-1} \pmod r$
g. $M \leftarrow (V*p) \bmod (n)$, dimana $n = (pqr)$
h. $M \leftarrow (M*q) \bmod (n)$
i. $M \leftarrow (M_{pq} + M) \bmod (n)$
j. DiperolehM yang merupakan solusi dari sistem kekongruenan.

Notasi algoritma tidak menggunakan tanda = (sama dengan) tetapi menggunakan simbol anak panah ke arah kiri (←)seperti yang terlihat pada langkah diatas.Sebagai contoh pada langkah pertama , arti dari notasi tersebut adalah nilai variabel V (yang ada di sebelah kanan anak panah) diberikan kepada variabel $M_q - M_p \bmod (q)$ (yang ada di sebelah kiri anak panah). Dalam penulisan matematis tanda anak panah kekiri (←) ini sama artinya dengan tanda sama dengan (=).

3. Algoritma Kriptografi RSA Multiprima yang Telah Memanfaatkan CRT dan Garner's Algorithm pada Kasus $n = pqr$

Sebelum menggunakan algoritma RSA multiprima maka pendekripsi terlebih dahulu harus membangkitkan sepasang kunci yaitu kunci publik dan kunci privat. Untuk membangkitkan kunci algoritma RSA multiprima yang telah dimodifikasi degan CRT dan *Garner's Algorithm* dimanfaatkan keuntungan CRT yang memungkinkan untuk membagi perpangkatan modulo yang besar kedalam tiga modulo eksponensial yang lebih kecil yaitup, q dan r. sehingga terbentuklah sistem kekongruenan yang dapat diselesaikan dengan metode *Chinese Remainder Theorem* selanjutnya sistem perkongruenan *Chinese Remainder Theorem* yang telah terbentuk diselesaikan degan menggunakan *garner's algorithm.*

a. Algoritma Pembangkit Kunci RSA Multiprima yang Telah Memanfaatkan CRT dan *Garner's Algorithm* Pada Kasus $n = pqr$

Algoritma untuk membangkitkan kunci RSA multiprima yang telah dimodifikasi menggunakan *Chinese Remainder Theorem* dan *Garner's Algorithm* adalah sebagai berikut:

1) Memilih tiga buah bilangan prima yang sangat besar. Misalkan ketinga bilangan prima itu adalah p, q dan r
2) Mengitung n=p*q*r
3) Mengitung φ(n)=(p-1)*(q-1)*(r-1)
4) Memilih sebuah bilangan d yang memenuhi FPB (e, φ(n)=1)
5) Menghitung $d \equiv e^{-1} \bmod \varphi(n)$
6) Sederhanakan masing dari kekongruenan,

$d_p \equiv d(\text{mod } (p-1))$

$d_q \equiv d(\text{mod } (q-1))$

$d_r \equiv d(\text{mod } (r-1))$

7) Temukan nilai dari :
   $p_{inv} \equiv p^{-1} \text{ (mod q)}$
   $pq_{inv} \equiv (pq)^{-1} \text{ (mod r)}$
8) Diperoleh kunci publik : (e, n) dan kunci privat : $(d_p, d_q, d_r, p_{inv}q, pq_{inv}r)$

b. Algoritma Enkripsi RSA Multiprima yang Telah Memanfaatkan CRT dan *Garner's Algorithm* Pada Kasus n= pqr

Algoritma Enkripsi RSA Multiprima yang Telah Memanfaatkan CRT dan *Garner's Algorithm* Pada Kasus n= pqr adalah sebagai berikut:

1) Ambil kunci publik penerima pesan, e, dan modulus n.
2) Nyatakan plainteks m menjadi blok-blok $m_1, m_2, ...$,sedemikian sehingga setiap blok merepresentasikan nilai didalam selang [0, n – 1].
3) Setiap blok $m_i$dienkripsi menjadi blok $c_i$dengan rumus$c_i = m_i^e \text{mod}(n)$

c. Algoritma Dekripsi RSA Multiprima yang Telah Memanfaatkan CRT dan Garner's Algorithm pada Kasus n=pqr

Algoritma dekripsi RSA multiprima yang telah dimodifikasi menggunakan *Chinese Remainder Theorem* akan digunakan untuk menghitung nilai plainteks m_i yang telah enkripsi dengan langkah – langkah berikut:

