CESS (Journal Of Computer Engineering, System And Science) **p-ISSN :2502-7131**
Vol 2, No 1, Januari 2017 **e-ISSN :2502-714x**

ANALISIS KEAMANAN DATA PADA BLOCK CIPHER ALGORITMA KRIPTOGRAFI RSA

Fadhillah Azmi[1], Winda Erika[2]
Teknik Informatika, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Sumatera Utara
Jalan Universitas No.24A, Kampus USU Medan
azmi_fa@yahoo.com

***Abstrak*— Komunikasi adalah proses dasar dari pertukaran informasi. Efektifitas komunikasi komputer secara umum adalah melalui internet atau beberapa saluran komunikasi lainnya. Tujuan utama tulisan ini adalah berdasarkan pada analisis hasil yang diberikan Weiner mengatakan bahwa jika private key d digunakan dalam algoritma kriptografi RSA kurang dari n^{292}, maka sistem tersebut kurang aman. Di sini penulis menganalisa pada hasil yang diberikan oleh Weiner dan mencoba untuk meningkatkan range dari private key d sampai $n^{0.5}$. Karena n adalah perkalian p dan q, yang mana bilangan relative prima. Sehingga mempengaruhi kinerja enkripsi algoritma yang lebih aman.**

***Keywords*— RSA, keamanan, data**

I. PENDAHULUAN

A. Latar Belakang Masalah

Tingkat keamanan suatu sistem sangatlah penting sehingga dibutuhkan suatu metode untuk mengamankannya dari pihak yang tidak berkepentingan, salah satu metode yang digunakan adalah algoritma RSA berupa pembentukkan *ciphertext* karena tingkat keamanannya dalam me-enkripsi informasi yang sangat baik karena sulitnya dalam pemfaktoran terhadap sebuah bilangan integer besar.

Wiener mengatakan bahwa jika kunci privasi d digunakan dalam algoritma RSA kurang dari n^{292}, maka sistem tersebut kurang aman. Di sini penulis menganalisa pada hasil yang diberikan Wiener dan mencoba untuk meningkatkan range $n^{0.5}$.

Penelitian (Upadhyay, 2012), pada *An Analysis of the Attack on RSA Sryptosystem Trhourgh Formal Methods*, dengan membentuk *plaintext* terlebih dahulu ke dalam blok yang terdiri dari tiga karakter huruf kapital, di dalam hasil analisanya diperoleh pendekatakan efektif untuk nilai e < N^1.875. Sehingga penulis tertarik untuk memnganalisa kembali pembentukkan *plaintext* ke dalam suatu blok yang terdiri lebih dari tiga karakter huruf kapital.

II. LANDASAN TEORI

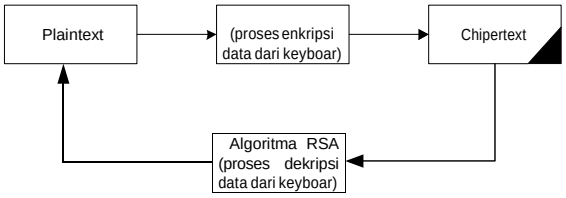
A. Kriptografi

Kriptografi adalah sutau ilmu dan seni untuk mengamankan informasi yang berupa pesan yang terbaca (*plaintext*) menjadi pesan yang tidak bisa dibaca (*ciphertext*), sehingga hanya pengirim pesan dan penerima pesan yang dapat mengganti, menghapus dan membaca pesan tersebut. (Konheim, 2007).

Salah satu algoritma dari kriptografi adalah algoritma RSA (Rivest-Shamir-Adleman) yang memiliki tingkat keamanan yang sangat baik karena sulitnya pemfaktoran terhadap sebuah bilangan yang besar menjadi faktor-faktor bilangan prima. (Yan, 2008).

B. Algoritma RSA

Algoritma RSA berasal dari gabungan nama tiga orang peneliti yaitu Ron RIvest, Adi Shamir dan dan Leonard Adleman. Metode kriptografi ini digolongkan kepada kriptografi modern yang teridiri dari dua kunci, yaitu kunci publik (*public key*) untuk melakukan enkripsi dan kunci privasi (*private key*) untuk melakukan dekripsi.



