Jurnal Sains Dan Teknologi Informasi
Vol 1, No 2, Maret 2022, Hal 49-53
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v1i2.1442
Website https://ejurnal.seminar-id.com/index.php/jussi

Analisa Dan Implementasi Keamanan Pesan Chatting Menggunakan Algoritma Challenge Response

Muhammad Fajar Bahari

Gram Studi Tenik Informatika, ProFakultas Ilmu Komputer Dan Teknologi Informasi, Universitas Budi Darma,
Jalan Sisingamangaraja No.338, Medan, Sumatera Utara, Indonesia
Email: fajarbaharimuhammad@gmail.com

Abstrak−Kemajuan pada penyampaian informasi berbasis komputer memiliki banyak keuntungan terlebih bisa mengurangi banyak hal yang tidak perlu atau bisa dikatakan berdampak efisiensi dalam banyak hal. Namun demikian seiring dengan aspek positif juga terjadi, seperti kejahatan, yang meliputi pencurian, penipuan dan pemerasan. Informasi rahasia perusahaan yang diketahui pihak lawan lawan bisnis misalnya dapat menimbulkan kerugian bagi perusahaan tersbut, seperti informasi tentang produk yang sedang dikembangkan, algoritma dan teknik yang digunakan menghasilkan produk, sehingga disini diperlukan keamanan sistem informasi yang harus menjamin hal tersebut memiliki batas tertentu. Dengan menggunakan Algoritma response challenge yang merupakan algortima kriptografi kunci rahasia, permasalahan tersebut dapat diatasi. Kekuatan algoritma ini terletak pada jaringan feistel (meliputi operasi subtitusi, permutasi dan modular arithmetic) dan bilangan delta yang berasal dari golden number. Perancangan aplikasi ini juga memudahkan proses pengamanan teks agar tidak mudah dibaca oleh orang lain sehingga terjaga keaslian data tersebut. Merupakan usaha untuk menjaga informasi dari yang tidak berhak mengakses atau dengan kata lain sebuah informasi rahasia yang tidak boleh diakses oleh orang lain dan hanya boleh diakses oleh yang diberikan akses saja.

Kata Kunci: Keamanan; Pesan; Chatt; Response Challenge

Abstract−Advances in the delivery of computer-based information has many advantages, especially it can reduce many things that are not necessary or can be said to have an impact on efficiency in many ways. However, along with positive aspects also occur, such as crime, which includes theft, fraud and extortion. Confidential information of the company that is known to the opposing party of the business, for example, can cause harm to the company, such as information about the product being developed, the algorithms and techniques used to produce the product, so that information system security is required here which must ensure that it has certain limits. By using the response challenge algorithm which is a secret key cryptographic algorithm, these problems can be overcome. The strength of this algorithm lies in the Feistel network (which includes substitution, permutation and modular arithmetic operations) and the delta numbers derived from the golden number. The design of this application also facilitates the process of securing the text so that it is not easily read by others so that the authenticity of the data is maintained. It is an effort to protect information from those who are not entitled to access or in other words a confidential information that cannot be accessed by others and can only be accessed by those who are given access.

Keywords: Security; Message; Chat; Response Challenge

1. PENDAHULUAN

Chatting sudah menjadi hal yang umum digunakan oleh masyarakat luas. Kemampuan pengiriman pesan secara cepat membuat user dapat berkomunikasi satu sama lain secara *real-time.* Pada proses komunikasi *chatting* dibutuhkan suatu keamanan dari pesan yang akan di kirimkan untuk menghindari kehilangan pesan, manipulasi pesan ataupun kerusakan pesan yang dapat dilakukan oleh pihak ketiga. Untuk menjamin keamanan dari pesan percakapan yang dilakukan oleh *user* maka dibutuhkan suatu algoritma pada teknik kriptografi.

Permasalahan yang ada dalam komunikasi terlebih mengenai pesan *chatting* adalah pesan yang dikirimkan tidak ada pengacakan pesan sehingga sangat beresiko informasi yang ada didalam pesan tersebut dapat dicuri atau dimanipulasi dan dimengerti maknanya oleh pihak yang tidak berwenang. Dalam ini maka dapat menyebabkan kerugian pada pengguna, bila pesan yang hendak akan dikirimkan berisikan suatu informasi yang bersifat rahasia, khususnya bagi perusahaan. Untuk itu maka diperlukan suatu teknik *kriptografi* dalam pengamanan pesan *chatting*.

