2nd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
21 Maret 2023 – Jakarta, Indonesia
Volume 2, Nomor 1, April 2023 - ISSN 2962-8628 (*online*)

SISTEM KEAMANAN PESAN TEKS *WEB-BASED* MENGGUNAKAN RSA PADA UNIT PELAYANAN PEMUNGUTAN PAJAK TAMBORA

Agus Setiawan[1*], Ferdiansyah[2], Pipin Farida Ariyani[3], Siswanto[4]

[1,2,3,4] Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, DKI Jakarta, Indonesia

Email: [1*]1911520227@student.budiluhur.ac.id, [2]ferdiansyah@budiluhur.ac.id, [3]pipin.faridaariyani@budiluhur.ac.id, [4]siswanto@budiluhur.ac.id
(*: corresponding author)

Abstrak-Salah satu aspek yang menjadi perhatian khusus dalam pertukaran informasi adalah aspek keamanan dan kerahasiaan suatu pesan komunikasi. Dalam melakukan komunikasi terkait percakapan yang dilakukan secara virtual para pegawai Unit Pelayanan Pemungutan Pajak Daerah Tambora masih menggunakan platform aplikasi WhatsApp walaupun aplikasi tersebut mengusung fitur enkripsi end-to-end, namun WhatsApp tetap saja mengurangi efisiensi keamanan serta hal yang berifat privasi pada penggunanya saat melakukan komunikasi virtual yang terjadi secara terus menerus setiap harinya karena sudah jelas server atau pusat data WhatsApp dimiliki pihak luar (eksternal). Sudah saatnya hal ini mendapat perhatian khusus untuk melakukan pengembangan sistem dalam hal komunikasi virtual yang berkaitan dengan ruang lingkup perusahaan agar setiap terjadinya pertukaran informasi data baik itu pesan percakapan yang bersifat teks yang dianggap penting hanya dapat diketahui oleh pihak-pihak internal yang terdapat pada ruang lingkup perusahaan. Untuk itu dibutuhkan algoritma dalam penerapan proses percakapan berbasis teks terenkripsi yang akan dilakukan. Salah satu metode algoritma kriptografi yang banyak digunakan adalah RSA. Metode algoritma RSA ini dibuat serta diperkenalkan oleh Ron Rivest, Adi Shamir, dan Leonard Adleman pada tahun 1976. Menggunakan kunci pubik dan kunci privat untuk enkripsi dan dekripsi pesan. Tujuan penelitian menerapkan RSA sebagai metode algoritma ini tentu menjadi alasan dikarenakan RSA memiliki salah satu keunggulan yang terletak pada sulitnya memfaktorkan bilangan besar menjadi faktor-faktor prima. Sehingga memaksimalkan kebutuhan sistem pada hasil proses enkripsi yang berisikan pesan komunikasi berbasis teks yang mungkin bersifat rahasia dan pihak dari luar perusahaan tidak dapat membaca isi pesan tersebut dengan mudah. Penelitian ini melakukan data uji pada 4 (empat) plain teks dengan panjang masing-masing 25, 67, 38 dan 30. Kesimpulan dari penelitian ini adalah menghasilkan rata-rata waktu pada proses enkripsi sebesar 23 milisekon (ms) dan rata-rata waktu pada proses dekripsi sebesar 15,75 milisekon (ms).

Kata Kunci: Komunikasi, Keamanan Pesan Teks, Enkripsi, RSA.

WEB-BASED TEXT MESSAGE SECURITY SYSTEM USING RSA AT TAMBORA TAX COLLECTION SERVICE UNIT

Abstract- *One aspect that is of particular concern in the exchange of information is the security and confidentiality aspects of a communication message. In conducting communication related to virtual conversations, employees of the Tambora Regional Tax Collection Service Unit still use the WhatsApp application platform even though the application has end-to-end encryption features, but WhatsApp still reduces security efficiency and matters that are privacy in nature for its users when carrying out transactions. virtual communication that occurs continuously every day because the WhatsApp server or data center is owned by an external party (external). It is time for this to receive special attention to carry out system development in terms of virtual communication related to the scope of the company so that any exchange of data information, whether it is a text conversation message which is considered important, can only be known by internal parties contained in the scope company. For this reason, an algorithm is needed in implementing encrypted text-based conversation processes to be carried out. One of the widely used cryptographic algorithm methods is RSA. This RSA algorithm method was created and introduced by Ron Rivest, Adi Shamir, and Leonard Adleman in 1976. It uses public keys and private keys for message encryption and decryption. The aim of this research is to apply RSA as an algorithmic method. This is of course the reason because RSA has one of the advantages which lies in the difficulty of factoring large numbers into prime factors. So as to maximize system requirements on the results of the encryption process which contains text-based communication messages that may be confidential and parties from outside the company cannot easily read the contents of the message. This study conducted test data on 4 (four) plain texts with lengths of 25, 67, 38 and 30 respectively. The conclusion of this study was to produce an average time for the encryption process of 23 milliseconds (ms) and an average time for decryption process of 15.75 milliseconds (ms).*