1) Nyatakan masing – masing chiperteks C menjadi blok-blok $c_1, c_2, \ldots$,sedemikian sehingga setiap blok merepresentasikan nilai didalam selang [0, n – 1].
2) Menentukan nilai dari $C_p, C_q,$ dan C_r, dimana :
   $C_p \equiv C \text{ (mod p)}$
   $C_q \equiv C \text{ (mod q)}$
   $C_r \equiv C \text{ (mod r)}$
3) Menentukan nilai dari M_p, M_q , dan M_r dengan$M_p \equiv C_p{}^{d_p} \text{ (mod p)}$
   $M_q \equiv C_q{}^{d_q} \text{ (mod q)}$
   $M_r \equiv C_r{}^{d_r} \text{ (mod r)}$
4) Mencari solusi dari sitem kekogruenan dengan menggunakan garner's algorithm
   $M \leftarrow \text{Garner pqr} \begin{pmatrix} M_p, M_q, M_r, p, q, r, \\ (p_{inv}q), (pq_{inv}\, r), n \end{pmatrix}$
5) Diperoleh *M*

4. Menerapkan Algoritma Kiptografi Algoritma RSA Multiprima yang Telah Dimodifikasi Menggunakan Chinese Remainder Theorem dan Garner's Algorithm

Menggunakan contoh yang sama dengan algoritma kriptografi RSA multiprima yang telah dibahas sebelumnya, misalkan dipilih tiga bilangan prima yaitu p = 17, q = 19 dan r = 23 diperoleh bahwa n = 6336, $\varphi(n) = 6336$, kunci publik e = 1841, dan d = 5393
Selanjutnya akan di tentukan kunci privat d_p, d_q, d_r, $(p_{inv}q)$, dan $(pq_{inv}\, r)$ yaitu:

$d_p \equiv 5393 (\text{mod } 16) = 1$
$d_q \equiv 5393 (\text{mod } 18) = 11$
$d_r \equiv 5393 (\text{mod } 22) = 3$

Kemudian mencari nilai $(p_{inv}q), (pq_{inv}\, r)$

$p_{inv}q \equiv p^{-1} \text{ (mod q)}$
$p_{inv}q \equiv 17^{-1} \text{ (mod 19)}$

Persamaaan ini dapat diubah menjadi
17 x≡1 (mod 19) .....(2)
Dengan menyelesaikan persamaan perkongruenan (2) diatas, diperoleh x = 9
Jadi, $p_{inv}q = 9$, dan $pq_{inv}\, r \equiv (pq)^{-1} \text{(mod r)}$
$pq_{inv}\, r \equiv (17*19)^{-1} \text{(mod 23)}$
$pq_{inv}\, r \equiv (323)^{-1} \text{(mod 23)}$
Persamaan ini dapat disubah menjadi,
323 x ≡ 1 (mod 23) .....(3)
dengan menyelesaikan persamaan perkongruenan diperoleh nilai $x = pq_{inv} = 1$
Jadi kunci privat d_p=13 , d_q=1 , d_r=3, $(p_{inv}q=9)$, $(pq_{inv}\, r=1)$ dan kunci publik yang akan di distribusikan adalah (e, n) = (37 , 7429)

Misalkan Aini menerima sebuah pesan:
C = 4205, 338, 114, 338, 115, 5010, 4581, 1800, 5568, 5010, 507, 3824, 5337,3010, 507, 4848,5955, 5010, 1800, 2125, 4581, 4848, 1461, 3824, 114, 115, 4848, 507, 5010, 115, 1800, 6929, 3824, 3299, 3824, 114, 4848, 1800, 5622, 5010, 1681, 5010, 4581, 3299
Untuk mengetahui isi yang terkandung dalam pesan maka Aini terlebih dahulu harus melakukan proses dekripsi dengan menggunakan kunci privatnya. yaitu d_p=1 , d_q=11 , d_r=3 , $(p_{inv}q=9)$, $(pq_{inv}\, r=1)$ dengan langkah – langkah sebagi berikut:

a. Menyatakan *ciphertext* yang diterima kedalam blok m_i, yang mana i adalah masing – masing karakter yang diterima

