GATOT KACA JOURNAL
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa

APLIKASI *SECRETCHATTING* DENGAN MENGIMPLEMENTASIKAN ALGORITMA *CAESAR CIPHER*

Erick Irwansyah[1)]; Maryaningsih[2)]; Yode Arliando[2)]

[1,2,3)] ***Program Studi Informatika Fakultas Ilmu Komputer Universitas Dehasen Bengkulu***

Email: *erickirwansyah5a@gmail.com*

How to Cite :

Erick Irwansyah,Maryaningsih,Yode Arliando. 2020. Aplikasi Secretchatting *dengan Mengimplementasikan Algoritma* Caesar Cipher. Gatotkaca Journal.Doi:Https://Doi.Org/10.37638/Gatotkaca.1.2.191-201

ARTICLE HISTORY

Received [8 Oktober 2020]
Revised [16 November 2020]
Accepted [30 Desember 2020]

KEYWORDS

Communication Patterns, Customs

ABSTRAK

perkembangan dunia teknologi sangat pesat, sehingga mengubah sudut pandang manusia dalam berkomunikasi dampak dari perkembangan teknologi tersebut adalah terciptanya aplikasi chatting, yang memungkinkan manusia untuk melakukan pertukaran informasi melalui jaringan internet secara langsung dan instan. Dalam melakukan pertukaran informasi manusia membutuhkan sebuah fitur yang bisa menjamin informasi yang ia pertukarkan agar tidak bisa dibaca oleh orang-orang yang tidak memiliki wewenang. Salah satu cara melakukan pengamanan data adalah dengan menkripsi pesan tersebut. Enkripsi dilakukan untuk merubah teks biasa (plaintext) menjadi teks yang tidak bisa dibaca dan difahami oleh manusia makna pesan tersebut (ciphertext). Maka diterapkan salah satu algoritma enkripsi yaitu Algoritma Caesar cipher. Pengujian dilakukan pada dua perangakat smart phone dan personal computer dalam suatu jaringan wifi, hasil pengujian sistem yang dibangun menujukan aplikasi chatting dapat melakukan pengamanan pesan.

ABSTRACT

The Development of technological world is very rapid, it changes the point of view of humans in communication, the impact of the development of these technologies is the creation of chat applications, which enable humans to exchange information through the internet network directly and instantly. In exchanging human information requires a feature that can guarantee the information so that it cannot be read by people who do not have the authority. One way to safeguard data is to encrypt the message. Encryption is done to change plain text (plaintext) into text that cannot be read and understood by humans the meaning of the message (ciphertext). Then applied one encryption algorithm, the Caesar cipher algorithm. Tests carried out on two smart

ISSN: XX32-XX45 GATOT KACA JOURNAL e-ISSN : XX67-XX89
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa

phone devices and personal computers in a Wi-Fi network, the results of testing the system that was built showed the chat application can do security.

PENDAHULUAN

Kebutuhan dasar manusia adalah komunikasi.Tanpa komunikasi manusia tidak dapat bersosialisasi satu dengan yang lainnya.Seiring dengan perkembangan teknologi in*form*asi dunia, berkembang pula teknologi komunikasi. Mulai dari surat, hingga sekarang yang paling banyak digunakan adalah internet. Internet semakin banyak diminati karena mudah digunakan, dan data diakses setiap orang dari berbagai kalangan.Bukti dari perkembangan teknologi in*form*asi pada bidang komunikasi yaitu dengan adannya e-mail. Dengan menggunakan e-mail, kita dapat mengirimkan pesan kepada orang lain secara cepat. Namun kita sering mengeluh atas lamanya respon/balasan pesan yang kita kirim, dan proses balas pesan tidak praktis. Atas dasar itulah dibuatnya aplikasi instant masseger atau yang biasa disebut aplikasi *chatting*. Aplikasi *Chatting* merupakan aplikasi yang mengijinkan penggunanya dapat mengirimkan pesan secara satu waktu atau real-time yang membuat jarak sebenarnya seolah-lah tidak berarti.