Keywords*: Communications, Text Message Security, Encryption, RSA.*

1. PENDAHULUAN

Secara umum, bahwa "*Chatting*" digambarkan sebuah aktivitas berkomunikasi yang dilakukan oleh dua orang atau lebih dengan memanfaatkan aplikasi *chatting* dan jaringan internet [1]. Untuk itu, aktivitas dalam pertukaran informasi harus memenuhi aspek keamanan dan kerahasiaan suatu pesan komunikasi [2]. Dikarenakan kemungkinan yang dapat saja terjadi adalah orang tersebut menyadap media komunikasi yang

digunakan oleh kedua orang yang sedang berkomunikasi tersebut. Hal inilah yang disebut dengan *man-in-the-middle-attack*, dalam keadaan ini, orang yang menyadap tersebut dapat mengetahui semua informasi yang dikirimkan satu sama lain. Keadaan ini muncul karena kedua orang yang sedang berkomunikasi tersebut tidak dapat mem-verifikasi status dari orang yang berkomunikasi dengannya tersebut hingga menjadikannya asumsi bahwa proses penyadapan tersebut tidak menyebabkan gangguan dalam jaringan [3] [4].

Sudah saatnya pihak Unit Pelayanan Pemungutan Pajak Daerah Tambora melakukan pengembangan sistem dalam hal pengamanan file *database* yang berfokus pada bentuk komunikasi virtual agar dalam pertukaran informasi data baik itu pesan percakapan yang bersifat teks yang dianggap penting (privasi) hanya dapat diketahui oleh pihak-pihak yang terdapat pada ruang lingkup Unit Pelayanan Pemungutan Pajak Daerah Tambora dikarenakan sejauh ini komunikasi terkait bentuk percakapan dan data-data pengiriman file komunikasi masih menggunakan platform aplikasi *WhatsApp*, sedangkan *WhatsApp* itu sendiri *server* atau pusat datanya dimiliki pihak luar yang mungkin saja mengurangi efisiensi keamanan dan privasi pada proses komunikasi.

Sebagai contoh ada dua karakter yaitu pengirim S dan penerima R dan pihak lain adalah L. Tujuan kriptografi adalah agar informasi yang dikirim S hanya bisa diterima R, walaupun L juga memungkinkan melihat pesan yang dikirim tetapi informasi didalamnya tidak bisa dibaca oleh L. Hal ini dilakukan dengan mengenkripsi *plaintext* menjadi *ciphertext*. "*Plaintext* adalah pesan informasi yang dapat dibaca" sedangkan "Enkripsi adalah teknik yang digunakan untuk membuat pesan menjadi tidak bisa dibaca atau disebut *ciphertext*" [5].

Salah satu algoritma kriptografi yang banyak digunakan adalah RSA. Algoritma RSA dibuat oleh Ron Rivest, Adi Shamir, dan Leonard Adleman pada tahun 1976. Menggunakan kunci pubik dan kunci privat untuk enkripsi dan dekripsi pesan [6]. Salah satu keunggulan metode algortima RSA terletak pada sulitnya memfaktorkan bilangan besar menjadi faktor-faktor prima [7] .

Rujukan penelitian ini berdasarkan literatur dari beberapa penelitian-penelitian yang telah ada sebelumnya khususnya pada implementasi sistem yang telah dibuat. Salah satu penelitian pada tahun 2020 yang berjudul "Implementasi Kriptografi Untuk Keamanan File Teks Dengan Menggunakan Metode MD5", dimana sistem yang dibangun masih menggunakan aplikasi berbasis desktop serta kekurangan pada algoritma yang digunakan yaitu MD5 cenderung rentan terhadap serangan *collision* yaitu suatu peristiwa di mana dua nilai yang berbeda dapat memiliki nilai hash yang sama [8]. Berikutnya, penelitian tahun 2021 berjudul "Penerapan Algoritma *Rivest Shamir Adleman* (RSA) Untuk Mengamankan *Database* Program Keluarga Harapan (PKH)" dengan menganalisa salah satu kekurangan yang terdapat pada penelitian ini yaitu sistem yang dibuat masih berbasis desktop dan perlu ada instalasi atau konfigurasi pada setiap komputer yang akan menggunakan aplikasi tersebut [9]. Penelitian berikutnya pada tahun 2022 berjudul "Implementasi Metode *Rivest Shamir Adleman* untuk Enkripsi dan Dekripsi *Text*" yang kekurangannya pun juga masih sama dalam mengimplementasikan aplikasinya masih berbasis desktop menggunakan Visual Basic 2010 [10].

