Jurnal Ilmiah Informatika dan Komputer Surya Intan (JIIKSI)
Volume 8 Nomor 1 Tahun 2021
ISSN: 2354-9157

METODE *KRIPTOGRAFI CAESAR CHIPER* PADA APLIKASI *CHATTING* BERBASIS *LOCAL AREA NETWORK* (STUDI KASUS STMIK SURYA INTAN KOTABUMI)

M. Abu Jihad Plaza R, S.Kom., M.T.I[1], Muhammad Ishak[2]
Program Studi Teknik Informatika
STMIK Surya Intan Kotabumi
Jl. Ibrahim Syarief No. 107, Kotabumi, Lampung Utara
Abujihad83@gmail.com[1], m.ishak21@gmail.com[2]

Abstract

The communication process always happens all the time. Various communication tools developed and used to support the achievement of the communication process. Various models of communication tools can be found, either in the form of physical (hardware) or in the form of applications (software). Interconnected computers allowing users to communicate with each other and share information.

In practice, computer network users are often faced with communication problems between users. The existence of such applications can support the successful use of a computer network within an agency.Chat application is used as a medium of communication among fellow computer users connected in a network, whether through text, image, or sound.

The built application uses the program aspect implemented into the Advanced Encryption Standard (AES) algorithm used as the standard cryptographic algorithm of Caesar Chiper. AES itself is a cryptographic algorithm by using a caesar chiper algorithm that can encrypt and decrypt data blocks. This software development is done in several stages of developer method, some of the stages, namely requirement analysis, system design, implementation, system testing and maintenance.

Keywords: Chat, Encryption, Decryption, Caesar Chiper

Abstrak

Proses komunikasi selalu terjadi setiap saat. Berbagai alat komunikasi dikembangkan dan digunakan untuk mendukung pencapaian proses komunikasi. Berbagai model alat komunikasi dapat ditemukan, baik dalam bentuk fisik (perangkat keras) maupun dalam bentuk aplikasi (perangkat lunak). Komputer yang saling berhubungan memungkinkan pengguna untuk berkomunikasi satu sama lain dan berbagi informasi.

Dalam prakteknya, pengguna jaringan komputer sering dihadapkan pada masalah komunikasi antar pengguna. Adanya aplikasi tersebut dapat mendukung keberhasilan penggunaan suatu jaringan komputer dalam suatu instansi.Aplikasi

chat digunakan sebagai media komunikasi antar sesama pengguna komputer yang terhubung dalam suatu jaringan, baik melalui teks, gambar, maupun suara.

Aplikasi yang dibangun menggunakan aspek program yang diimplementasikan ke dalam algoritma Advanced Encryption Standard (AES) yang digunakan sebagai algoritma kriptografi standar Caesar Chiper. AES sendiri merupakan algoritma kriptografi dengan menggunakan algoritma caesar chiper yang dapat mengenkripsi dan mendekripsi blok data. Pengembangan perangkat lunak ini dilakukan dalam beberapa tahapan metode pengembang, beberapa tahapan yaitu analisis kebutuhan, perancangan sistem, implementasi, pengujian sistem dan pemeliharaan.

Kata kunci: Obrolan, Enkripsi, Dekripsi, Caesar Chiper

1. PENDAHULUAN

Kriptografi merupakan salah satu teknik yang digunakan untuk meningkatkan aspek keamanan suatu informasi[1], dengan menggunakan teknik *Kriptografi Cesar Chiper*, proses yang dilakukan *kriptografiCaesar Cipher* sangat mudah untuk digunakan. Inti dari algoritma kriptografi ini adalah melakukan pergeseran terhadap semua karakter pada plainteks dengan nilai pergeseran yang sama, untuk mengamankan sebuah pesan (yang disebut *plaintext*) menjadi pesan yang tersembunyi (disebut *ciphertext*) adalah enkripsi (*encryption*)[2][3]. Proses sebaliknya, untuk mengubah *ciphertext* menjadi *plaintext*, disebut dekripsi.Prosedur enkripsi sangat bervariasi tergantung pada kunci yang akan mengubah rincian dari operasi algoritma.

Jaringan yang terhubung, terdapat beberapa aplikasi pendukung yang mempermudah pengguna nya.Beberapa contoh aplikasi yang dimaksud di antaranya aplikasi *chatting* yang berguna untuk berkomunikasi, *telnet* sebagai fasilitas *remotlogin*, *FTP* untuk transfer data dan masih banyak yang lainnya[4].

Penelitian ini akan mengembangkan aplikasi *chatting* berbasis *localareanetwork* yang dapat dipakai secara bersama-sama dalam satu *listroom* pada suatu jaringan komputer. Adapun tujuan yang ingin dicapai dalam penelitian ini adalah memberikan solusi alternatif penggunaan aplikasi *chatting* yang mempermudah komunikasi secara bersama-sama antar pengguna jaringan di STMIK Surya Intan Kotabumi. Harapannya, aplikasi yang dibuat akan memberikan manfaat antara lain memudahkan penyampaian informasikepada pengguna lain dalam sebuah jaringan yang dapat bekerja secara praktis, karena tidak akan sulit dengan penyampaian informasi yang berulang-ulang.

2. METODOLOGI PENELITIAN

2.1. Teknik Pengumpulan Data

Adapun teknik pengumpulan data yang digunakan dalam penelitian ini adalah sebagai berikut :

A. Observasi

Observasi dilakukan dibidang pengelolaan dan pengamatan informasi secara sistematis.

