BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 1, No 3, Agustus 2021
Hal 79-82
https://hostjournals.com/bulletincsr

Implementasi Algoritma Massey-Omura Cryptosistem Dalam Pengamanan Dokumen

Irma Wahyuni

Program Studi Teknik Informatika STMIK Budi Darma Medan, Indoensia
Email: irmas4ri@gmail.com

Abstrak−Sistem keamanan pengiriman data (komunikasi data yang aman) dipasang untuk mencegah pencurian, kerusakan, dan penyalahgunaan data yang terkirim melalui jaringan komputer. Dalam praktek, pencurian data berwujud pembacaan oleh pihak yang tidak berwenang biasanya dengan menyadap saluran publik. Teknologi jaringa nkomputer telah dapa tmengurangi bahkan membuang kemungkinan adanya kerusakan data akiba tburuknya konektivitas fisik, namun gangguan tetap bisa terjadi karena ada unsur kesengajaan yang mengarah kepenyalahgunaan sistem dari pihak -pihak tertentu. Cryptosystem ini merupakan algoritma yang menyediakan keamanan cukup tinggi yang tidak didasarkan atas kerahasiaan algoritmanya (algoritma restricted), akan tetapi lebih ditekankan pada keamanan/kerahasian kunci yang digunakan (algoritma kriptografi modern). Algoritma restricted biasanya digunakan oleh sekelompok orang untuk bertukar pesan satu samalain, mereka membuat suatu algoritma enkripsi yang hanya diketahui oleh anggota kelompok itu saja, sehingga setiap kali ada anggota kelompok yang keluar, maka algoritma restricted tersebut harus diganti karena kemungkinan anggota kelompok yang keluar itu dapat membocorkan algoritmanya.Sehingga setiap kali ada anggota kelompok yang keluar, maka algoritma yang dipakai tidak perlu diganti, namun cukup mengganti kuncinya saja. Oleh sebab itu, penulis mencoba untuk menggunakan Algoritma Massey- Omura yang pengimplementasiannya menggunakan ThreePass Protocol untuk membangkitkan bilangan prima karena algoritma Massey-Omura ini merupakan salah satu algoritma asimetri yang melakukan pemfaktoran bilangan besar untuk mendapatkan kunci privat.

Kata Kunci: Implementasi; Massey-Omura Cryptosystem; Keamanan Dokumen

Abstract−A data transmission security system (secure data communication) is installed to prevent theft, damage, and misuse of data sent via computer networks. In practice, data theft takes the form of reading by unauthorized parties usually by tapping public channels. Computer network technology has been able to reduce and even eliminate the possibility of data damage due to poor physical connectivity, but interference can still occur because there is an element of intent that leads to misuse of the system from certain parties. This cryptosystem is an algorithm that provides a fairly high security which is not based on the secrecy of the algorithm (restricted algorithm), but is more emphasized on the security/confidentiality of the key used (modern cryptographic algorithms). The restricted algorithm is usually used by a group of people to exchange messages with each other, they create an encryption algorithm that is only known to members of that group, so that every time a group member leaves, the restricted algorithm must be replaced because of the possibility that group members who leave the group can leaking the algorithm. So every time a group member leaves, the algorithm used does not need to be changed, but only changes the key. Therefore, the author tries to use the Massey-Omura Algorithm whose implementation uses the ThreePass Protocol to generate prime numbers because the Massey-Omura algorithm is one of the asymmetric algorithms that factorizes large numbers to get the private key.

Keywords: Implementation; Massey-Omura Cryptosystem; Document Security

1. PENDAHULUAN

Dewasa ini penggunaan teknologi Internet didunia sudah berkembang pesat. Semua kalangan telah menikmati Internet. Bahkan, perkembangan teknologi Internet tersebut semakin memudahkan penggunanya dalam berkomunikasi melalui bermacam-macam media maupun aplikasi. Sistem keamanan pengiriman data (komunikasi data yang aman) dipasang untuk mencegah pencurian, kerusakan, dan penyalahgunaan data yang terkirim melalui jaringan komputer. Dalam praktek, pencurian data berwujud pembacaan oleh pihak yang tidak berwenang biasanya dengan menyadap saluran publik. Teknologi jaringan computer telah dapat mengurangi bahkan membuang kemungkinan adanya kerusakan data akibat buruknya konektivitas fisik, namun gangguan tetap bisa terjadi karena ada unsur kesengajaan yang mengarah kepenyalah gunaan sistem dari pihak-pihak tertentu.

