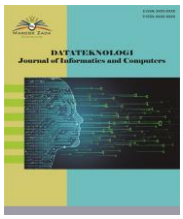
DATA TEKNOLOGI
Journal of Informatics and Computers
Vol. 1, No. 1, April (2023), Page 1-8
P-ISSN (2985-9689) & E-ISSN (2986-0687)



Implementasi Algoritma Vigenere Cipher Dan Rot13 Untuk Keamanan Pesan Pada Aplikasi Chatting

Desi Puspita Sari[1], Nidia Enjelita Saragih[2]

[12]Prodi Teknik Informatika, Fakultas Teknik dan Ilmu Komputer, Universitas Potensi Utama, Indonesia
*Corresponding Author. E-mail: desipuspita1112@gmail.com

Abstrak

Android adalah salah satu alat komunikasi yang umum digunakan oleh sebagian masyarakat untuk pertukaran informasi dan mengirimkan pesan. Android menyediakan media untuk melakukan komunikasi pertukaran pesan yaitu aplikasi chatting. Pertukaran pesan melalui chatting ini sangat popular penggunaannya di kalangan masyarakat dikarenakan begitu mudah tanpa khawatir jarak dan waktu.Salah satu algoritma yang dapat diterapkan dalam mengamankan pesan adalah ROT 13 (*Roll Over Test*) dan *Vigenere Cipher*. Algoritma ROT 13 (*Roll Over Test*) yaitu algoritma enkripsi sederhana dari Caesar Cipher dengan pergeseran 13, sedangkan algoritma *Vigenere Cipher* menyembunyikan pesan berupa teks melalui teknik substitusi dengan mengubah setiap huruf menjadi huruf lain berdasarkan tabel kunci yang digunakan. algoritma ini melakukan pengamanan dengan mengacak pesan sehingga pesan yang disampaikan tidak dapat untuk dimengerti dan juga kerahasiaan pesan asli dapat terjaga dengan aman.

Kata kunci: *android, chat, rot13, vigenere chiper*

Abstract

Android is a communication tool that is commonly used by some people to exchange information and send messages. Android provides a medium for exchanging messages, namely chat applications. The exchange of messages through chat is very popular among the people because it is so easy without worrying about distance and time. One of the algorithms that can be applied to secure messages is ROT 13 (Roll Over Test) and Vigenere Cipher. The ROT 13 (Roll Over Test) algorithm is a simple encryption algorithm from Caesar Cipher with a shift of 13, while the Vigenere Cipher algorithm hides messages in the form of text through a substitution technique by changing each letter into another letter based on the key table used. This algorithm performs security by randomizing the message so that the message conveyed cannot be understood and also the confidentiality of the original message can be maintained safely.

***Keywords**: android, chat, rot13, vigenere chiper*

PENDAHULUAN

Aplikasi chatting merupakan suatu jenis dari perkembangan suatu teknologi. Dengan kecanggihan teknologi saat ini, fungsi aplikasi chating tidak hanya sebagai alat komunikasi biasa, tetapi manusia juga dapat mengirimkan foto dan lain-lainya. Dampak yang ditimbulkan dari chatting mungkin tidak disadari sama sekali. Selain memudahkan dalam berkomunikasi sebagai dampak positif yang didapatkan manusia, terdapat pula dampak negatif yang didapatkan manusia sebagai akibat menggunakan chatting ini (Situmorang et al., 2017).

Penggunaan *smartphone* yang saat ini begitu banyak yang dapat dimanfaatkan, contoh nya dengan menggunakan aplikasi

Submitted 04-02-2023 **Accepted** 06-02-2023 **Published** 12-02-2023 : https://doi.org/10.56248/datateknologi.v1i1.48

chatting. Aplikasi chatting merupakan aplikasi untuk berkomunikasi yang dilakukan oleh dua orang atau lebih dengan mengirim pesan teks. Aplikasi chatting saat ini seperti whatsapp, bbm, line, dan lainnya sangat membantu dengan banyaknya fitur didalamnya. Contohnya, pengiriman pesan berupa teks, gambar, audio maupun video (Khairil & Hayati, 2020).