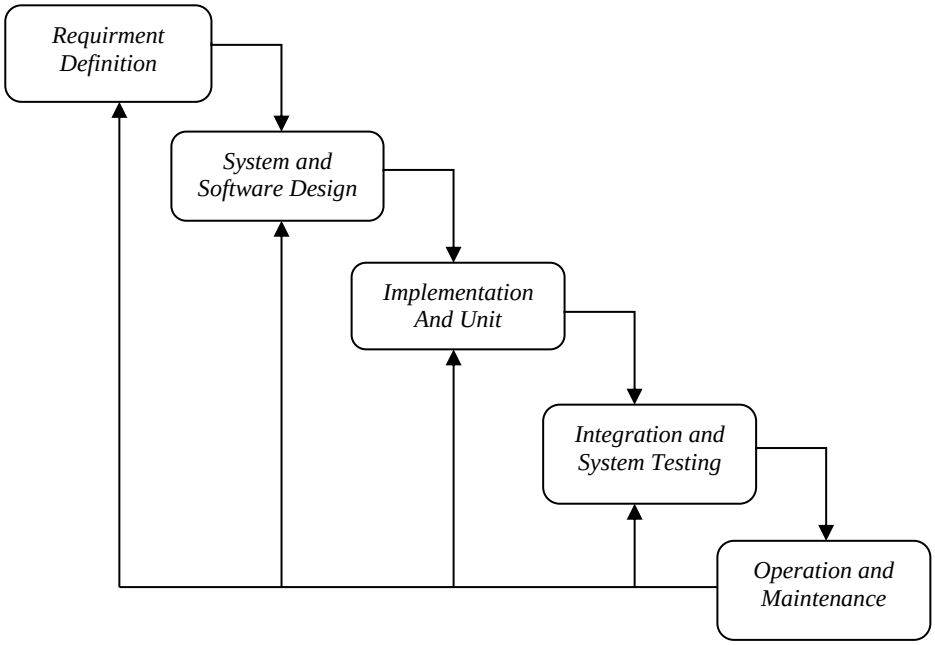
B. Studi Pustaka

Metode ini dilakukan dengan cara mempelajari dan mengumpulkan data serta bahan-bahan yang berhubungan dengan internet dan sumber-sumber yang berkaitan dengan Metode *KriptografiCaesar Chiper* pada Aplikasi *Chatting*Berbasis *Local Area Network*.

2.2. Metode Perancangan

Pada tahap penelitian ini, Penulis akan menggunakan metode *waterfall* sebagai metode pengembangnya. Metode *waterfall* merupakan model klasik yang bersifat sistematis, berurutan dalam membangun sebuah *software* mulai dari level kebutuhan sistem kemudian menuju ketahap analisis, desain, *coding testing/verification* dan *maintenance*[5].

Menurut Pressman dan Sommerville (2010)[5], metode ini terdiri dari beberapa *step*, yang meliputi *Requrment Definition* (Analisi dan Definisi Kebutuhan), *System and Software Design* (Perancangan Sistem), *Implementation and Unit* (Implementasi dan Pengujian Unit), *Integration and System Testing* (Integrasi dan Pengujian Sistem)dan *Operation and Maintenance* (Operasi dan Pemeliharaan), seperti yang ditunjukkan pada gambar berikut ini :



Gambar 1. Tahapan Dalam Metode *Waterfall*

3. HASIL DAN PEMBAHASAN

3.1. Perancangan Sistem

3.1.1. Bagan Alir Sistem Yang Diusulkan

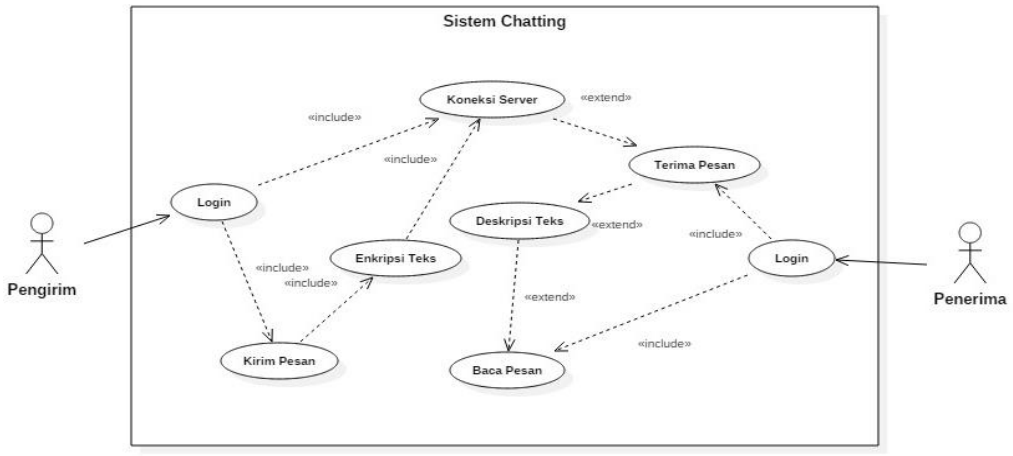
Dalam sistem yang ada saat ini proses *chatting* secara umum tidak menggunakan pengamanan data, kedua belah pihak dapat langsung melihat isi dari

percakapan yang diterima. Tetapi pemakai tidak menyadari pesan *chatting* dapat dilihat oleh orang lain dalam *server*, sehingga dengan mudah isi yang tertulis didalam form *chatting* dapat dengan mudah dibaca pihak lain. Sedangkan pada aplikasi yang akan dirancang nantinya, pesan *chatting* yang di kirim secara otomatis terenkripsi dan diterima oleh lawan *chatting* keadaan yang telah terdekripsi secara otomatis, sehingga pihak yang lain tidak dapat mengertikan arti yang sesungguhnya yang berada pada *log* status.