Aplikasi *Chating* merupakan suatu jenis dari perkembangan teknologi.Dengan kecanggihan teknologi saat ini, fungsi aplikasi *chating* tidak hanya sebagai alat komunikasi biasa, tetapi manusia juga dapat mengirimkan foto dan lain-lainya. Aplikasi ini berbasis Web sehingga Dampak yang ditimbulkan dari Web *Chating* mungkin tidak disadari sama sekali. Selain memudahkan dalam berkomunikasi sebagai dampak positif yang manusia dapatkan, terdapat pula dampak negatif yang manusia dapatkan sebagai akibat menggunakan Web *Chating* ini. Kerahasiaan dan keamanan saat melakukan pertukaran data adalah hal yang sangat penting dalam komunikasi data, baik untuk tujuan keamanan bersama, maupun untuk privasi individu. Mereka yang menginginkan agar datanya tidak di ketahui oleh pihak - pihak yang sama sekali tidak berkepentingan selalu berusaha menyiasati cara mengamankan informasi yang akan dikomunikasikannya. Perlindungan terhadap kerahasiaan datapun meningkat, mulai dari menggunakan protocol jaringan tertentu yang mana sudah banyak diterapkan dibanyak aplikasi perturakan data.Akan tetapi, hal tersebut tidaklah sepenuhnya aman karena pesan masih bisa dibaca, dalam hal ini dibutuhkan pengaman ganda baik secara protocol maupun pengamanan secara display. Maka, selain memasang layer-layer protocol hendaknya juga menyandikan pesan tersebut atau disebut juga dengan proses enkripsi.

Di era mordern seperti sekarang banyak sekali alternatif algoritma enkipsi yang tersebar di dunia kriptografi, mulai dari algoritma enkripsi klasik sampai dengan algoritma enkripsi modern. Dalam penggunaannya juga bervariasi ada yang rumit, yang membutuhkan kunci berupa matriks-matriks tertentu, ada yang membutuhkan kunci yang ditentukan panjang minimal dan maksimal bit-nya, ada juga yang menggunakan dua kunci dalam implementasinya. Dalam aplikasi *chating* ini penulis memilih algoritma klasik Caesar Cihper karena pertimbangan penggunaanya yang jauh lebih simple dari algoritma-algoritma kriptografi yang lain, walaupun demikian *Caesar cipher* masih tetap algoritma enkripsi yang cukup powerfull karena merupakan penghulu dari semua algoritma enkripsi yang ada di dunia sampai saat ini.

Oleh karena itu, dengan berbagai pertimbangan alasan tersebut, maka perlu dikembangkan aplikasi *chatting* dengan algoritma kriptografi *Caesar cipher* sebagai

mekanisme keamanan dalam pengiriman data. Berdasarkan latar belakang di atas penulis mengakat judul "Aplikasi *Secretchatting* Dengan Mengimplementasikan Algoritma *Caesar cipher*" .

LANDASAN TEORI

Program Aplikasi

Program aplikasi adalah program yang melakukan suatu pekerjaan tertentu, seperti program gaji pada perusahaan. Oleh karena itu program ini hanya digunakan oleh bagian keuangan saja [4]. Biasanya program aplikasi ini dibuat oleh seorang programmer komputer sesuai dengan permintaan/kebutuhan sesorang atau lembaga atau perusahaan guna keperluan internalnya, seprti GL, MYOB, Payroll, dan lain-lain.

Cyber Espionage

Cyber Espionage terdiri dari kata *Cyber dan Espionage*. *Cyber* diartikan sebagai dunia maya atau internet sedangkan Espionage adalah tindak pidana mata-mata atau spionase, dengan kata lain *Cyber Espionage* adalah tindak pidana mata-mata terhadap suatu data elektronik atau kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain [5], dengan memasuki sistem jaringan komputer. Salah satu contoh kejahatan dari Cyber Espionage adalah.

Sniffing

Sniffing adalah tindakan penyadapan yang dilakukan dalam jaringan dengan tujuan untuk dapat mencuri data-data pribadi ataupun account lain yang bersifat pribadi. Karena data yang mengalir pada suatu jaringan bersifat bolak-balik, maka dengan proses *sniffing* ini dapat menangkap paket yang dikirimkan dan terkadang menguraikan isi dari RFC (Request for Comments).