Massey-Omura Cryptosystem ini merupakan algoritma yang menyediakan keamanan cukup tinggi yang tidak didasarkan atas kerahasiaan algoritmanya (algoritma *restricted*), akan tetapi lebih ditekankan pada keamanan/kerahasian kunci yang digunakan (algoritma *kriptografi modern*). Algoritma *restricted* biasanya digunakan oleh sekelompok orang untuk bertukar pesan satu samalain, mereka membuat suatu algoritma enkripsi yang hanya diketahui oleh anggota kelompok itu saja, sehingga setiap kali ada anggota kelompok yang keluar, maka algoritma *restricted* tersebut harus diganti karena kemungkinan anggota kelompok yang keluar itu dapat membocorkan algoritmanya.

Algoritma *kriptografi modern*, seperti *Massey-Omura Cryptosystem* ini, dapat mengatasi masalah tersebut dengan menggunakan kunci, yang dalam hal ini algoritmanya tidak lagi dirahasiakan, tetapi kunci harus di jaga kerahasiaannya. Sehingga setiap kali ada anggota kelompok yang keluar, maka algoritma yang dipakai tidak perlu diganti, namun cukup mengganti kuncinya saja. Oleh sebab itu penulis mecoba untuk menggunakan Algoritma *Massey-Omura* yang pengimplementasiannya menggunakan *Three Pas Protocol* untuk membangkitkan bilangan prima karena algoritma *Massey-Omura* ini merupakan salah satu algoritma simetri yang melakukan pemfaktoran bilangan besar untuk mendapatkan kunci privat. Dengan perkataan lain, diperlukan algoritma *kriptografi modern* yang dapat digunakan dan gampang dimengerti oleh semua orang, juga algoritma yang menyediakan keamanan cukup tinggi yang

tidak didasarkan atas kerahasiaan algoritmanya[1].

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kriptografi berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu kripto dan graphia. Kripto artinya menyembunyikan, sedangkan graphi artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integrasi data, serta auetentikasi data. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi. Kriptografi dapat pula di artikan sebagai ilmu dan seni untuk menjaga kerahasiaan berita[2]–[4].

2.2 Algoritma *Massey-Omura*

Algoritma *Massey-Omura* adalah algoritma kriptografi modern yang menggunakan sistem kriptografi asimetri (kunci privat). Algoritma *Massey-Omura* diusulkan oleh *James Massey* dan *Jim K. Omura* pada tahun 1982 ini, melakukan pemfaktoran bilangan yang sangat besar untuk mendapatkan kunci privat. Oleh karena alasan tersebut, *Massey-Omura* dianggap aman. Selain itu, *Massey-Omura* adalah salah satu algoritma yang pengimplementasiannya menggunakan *three pass protocol*[5].

Berikut adalah proses enkripsi dekripsi dengan menggunakan algoritma *Massey-Omura*:

1. Bilangan prima yang diambil harus lebih besar dari plainteks (p > m).
2. Ambil eA :
   a. $2 < eA < p - 1$
   b. GCD (eA , p-1) = 1
3. Hitung $dA \equiv eA^{-1} \pmod{p-1}$
4. Hitung $C_1 = m^{eA} \bmod p$
5. Kirim C_1 ke penerima
6. Penerima menerima C_1
7. Ambil eB :
   a. $2 < eB < p-1$
   b. GCD (eB, p-1) = 1
8. Hitung $dB \equiv eB^{-1} \pmod{p-1}$
9. Hitung $C_2 = C_1^{eB} \bmod p$
10. Kirim C_2 ke pengirim
11. Pengirim menerima C_2
12. Hitung $C_3 = C_2^{dA} \bmod p$
13. Kirim C_3 ke penerima
14. Penerima menerima C3
15. Hitung $m = C_3^{dB} \bmod p$