Adapun *bagan alir sistem* yang diusulkan adalah sebagai berikut :

A. *Usecase Diagram* Yang diusulkan

Adapun *usecase* diagram yang disusulkan adalah sebagai berikut :



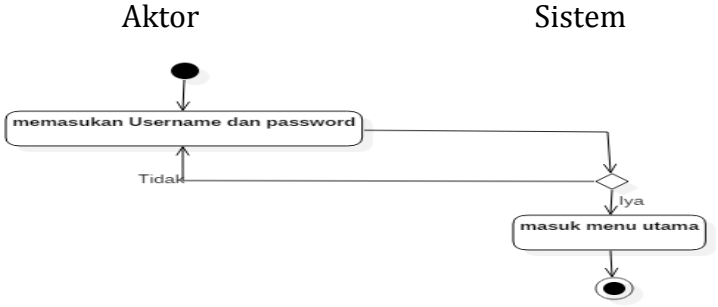
Gambar 2. *Usecase Diagram* Yang diusulkan

B. *Activity Diagram* Yang Diusulkan

Activity Diagram merupakan bagian dari penggambaran sistem secara fungsional menjelaskan proses-proses logika atau fungsi yang terimplementasi oleh kode program.

1. *Activity Diagram Login*

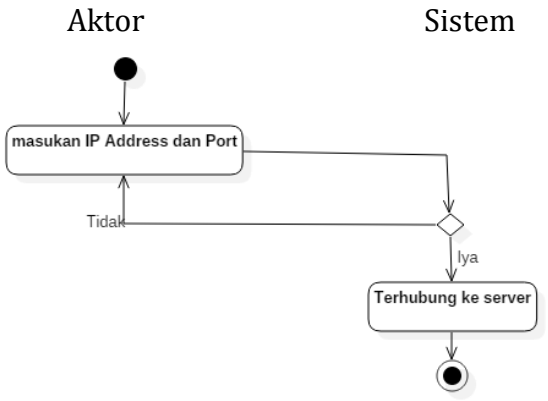
   Adapun *activitydiagram* pada *login* adalah sebagai berikut :



Gambar 3. *Activity Login* Yang Diusulkan

Berikut merupakan penjelasan dari gambar Activity diatas, user mengawali dengan *login* yaitu dengan memasukkan *username* dan *password* kemudian di verifikasi oleh sistem untuk menentukan proses akan dilanjutkan atau tidak, jika *user* berhasil *login* maka akan masuk ke menu utama, tetapi jika terdapat kesalahan , maka sistem akan mengembalikan verifikasi tersebut untuk di *entry* ulang.

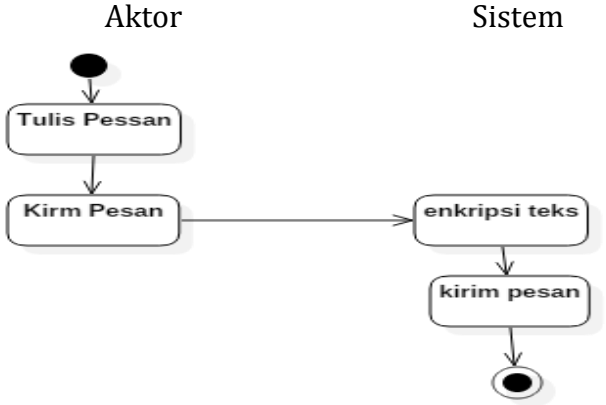
2. *Activity Diagram* Koneksi *Server*
   Activity diagram koneksi *server* yang berguna untuk menghubungkan jaringan server dengan sistem. Adapun *Activity Diagram* nya adalah sebagai berikut :



Gambar 4. *Activity* Koneksi *Server* Yang Diusulkan

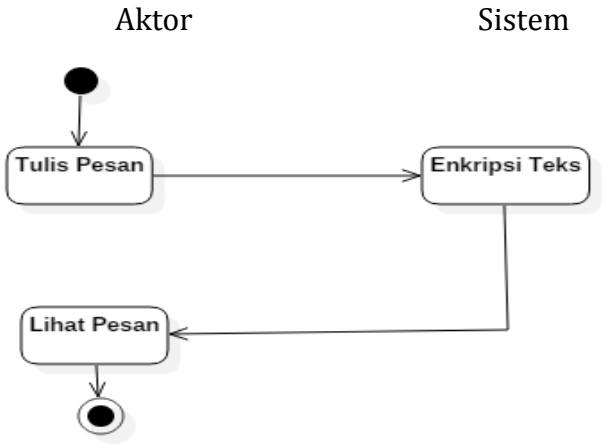
User menginput alamat *IP Address* dan *Port* kemudian di verifikasi, jika data yang dimasukkan dengan benar, maka *user* akan terhubung dengan *server*, tetapi jika tidak maka *user* akan mengentry kembali.

3. *Activity Diagram* Kirim Pesan
   Adapun *activity* diagram pada pengiriman pesan adalah sebagai berikut :



Gambar 5. *Activity* Kirim Pesan Yang Diusulkan

4. *Activity Diagram Enkripsi Teks*
   Adapun activity diagram pada enkripsi teks adalah sebagai berikut :

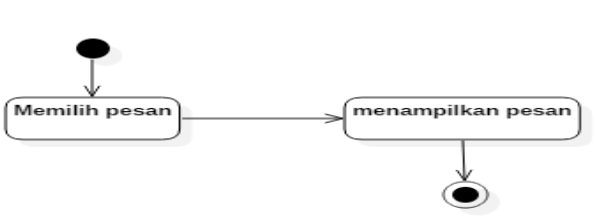


Gambar 6. *Activity Enkripsi Teks* Yang Diusulkan

Berikut penjelasan dari gambar *Activity* Pada enkripsi teks :

a) *User* mengetik pesan.
b) Pesan di enkripsi oleh sistem.
c) *User* melihat pesan.

