PENERAPAN *KRIPTOGRAFI CAESAR CHIPER* PADA APLIKASI *CHATTING* BERBASIS *LOCAL AREA NETWORK*

M. Abu Jihad Plaza R[1], Rudi Hartono[2]

[1,2]STMIK Surya Intan

[1] abujihad83@gmail.com, [2] hartono26rudi@gmail.com

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; Encryptio; 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: *Chat*; Enkripsi; Dekripsi; Caesar Chiper

1. PENDAHULUAN

Sebuah komunikasi akan efektif apabila *audience* menerima pesan, pengertian dan lain-lain sama seperti yang dikehendaki oleh penyampai (Suprapto, 2006). Proses komunikasi senantiasa terjadi setiap waktu. Berbagai perangkat komunikasi dikembangkan dan digunakan untuk menunjang tercapainya proses komunikasi. Berbagai macam model alat komunikasi dapat dijumpai, baik yang berupa fisik (hardware) atau berupa aplikasi (*software*).

Penggunaan jaringan komputer sering dihadapkan pada masalah komunikasi antar pengguna, misalkan seorang pengguna ingin membagikan informasi kepada pengguna lain yang berada di tempat berbeda maka dibutuhkan sebuah aplikasi komunikasi atau *chat*. Keberadaan aplikasi tersebut dapat menunjang suksesnya penggunaan sebuah jaringan komputer di dalam sebuah instansi. Aplikasi *chatting* digunakan sebagai media komunikasi antar sesama pengguna komputer yang terhubung dalam suatu jaringan, baik itu berupa melalui teks, *image*, ataupun suara. Aplikasi chatting yang tersedia biasanya hanya dapat digunakan oleh dua pengguna saja, dan apabila ada penyampaian informasi antar pengguna, maka harus dilakukan berulang pada pengguna yang lain, oleh sebab itu dibutuhkan sebuah aplikasi chatting.

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.

Pada realitasnya tidak seluruh pc yang terdapat baik di kantor ataupun rumah memiliki koneksi ke internet. Pada mayoritas pc yang terdapat di perkantoran sebagian masih tersambung dalam jaringan *local area network* (LAN). Sehingga butuh terdapatnya suatu layanan aplikasi *chat* yang bisa berjalan dalam suatu jaringan. Pesan yang dikirimkan antar pengguna aplikasi *chat* butuh diberikan layanan keamanan informasi dan hanya orang- orang yang mempunyai otoritas saja yang bisa mengenali isi pesan yang di nformasikan tersebut. Meski komunikasi dilakukan dalam *fashion offline* hanya lewat jaringan LAN namun tidak menutup mungkin jalan komunikasi tersebut disusupi oleh *cracker* yang bisa mengakses pesan yang ditransmisikan. Perlu dibuat mekanisme supaya pesan yang dikirimkan bisa terpelihara kerahasiaannya.

Kriptografi ialah salah satu metode yang bisa digunakan untuk tingkatkan aspek keamanan suatu data, dengan memakai metode Kriptografi Cesar Chiper, tahapan yang dilakukan kriptografi Caesar Cipher sangat mudah untuk dilakukan. Inti dari algoritma kriptografi ini adalah melaksanakan perpindahan terhadap seluruh karakter pada plainteks dengan nilai perpindahan yang sama, untuk mengamankan suatu pesan (*plaintext*) jadi pesan yang tersembunyi (*ciphertext*) merupakan enkripsi (*encryption*). Proses kebalikannya, untuk mengubah *ciphertext* menjadi plaintext, disebut dekripsi. Prosedur enkripsi sangat bermacam- macam tergantung pada kunci yang hendak mengubah rincian dari operasi algoritma.

Penelitian ini akan mengembangkan aplikasi chatting berbasis *local area network* yang dapat dipakai secara bersama-sama dalam satu *list room* 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 informasi kepada pengguna lain dalam sebuah jaringan yang dapat bekerja secara praktis, karena tidak akan sulit dengan penyampaian informasi yang berulang-ulang.

2. KERANGKA TEORI

2.1. Kriptografi

Kriptografi (*Cryptography*) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu kripto dan graphia. Kripto artinya menyembunyikan, sedangkan graphia artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasian data, keabsahan data, integritas data, serta autentikasi data. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan

kriptografi (Amin, 2017).