3. HASIL DAN PEMBAHASAN

Dalam perancangan sebuah sistem diperlukan analisis untuk menentukan kebutuhan sistem. Dengan adanya analisis sistem, sistem yang dirancang diharapkan akan lebih baik dan memudahkan dalam pengembangan sistem selanjutnya. Tujuan dari analisis sistem ini sendiri adalah untuk membantu pemodelan rancang bangun sistem yang nantinya akan diimplementasikan dalam bentuk nyata. Sebagai contoh, A ingin mengirimkan pesan "ILKOM" kepada B. A menggunakan eA = 89 dan B menggunakan eB = 67. Dengan begitu, maka proses yang akan terjadi adalah sbb :

1. Pilih bilangan prima p dengan menggunakan Pengecekan bilangan prima yang dibangkitkan, Misalnya : Bangkitkan bilangan prima 101, dan dilakukan pengecekan apakah bilangan ini merupakan bilangan prima atau bukan dengan cara sebagai berikut :
   a. Pilih sebuah bilangan a dimana $1 < a < 101$.
   b. Misalkan nilai *random* yang terpilih untuk nilai a adalah 2.
   c. Hitung nilai L (*Legendre*), dimana $L \equiv a^{(p-1)/2} \bmod p$, dimana p = 101.

      $L \equiv a^{(p-1)/2} \bmod p$

      $\equiv 2^{(101-1)/2} \bmod 101$

      $\equiv 2^{50} \bmod 101$

≡ 1125899906842624 mod 101 ≡ -1

d. Di karenakan 101 memiliki 3 digit, yaitu 1, 0 dan 1, maka pembuktian nilai 101 merupakan prima adalah dicari sebanyak 3 kali. Maka pilih kembali nilai a. misal a = 3, maka

$L \equiv a^{(p-1)/2} \bmod p$

$\equiv 3^{(101-1)/2} \bmod 101$

$\equiv 3^{50} \bmod 101$

≡ 717897987691852588770249 mod 101 ≡ -1

A = 4, maka

$L \equiv a^{(p-1)/2} \bmod p$

$\equiv 4^{(101-1)/2} \bmod 101$

$\equiv 4^{50} \bmod 101$

≡ 1267650600228224014967032053 76 mod 101 ≡ 1

Maka benar bahwa 101 merupakan bilangan prima.

2. Enkripsi pesan dengan menggunakan *algoritma Massey-Omura.*

Karakter “I” dalam ASCII bernilai 73,
Karakter “L” dalam ASCII bernilai 76,
Karakter “K” dalam ASCII bernilai 75,
Karakter “O” dalam ASCII bernilai 79,
Karakter “M” dalam ASCII bernilai 77,
Kemudian diketahui bahwa untuk mencari cipherteks maka kita menggunakan rumus :

$C_1 = m^{eA} \bmod p$

Dimana eA telah ditentukan sebelumnya bernilai 89 dan p bernilai 101, sehingga :

$C_1 = m^{eA} \bmod p = 73^{89} \bmod 101 = 59$

$C_1 = m^{eA} \bmod p = 76^{89} \bmod 101 = 77$

$C_1 = m^{eA} \bmod p = 75^{89} \bmod 101 = 11$

$C_1 = m^{eA} \bmod p = 79^{89} \bmod 101 = 19$

$C_1 = m^{eA} \bmod p = 77^{89} \bmod 101 = 47$

Plainteks “Ilkom” setelah dienkripsi dengan Massey-Omura menjadi “59 77 11 19 47”. Cipherteks ini kemudian dikirim ke B.