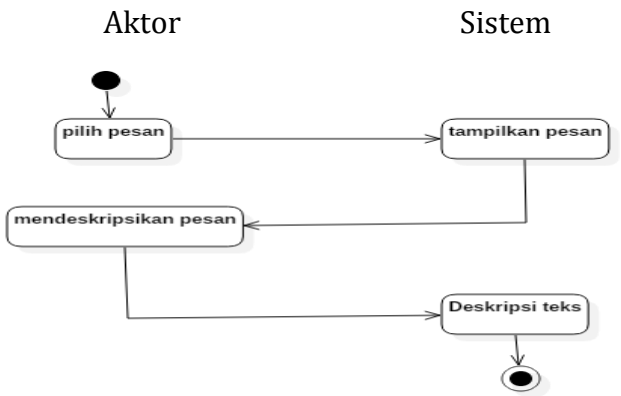
5. *Activity Diagram* Terima Pesan
   Activity diagram ini berfungsi untuk menggambarkan proses Aktor menerima pesa yang dikirim oleh sistem. Adapun *Activity Diagram* pada penerimaan pesan adalah sebagai berikut :



Gambar 7. *Activity* Terima Pesan Yang Diusulkan

Dari gambar di atas dapat disimpulkan bahwa, user menerima pesan dan sistem akan menampilkan pesan.

6. *Activity Diagram* Deskripsi Teks
   Adapun *activity* diagram pada dekripsi teks adalah sebagai berikut :

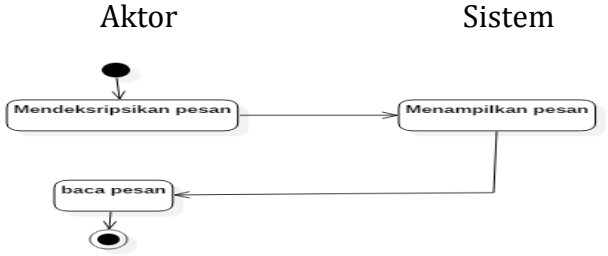


Gambar 8. *Activity Deskripsi Teks* Yang Diusulkan

Berikut penjelasan dar gambar *Activity* pada dekripsi teks :

a) *User* memilih pesan.
b) Sistem menampilkan pesan.
c) Sistem mendekripsikan pesan kepada *user*.
d) Sistem menampilkan pesan.

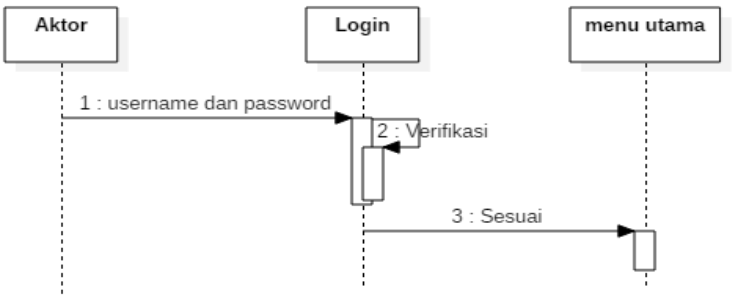
7. *Activity Diagram* Baca Pesan



Gambar 9. *Activity* Baca Pesan Yang Diusulkan

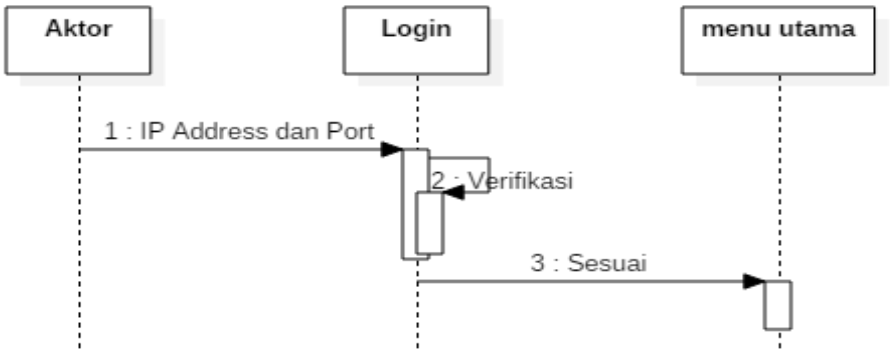
C. *Sequence Diagram* Yang Diusulkan

1. *Sequence Diagram Login* Yang Diusulkan



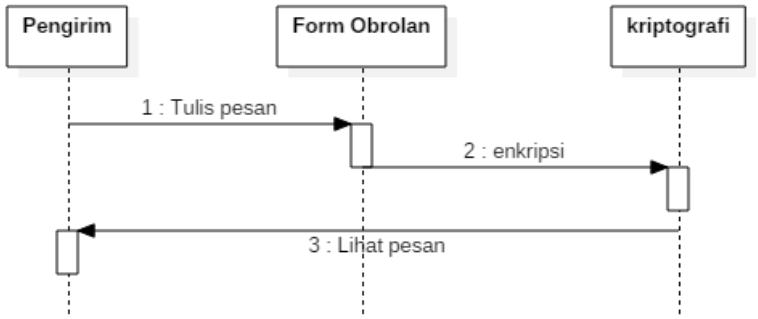
Gambar 10. *Sequence Diagram Login* Yang Diusulkan

2. *Sequence Diagram* Koneksi *Server* Yang Diusulkan
   Adapun *sequence* diagram koneksi *server* yang diusulkan adalah sebagai berikut :