Definisi lain kriptografi yaitu seni untuk menjaga keamanan pesan. Ketika suatu pesan dikirim dari suatu tempat ke tempat lain, isi pesan tersebut mungkin dapat disadap oleh pihak lain yang tidak berhak untuk mengetahui isi pesan tersebut. Untuk menjaga pesan, maka pesan tersebut dapat diubah menjadi sebuah kode yang tidak dapat dimengerti pihak lain (Cossio et al., 2012).

2.2. Enkripsi dan Dekripsi

Proses menyandikan plainteks menjadi cipherteks disebut enkripsi (*encryption*) atau *enciphering*. Sedangkan proses mengembalikan cipherteks menjadi plainteks semula dinamakan dekripsi (*decryption*) atau *deciphering*. Enkripsi dan dekripsi dapat diterapkan baik pada pesan yang dikirim maupun pada pesan tersimpan (Wardoyo et al., 2016), (Program et al., 2016).

2.3. Jaringan Komputer

Jaringan komputer adalah terhubungnya dua komputer atau lebih dengan kabel penghubung (pada beberapa kasus, tanpa kabel atau wireless sebagai penghubung), sehingga antar komputer dapat saling tukar informasi (Hasan & Dkk, 2016). Tujuan penggunaan jaringan komputer adalah:

a. Untuk berbagi sumber daya, sepert berbagi *printer*, CPU, memori, hardisk, dan lain-lain.
b. Untuk komunikasi, seperti *e-mail*, *instant messaging*, *chatting*, dan lain-lain.
c. Untuk mengakses informasi, seperti *web browsing*, *file server*, dan lain-lain.

Untuk mencapai tujuan yang sama maka setiap bagian dalam suatu jaringan akan meminta dan memberikan layanan. Jadi, dalam jaringan terlibat dua pihak, yaitu pihak yang meminta layanan disebut klien (*client*) dan pihak yang memberikan layanan disebut pelayan (server). Arsitektur jaringan ini disebut dengan sistem *client-server* dan digunakan oleh seluruh jaringan.

Jaringan diklasifikasikan berdasarkan jarak dan lokasi, yaitu *Local Area Network* (LAN), *Metropolitan Area Network* (MAN), *Wide Area Network* (WAN), Internet, dan jaringan tanpa kabel (*Wireless*) (Tanenbaum, 2007). Berikut penjelasan klasifikasi jaringan tersebut:

a. *Local Area Network* (LAN), merupakan jaringan yang saling terhubung ke satu komputer server menggunakan topologi tertentu, biasanya digunakan dalam kawasan satu gedung atau kawasan yang jaraknya tidak lebih dari 1 km.
b. *Metropolitan Area Network* (MAN), merupakan jaringan yang saling terkoneksi dalam satu kawasan kota dan jaraknya dapat lebih dari 1 km sehingga menjadi pilihan untuk membangun jaringan komputer antar kantor atau kampus dalam satu kota.
c. *Wide Area Network* (WAN), merupakan jaringan yang menghubungkan banyak LAN dan MAN kedalam suatu jaringan terpadu, antara satu jaringan dengan jaringan lain dapat berjarak ribuan kilometer atau terpisahkan letak geografi menggunakan metode komunikasi tertentu.

2.4. Jaringan Tanpa kabel

Jaringan tanpa kabel atau sering juga disebut jaringan nirkabel yaitu jaringan yang menggunakan sinyal frekuensi radio untuk mengirimkan data dan karena alasan ini lebih rentan terhadap ancaman keamanan daripada jaringan kabel karena sifat siarannya (Arief, 2013). Tiap komputer, printer atau *peripheral* yang terhubung dalam jaringan disebut dengan node. Sebuah jaringan komputer sekurang-kurangnya terdiri dari dua unit komputer atau

lebih, dapat berjumlah puluhan komputer, ribuan atau bahkan jutaan node yang saling terhubung satu sama lain (Ikhsan & Syahfitri, 2009).