Atas dasar hal tersebut diatas dalam penelitian yang akan dilakukan ini akan mengembangkan sebuah aplikasi komunikasi antar pengguna (*chatting*) dalam proses pengamanan file pesan berbasis teks yang terkirim ke *database* yang kemudian penelitian ini diberi judul "Sistem Keamanan Pesan Teks Berbasis *Web* Menggunakan Algoritma RSA Pada Unit Pelayanan Pemungutan Pajak Daerah Tambora".

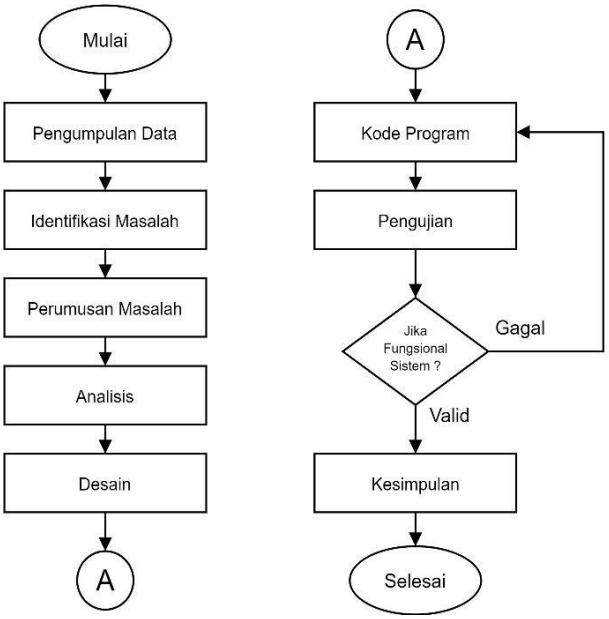
2. METODE PENELITIAN

2.1 Data Sumber Penelitian

Data sumber yang digunakan pada penelitian ini berupa *screenshot* dalam format file .jpeg tentang data-data obrolan atau komunikasi para pegawai via *chat WhatsApp* yang menjadi rutinitas sehari-hari para pegawai dalam ruang lingkup perusahaan pada saat melakukan komunikasi virtual (*chatting*) dari proses mengirim dan menerima pesan. Pesan itu berupa pesan obrolan dalam format teks yang berlangsung di kantor Unit Pelayanan Pemungutan Pajak Daerah Tambora baik itu pesan teks yang bersifat privasi atau umum berkaitan dengan internal atau ruang lingkup perusahaan.

2.2 Tahapan Penelitian

Pada Gambar 1 di bawah ini memberikan gambaran terkait tahapan penelitian dari awal hingga akhir yang telah digambarkan pada skema berikut ini.



Gambar 1. Tahapan Metode Penelitian

Berikut akan dipaparkan secara detail tentang tahapan dari metode penelitian yang terdapat pada Gambar 1 di atas, yaitu:

a. Pengumpulan Data

Tahapan ini terbagi menjadi 3 (tiga) bagian, yaitu tahap berupa tinjauan lapangan, tinjauan pustaka referensi dan tinjauan studi penelitian sebagai berikut.

1. Tinjauan Lapangan

   Pada tahapan ini akan dilakukannya pengamatan langsung terkait proses kerja para pegawai yang terjadi pada Unit Pelayanan Pemungutan Pajak Daerah Tambora, dimana rutinitas pegawai dalam melakukan komunikasi virtual (*chatting*) saat proses mengirim dan menerima pesan. Pesan itu berupa pesan obrolan dalam format teks yang nantinya pesan tersebut akan terkirim ke *database* dan telah otomatis terenkripsi untuk mengamankan data pesan tersebut.

2. Tinjauan Pustaka Referensi

   Tahapan ini akan dilakukannya pengumpulan data pustaka yang bersumber dari buku-buku maupun kajian jurnal berlisensi untuk mendapatkan referensi yang bersifat teori.