Pada kriptografi, terdapat proses enkripsi yang mengubah teks polos menjadi ciphertext, dan proses dekripsi yang mengubah ciphertext menjadi teks polos kembali algoritma ini juga dapat memanfaatkan kunci yang dimasukkan dari luar[1]. Untuk melakukan pengamanan pesan chatting ini maka digunakan teknik kriptografi dengan menggunakan algoritma *Challenge Response.*

Algoritma *challenge response* adalah salah satu metode yang menerapkan konsep pengiriman *password* secara tak langsung yaitu dengan menggunakan protokol authentikasi '*challenge-response'*. Pada protokol ini, pihak yang ingin memverifikasi pihak lain (*server*) bertindak sebagai penyedia pertanyaan/tantangan (*challenge*) dan *client* diharuskan untuk menjawab tantangan ini (*response*). Jika kedua pihak sederajad posisinya, maka keduanya sekaligus dapat bertindak sebagai *server* dan *client* sehingga protokol *challenge-response* membutuhkan 4 langkah verifikasi (4-ways handshaking). Untuk mengamankan komunikasi *chatting* maka dibangun suatu sistem percakapan antar *user*, dimana sistem ini menerapkan algoritma *Challenge Response* yang terdapat pada teknik kriptografi untuk meningkatkan keamanan pesan *chatting* [2].

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Jurnal Sains Dan Teknologi Informasi
Vol 1, No 2, Maret 2022, Hal 49-53
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v1i2.1442
Website https://ejurnal.seminar-id.com/index.php/jussi

Untuk mendukung kelancaran penelitian ini, maka dilakukan tahapan penelitian sebagai berikut:

a. Studi Literatur
   Pada tahap ini dilakukan pengumpulan referensi yang diperlukan dalam penelitian. Hal ini dilakukan untuk memperoleh informasi dan data yang diperlukan untuk penelitian ini. Referensi yang digunakan dapat berupa buku, jurnal, artikel, paper, makalah baik berupa media cetak maupun media internet mengenai topik penelitia .
b. Analisis Sistem
   Pada tahap ini akan dianalisis sistem yang akan dibuat, batasan sistem, kinerja sistem dan cara kerja sistem. Sehingga sistem dapat menerapkan algoritma *Challenge Response*.
c. Perancangan Sistem
   Merancang *input*, *output*, struktur file, program, prosedur, perangkat keras dan perangkat lunak yang diperlukan untuk medukung sistem informasi
d. Implementasi Sistem
   Sistem diimplementasikan dengan menggunakan algoritma *Challenge Response*.
e. Pengujian Sistem
   Pada tahap ini dilakukan pengujian kinerja sistem dan kebenaran hasil keamanan yang dilakukan dengan algoritma algoritma *Challenge Response*..
f. Dokumentasi Sistem
   Merupakan langkah yang terakhir dilakukan, melakukan validasi dan hasil akhir (output) yang diperoleh dari sistem yang dirancang setelah melakukan evaluasi ketepatan maupun kecepatan terhadap kinerja sistem untuk membuat kesimpulan dari topik yang dikaji.

2.2 Kriftografi

Kriptografi adalah studi yang bertujuan untuk mengamankan dan merahasiakan dengan melakukan proses enkripsi dan dekripsi pada data yang akan diamankan[3]. Enkripsi merupakan proses pengubahan data menjadi bentuk sandi yang tidak dipahami dan dibaca, sedangkan dekripsi merupakan proses pengembalian data dalam bentuk sandi ke dalam bentuk semula yang dapat dipahami dan memiliki makna. Dalam kriptografi terdapat beberapa teknik penyandian data yaitu simetris dan asimetris. Kriptografi simetris menggunakan kunci yang sama (kunci simetris) untuk melakukan proses enkripsi dan dekripsi. Kriptografi asimetris menggunakan kunci yang berbeda untuk proses enkripsi (menggunakan kunci publik) dan dekripsi (menggunakan kunci privat)[4][5].

2.3 Pesan

Pesan merupakan bagian dari unsur-unsur komunikasi, Hafied Cangara dalam bukunya *Pengantar Ilmu Komunikasi* menyatakan bahwa "Dalam proses komunikasi, pengertian pesan adalah sesuatu yang disampaikan pengirim kepada penerima. Pesan dapat disampaikan dengan cara tatap muka atau melalui media komunikasi. Isinya bisa berupa ilmu pengetahuan, hiburan, informasi, nasihat atau propaganda". Pengertian pesan itu sendiri menurut Onong Uchjana Effendy adalah merupakan terjemahan dari bahasa asing "*message*" yang artinya adalah lambang bermakna (*meaningful symbols*), yakni lambang yang membawakan pikiran atau perasaan komunikator [6].