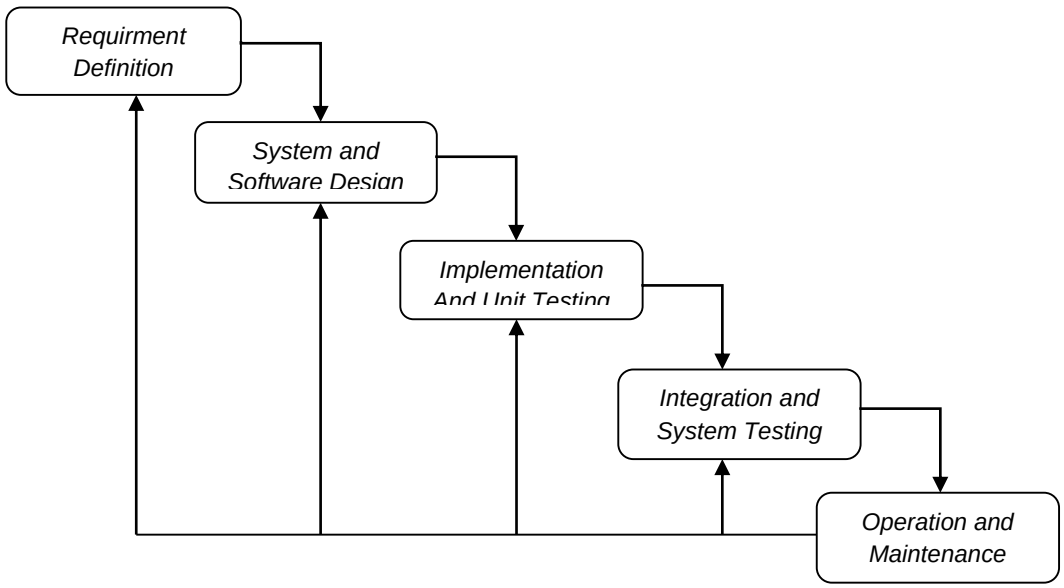
3. METODOLOGI

3.1. Metode Waterfall

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 (, et al., 2017). Disebut dengan waterfall karena tahap yang dilalui harus menunggu selesainya tahap sebelumnya dan berjalan sesuai berurutan.

3.2. Tahapan Metode Waterfall

Metode ini terdiri dari beberapa *step*, yang meliputi *Requirement 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) (Pressman, 2015). seperti yang ditunjukkan pada gambar 1 berikut ini :



Gambar 1. Tahapan Dalam Metode *Waterfall*

Adapun tahapan yang dilakukan pada penelitian ini adalah sebagai berikut:

a. Analisis dan definisi kebutuhan

   Layanan, batasan dan tujuan sistem ditentukan melalui konsultasi dengan *user* atau pengguna.

b. Perancangan sistem

   Adapun tahap *design* yang digunakan antara lain:

   1) *Use Case*, Model *use case* digunakan untuk menggambarkan serangkaian kegiatan yang dilakukan *actor* terhadap aplikasi yang dibangun (Haviluddin, 2011), Hal-hal tersebut antara lain pengguna dapat melakukan enkripsi dan deskripsi pesan yang dikirim dan diterima menggunakan aplikasi yang dibangun.

2) *Activity Diagram*, adalah suatu diagram yang menjelaskan tentang analisa proses dari suatu bagian dari awal sampai akhir. Diagram ini menjelaskan tentang bagaimana program tersebut dapat berjalan (Rumbaugh, 2010).

Pada tahapan ini dilakukan perancangan antarmuka aplikasi yang dibangun. Antarmuka yang dirancang terdiri dari :

a) Antarmuka Menu Utama *Server*

Antarmuka yang dirancang pada aplikasi ini adalah berfungsi sebagai navigasi awal untuk menerima interaksi dari pengguna/*client*.

b) Antarmuka *Chatting Server*

Rancangan antarmuka yang dibangun kali ini berfungsi sebagai inti dari aplikasi ini, yang didalamnya berfungsi untuk menulis pesan, melihat pesan masuk, dan melihat *client* yang sedang aktif.

c. Implementasi dan pengujian unit

Perancangan perangkat lunak direalisasikan dengan program atau unit program. Pengujian ini melibatkan verifikasi bahwa setiap unit telah memenuhi spesifikasinya.

d. Integrasi dan pengujian sistem

Unit program atau program individual diintegrasikan dan diuji sebagai sistem yang lengkap untuk menjamin bahwa kebutuhan sistem telah dipenuhi.