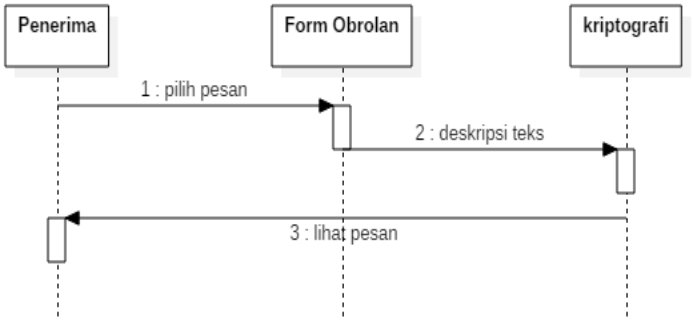
Gambar 11. *Sequence Diagram* Koneksi *Server* Yang Diusulkan

3. *Sequence Diagram* Kirim PesanYang Diusulkan
   Adapun *sequence* diagram pada pengiriman pesan yang diusulkan adalah sebagai berikut :



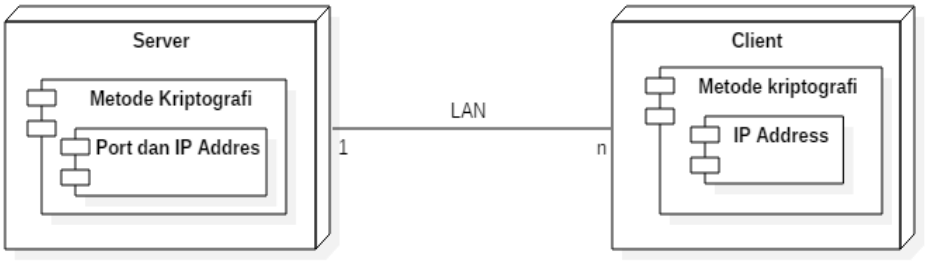
Gambar 12. *Sequence Diagram* Kirim Pesan Yang Diusulkan

4. *Squence Diagram* Terima Pesan Yang Diusulkan
   Adapun *sequence* diagram pada penerimaan pesan yang diusulkan adalah sebagai berikut :



Gambar 13. *Squence Diagram* Terima Pesan Yang Diusulkan

D. *Deployment Diagram*

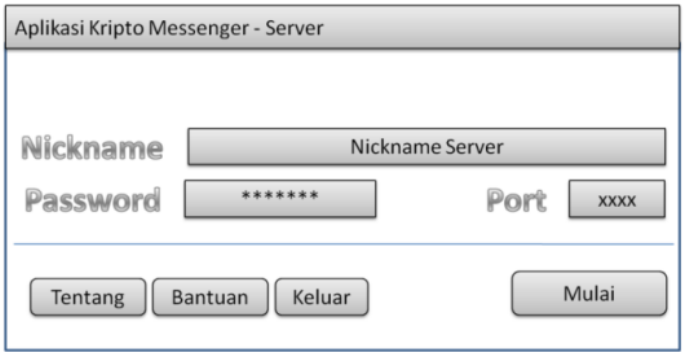


Gambar 14. *Deployment Diagram*

Deployment diagram yang dapat dilihat pada Gambar 4.23 menunjukan bahwa *server* yang digunakan hanya 1 dan *client* dapat digunakan dalam jumlah banyak yang disimbolkan dengan tanda "n". Dimana *server* dan *client* pengguna dihubungkan melalui LAN (*Local Area Network*). Didalam *server* ada komponen *kriptografi*, *port* dan *IP Address*, didalam *client* ada komponen *kriptografi* dan *IP Address*.