Pengertian *Chat* Messaging

Chatting adalah "percakapan dua orang atau lebih secara realtime melalui jaringan internet" [2].*Chatting* adalah salah satu fasilitas yang ditawarkan oleh internet pada penggunanya untuk berkomunikasi langsung lewat percakapan. Cara *chatting* yang lebih umum dikenal dengan cara mengetikan pesan pada layar dan akan dibalas dengan bentuk pesan kembali, seperti cara mengirimkan SMS (Short Message Service). Namun *chatting* di internet terbatas pada jumlah karakter sehingga pengguna dapat menulis pesan cukup panjang".

Pengertian Kriptografi

Kriptografi mempunyai sejarah yang sangat menarik dan panjang.Kriptografi sudah digunakan 4000 tahun lalu, diperkenalkan oleh orang-orang Mesir lewat *hieroglyph*. Jenis tulisan ini bukanlah bentuk standar untuk menulis pesan pada zaman Romawi Kuno, pada suatu saat Julius Caesar ingin mengirimkan pesan rahasia kepada seorang jendral di medan perang. Pesan tersebut harus dikirimkan melalui seorang kurir. Karena pesan tersebut mengandung rahasia.Julius Caesar tidak ingin pesan rahasia tersebut sampai terbuka di jalan.Julius Caesar kemudian memikirkan bagaimana mangatasinya.Ia kemudian mengacak pesan tersebut hingga menjadi suatu pesan yang tidak dapat dipahami oleh siapapun terkecuali oleh jendralnya saja. Tentu sang jendral telah diberi tahu sebelumnya bagaimana cara membaca pesan teracak

tersebut. Yang dilakukan Julius Caesar adalah mengganti semua sususan alphabet dari a,b,c yaitu a menjadi d, b menjadi e, c menjadi f dan seterusnya [3].

Algoritma Kriptografi

Ditinjau dari asal-usulnya, kata algoritma mempunyai sejarah yang menarik.Kata ini muncul di dalam kamus *Webster* sampai akhit tahun 1957. Kata *algorism* mempunyai arti proses perhitungan dalam bahasa Arab. Algoritma berasal dari nama penulis buku Arab yang terkenal, yaitu Abu Ja'far Muhammad Ibnu Musa al-Khuwarizmi (al-Khuwarizmi dibaca orang barat sebagai algorism). Kata algorism lambat laun berubah menjadi algorithm [3]

Algoritma kriptografi terdiri dari tiga fungsi dasar, yaitu:

1. Enkripsi, merupakan hal yang sangat penting dalam kriptografi, merupakan pengamanan data yang dikirimkan agar terjaga kerahasiaanya. Pesan alsi disebut *plaintext*, yang diubah mejadi kode-kode yang dimengerti. Proses enkripsi adalah" proses mengubah *plaintext* menjadi *ciphertext*". *Plaintext* adalah data awal dan *ciphertext* adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi [6]
2. Dekripsi, merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya (teks-asli), disebut dengan dekripsi pesan. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan algoritma yang digunakan untuk enkripsi. Dekripsi adalah "kebalikan dari enkripsi yakni mengubah *ciphertext* menjadi *plaintext*, sehingga berupa data awal/asli" [6].
3. Kunci, yang dimaksud di sini adalah "kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci terbagi menjadi dua bagian, kunci rahasia(*private key*) dan kunci umum (*public key*)" [3].

Macam –Macam Algoritma Kriptografi

Algoritma kriptografi dibagi menjadi tiga bagian berdasarkan kunci yang dipakainya:

1. Algoritma Simetri (menggunakan satu kunci untuk enkripsi dan dekripsinya).
2. Algoritma Asimetri (menggunakan kunci yang berbeda untuk enkripsi dan dekripsi).
3. *HashFunction*.

Algoritma Simetri

Algoritma simetri sering disebut dengan algoritma klasik karena memakai kunci yang sama untuk kegiatan enkripsi dan dekripsi [3]. Algoritma ini sudah ada sejak lebih dari 4000 tahun yang lalu.Bila mengirimkan pesan dengan menggunakan algoritma ini, si penerima pesan harus diberitahu kunci dari pesan tersebut agar bisa mendekripsikan pesan yan dikirim.Keamanan pesan yang menggunakan algoritma ini tergantung pada kunci. Jika kunci tersebut diketahui oleh orang lain maka orang tersebut akan dapat melakukan enkripsi dan dekripsi terhadap pesan. Algoritma yang memiliki kunci simetri di antaranya adalah:

1. *Caesar cipher*.
2. Data Encryption Standard(DES).
3. RC2,RC4,RC5,RC6.
4. International Data Encryption Algorithm (IDEA).
5. Advanced Encryption Standard (AES).
6. One Time Pad(OTP).
7. A5,dan lain sebagainya.