e. Operasi dan pemeliharaan

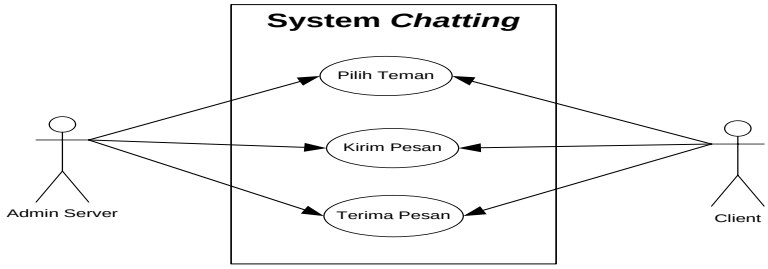
Merupakan tahap akhir dari metode *waterfall*. *Software* yang sudah jadi dijalankan serta dilakukan pemeliharaan. Mengoperasikan program di lingkungannya dan melakukan pemeliharaan. Tahap ini merupakan fase siklus hidup yang paling lama. Pemeliharaan mencakup koreksi dari berbagai *error* yang tidak ditemukan pada tahap-tahap sebelumnya, melakukan perbaikan atas implementasi unit sistem dan persyaratan-persyaratan baru ditambahkan.

4. HASIL DAN PEMBAHASAN

4.1. Perancangan Sistem

4.1.1. Usecase Diagram berjalan

Bagan alir sistem yang berjalan merupakan penjabaran dari proses pengolahan data yang mencakup tiga tahapan yaitu *input*, *process* dan *output* sehingga tahapan untuk membuatnya adalah menentukan data atau dokumen dan sumbernya (*input*), mementukan prosesnya dan siapa yang memproses (*process*) dan menentukan prosesnya dan siapa yang menerima (*output*). Use case diagram sistem yang berjalan ditunjukkan gambar 2.

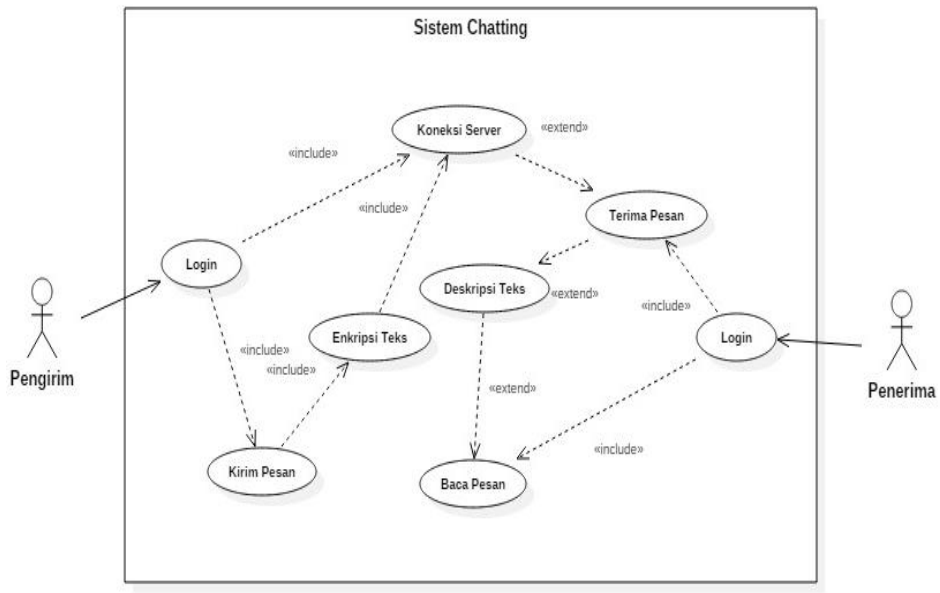


Gambar 2. *Use Case Diagram* Berjalan

4.1.2. Usecase Diagram 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 mengetahui arti yang sesungguhnya yang berada pada *log status*. Setelah melakukan penelitian di Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Surya Intan Kotabumi, peneliti membuat sistem yang diusulkan yang berguna untuk memudahkan penyampaian informasi kepada pengguna lain dalam sebuah jaringan lokal.