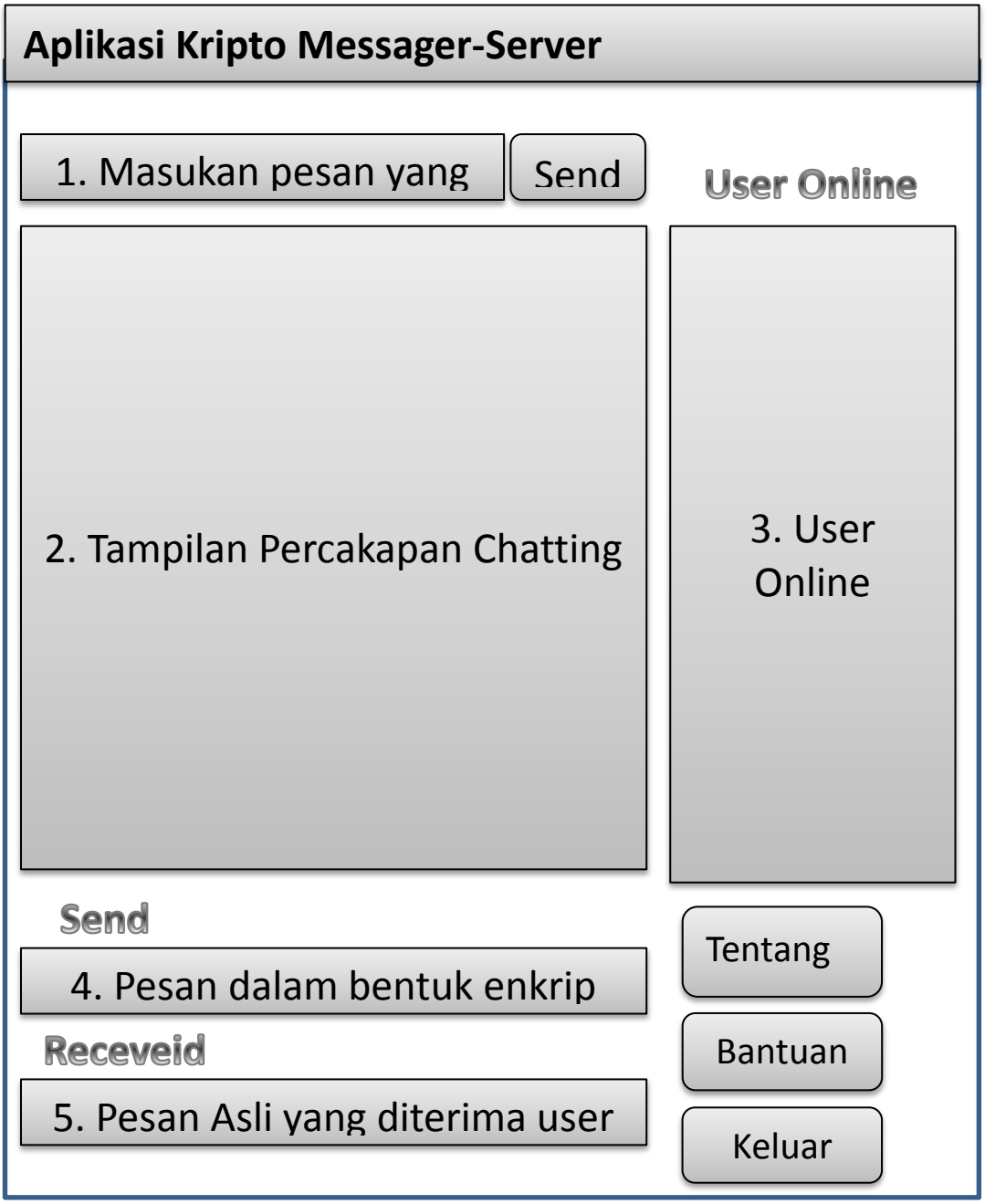
3.1.2. Rancangan Awal Antarmuka Program

Rancangan awal antarmuka program yang digunakan untuk menjelaskan suatu rancangan yang telah dianalisis atau yang dirancang sebelum diterapkannya metode *kriptografi caesar chiper*. Rancangan Antarmuka Menu Utama *Server.*



Gambar 15. Antarmuka Menu Utama *Server*

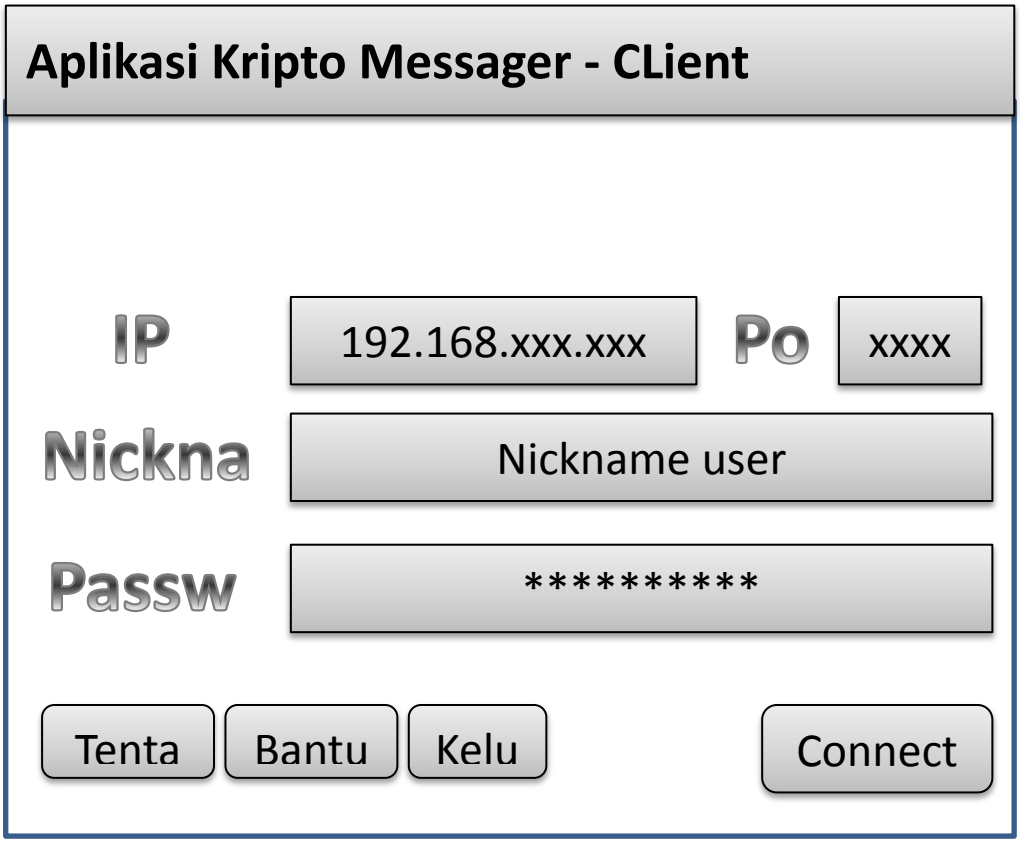
A. Rancangan Antarmuka *Chatting Server*
Rancangan antarmuka yang dibangun kali ini berfungsi sebagai inti dari aplikasi ini. Gambar antarmuka *chatting server* adalah sebagai berikut :



Gambar 16. Antarmuka *Chatting Server*

B. Rancangan Antarmuka Menu Utama Client

Gambar rancangan masukan antarmuka menu utama *client* adalahsebagaiberikut :



Gambar 17. Antarmuka Menu Utama *Client*

C. Rancangan Antarmuka *Chatting Client*

Rancangan antarmuka yang dibangun kali ini memiliki kesamaan dengan antarmuka *chatting server* baik dari segi tampilan serta fungsinya seperti yang terlihat pada gambar berikut ini :



Gambar 18. Antarmuka *Chatting Client*

3.2. Spesifikasi dan Pembahasan Program

3.2.1. Spesifikasi Program

A. Enkripsi Pesan Menggunakan Metode *KriptografiCaesar Chiper*

Aplikasi yang dibangun menggunakan algoritma *caesarchiper*, pengguna harus dapat membuat suatu pesan dan pesan tersebut dapat di enkripsi oleh aplikasi, kemudian aplikasi tersebut harus dapat mengirimkan pesan ke tempat yang dituju dengan baik.