Algoritma Asimetri

Algoritma asimetri sering disebut juga algoritma kunci publik, dengan arti kata kunci yang digunakan untuk melakukn enkripsi dan dekripsi berbeda [3]. Pada algoritma asimetri kunci terbagi menjadi dua bagian, yaitu:

1) Kunci umum (*public key*). Kunci yang boleh semua orang tahu (dipublikasikan).
2) Kunci rahasia (*private key*). Kunci yang dirahasiakan (hanya boleh diketahui oleh satu orang).

Kunci-kunci tersebut berhubungan satu sama lain. Dengan kunci publik orang dapat mengenkripsi pesan tetapi tidak bisa mendekripsikannya.Hanya orang yang memiliki kunci rahasia yang dapat mendekripsikan pesan tersebut.
Algoritma yang memakai kunci public di antaranya adalah:

1. Digital Signature Algorithm (DSA).
2. RSA.
3. Diffie-Hellman (DH).
4. Elliptic Curve Cryptografy (ECC).
5. Kriptografi Quantum, dan lain sebagainya.

Fungsi *Hash*

Fungsi Hash sering disebut dengan fungsi Hash satu arah (one way function), message digest, fingerprint, fungsi kompresi dan message authentication code(MAC), merupakan suatu fungsi matematika yang mengambil masukan panjang variabel dan mengubahnya kedalam urutan biner dengan panjang yang tetap. Fungsi Hash biasanya diperlukan bila ingin membuat sidik jari dari suatu pesan.Sidik jari pada pesan merupakan suatu tanda bahwa pesan tersebut benar-benar berasal dari orang yang diinginkan.

Algoritma *Caesar cipher*

Algoritma adalah urutan langkah-langkah untuk memcahkan suatu masalah, [7] Kata logis merupakan kata kunci dalam algoritma.Langkah-langkah dalam algoritma harus logis dan harus dapat ditentukan bernilai salah atau benar.Dalam beberapa konteks, algoritma adalah spesifikasi urutan langkah untuk melakukan pekerjaan tertentu.

Perangkat Lunak Yang Digunakan

1) PHP (HYPERTEXT PROCESSOR)

Sejarah singkat PHP, Rasmus Lerdorf kurang puas dengan sistem yang ada pada saat itu sehingga dia menciptakan suatu model interface (antarmuka) yang dapat digunakan untuk menampung informasi tentang para pengunjung situsnya. Pertama kali, Rasmus membuat interace dengan menggunakan PERL dan selanjutnya dia mengembangkan dengan menggunakan bahasa C untuk memberikan fleksibelitas pada interface/parser tersebut [8].

2) MYSQL (MY STRUCTURED QUERY LANGUAGE)

MySQL merupakan salah satu database server yang berkembang di lingkungan open source dan didistribusikan secara free (gratis) dibawah lisensi GPL. MySQL merupakan RDBMS (*Relational Database Management System)server*.RDBMS adalah program yang memungkinkan pengguna database untuk membuat, mengelola, dan

menggunakan data pada suatu model relational. Dengan demikian, tabel-tabel yang ada pada database memiliki relasi antara satu tabel dengan tabel lainnya [9]

3) NoSQL (Not Only SQL)

Menurut Feri ardiansyah (2016:3) NoSQL meliputi berbagai macam teknologi database yang berbeda dan dikembangkan dalam menanggapi kenaikan volume data yang tersimpan tentang pengguna, objek dan produk, frekuensi dimana data ini diakses, dan kinerja pengolahan kebutuhan. Database relasional, disisi lain tidak dirancang untuk mengatasi dengan skala dan kelincahan tantangan yang dihadapi aplikasi moderen, mereka juga tidak dibangun untuk mengambil keuntulangan dari penyimpanan murah dan kekuatan pemrosesan yang tersedia saat ini.