Usecase Diagram yang diusulkan merupakan diagram sistem yang akan dibangun yang berguna untuk menggambarkan seluruh sistem yang berjalan baik sistem untuk *server* maupun *client* atau untuk pengirim maupun penerima, serta menggambarkan *Activity* apa saja yang ada di sistem tersebut. Adapun *usecase* diagram yang disusulkan adalah sebagai berikut :



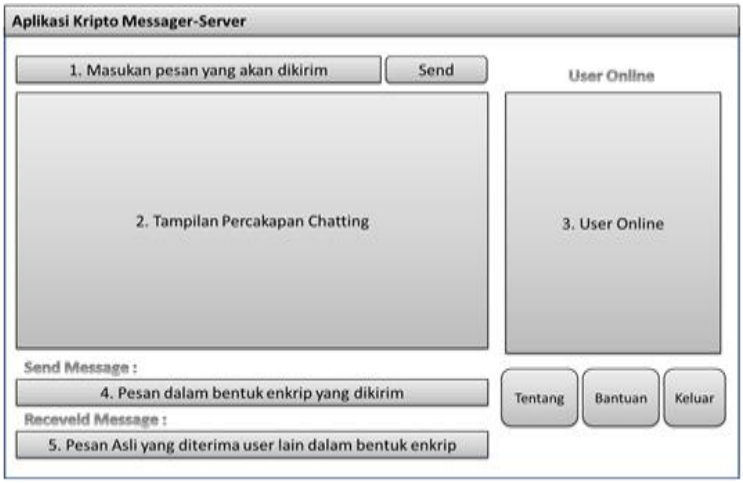
Gambar 3. *Usecase Diagram* diusulkan

4.1.3. 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*. Oleh karena itu peneliti akan menjelaskan tentang rancangan awal program yang akan dirancang. Adapun rancangan awal antarmuka program adalah sebagai berikut:

1. Rancangan Antarmuka Menu Utama *Server*

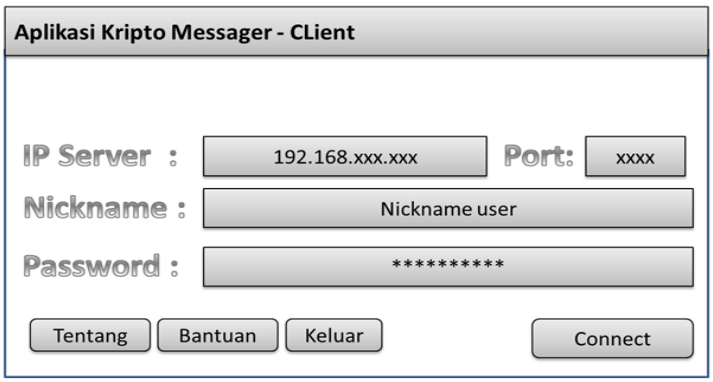
   Rancangan antarmuka yang dibangun kali ini berfungsi sebagai inti dari aplikasi ini yang didalamnya berfungsi untuk menulis pesan, melihat pesan masuk, dan melihat *client* yang sedang aktif. Gambar antarmuka *chatting server* adalah sebagai berikut:



Gambar 4. Antarmuka *Chatting Server*

2. Rancangan Antarmuka *Chatting Server*

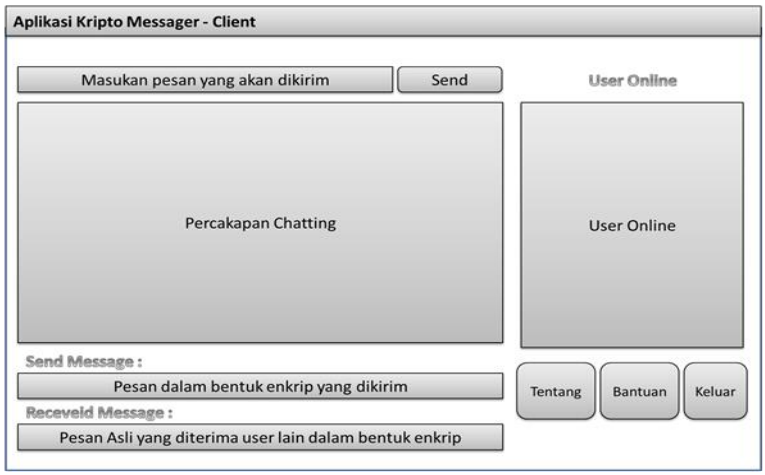
   Rancangan antarmuka yang dibangun kali ini memiliki fungsi yang sama dengan rancangan antarmuka menu utama *server*. Perbedaan terdapat tambahan atribut yaitu *IP server*. Gambar rancangan masukan antarmuka menu utama *client* adalah sebagai berikut :