Gbr. 1 Proses metode Algoritma RSA

Enkripsi memngubah data asli (*plaintext*) ke data yang disandikan (*ciphertext*), sedangkan dekripsi adalah mengembalikan *ciphertext* ke *plaintext*. Adapun proses membangkitkan kunci publik dan kunci privasi adalah sebagai berikut :

1. Menentukan dua buah bilangan prima, dimisalkan dengan p dan q.
2. Menghitung modulus kunci publik,
   $$n = p \times q \quad (1)$$
   $$\varphi(n) = (p-1)\times(q-1) \quad (2)$$
   $$\text{GCD}(e, \varphi(n)) = 1 \quad (3)$$
3. Menghitung modulus kunci privasi.
   $$e\ d\ mod\ \varphi(n) = 1$$
   Proses enkripsi : $C_i = P_i^e\ mod\ n$ (4)
   Proses dekripsi : $P_i = C_i^d\ mod\ n$ (5)
   Keterangan :
   C_i = *Ciphertext* ke-i
   n = dua buah bilangan prima yang dikalikan

$\varphi(n) = (p-1)\times(q-1)$

e = kunci public

d = kunci privasi

III. METODOLOGI PENELITIAN

Adapun informasi dan data-data yang diperlukan dalam penelitian ini adalah sebagai berikut :

a. Observasi
   Dilakukan untuk mengumpulkan data dengan cara pengamatan langsung pada hal-hal yang berkaitan dengan perpustakaan.
b. Studi kepustakaan
   Dilakukan dengan cara membaca buku-buku yang berkaitan dengan masalah peminjaman buku.
c. Analisa beberapa kasus yang ada, dengan menngambil masalah yang berkaitan dengan pembahasan.
d. Pembahasan kasus yang ada.

IV. ANALISA DAN PEMBAHASAN

Data yang digunakan adalah karakter huruf kapital [A…Z] yang dikonversi ke bentuk karakter 26 yaitu A = 0, B=1, C = 2, … Z = 25. Analisa terlebih dahulu menggunakan algoritma kriptografi RSA sebagai perbandingan keamanan data. Misalnya *plaintext* yang akan di-enkripsi (*ciphertext*) adalah MAGISTER USU, maka dikonversi ke bentuk numeric M = 12, A = 0, G = 6, I = 8, S = 18, T = 19, E = 4, R = 17, U = 20, S = 18, U = 20. Berdasarkan tahap algoritma kriptografi RSA diperoleh :

1. Menentukan dua buah bilangan prima, dimisalkan dengan p dan q. (p = 17, q = 13)
2. Menghitung modulus kunci publik,
   $n = p\times q = 17\times 13 = 221$
   $\varphi(n) = (p-1)\times(q-1)$
   $= (17-1)\times(13-1) = 192$
   $\mathrm{GCD}(175,192) = 1$
3. Menghitung modulus kunci privasi.
   $e\ d\ mod\ \varphi(n) = 1$

Sehingga dari perhitungan di atas diperoleh:
Public key (n, e) = (221, 175)
Private key (n, d) = (221, 79)

Dengan menggunakan persamaan (4), enkripsi yang dihasilkan adalah sebagai berikut:

M = 12, $C_M = 12^{175}\ mod\ 221 = 129$
A = 0, $C_A = 0^{175}\ mod\ 221 = 0$
G = 6, $C_G = 6^{175}\ mod\ 221 = 20$
I = 8, $C_I = 8^{175}\ mod\ 221 = 83$
S = 18, $C_S = 18^{175}\ mod\ 221 = 86$
T = 19, $C_T = 19^{175}\ mod\ 221 = 111$
E = 4, $C_E = 4^{175}\ mod\ 221 = 30$
R = 17, $C_R = 17^{175}\ mod\ 221 = 17$
U = 20, $C_U = 20^{175}\ mod\ 221 = 6$
S = 18, $C_S = 18^{175}\ mod\ 221 = 86$
U = 20, $C_U = 20^{175}\ mod\ 221 = 6$

Dengan menggunakan persamaan (5), dekripsi yang dihasilkan adalah sebagai berikut:

M = 12, $P_{129} = 129^{79}\ mod\ 221 = 12$
A = 0, $P_0 = 0^{79}\ mod\ 221 = 0$
G = 6, $P_{20} = 20^{79}\ mod\ 221 = 6$
I = 8, $P_{83} = 83^{79}\ mod\ 221 = 8$
S = 18, $P_{86} = 86^{79}\ mod\ 221 = 18$
T = 19, $P_{111} = 111^{79}\ mod\ 221 = 19$
E = 4, $P_{30} = 30^{79}\ mod\ 221 = 4$
R = 17, $P_{17} = 17^{79}\ mod\ 221 = 17$
U = 20, $P_6 = 6^{79}\ mod\ 221 = 20$
S = 18, $P_{86} = 86^{79}\ mod\ 221 = 18$
U = 20, $P_6 = 6^{79}\ mod\ 221 = 20$

Berdasarkan penelitian (Upadhyay, 2012), dengan menggunakan karakter dalam tiga blok. Di sini penulis akan menggunakan karakter ke dalam empat blok dan mengkonversi ke dalam bilangan bulat untuk masing-masing karakter huruf kapital.