$m_1 = 4205$	$m_2 = 338$	$m_3 = 114$
$m_4 = 338$	$m_5 = 115$	$m_6 = 5010$
$m_7 = 4581$	$m_8 = 1800$	$m_9 = 5568$
$m_{10} = 5010$	$m_{11} = 507$	$m_{12} = 3824$
$m_{13} = 3373$	$m_{14} = 5010$	$m_{15} = 507$
$m_{16} = 4848$	$m_{17} = 5955$	$m_{18} = 5010$

b. Mencari nilai dari C_p, C_q, dan C_r untuk masing – masing blok m_i

Untuk blok $m_1 = 4205$ nilai nilai C_p, C_q, dan C_r adalah
$C_p \equiv 4205 \text{ (mod 17)} = 6$
$C_q \equiv 4205 \text{ (mod 19)} = 6$
$C_r \equiv 4205 \text{ (mod 23)} = 19$

c. Mencari nilai M_p , M_q dan M_r untuk masing – masing blok m_i

Untuk blok $m_1 = 4205$ nilai nilai M_p , M_q dan M_r adalah
$M_p \equiv 6^1 \text{ (mod 17)} = 6$

$M_q \equiv 6^{11} \pmod{19} \equiv 6^{10}.6 \pmod{19} = 17$

$M_r \equiv 19^3 \pmod{23} = 5$

Jika diperoleh nilai $M_p = M_q = M_r = a$ maka *Chinese Remainder Theorem* tidak perlu dilanjutkan, karena a adalah solusi dari sistem perkongruenan.

Selanjutnya menyelesaikan sitem kekongruenan dengan *Garner's Algorithm*

a. $V \leftarrow (17\text{-}6) \pmod{19} = 11$
b. $V \leftarrow 11*9 \pmod{19} = 99 \pmod{19} = 4$
c. $M_{pq} \leftarrow 4*17 \ (\mathrm{mod}(17*19)) = 68$
d. $M_{pq} \leftarrow 68 + 6 \pmod{323} = 74$
e. $V \leftarrow (5\text{-}74) \pmod{23} = 0$
f. $V \leftarrow (0*1) \pmod{23} = 0$
g. $M \leftarrow (0*17) \pmod{7429} = 0$
h. $M \leftarrow (0*19) \pmod{7429} = 0$
i. $M \leftarrow (74+0) \pmod{7429} = 74$
j. Diperoleh M =74 yang merupakan solusi dari sistem kekongruenan.

Jika pada pada salah satu langkah ditemukan nilai V sama dengan nol maka *Garner's Algorithm* tidak perlu dilanjutkan.

Dengan menggunakan cara yang sama dengan m_1 untuk semua blok maka diperoleh plainteks dalam bentuk decimal ASCII. yaitu:

M = "74, 117, 114, 117, 115, 97, 110, 32, 77, 97, 116, 101, 109, 97, 116, 105, 107, 97, 32, 85, 110, 105, 118, 101,114, 115, 105, 116, 97, 115, 32, 78, 101, 103, 101, 114, 105, 32, 80, 97, 100, 97, 110, 103"

Selanjutnya plainteks yang telah diperoleh dalam bentuk decimal ASCII ini dikonversikan kedalam nilai ASCII. Jadi pesan yang ingin disampaikan .yaitu: "Jurusan Matematika Universitas Negeri Padang".

SIMPULAN

1. Algoritma kriptografi RSA multiprima dapat dimodifikasi menggunakan *Chinese Reminder Theorem* dan *Garner's Algorithm*.
2. Pengaplikasian *Chinese Remainder Theorem* pada modifikasi algoritma kriptografi RSA multiprima dimulai dengan menggunakan Teorema Fermat dan Teorema Akibat sehingga terbentuk *Chinese Reminder Theorem* yang kemudian diselesaikan menggunakan *Garner's Algorithm*.
3. Hasil dari modifikasi algoritma kriptografi RSA multiprima menggunakan *Chinese Reminder Theorem* dan *Garner's Algorithm* meghasilkan kunci privat baru yang dapat digunakan untuk melakukan dekripsi.

REFERENSI

[1] Hinek, M. Jason.2006 *On the Security of Multi-prime RSA:*University of Waterloo.

[2] Sadikin Rifki. 2012. *Kriptografi Untuk keamananan Jaringan* . Yogyakarta : And

[3] Stinson. D. R 1995. *Criphtography Teory and Practise.* CRC Press. Boca Raton : Florida

[4] Takagi, Tsuyoshi. 2003. *Efficiency Comparison of Several RSA 'Variants.* Camille Vuillaume

[5] Johari, Fatimah Putri. 2016. *Modifikasi Algoritma Kriptografi RSA Multiprima Menggunakan Chinesee Remainder Theorem dan Garner's Algorithm.* Padang: Universitas Negeri Padang