4) *Firebase Real Time Database*

Basis Data Realtime adalah basis data NoSQL dan karena itu memiliki optimalisasi dan fungsionalitas yang berbeda dibandingkan dengan basis data relasional.API Database Realtime dirancang hanya untuk memungkinkan operasi yang dapat dijalankan dengan cepat.Ini memungkinkan Anda untuk membangun pengalaman real-time yang hebat yang dapat melayani jutaan pengguna tanpa kompromi pada daya tanggap.Karena itu, penting untuk memikirkan bagaimana pengguna perlu mengakses data Anda dan kemudian menyusunnya [10].

5) Firebase Storage

Cloud Storage for Firebase adalah layanan penyimpanan objek yang kuat, sederhana, dan hemat biaya yang dibangun untuk skala Google.Firebase SDKs untuk Penyimpanan Cloud menambahkan keamanan Google ke file unggahan dan unduhan untuk aplikasi Firebase Anda, terlepas dari kualitas jaringan.Anda dapat menggunakan SDK kami untuk menyimpan gambar, audio, video, atau konten buatan pengguna lainnya. Di server, Anda dapat menggunakan Google Cloud Storage, untuk mengakses file yang sama [11].

6) Protokol Pada Jarigan Komputer

Perkembangan jaringan komputer dan perkembangan teknologi dalam bentuk perangkat keras dan perangkat lunak, turut berperan di dalam munculnya sejumlah protokol baru maupun versi baru dari suatu protokol. Hal ini cukup mendasar mengingat banyaknya aplikasi dan layanan yang dijalankan di jaringan komputer (terutama internet), yang mana memerlukan adanya protokol dan port [12].

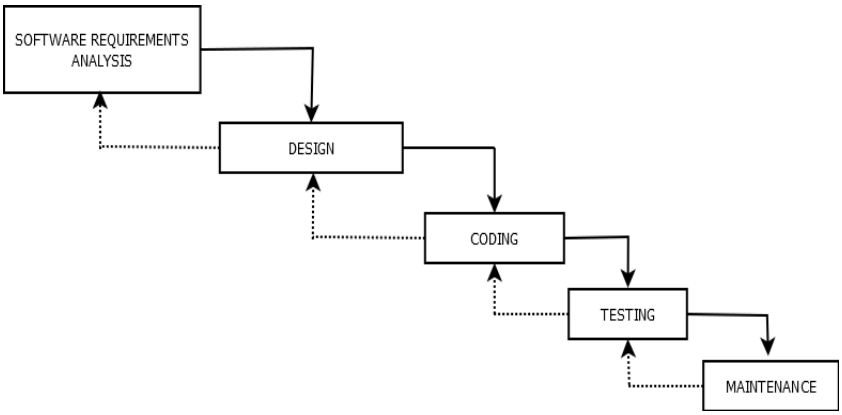
7) TCP/IP (Transmisson Control Protocol / Internet Protocol)

Protokol TCP/IP “merupakan sepasang protokol yang umum digunakan di hampir semua layanan dan aplikasi di dalam jaringan inteirnet” [12].Pasangan protokol ini umum disebut dengan protocol suite dan menjadi pemodelan untuk layering pada jaringan komputer sebagaimana layering OSI.Tidak seperti protokol lainnya, pada protokol TCP/IP terdapat empat buah sub protokol yang memiliki fungsionalitas masing-masing.

METODE PENELITIAN

Metode yang digunakan dalam pengembangan aplikasi *chat* ini adalah metode waterfall. Alasan menggunakan metode ini adalah karena metode waterfall melakukan pedekatan secara sistematis dan berurutan dalam membangun suatu sistem. Proses metode waterfall yaitu pengerjaan dari suatu sistem dilakukan secara berurutan. Sistem

yang dihasilkan akan berkualitas baik, dikarenakan pelaksanaanya secara bertahap sehingga tidak terfokus pada tahapan tertentu. Tahapan metode waterfall adalah:



Gambar 1 Tahapan Metode *Waterfall*

Software dan *Hardware*

1) Perangkat Lunak *(Software)*
   Perangkat lunak digunakan pada penelitian adalah sebagai berikut:
   a. *Sistem operasi linux cinamon 19.1 x64*
   b. *Sublime Text 3*
   c. *Xampp versi v3*
2) PerangkatKeras *(Hardware)*
   Perangkat keras digunakan untuk melakukan percobaan terhadap aplikasi *secretchatting* ini spesifikasinya sebagai berikut:
   a. *Processor : Inte® Core™ i-3, ~ 2.3GHz.*
   b. *VGA : intel® HD Graphics 3000.*
   c. *RAM : 2GB.*
   d. *Hardisk Internal : 500 GB.*
   e. *Mouse : Votre 3D Optical Mouse.*