3. Tinjauan Studi Penelitian

   Tahapan ini akan dilakukannya studi banding atas tinjauan penelitian terdahulu yang telah dilakukan terhadap tema penelitian yang sedang dilakukan saat ini tentang konsep penerapan algoritma RSA (*Rivest Shamir Adleman*) yang bertujuan agar ditemukannya sisi pembeda terhadap penelitian terdahulu.

b. Identifikasi Masalah

Tahapan ini akan dilakukannya identifikasi hal-hal apa saja yang ditemukan terhadap hasil dari tinjauan lapangan sehingga dapat menemukan masalah apa saja yang terjadi untuk selanjutnya menemukan solusi dari permasalahan tersebut.

c. Perumusan Masalah

Tahapan ini akan dilakukannya proses merangkum hasil dari tinjauan lapangan beserta identifikasi masalah yang telah dijabarkan pada studi kasus terkait yang diangkat untuk menentukan hasil nantinya di akhir penelitian.

d. Analisis

Tahapan ini akan dilakukannya proses analisis secara berurutan, mulai dari analisis data masukan, analisis penerapan algoritma dan analisis terhadap sistem keluaran yang akan dibangun sebagai berikut.

1. Analisis Data Masukan (*Input*)

   Tahapan ini akan melakukan analisis data masukan terkait file masukan berupa obrolan (*chat*) berupa format teks yang dikirimkan antar pengguna pada aplikasi.

2. Analisis Penerapan Algoritma
   Tahapan ini melakukan proses kerja penerapan algoritma RSA saat proses enkripsi pesan obrolan (*chat*) para pengguna (*user*) saat menggunakan aplikasi ini. Ruang obrolan ini akan saling bertukar informasi baik mengobrol dalam format teks.
3. Analisis Data Keluaran (*Output*)
   Tahapan ini merupakan tahap untuk melakukan pengamanan pada *database* sistem, dimana data-data riwayat *chat* para pegawai satu dengan yang lainnya berupa isi pesan dalam format teks yang telah terkirim ke MySQL *Database Mangement* dan telah melalui proses enkripsi.

e. Desain
Tahapan ini menggambarkan desain dari perangkat lunak yang akan dibangun berupa *web system cryptography*. Untuk itu, perlu menggambarkan beberapa perancangan, seperti: rancangan UML dan rancangan UI (*User Interface*). Perlu adanya UML agar dapat memberikan bahasa pemodelan visual atau gambar kepada para pengguna dari berbagai macam pemrograman maupun proses umum rekayasa. Menyatukan informasi-informasi terbaik yang ada dalam pemodelan.

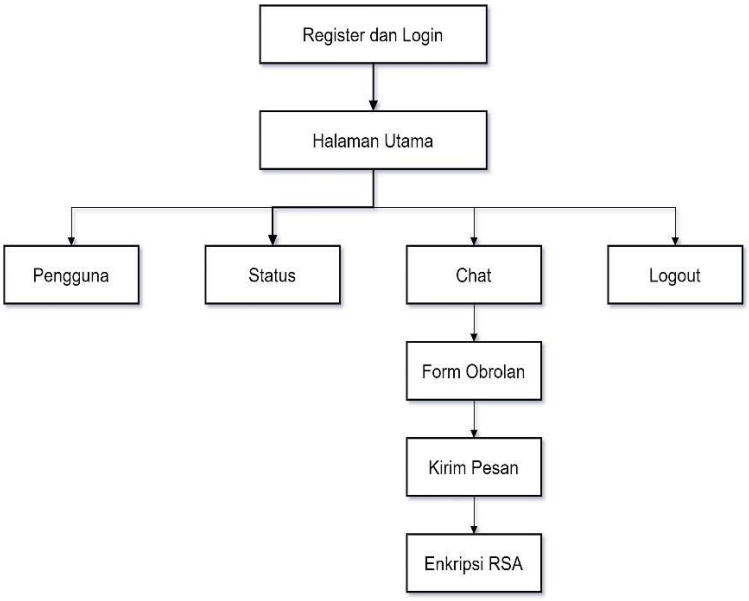
f. Pembuatan Kode Program
Tahapan ini merupakan suatu bentuk kegiatan yang merupakan rangkaian lanjutan dari kegiatan desain dan perancangan perangkat lunak. Implementasi program dimaksudkan sebagai usaha untuk mewujudkan hasil dari perancangan perangkat lunak. Program yang dibuat dan diuji akan mengimplementasikan bahasa pemrograman PHP dan HTML.

g. Pengujian
Tahapan ini penulis melakukan pengujian terhadap sistem agar memastikan sistem telah valid dan telah sesuai dengan konsep yang dan tujuan yang diharapkan. Pengujian akan dilakukan dari sisi fungsional sistem dengan menggunakan teknik pengujian *black box*.

h. Kesimpulan
Tahap ini merupakan bagian dari penutup penelitian yang menjelaskan hasil penelitian yang telah dilakukan beserta dengan hasilnya. Kemudian akan dilengkapi juga dengan saran untuk menyempurnakan hasil penelitian tersebut.