Chatting merupakan salah satu metode komunikasi yang bersifat real-time. Untuk dapat menggunakan aplikasi tersebut kita terlebih dahulu melakukan penginstalan, tetapi jika tidak ingin maka ada sebuah aplikasi chatting, yang berbasis web (Adinta & Neforawati, 2019).

Dalam pertukaran data menggunakan LAN dan WLAN. Begitu juga dalam pertukaran informasi pesan chatting, pencuri informasi dapat menyusup ke alamat IP pada jaringan LAN dan WLAN sehingga dapat mencuri dan memiliki akses yang sama dengan pengguna jaringan LAN dan WLAN yang lain (Anwar, Roslina & Agustin, 2020).

Pertukaran informasi melalui ruang publik masih menyisakan kerentanan keamanan, sehingga perlu mekanisme pengamanan melalui proses kriptografi. Salah satu model kriptografi yang dapat bertahan hingga lebih dari 300 tahun adalah Vigenere Cipher, sebelum dipecahkan oleh Kasiski dan Friedman (Ardhianto et al., 2021).

Vigenere cipher adalah salah satu algoritma kriptografi klasik yang diperkenalkan kira-kira pada tahun 1986. Algoritma kriptografi ini dipublikasikan oleh seorang diplomat dan juga kriptologis yang berasal dari Prancis, yaitu Blaise de Vigenere. Model matematika dari enkripsi pada algoritma vigenere cipher ini adalah seperti berikut: 1. Model enkripsi Ci = Ek (Mi) = (Mi+Ki) mod 26 2. Model deskripsi Mi = Dk (Ci) = (Ci-Ki) mod 26 (Ryan, Perdana & Budiman, 2020).

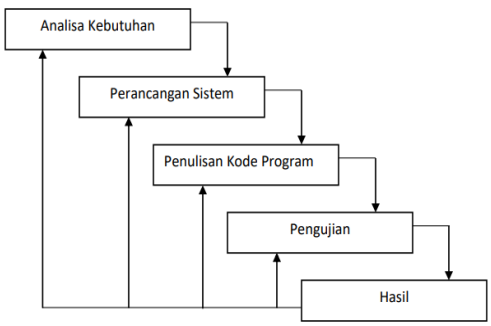
Kriptografi adalah sebagai ilmu untuk menjaga sebuah kerahasiaan data, dan seperti authentikasi data. Namun pada pengertian modern kriptografi terdiri dari dua kegiatan yang saling berkaitan. dua proses tersebut disebut enkripsi dan deskripsi. Enkripsi adalah mengubah data atau yang disebut istilah plain text dalam kriptografi menjadi sebuah kode acak yang tidak dapat dibaca yang disebut cipher text (Fajri, Sembiring & Hasan, 2020).

Firebase Realtime Database Merupakan salah satu layanan dari firebase yang bertujuan untuk melakukan manajemen database, bersifat NoSQL dan dalam bentuk JSON. Layanan ini sangat optimal untuk digunakan karena kemampuannya dalam melakukan proses komunikasi dengan Client sangat cepat (Kurniawan & Samsudin, 2021).

Rot13 (Rotate 13) ialah enkripsi cipher substitution yang pada umum nya digunakan di operasi sistem UNIX. Sistem pada enkripsi Rot13 huruf digantikan dengan sebuah huruf yang terletak di atas posisi 13 darinya (Kurniawan, & Samsudin, 2021).