Metode Perancangan Sistem

1) Analisa Sistem

Dalam merancang sebuah sistem. Analisis mutlak harus dilakukan. Dengan melakukan analisis yang baik tehadap sistem yang akan dikerjakan, akan memudahkan kita dalam melakukan perancangan sistem, dan apabila di kemudian hari sistem kita ingin dilengkapi maka akan mudah dalam menyelesaikannya.
Salah satu unsur terpenting yang harus dipertimbangkan dalam tahapan analisis sistem ini yaitu masalah aplikasi, karena nantinya aplikasi yang digunakan haruslah sesuai dengan masalah yang akan diselesaikan. Untuk itu, analisis yang dilakukan terhadap aplikasi algoritma *Caesar cipher* ini akan dibagi kedalam beberapa aspek, yaitu analisis kebutuhan perangkat lunak *Caesar cipher*, analisis proses enkripsi dan dekripsi algoritma *Caesar cipher* .

2) Analisa Kebutuhan

ISSN: XX32-XX45 GATOT KACA JOURNAL e-ISSN : XX67-XX89
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa

Faktor yang mendasari dibentuknya aplikasi dengan algoritma *Caesar cipher* adalah keamanan data. Keamanan data telah menjadi aspek yang sangat penting dari suatu in*forma*si. Sebuah in*forma*si umumnya hanya ditujukan bagi segolongan orang tertentu. Oleh karena itu sangatlah penting untuk mencegahnya agar tidak jatuh kepada pihak-pihak yang tidak yang tidak berhak. Untuk keperluan tersebut, maka diperlukan sebuah kriptografi dengan metode enkripsi dan dekripsi pesan. Aplikasi ini nantinya akan mengenkripsi pesan / *chat*. Aplikasi ini akan mengenkripsikan pesan yang akan dikirimkan menjadi cipertext dan mendekripsikannya menjadi *plaintext*. Dalam membangun aplikasi nanti, diperlukan batasan yang jelas sebagai tujuan agar tidak keluar dari rencana yang telah ditetapkan.

Perancangan Pengujian

Black-boxtesting adalah metode pengujian perangkat lunak yang mengetes fungsionalitas dari aplikasi yang bertentangan dengan struktur internal atau kerja. Pengetahuan khusus dari kode aplikasi / structural internal dan pengetahuan pemrograman pada umunya tidak diperlukan. Uji kasus dibangun di sekitar spesifikasi dan persayaratan, yakni, aplikasi apa yang harusnya dilakukan. Melakukan deskripsi eksternal perangkat lunak, temasuk spesifikasi, persyaratan, dan desain untuk menurunkan uji kasus. Tes ini dapat menjadi fungsionalitas atau non-fungsionalitas, meskipun biasanya fungsional. Perancang uji memilih input yang valid dan tidak valid dan menentukan output yang benar. Tidak ada pengetahuan tentang struktur internal benda uji itu.
Metode Black Box memungkinkan perekayasa perangkat lunak mendaptkan serangkaian kondisi input yang sepenuhnya menggunakan semua persyaratan fungsionalitas untuk suatu program.

HASILDAN PEMBAHASAN

Aplikasi *secretchatting* ini dibuat dengan bahasa pemrograman PHP&MYSQL dan JavaScript. Aplikasi ini digunakan untuk melakukan pertukaran data dan in*forma*si yang berupa pesan yang *formal* dan non-*forma*l. Selain *user* dapat melakukan pertukaran pesan, *user* juga mendapatkan fasilitas keamanan dalam melakukan proses pertukaran pesan. Dalam melakukan pengenkripsian aplikasi *secretchatting* ini menerapkan algoritma kriptografi dengan metode caeser *cipher*. Aplikasi ini terdiri dari dua level pengguna dan terdiri dari beberapa menu dan *form*, yang akan dijelaskan dipoin pembahasan di bawah ini

Pembahasan Menu dan *Form* Level *user*

Berikut ini adalah menu-menu dan *form-form* yang ada pada level *user* pada aplikasi *secretchatting* dengan mengimplementasikan algoritma *Caesar cipher*.