2.3 Rancangan Struktur Menu

Rancangan struktur menu menyediakan suatu struktur guna memahami fungsi-fungsi dari sistem serta untuk lebih menekankan fungsi-fungsi yang harus diselesaikan oleh program, bukannya menunjukkan statement- statement program yang digunakan untuk melaksanakan fungsi tersebut. Tahap ini bagian paling penting dalam pengembangan sistem untuk dapat menjadi sebuah sistem. Karena struktur menu ini adalah alur bagaimana *input*, proses dan *output* itu berjalan secara tersistematis. Berikut rancangan struktur menu pada sistem diperlihatkan Gambar 2 dibawah ini.



Gambar 2. Rancangan Struktur Menu Pada Aplikasi

3. HASIL DAN PEMBAHASAN

Algoritma pada program merupakan deskripsi proses untuk mengerjakan sesuatu yang disusun dalam sederet aksi. Secara sederhana, prinsip kerja algoritma terbagi menjadi, masukan (*input*), proses dan keluaran (*output*).

3.1 Algoritma Proses Enkripsi Pesan Teks

Algoritma proses enkripsi RSA menjelaskan bagaimana alur dari proses atau cara kerja dari implementasi sistem yang telah dibuat sebagai berikut ini. Inti dari proses enkripsi adalah perhitungan $c = m^e \ mod \ n$ dimana c, m dan n dalam bilangan bulat positif dan e yang telah direpresentasikan dalam biner. Proses pengubahan tiap karakter pesan dari bentuk text kedalam bentuk bilangan bulat positif sangat diperlukan.

Algoritma Enkripsi RSA
Input $K_{publik} = (e,n)$, m € Z_n
Output $c = m^e \bmod n$

Gambar 3. Algoritma Enkripsi RSA

3.2 Algoritma Proses Deskripsi Pesan Teks

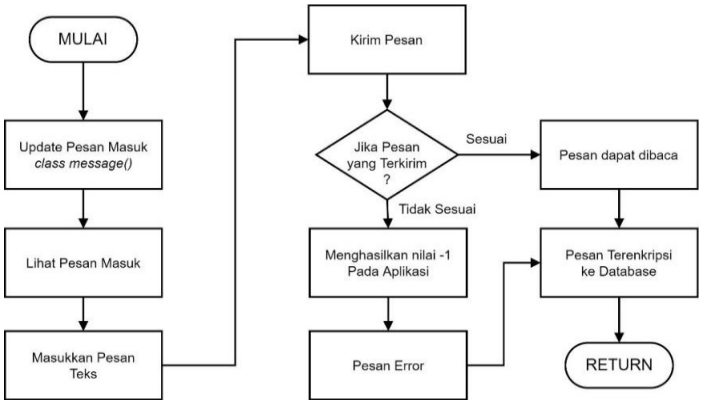
Dalam proses dekripsi yang menjadi intinya adalah perhitungan $m = c^d \ mod \ n$ dimana c, m dan n dalam bilangan bulat positif dan d yang telah direpresentasikan dalam bentuk biner. Proses yang digunakan dalam pesan adalah mengembalikan nilai m yang semula dalam bentuk text (*plaintext*) menjadi m ke bentuk bilangan bulat (*ciphertext*). Dengan kata lain proses ini adalah invers hasil dari proses enkripsi pada pesan tersebut.

Algoritma Dekripsi RSA
Input $K_{privat} = d$, $K_{publik} = (e,n)$, c € Z_n
Output $m = c^d \bmod n$

Gambar 4. Algoritma Dekripsi RSA

3.3 *Flowchart*

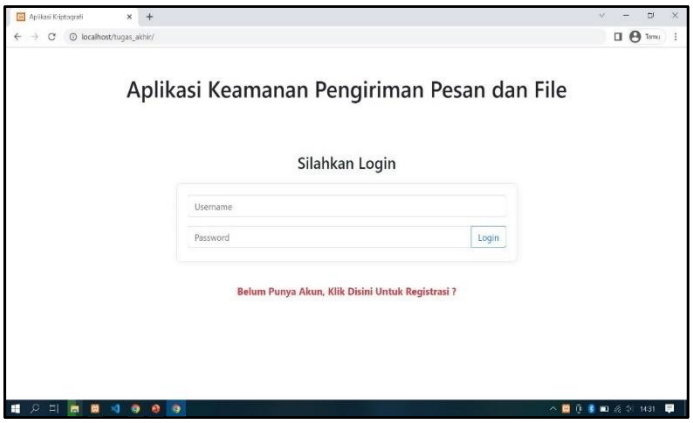
Apabila akan mengirim pesan yang pertama kali dilakukan adalah menulis pesan kepada pengguna, kemudian setelah itu sistem akan melakukan proses enkripsi dari pengiriman pesan akan yang telah disandikan serta mengirimkan kunci D dan kunci N yang telah diset pada program. Pada saat adanya pesan sandi yang masuk, maka terdapat list-list pesan dalam bentuk *ListView* atau *Array*. Kemudian setelah pesan yang diterima masuk pada *chat box dan* terkirim ke *database*, maka langkah selanjutnya menampilkan pesan yang tersandikan oleh proses enkripsi yang kemudian pesan asli hanya dapat dilihat pada *chat box* setelah proses otomatis sistem pada program memebrikan perintah memasukkan kunci-kunci yang diperlukan.