B. Deskripsi Pesan Menggunakan Metode *KriptografiCaesarChiper*

Aplikasi yang dibangun harus dapat menerima pesan yang terenkripsi dan dapat menskripsikan pesan yang masuk dengan menggunakan data kunci. Untuk memenuhi kedua fungsi utama tersebut, maka aplikasi yang dibangun memiliki kebutuhan fungsional sebagai berikut:

1. Aplikasi menyediakan antarmuka untuk pembuatan pesan.
2. Aplikasi dapat mealukan enkripsi dengan menggunakan metode *KriptografiCaesar Chiper.*
3. Aplikasi dapat mengirimkan pesan yang terenkripsi.
4. Aplikasi dapat melakukan deskripsi terhadap pesan masuk yang terenkripsi menggunakan metode *KriptografiCaesar Chiper.*

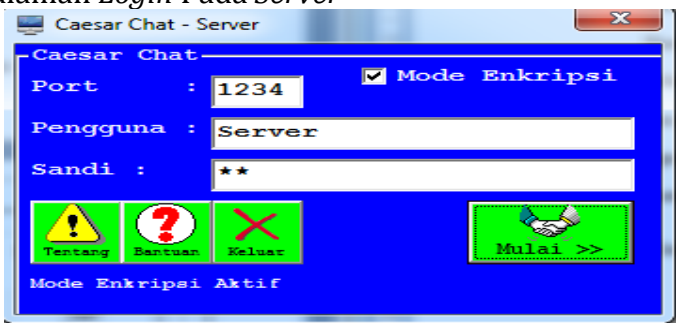
Adapun kebutuhan non-fungsional adalah sebagai berikut :

1. Aplikasi memiliki antarmuka yang menarik dan mudah di mengerti oleh pengguna.
2. Aplikasi memiliki menu bantuan untuk memudahkan pengguna dalam menggunakan aplikasi. Aplikasi memiliki menu tentang untuk memberitahukan informasi tentang aplikasi yang dibuat.

3.2.2. Pembahasan Program

Adapun penjelasan dari aplikasi yang dibangun adalah sebagai berikut :

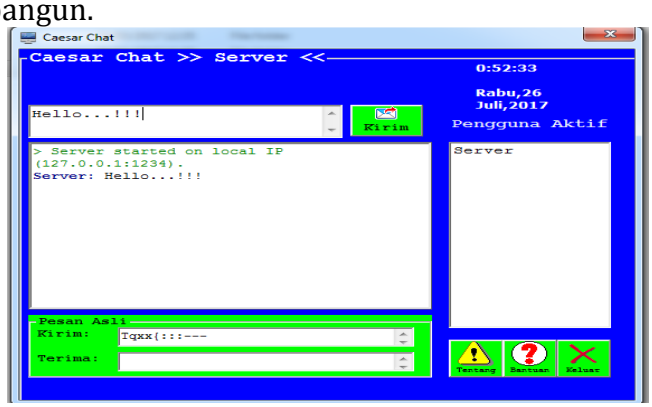
A. Menjalankan Halaman *Login* Pada *Server*



Gambar 19. Halaman *Login Server*

B. Menjalankan Halaman *Chatting* Pada *Server*

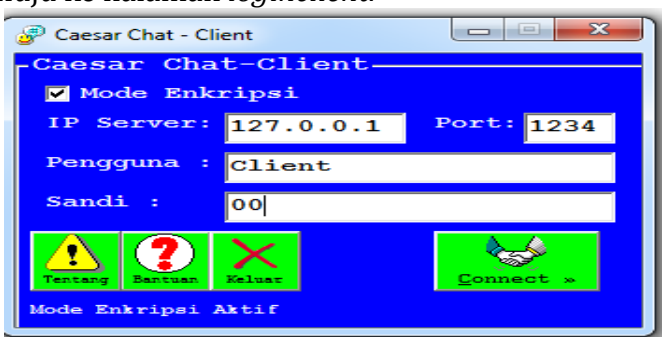
Halaman *ChattingServer* yaitu halaman yang berfungsi sebagai inti dari aplikasi yang dibangun.



Gambar 20. Halaman *Chatting Server*

C. Menjalankan Halaman *Login* Pada *Client*

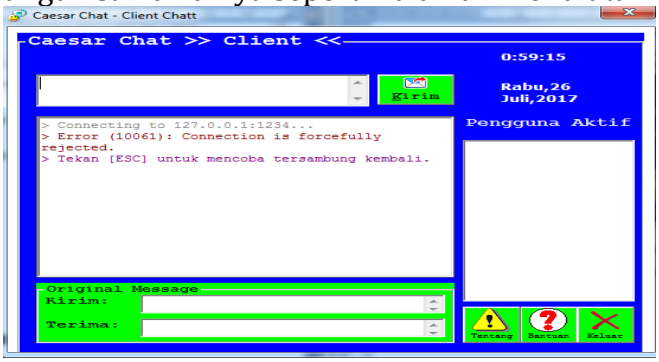
Halaman *loginClient* yaitu halaman utama pada aplikasi yang berfungsi untuk *client*, untuk menuju ke halaman *loginclient.*