1) Form Login

Form login adalah *form* yang pertama kali muncul pada saat aplikasi ini dibuka jika *user* belum pernah login sebelumnya, dan atau *user* sudah keluar dari menu pengguna.

2) Form Registrasi

Form registrasi adalah *form* yang akan muncul saat *user* mengklik/menekan tombol daftar yang berada di bawah tombol login.

3) Menu Pengguna

Menu pengguna adalah menu utama yang digunakan sebagai tempat *user* untuk melakukan pertukaran pesan dan menggunakan berbagai feature yang ada pada aplikasi *secretchatting* ini.

4) Card Contacts

Feature card contacts ini menampilkan data *user* yang login berdasarkan session login *user* dan juga menampilkan semua *user* yang telah terdaftar pada aplikasi *secretchatting* ini lengkap dengan foto profil, status *online*/*offline*, *iconreportuser*, notifikasi pesan yang masuk.

5) Card Group Chat

Feature ini berfungsi untuk menampilkan percakapan yang dilakukan seluruh *user* yang sudah terdaftar pada aplikasi *secretchatting* ini.

6) Card Caesar cipher

Card ini berfungsi untuk melakukan dekripsi dari *ciphertext*/pesan yang sudah dienkripsi *user* dengan cara memasukan pesan yang berupa *ciphertext* dan juga kunci yang digunakan.

7) Menu user info

Menu ini digunakan untuk melakukan pengeditan untuk masing-masing data yang ada pada *user* yang sudah login.

8) Menu Private Chat

Menu ini digunakan *user* untuk melakukan *chat* secara private dengan *user* lain yang telah terdaftar pada aplikasi*secretchatting* ini.

9) Menu History Cipher

Menu ini digunakan untuk menampilkan semua pesan-pesan yang dienkripsi sehingga *user* dapat melakukan dekripsi ulang dikemudian hari.

10) Menu *About Author*

Menu ini digunakan unutk menampilkan in*form*asi terkait dengan penulis/peneliti dari program ini.

Pembahasan Menu dan *form* Level Administator

1) *Form Login*
   Form login yang ada pada *leveladmnistrator* ini digunakan sebagai tempat admin untuk melakukan login agar bisa masuk ke menu utama admin, agar bisa memanage data *user* yang ada pada aplikasi *secretchatting* ini.
2) *Menu Utama Admnistrator*
   Menu ini digunakan oleh admin untuk memantau aktifitas *chatting* yang dilakukan oleh semua *user* yang telah terdaftar pada aplikasi ini, selain itu menu ini juga menampilkan semua *user* yang telah terdaftar lengkap berserta dengan status *online* dan juga *offline*.
3) *Menu History Report*
   Menu ini berfungsi untuk menampilkan data *history* dari *report* yang telah dilakukan oleh *user* yang terdaftar pada aplikasi *secretchatting* ini.
4) *Form Banned user*
   Form ini dapat digunakan admin untuk melakukan banned pada *user* yang telah dilaporkan sebagai tidak lanjut dari laporan *user*.

ISSN: XX32-XX45 GATOT KACA JOURNAL e-ISSN : XX67-XX89
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa

PengujianAlgoritma *Caesar cipher*

Dalam pembahasan ini akan dilakukan pengujian untuk algoritma enkripsi *Caesar cipher*. Apakah sudah berjalan dengan baik atau belum, dari proses enkripsi dan dekripsi. Dalam pengujian ini kita asumsikan *user*1 mengirim pesan yang terenkripsi dengan kunci 3 kepada *user*2.Berikut pembahasan enkripsi dan dekripsinya.

1) Proses Enkripsi
   Proses enkripsi dilakukan dengan cara menggeser ke kanan huruf yang sudah dirubah ke dalam bentuk karakter ASCII dengan jumlah kunci yang digunakan atau yang sudah disepakati oleh kedua belah pihak.
2) Proses Dekripsi
   Sebaliknya Proses dekripsi dilakukan dengan cara menggeser ke kiri huruf yang sudah dirubah ke dalam bentuk karakter ASCII dengan jumlah kunci yang digunakan atau yang sudah disepakati oleh kedua belah pihak.