Gambar 5. *Flowchart* Cara Kerja Aplikasi

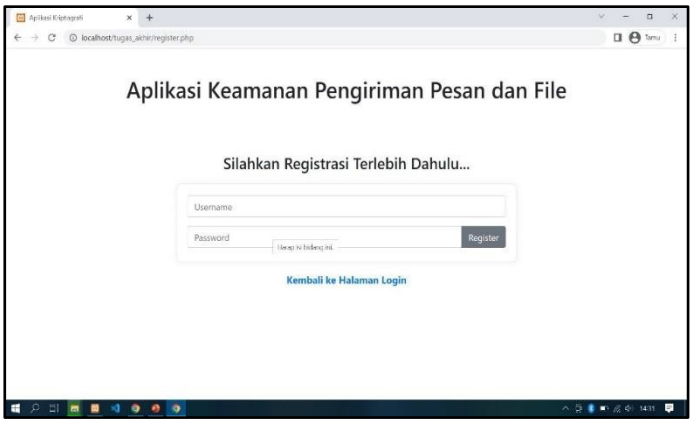
3.4 Rancangan Aplikasi

Pada hasil rancangan aplikasi berbasis *web* akan memuat tampilan layar dari sistem yang telah dibuat menggunakan pemrograman php dan html. Berikut ini akan diberikan penjelasan gambar mengenai tampilan- tampilan yang ada pada aplikasi ini.



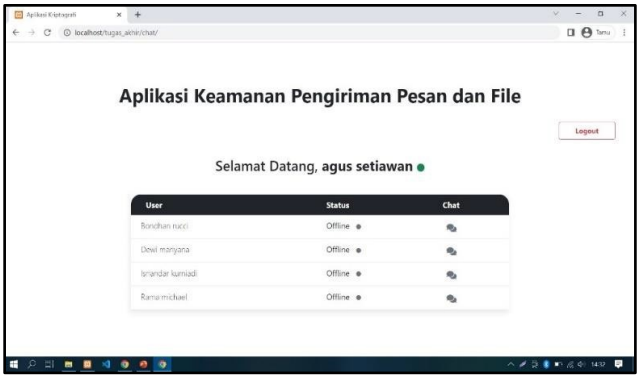
Gambar 6. Halaman Login *User*

Pada Gambar 8 diatas merupakan halaman *login* halaman *login* pengguna pada aplikasi menampilkan halaman dimana terdapat kolom *username* dan *password* yang harus di-*input* untuk dapat mengakses ke halaman utama sistem.



Gambar 7. Halaman Registrasi *User* Baru

Pada Gambar 9 diatas merupakan halaman aplikasi pendaftaran *user* atau register diharuskan untuk mengisi data *user* terlebih dahulu dengan mengisi *username* dan *password* untuk dapat akses *login* awal aplikasi.

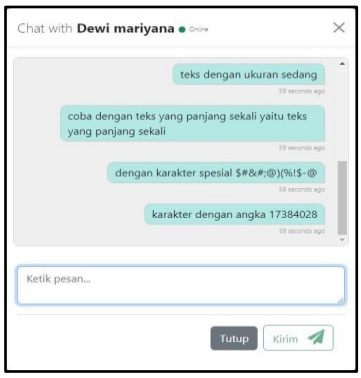


Gambar 8. Halaman Utama Aplikasi Pengguna Dalam Status *Offline*

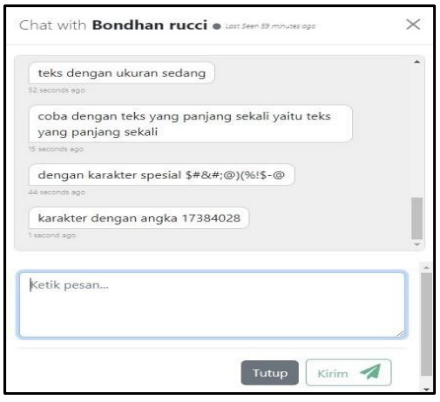
Pada Gambar 10 diatas merupakan halaman utama aplikasi pengguna dalam status *offline* yang ditandai pada indikator atau notifikasi status icon berwarna abu-abu (*grey*) disamping tulisan keterangan "*offline*".