MAGISTER USU = MAGI STER USUX

$MAGI = 12\times 26^3 + 0\times 26^2 + 6\times 26^1 + 8$
$= 211076$

$STER = 18\times 26^3 + 19\times 26^2 + 4\times 26^1 + 17$
$= 329333$

$USUX = 20\times 26^3 + 18\times 26^2 + 20\times 26^1$
$+23 = 64231$

Dalam kasus ini, harus memiliki nilai maksimum untuk blok plainteks ini (AAAA) yaitu $26^4 - 1 = 456975$, sehingga nilai modulus untuk mencari kunci publik dan privasi harus lebih besar daripada nilai tersebut. Berdasarkan tahap algoritma kriptografi RSA diperoleh :

1. Menentukan dua buah bilangan prima, dimisalkan dengan p dan q. (p = 727, q = 751)
2. Menghitung modulus kunci publik,
   $n = p\times q = 727\times 751 = 545977$
   $\varphi(n) = (p-1)\times(q-1)$
   $= (727-1)\times(751-1)$
   $= 544500$
   $\mathrm{GCD}(7,192) = 1$
3. Menghitung modulus kunci privasi.
   $e\ d\ mod\ \varphi(n) = 1$

Sehingga dari perhitungan di atas diperoleh:
Public key (n, e) = (544500, 7)
Private key (n, d) = (544500, 311143)

Dengan menggunakan persamaan (4), enkripsi yang dihasilkan adalah sebagai berikut:

MAGI = 211076,
$C_{MAGI} = 211076^7\ mod\ 544500 = 65276$
STER = 329333
$C_{STER} = 329333^7\ mod\ 544500 = 339377$
USUX = 64231

$$C_{USUX} = 64231^{7} \ mod \ 544500 = 9511$$

Dengan menggunakan persamaan (5), dekripsi yang dihasilkan adalah sebagai berikut:

$$P_{65276} = 65276^{311143} \ mod \ 544500 = INF$$

$$P_{65276} = 339377^{311143} \ mod \ 544500 = INF$$

$$P_{65276} = 9511^{311143} \ mod \ 544500 = INF$$

Berdasarkan dari perhitungan pada proses dekripsi (*ciphertext – plaintext*), tidak dapat dilakukan karena nilai eksponen kunci privasi terlalu besar.

V. KESIMPULAN

Berdasarkan hasil analisis keamanan data dengan menggunakan algoritma kriptografi rsa pada umumnya nilai eksponen yang diperoleh untuk kedua kunci publik dan privasi tidak terlalu besar, jika dibanding dengan pembentukkan blok plainteks dimana karekter huruf kapital dikelompokkan dalam 1 blok terdiri 4 karakter. Sehingga tidak dapat dikembalikannya *ciphertext* ke *plaintext*. Pemilihan bilangan prima merupakan aturan penting agar hasil yang diperoleh bias diatasi.

REFERENSI

[1] Akiwate,Bahubali& Desai,Vennai. 2013. Artificial Neural Networks for Cryptanalysis of DES. *International Journal of Innovations in Engineering and Technology (IJIET)*. Vol. **2** (4).

[2] Gaines,H.F. 1956. *Cryptanalysis: a study of ciphers and their solution*. Dover: New York, USA.

[3] Goyal, Kashish & Kinger Supriya. 2013. Modified Caesar Cipher for better Security. Enhancement. *International Journal of Computer Applications (0975 – 8887)*. Vol.**73**(3).

[4] Upadhyay, Sachin., Singh, Yasphal., and Jain, Kumar, Amit. "An Analysis of the Attack on RSA Sryptosystem Trhourgh Formal Methods". International Journal of Soft Computing and Engineering (IJSCE). Vol(2): 2231-2307, 2012.

[5] Yan, Y Song. 2007. Cryptanalystic Attack on RSA. *Springer*: University of Bedfordshire, UK.