2.4 Chatting

Chatting secara umum adalah aktivitas berkomunikasi yang dilakukan oleh dua orang atau lebih dengan memanfaatkan aplikasi chatting dan jaringan internet. Aplikasi chatting saat ini sudah sangat maju. Tidak hanya mengirim pesan teks saja, aktivitas chatting sekarang ini juga bisa mengirimkan emoticon, pesan suara, bahkan video. Chatting merupakan salah fitur dari kecanggihan teknologi informasi saat ini. Mulai dari anak kecil hingga orang dewasa saat ini sudah familiar dengan istilah chatting. Singkatnya, pengertian chatting adalah suatu program yang melibatkan koneksi internet untuk saling bertukar pesan antar satu orang dengan orang lain. Chatting adalah bentuk komunikasi yang paling efektif dan efisien sata ini[7].

2.5 Algoritma Response Challenge

Sandi yang diciptakan oleh Bruce Schneier semata-mata untuk novel fiksi Newton, Cryptonomicon. Bruce Schneier memiliki latar belakang yang kuat dalam memahami dan membuat kode dan sandi, karena profesinya adalah konsultan keamanan. Dia menciptakan cipher hanya untuk novel, dan itu tidak digunakan untuk aplikasi kata nyata. Cipher menggunakan 52 kartu remi dan 2 pelawak; itu juga tidak ada hubungannya dengan permainan kartu Solitaire. Schneier menggunakan kartu dan urutan penyusunan ulang sebagai cara untuk membuat aliran kunci untuk mengenkripsi pesan. Semakin besar panjang kunci membuatnya sulit untuk memecahkan sandi ini. Karena itu, para ahli mengatakan bahwa sulit bagi penyerang untuk mendekripsi [1].

Algoritma untuk menghasilkan kunci untuk proses enkripsi dan dekripsi terdiri dari enam langkah. Enam tahap ini akan menghasilkan sebuah angka yang merupakan salah satu bagian aliran kunci. Berikut adalah proses enkripsi dekripsi dengan menggunakan algoritma menggunakan *Response Challenge*:

a. Bilangan prima yang diambil harus lebih besar dari plainteks (p > m).
b. Ambil eA :
   1. $2 < eA < p - 1$ (1)

Jurnal Sains Dan Teknologi Informasi
Vol 1, No 2, Maret 2022, Hal 49-53
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v1i2.1442
Website https://ejurnal.seminar-id.com/index.php/jussi

2. GCD (eA , p-1) = 1 (2)

c. Hitung $dA \equiv eA^{-1} \pmod{p-1}$ (3)

d. Hitung $C_1 = m^{eA} \bmod p$ (4)

e. Kirim C_1 ke penerima

f. Penerima menerima C_1

g. Ambil eB :
   1. $2 < eB < p-1$ (5)
   2. GCD (eB, p-1) = 1 (6)

h. Hitung $dB \equiv eB^{-1} \pmod{p-1}$ (7)

i. Hitung $C_2 = C_1^{eB} \bmod p$ (8)

j. Kirim C_2 ke pengirim

k. Pengirim menerima C_2

l. Hitung $C_3 = C_2^{dA} \bmod p$ (9)

m. Kirim C_3 ke penerima

n. Penerima menerima C3

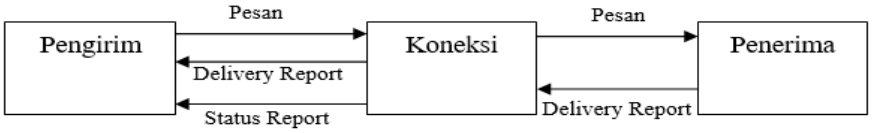
o. Hitung $m = C_3^{dB} \bmod p$ (10)

3. HASIL DAN PEMBAHASAN

3.1 Pembahasan

Timbulnya kejahatan-kejahatan dalam pengiriman pesan *chatt* tentu saja memicu para pakar teknologi informasi untuk meningkatkan keamanan dalam pertukaran informasi. Beberapa penerapan sistem kriptografi sebagai sistem pengaman data antara lain, meningkatkan keamanan informasi dalam sistem berbasis pada kriptografi kunci publik. Hal ini sangat rentan dengan terjadinya kecurangan yang dapat dilakukan oleh pihak–pihak yang tidak bertanggung jawab. Karena data tersebut dapat dengan mudah dimanipulasi karena tidak ada sistem yang dapat mengamankan data tersebut.

Menerapkan sistem enkripsi pada proses *chat* yang dilakukan untuk mencegah terjadinya penyadapan dan kecurangan. Dalam pengamanan pesan *chat* ini dilakukan dilakukan proses enkripsi dan dekripsi dengan menggunakan metode *response challenge*. Dalam prosedur mekanisme pada proses chating pengirim pesan melakukan koneksi ke penerima pesan dengan menggunakan media seperti Nirkabel atau kabel setelah koneksi terhubung maka penerima pesan mengirimkan pesan setelah terkirim selanjutnya pesan dapat diterima oleh penerima pesan.