Gambar 9. Halaman Utama Aplikasi Pengguna Dalam Status *Online*

Pada Gambar 11 diatas merupakan halaman utama aplikasi pengguna dalam status *online* yang ditandai pada indikator atau notifikasi status icon berwarna hijau (*green*) disamping tulisan keterangan "*online*" yang dapat dilihat bahwa *icon chatting* pun menampilkan warna biru pada layar aplikasi yang berarti memberikan keterangan bahwa antar pengguna dapat saling mengirimkan pesan dan untuk tampilan pada layar aplikasi *chatting* saat masing-masing pengguna mengirim dan menerima pesan ditujukkan pada Gambar 12 dan Gambar 13 dibawah ini.



Gambar 10. Tampilan Aplikasi Proses Mengirim Pesan Format Teks



Gambar 11. Tampilan Aplikasi Proses Menerima Pesan Format Teks

3.5 Pengumpulan Data Uji

Pengumpulan data teks berupa pesan yang dikirim antar pengguna yang akan di lakukan sebagai salah satu variabel dalam proses pengujian enkripsi dan dekripsi dapat dilihat pada Tabel 1

Tabel 1. Data Teks Yang Akan Diuji

No	Data Pesan Teks	Panjang Teks
1	teks dengan ukuran sedang	25
2	coba dengan teks yang panjang sekali yaitu teks yang panjang sekali	67
3	dengan karakter spesial $#&#;@)(%!$-@	38
4	karakter dengan angka 17384028	30

Dalam pengujian setiap proses dicatat pada log aplikasi yang diperlihatkan pada Tabel 2, berdasarkan log ini maka diketahui variabel yang akan diuji. Variabel tersebut, antara lain:

a. *Plaintext:* Yaitu teks yang akan di enkripsi, teks ini di dapat berdasarkan masukkan data dari user.
b. Panjang *Plaintext:* Yaitu banyaknya karakter pada teks.
c. Waktu Enkripsi: Waktu enkripsi di dapatkan dengan mencatat log sebelum dan setelah proses enkripsi, selisih dari kedua waktu yang dicatat ini yang di jadikan acuan sebagai waktu enkripsi.
d. Panjang *Ciphertext:* Adalah proses enkripsi dalam satuan bit.
e. *Ciphertext:* Yaitu hasil dari proses enkripsi pada *plaintext*.
f. Waktu Dekripsi: Adalah waktu yang di butuhkan untuk proses dekripsi. Seperti waktu enkripsi, waktu dekripsi didapatkan dari selisih waktu pada saat mulai proses dekripsi sampai dengan selesai proses dekripsi.

Tabel 2. Hasil Pengujian Waktu Enkripsi dan Dekripsi Teks

No	*Plaintext*	Panjang *Plaintext*	Waktu Enkripsi	*Ciphertext*	Panjang *Ciphertext*	Waktu Dekripsi	Hasil Dekripsi
1	teks dengan ukuran sedang	25	23 ms	8 bit	140021448101545521013211287611 127624481026153132481114589261 531287611679771545521679772273 791145892615312876110132144810 11276211458926153132481	11 ms	teks dengan ukuran sedang
2	coba dengan teks yang panjang sekali yaitu teks yang panjang sekali	67	23 ms	8 bit	297041831465915958311417348 512968234451595896823114986 051210203144123114260315958 968234453114149551595896821 510115958968234453114144125 121020315958385969173114260 315958691798601426931149860 512102031441231142603159589 682344531141495515958968215 101159589682344531141441251 2102031595838596917	18 ms	coba dengan teks yang panjang sekali yaitu teks yang panjang sekali
3	dengan karakter spesial $#&#;@)(%!$-@	38	29 ms	8 bit	565517877112337987872311233 146891375087231714587231375 061021787717145146892239128 451787722395698723122611468 910498671763567176510903814 684976314495178581049873090 38	19 ms	dengan karakter spesial $#&#;@)(%!$-@
4	karakter dengan angka 17384028	30	17 ms	8 bit	184015131902180259131902184 015259611249530180259327682 192292495302971551699131902 297153276813190229715516991 840151319023276811764916637 513265117561614060811059212 5000175616	15 ms	karakter dengan angka 17384028

3.6 Hasil Pengujian

Perbandingan panjang teks dengan, waktu enkripsi serta waktu dekripsi.