Pengujian *Sniffing*

Pengujian *sniffing* ini dilakukan untuk memastikan bahwasanya protocol tcp/ip yang dipasang pada aplikasi ini berkerja dengan baik, sehingga dapat mengenkripsi pertukaran data yang ada pada aplikasi *secretchatting* ini.
Dari pengamatan pengujian *sniffing* pada aplikasi *secretchatting* tanpa menggunakan SSL dapat dilihat pada bagian yang diwarnai kuning, bahwasanya paket data yang muncul berupa teks biasa tanpa terenkripsi dan dapat dengan mudah dibaca oleh para *sniffers*. Sehingga dapat disimpulkan bahwasanya pengujian dengan teknik *sniffing* berhasil dan diterima.

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan pembahasan dan hasil pengujian didapatkan kesimpulan sebagai berikut:

1) Dihasilkan Aplikasi *secretchatting* yang mampu menerapkan algoritma kriptografi *Caesar cipher* sebagai salah satu *alternative* untuk mengamankan pesan teks.
2) Dan untuk membangun aplikasi *secretchatting* yang aman selain menggunakan algoritma kriptografi *Caesar cipher* juga diperlukan penerapan protocol TCP/IP pada aplikasi *secretchatting*.
3) Dalam pengaplikasiannya Algorima *Caesar cipher* tidak dapat mengenkripsi data yang berupa gambar

Saran

Pada penelitian ini tentu masih terdapat kekurangan yang dapat disempurnakan lagi pada pengembangan sistem berikutnya. Beberapa saran yang dapat dipergunakan diantaranya:

1) Aplikasi *secretchat* ini perlu ditambah fitur pengiriman berupa file dokumen, file media.
2) Aplikasi *secretchat* ini perlu ditambahkan fitur panggilan suara dan panggilan video.
3) Aplikasi *secretchatting* ini perlu dilakukan perbaikan dalam hal *design* dan layout agar lebih *flexible* dan lebih *mobile friendly.*

DAFTAR PUSTAKA

Ardiansyah,Feri. 2016. *Perangkat Lunak Pengajaran Basis Data NoSQL Berbasis Mobile.Skripsi Tidak Diterbitkan*.Palembang. In*form*atika Universitas Binadarma.

Asprina,Tasya. 2018. *Pembangunan Aplikasi Keamanan Pesan Chatting Dengan Menerapkan Algoritma Tiny Encryption Algorithm(TEA) Berbasis Client Server.*skripsi tidak diterbitkan. Kendari.Teknik Universitas Halu Oleo.

Ariyus, Dony. 2008. *Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasinya.*Yogyakarta. Penerbit Andi. 437 hal.

Simarmata, Janner. 2006. *Pengenalan Teknologi Komputer dan Informasi.Yogyakarta. Penerbit Andi.*513 hal (2002) The IEEE website.[*Online*]. Available: http://www.ieee.org

Nicko Shelly. 2010. *Tindak Pidana Cyber Espionage*.Skripsi tidak diterbitkan. Hukum Universitas Airlangga. 70 hal

Srimulyani. 2016. *Algoritma Camellia Untuk Keamanan Data Menggunakan Aplikasi Kriptografi* . Riau. Politeknik Caltex Riau. 126 hal.

Munir, Renaldi.2007. *Algoritma & Pemrograman Dalam Bahasa Pascal dan C*. Bandung.In*form*atika Bandung.591 hal.

Sakur, B, Stendy. 2010. PHP 5 dan Pemrograman Berorientasi Objek-Konsep Dan Implementasi.Yogyakarta. Andi. 386 **Hal** *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Std. 802.11, 1997.

Irwan. 2017. *Implementasi Kriptografi Rsa (Rivest-Shamiradleman) Pada Sistem Aplikasi File Transfer Berbasis Web : Kriptografi Rsa*. Skripsi Tidak Diterbitkan.Malang, Teknik Universitas Muhammadiyah Malang. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Std. 802.11, 1997.

Firebase, 2018, Firebase Realtime Database.https://firebase.google.com/docs/database/, diakses 30 maret 2019.

Firebase,2018,CloudStorage. https://firebase.google.com/docs/storage/, diakses 30 maret 2019.

Putu, Agus, I . 2014. Handbook Jaringan Komputer. Bandung.In*form*atika Bandung.