Gambar 1. Mekanisme Proses Chatting

3.2 Penerapan Metode Response Challenge

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 sebagai berikut :

a. 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 :
   1. pilih sebuah bilangan a dimana $1 < a < 101$.
   2. misalkan nilai *random* yang terpilih untuk nilai a adalah 2.
   3. Hitung nilai L (*Legendre*), dimana $L \equiv a^{(p-1)/2} \bmod p$, dimana p = 101.

      $L \equiv a^{(p-1)/2} \bmod p$
      $\equiv 2^{(101-1)/2} \bmod 101$
      $\equiv 2^{50} \bmod 101$
      $\equiv 1125899906842624 \bmod 101 \equiv -1$
   4. Dikarenakan 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

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

Jurnal Sains Dan Teknologi Informasi
Vol 1, No 2, Maret 2022, Hal 49-53
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v1i2.1442
Website https://ejurnal.seminar-id.com/index.php/jussi

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

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

$\equiv 717897987691852588770249 \bmod 101 \equiv -1$

A = 4, maka

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

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

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

$\equiv 1267650600228224014967032053 76 \bmod 101 \equiv 1$

Maka benar bahwa 101 merupakan bilangan prima.

b. Enkripsi pesan dengan menggunakan algoritma response challange.
Karakter "F" dalam ASCII bernilai 73,
Karakter "A" dalam ASCII bernilai 76,
Karakter "J" dalam ASCII bernilai 75,
Karakter "A" dalam ASCII bernilai 79,
Karakter "R" 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 "FAJAR" setelah dienkripsi dengan response challenge menjadi "59 77 11 19 47". Cipherteks ini kemudian dikirim ke B.

Setelah B menerimam 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 :

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

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

Jurnal Sains Dan Teknologi Informasi
Vol 1, No 2, Maret 2022, Hal 49-53
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v1i2.1442
Website https://ejurnal.seminar-id.com/index.php/jussi

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

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

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

Nilai 73 dalam kode ASCII adalah karakter F
Nilai 76 dalam kode ASCII adalah karakter A
Nilai 75 dalam kode ASCII adalah karakter J
Nilai 79 dalam kode ASCII adalah karakter A
Nilai 77 dalam kode ASCII adalah karakter R
Setelah B mendekripsi pesan tersebut, maka diketahuilah bahwa pesan yang dikirim oleh A adalah "FAJAR".

4. KESIMPULAN

Kesimpulan yang dapat diambil setelah melakukan hasil dan pembahasan dari pengamanan pesan chatt dengan menerapkan algoritma metode *response challenge*. Algoritma Challenge Response dapat mengamankan pesan chatt dengan aman sampai ke penerima pesan. Dalam proses enkripsi dan dekripsi meminimalkan memory dapat memaksimalkan proses, selain itu kapasitas file plaintext sama dengan kapasitas ciphertext sehingga dapat dijadikan otentikasi data.

REFERENCES

[1] Bambang Soelistijanto, 2010, Implementasi Authentifikasi Client Dengan Metode Challenge Response Pada Transaksi Perbankan Elektronik, Seminar Nasional Informatika, ISSN : 1979-2328
[2] Zulfikar, iqbal.M, 2019, Kriptografi Untuk Keamanan Pengiriman Email Menggunakan Blowfish dan Rivest Shamir Adleman (RSA), SNATI, ISSN : 1907-5022
[3] SB Sinaga, 2018, Pengamanan Pesan Komunikasi Menggunakan Algoritma RSA, Rabbin Miller dan Fungsi SHA-1 Serta Penanganan Man In The Middle Attact Dengan Interlock Protocol, Jurnal Teknik Informatika Santo Thomas (JTIUST), Vol. 03, No.01, ISSN : 2548-1916.
[4] Sianipar, R.H, 2016, "Kompilasi Proyek Kriptografi Dengan Visual Basic.Net". Edisi Pertama, Andi Publishier
[5] Sadikin, Rifki, 2012, "Kriptografi Untuk Keamanan Jaringan", Penerbit Andi, Yogyakarta.
[6] Sianipar, R.H, 2017, "Java Untuk Kriptografi, Andi, Yogyakarta.
[7] http://www.e-jurnal.com/2014/02/pengertian-pesan.html, diakses tanggal 6 Mei 2020
[8] https://www.maxmanroe.com/vid/teknologi/pengertian-chatting.html,diakses tanggal 6 Mei 2020..