Tabel 3. Perbandingan Hasil Pengujian

Keterangan	Pengujian Nomor			
	1	2	3	4
Panjang Teks	25	67	38	30
Waktu Enkripsi (ms)	23	23	29	17
Waktu Dekripsi (ms)	11	18	19	15

Rata-rata Nilai rata-rata dihitung hanya pada sampel yang berhasil dilakukan enkripsi dan dekripsi:
N = 4

Rata-rata panjang teks $= \frac{\sum Panjang\ Teks}{N}$
$= \frac{25+67+38+30}{4}$
= 40 ms

Rata-rata waktu enkripsi $= \frac{\sum Panjang\ Teks}{N}$
$= \frac{23+23+29+17}{4}$
= 23 ms

Rata-rata waktu dekripsi $= \frac{\sum Panjang\ Teks}{N}$
$= \frac{11+18+19+15}{4}$
= 15,75 ms

4. KESIMPULAN

Dari hasil penelitian yang telah dilakukan dalam mengimplementasikan Sistem Keamanan Pesan Teks Terenkripsi Menggunakan Metode Algoritma RSA Pada Unit Pelayanan Pemungutan Pajak Daerah Tambora Berbasis Web mendapatkan kesimpulan bahwa penelitian ini melakukan data uji pada 4 (empat) plain teks dengan panjang masing-masing *plaintext* 25, 67, 38 dan 30. Kesimpulan dari penelitian ini adalah menghasilkan rata-rata waktu pada proses enkripsi sebesar 23 milisekon (ms) dan rata-rata waktu pada proses dekripsi sebesar 15,75 milisekon (ms).

DAFTAR PUSTAKA

[1] M. F. Bahari, "Analisa Dan Implementasi Keamanan Pesan Chatting Menggunakan Algoritma Challenge Response," *JUSSI J. Sains Dan Teknol. Inf.*, vol. 1, no. 2, pp. 49–53, 2022.

[2] M. K. Harahap and Rina, "Kombinasi Kriptografi RSA dengan Linear Congruential Generator," *Sink. (Jurnal Penelit. Tek. Inform.*, vol. 3, no. 1, pp. 267–271, 2018, doi: 10.33395/sinkron.v3i1.211.

[3] S. B. Sinaga, "Pengamanan Pesan Komunikasi Menggunakan Algoritma Rsa, Rabbin Miller Dan Fungsi Sha-1 Serta Penanganan Man In The Middle Attack Dengan Interlock …," *J. Tek. Inform. UNIKA St. Thomas*, vol. 03, pp. 64–71, 2018, [Online]. Available: http://103.76.21.184/index.php/JTIUST/article/view/248%0Ahttp://103.76.21.184/index.php/JTIUST/article/download/248/266

[4] I. Putra Sinaga, "Implementasi Kriptografi Hybrid Algoritma Elgamal Dan Double Playfair Cipher Dalam Pengamanan File Jpeg Berbasis Dekstop," *J. Informatics, Electr. Electron. Eng.*, vol. 1, no. 2, pp. 67–74, 2021, [Online]. Available: https://djournals.com/jieeeJIEEE,

[5] N. Sinaga, S. Aini, and B. Gulo, "Penerapan Algoritma Skipjack Untuk Menyandikan Short Message Service," *J-SAKTI (Jurnal Sains Komput. dan Inform.*, vol. 02, no. 01, pp. 33–46, 2018, doi: 10.30645/j-sakti.v2i1.54.

[6] D. Apdilah and H. Swanda, "Penerapan Kriptografi RSA Dalam Mengamankan File Teks Berbasis PHP," *J. Teknol. Inf.*, vol. 2, no.1, pp. 45–52, 2018, doi: 10.36294/jurti.v2i1.407.

[7] A. Aziz, "Aplikasi Keamanan Data Multimedia Message Service (MMS) Pada Microsoft Office File Memanfaatkan Algoritma Rivest-Shamir Adleman (RSA) Dan Blowfish Berbasis Android," *J. Ilmu-ilmu Inform. dan Manaj. STMIK*, vol. 14, no. 2, pp. 144– 153, 2020.

[8] A. Z. F. Rangkuti and H. Fahmi, "Implementasi Kriptografi Untuk Keamanan File Text Dengan Menggunakan Metode MD5," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 3, no. 2, pp. 170–175, 2020, doi: 10.32672/jnkti.v3i2.2384.

[9] A. Cahya Putra, M. Simanjuntak, and Nurhayati, "Penerapan Algoritma Rivest Shamir Adleman (RSA) Untuk Mengamankan Database Program Keluarga Harapan (PKH)," *J. Tek. Inform. Kaputama*, vol. 5, no. 1, pp. 76–84, 2021.

[10] Fatonah, D. I. Mulyana, A. P. Heryani, and V. Khoirunnisa, "Implementasi Metode Rivest Shamir Adleman untuk Enkripsi dan Dekripsi Text," *J. Inform. dan Teknol. Komput. (J-ICOM)*, vol. 3, no. 1, pp. 32–39, 2022, doi: 10.33059/j-icom.v3i1.4990.