3. Penerapan Three Pass Protocol untuk mendapatkan plainteks.

Setelah B meneriman pesan dari A yang merupakan cipherteks, B tidak dapat langsung mendekripsi pesan tersebut untuk mendapatkan plainteksnya. Tetapi, B harus mengenkripsi cipherteks tersebut dengan rumus :

$C_2 = C_1^{eB} \bmod p$

Dimana eB bernilai 67 dan p bernilai 101, sehingga :

$C_2 = C_1^{eB} \bmod p = 59^{67} \bmod 101 = 86$

$C_2 = C_1^{eB} \bmod p = 77^{67} \bmod 101 = 96$

$C_2 = C_1^{eB} \bmod p = 11^{67} \bmod 101 = 12$

$C_2 = C_1^{eB} \bmod p = 19^{67} \bmod 101 = 68$

$C_2 = C_1^{eB} \bmod p = 47^{67} \bmod 101 = 23$

Cipherteks “59 2 17 10 26” setelah dienkripsi lagi oleh B menjadi “86 96 12 68 23”. Cipherteks ini kemudian dikirim ke A. Kemudian A mendekripsi cipherteks tersebut dengan rumus :

$C_3 = C_2^{dA} \bmod p$

Dimana $dA \equiv eA^{-1} \pmod{p-1}$, sehingga :

$C_3 = C_2^{dA} \bmod p = 86^{9} \bmod 101 = 46$

$C_3 = C_2^{dA} \bmod p = 96^{9} \bmod 101 = 13$

$C_3 = C_2^{dA} \bmod p = 12^9 \bmod 101 = 18$

$C_3 = C_2^{dA} \bmod p = 68^9 \bmod 101 = 92$

$C_3 = C_2^{dA} \bmod p = 23^9 \bmod 101 = 96$

Dimana $dB \equiv eB^{-1} \pmod{p-1}$, sehingga :

$C_4 = C_3^{dE} \bmod p = 46^3 \bmod 101 = 73$

$C_4 = C_3^{dE} \bmod p = 13^3 \bmod 101 = 76$

$C_4 = C_3^{dE} \bmod p = 18^3 \bmod 101 = 75$

$C_4 = C_3^{dE} \bmod p = 92^3 \bmod 101 = 79$

$C_4 = C_3^{dE} \bmod p = 96^3 \bmod 101 = 77$

Nilai 73 dalam kode ASCII adalah karakter I
Nilai 76 dalam kode ASCII adalah karakter L
Nilai 75 dalam kode ASCII adalah karakter K
Nilai 79 dalam kode ASCII adalah karakter O
Nilai 77 dalam kode ASCII adalah karakter M
Setelah B mendekripsi pesan tersebut, maka diketahuilah bahwa pesan yang dikirim oleh A adalah “ILKOM”.

4. KESIMPULAN

Kesimpulan dari penelitian yakni sistem ini menjadi salah satu alat evaluasi yang mampu memberikan hasil dari proses suatu perangkat lunak pada system keamanan data menggunakan *Massey-Omura Cryptosystem*. Sistem ini mampu menampilkan Hasil yang diinginkan sesuai dengan keamanan data atau bidang kriptografi bagian algoritma simetris. Sistem ini dapat memberikan laporan hasil dengan tingkatan dari proses enkripsi dan dekripsi sesuai dengan keamanan dokumen yang dirancang sesuai dengan sistem yang digunakan.

REFERENCES

[1] D. P. Precilia and A. Izzuddin, “Aplikasi Tanda Tangan Digital (Digital Signature) Menggunakan Algoritma Message Digest 5 (MD5),” *Energy*, vol. 5, no. 1, pp. 14–19, 2016.
[2] E. Setyaningsih, *Kriptografi & Implementasinya Menggunakan Matlab*. Yogyakarta: CV.ANDI OFFSET, 2015.
[3] Ariyus and Dony, *Kriptografi Keamanan Data dan Komunikasi*. Yogyakarta: Grahailmu, 2006.
[4] R. Munir, *Belajar Ilmu Kriptografi*. ANDI Yogyakarta, 2008.
[5] H. Barasa, “Penyembunyian Pesan Teks Tersandi dengan Algoritma Massey Omura Pada Gambar Berdasarkan Metode Stegano F5,” vol. 1, no. 1, pp. 13–22, 2021.