Gambar 5. Antarmuka Menu Utama *Client*

3. *Rancangan Antarmuka Menu Utama Client*

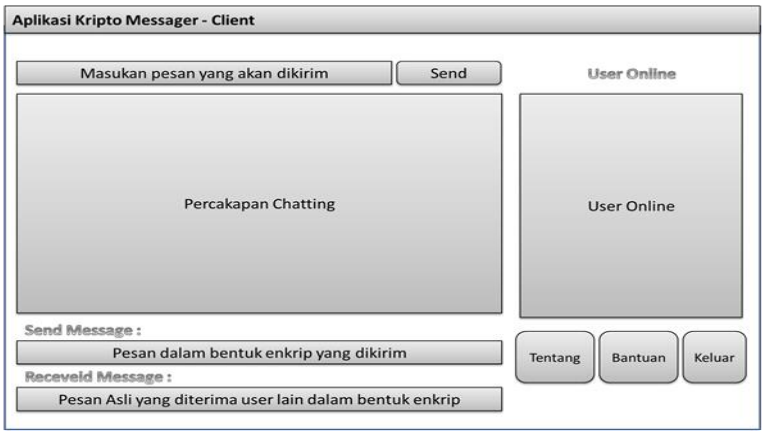
   Rancangan antarmuka yang dibangun kali ini memiliki kesamaan dengan antarmuka *chatting server* baik dari segi tampilan serta fungsinya seperti yang terlihat pada gambar berikut ini :



Gambar 6. Antarmuka Menu Utama *Client*

4. *Rancangan Antarmuka Chatting Client*

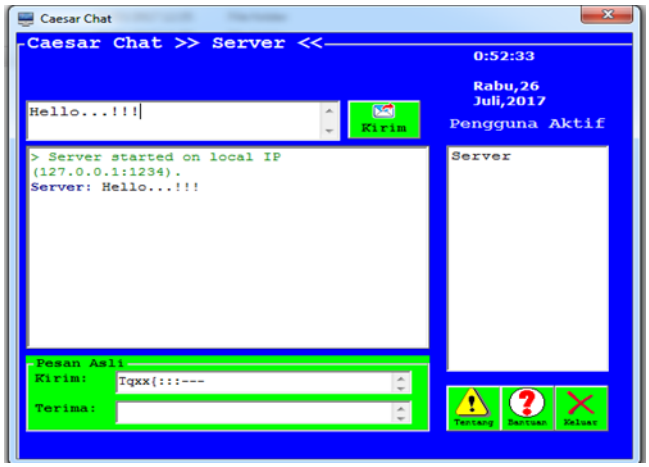
   Rancangan antarmuka yang dibangun kali ini memiliki kesamaan dengan antarmuka *chatting server* baik dari segi tampilan serta fungsinya seperti yang terlihat pada gambar berikut ini :



Gambar 7. Antarmuka *Chatting Client*

5. Halaman *Chatting* Pada *Server*

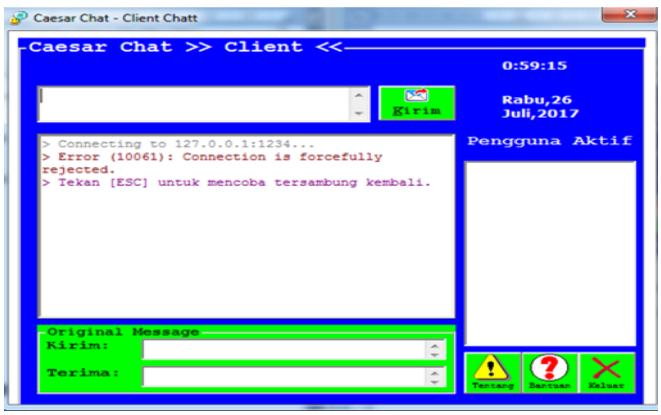
   Halaman *Chatting Server* yaitu halaman yang berfungsi sebagai inti dari aplikasi yang dibangun. Setelah *server* berhasil *login* maka akan tampil halaman *chatting* dari masing-masing pengguna yang di dalamnya berfungsi untuk menulis pesan, melihat pesan yang masuk dan melihat user yang sedang aktif. Berikut adalah gambar halaman *chatting server*:



Gambar 8. Halaman *Chatting Server*

6. Halaman *Chatting* Pada *Client*

   Halaman *Chatting Client* yaitu halaman yang berfungsi sebagai inti dari aplikasi yang dibangun sama halnya seperti halaman menu utama *server*. Setelah *clinet* berhasil *login* maka akan tampil halaman *chatting* dari masing-masing pengguna yang di dalamnya berfungsi untuk menulis pesan, melihat pesan yang masuk dan melihat *user* yang sedang aktif. Berikut adalah gambar halaman *chatting client*:



Gambar 9. Halaman *Chatting Client*

5. KESIMPULAN

Berdasarkan hasil penelitian maka dapat ditarik kesimpulan bahwa pada aplikasi *chatting* berbasis *local area network* dibangun untuk memudahkan pengguna dalam melakukan komunikasi antar pengguna dalam area lokal. Aplikasi *chatting* lebih aman apabila pada proses pengiriman pesan dilakukan proses enkripsi didalamnya. Hal ini dikarenakan pesan yang dikirimkan dalam bentuk *chipertext*. Implementasi metode kriptografi *Caesar Chiper* pada perangkat lunak yang dibangun adalah dalam bentuk enkripsi dan dekripsi yang dilakukan pada pesan yang terdapat pada aplikasi yang dibangun. Dengan sistem enkripsi tersebut, penyadapan yang dilakukan ketika pesan ditransmisikan semakin sulit karena pesan yang ditangkap berupa *chipertext.* Pengiriman dan penerimaan pesan berlangsung dengan baik apabila pengirim dan penerima menggunakan kunci yang sama dalam proses

komunikasinya.

DAFTAR PUSTAKA

Amin, M. M., 201). IMPLEMENTASI KRIPTOGRAFI KLASIK PADA KOMUNIKASI BERBASIS TEKS. *Pseudocode*. https://doi.org/10.33369/pseudocode.3.2.129-136

Arief, M. R., 2013. Teknologi Jaringan Tanpa Kabel (Wireless). *Seminar Nasional Teknologi 2007*.

Cossio, M. L. T., Giesen, L. F., Araya, G., Pérez-Cotapos, M. L. S., VERGARA, R. L., Manca, M., Tohme, R. A., Holmberg, S. D., Bressmann, T., Lirio, D. R., Román, J. S., Solís, R. G., Thakur, S., Rao, S. N., Modelado, E. L., La, A. D. E., Durante, C., Tradición, U. N. A., En, M., … Héritier, F., 2012. Penerapan Algoritma Kriptografi WAKE pada Aplikasi Chatting & Internet Monitor Berbasis LAN. *Uma Ética Para Quantos?*

Hasan, M., & Dkk., 2016. Analisa Dan Pengembangan Jaringan Wireless Berbasis Mikrotik Router Os V.5.20 Di Sekolah Dasar Negeri 24 Palu. *Jurnal Elektronik Sistem Informasi Dan Komputer*.

Haviluddin., 2011. Memahami Penggunaan UML (Unified Modelling Language). *Memahami Penggunaan UML (Unified Modelling Language)*.

Ikhsan, M., & Syahfitri, Y., 2009. Memahami Jaringan Komputer Untuk Membangun *Local Area Network* (LAN). *Saintikom*.

M., Hasan, S., & Ambarita, A., 2017. Penggunaan Model *E-Learning* Dalam Meningkatkan Hasil Belajar Mahasiswa Pada Materi Microprocessor. *IJIS - Indonesian Journal On Information System*. https://doi.org/10.36549/ijis.v2i1.26

Pressman, R S., 2015. Software Engineering Seventh Edition. *Metode Waterfall*.

Program, C., Magister, S., Kunci, K., Kriptografi, :, & Publik, K., 2016. Keamanan Data Dengan Metode Kriptografi Kunci Publik. *Jurnal TIMES*.

Rumbaugh, J. (2010). Unified Modeling Language (UML). In *Encyclopedia of Software Engineering*. https://doi.org/10.1081/e-ese-120044214

Suprapto, M. S. T., 2006. Pengantar Teori & Manajemen Komunikasi. In *Media Pressindo*.

Tanenbaum, A. S. 2007. Computer Networks 4th Edition. *Sba: Controle & Automação Sociedade Brasileira de Automatica*.

Wardoyo, S., Imanullah, Z., & Fahrizal, R., 2016. Enkripsi dan Dekripsi File dengan Algoritma Blowfish pada Perangkat Mobile Berbasis Android. *JURNAL NASIONAL TEKNIK ELEKTRO*. https://doi.org/10.25077/jnte.v5n1.199.2016