Gambar 21. Halaman *Login Client*

D. Menjalankan Halaman *Chatting* Pada *Client*

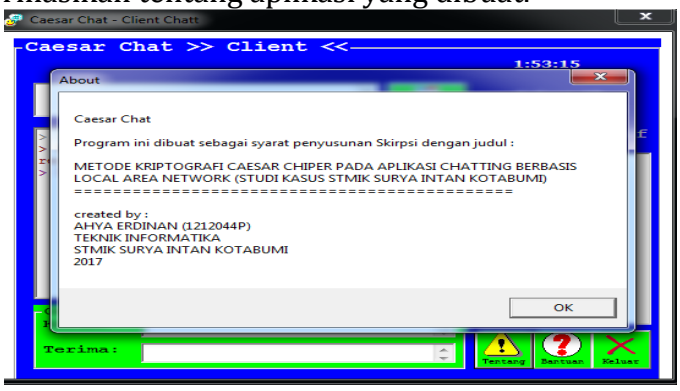
Halaman *ChattingClient* yaitu halaman yang berfungsi sebagai inti dari aplikasi yang dibangun sama halnya seperti halaman menu utama *server*.



Gambar 22. Halaman *Chatting Client*

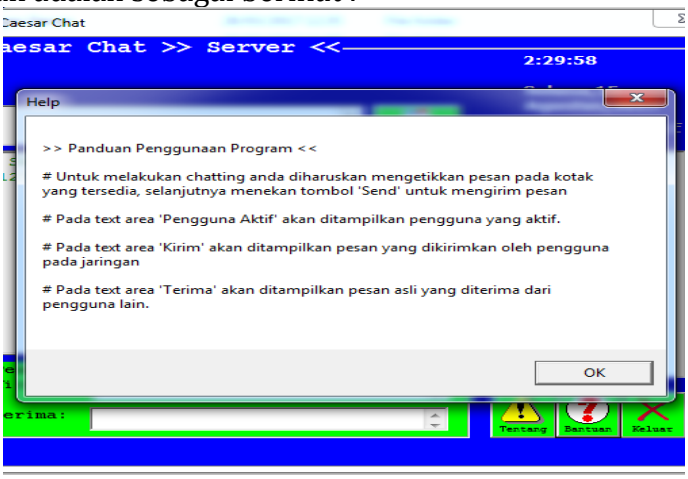
E. Menjalankan Menu Tentang *(About)*

Pada menu bantuan ini berfungsi sebagai *form* yang berisikan teks dialog untuk menginformasikan tentang aplikasi yang dibuat.



Gambar 23. Halaman Tentang

F. Menjalankan Menu Bantuan *(Help)*
Halaman bantuan yaitu halaman yang berfungsi sebagai bantuan berupa teks dialog yang berisikan tentang penggunaan aplikasi yang dibangun. Adapun halaman bantuan adalah sebagai berikut :



Gambar 24. Halaman Bantuan

4. SIMPULAN

Simpulan dari Metode *Kriptografi Caesar Chiper* Pada Aplikasi *Chatting* Berbasis *Local Area Network* (Studi Kasus STMIK Surya Intan Kotabumi) adalah sebagai berikut :

A. Aplikasi *chatting* dibangun untuk memudahkan pengguna dalam melakukan komunikasi antar pengguna dalam area lokal.
B. Aplikasi *chatting* lebih aman apabila pada proses pengiriman pesan dilakukan proses enkripsi didalamnya. Hal ini dikarenakan pesan yang dikirimkan dalam bentuk *chipertext*.
C. Implementasi metode kriptografi *Caesar Chiper* pada perangkat lunak yang dibangun adalah dalam bentuk endkripsi dan deskripsi yang dilakukan pada pesan yang terdapat pada aplikasi yang dibangun.
D. Dengan sistem enkripsi tersebut, penyadapan yang dilakukan ketika pesan ditransmisikan semakin sulit karena pesan yang ditangkap berupa *chipertext.*
E. Pengiriman dan penerimaan pesan berlangsung dengan baik apabila pengirim dan penerima menggunakan kunci yang sama dalam proses komunikasinya.

DAFTAR PUSTAKA

[1] C. Program, S. Magister, K. Kunci, : Kriptografi, and K. Publik, “KEAMANAN DATA DENGAN METODE KRIPTOGRAFI KUNCI PUBLIK,” *J. TIMES*, 2016.
[2] S. Wardoyo, Z. Imanullah, and R. Fahrizal, “Enkripsi dan Dekripsi File dengan Algoritma Blowfish pada Perangkat Mobile Berbasis Android,” *J. Nas. Tek. ELEKTRO*, 2016, doi: 10.25077/jnte.v5n1.199.2016.
[3] A. Zelviana, S. Efendi, and A. Dedy, “Perancangan Aplikasi Pembelajaran

Kriptografi Kunci Publik ElGamal Untuk Mahasiswa," *J. Dunia Teknol. Inf.*, 2012.

[4] M. J. N. Yudianto, "Jaringan Komputer dan Pengertiannya," *Ilmukomputer.Com*, 2014.

[5] , M., S. Hasan, and A. Ambarita, "PENGGUNAAN MODEL E-LEARNING DALAM MENINGKATKAN HASIL BELAJAR MAHASISWA PADA MATERI MICROPROCESSOR," *IJIS - Indones. J. Inf. Syst.*, 2017, doi: 10.36549/ijis.v2i1.26.

[6] J. Rumbaugh, "Unified Modeling Language (UML)," in *Encyclopedia of Software Engineering*, 2010.

[7] Haviluddin, "Memahami Penggunaan UML (Unified Modelling Language)," *Memahami Pengguna. UML (Unified Model. Lang.*, 2011.