METODE PENELITIAN

Pengembangan sistem dapat berupa menyusun suatu sistem yang baru dan menggantikan sistem yang lama secara keseluruhan atau memperbaiki sistem yang telah ada (Rosa & Shalahuddin, 2018: 39). Setiap tahap harus diselesaikan terlebih dahulu kemudian diteruskan ketahap berikutnywa untuk menghindari terjadinya pengulangan tahap. Metodologi pengembangan sistem *Waterfall* dapat dilihat pada gambar 1 berikut :



Gambar 1. Prosedur Perancangan Sistem

Dalam pengembangannya metode *waterfall* memiliki beberapa tahapan yaitu : *requirement* (analisis kebutuhan), design

sistem (*system design*), *coding*, pengujian program, pemeliharaan sistem

1. Analisis Kebutuhan

Peneliti menganalisis kebutuhan untuk perancangan sistem berupa perangkat lunak yaitu *Android Studio* yang digunakan untuk merancang aplikasi sertaa perangkat keras seperti laptop untuk membangun sebuah aplikasi.

2. Desain Sistem

Pada tahap ini peneliti merancang sebuah desain dari aplikasi pengamanan pesan *chatting* dengan menggunakan algoritma *Rot* 13 dan *Vigenere Cipher*. Serta menggunakan pemodelan UML yaitu *use case diagram, class diagram, activity diagram, dan Sequence diagram* untuk perancangan sistem.

3. Penulisan Sinkode Program

Pada proses pengamanan aplikasi *chatting*, peneliti menggunakan metode *Rot* 13 dan *Vigenere Cipher* dengan menggunakan bahasa *Java* pada aplikasi *Android Studio*.

4. Pengujian Program

Pada tahap ini peneliti melakukan pengujian aplikasi pengamanan pesan pada aplikasi *chatting* dengan Algoritma *Rot* 13 dan *Vigenere Cipher* secara keseluruhan. Seperti pengujian fungsional dan pengujian kemampuan aplikasi dalam mengamankan pesan apakah sudah berjalan dengan baik.

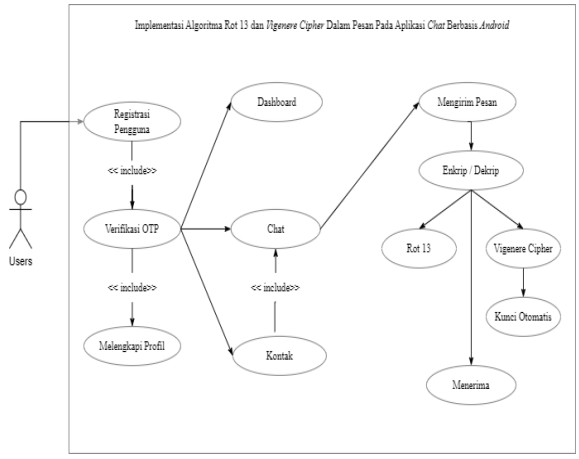
5. Pemeliharaan Sistem

Pada tahapan ini peneliti telah menyelesaikan seluruh penelitian baik teori maupun aplikasi yaitu "Implementasi Algoritma *Vigenere Cipher* dan *Rot* 13 untuk Keamanan Pesan pada Aplikasi *Chatting*"

HASIL DAN PEMBAHASAN

Use Case Diagram

Sistem yang akan dirancang digambarkan dengan *usecase diagram* yang terdapat pada Gambar 2 berikut :



Gambar 2. *Usecase* Diagram

Aktivitas *usecase* yang dilakukan dapat diterangkan dengan langkah-langkah *state* berikut :

a. Users harus terlebih dahulu untuk melakukan registrasi pengguna dengan memasukan no telepon yang valid.
b. Apabila no telepon yang dimasukan valid, maka akan otomatis melalui proses verifikasi OTP.
c. Setelah verifikasi OTP berhasil, maka users sudah bisa melengkapi profil secara benar.
d. Setelah melengkapi profil, user akan melihat tampilan dashboard, chat, dan kontak pada aplikasi
e. Proses enkripsi dan dekripsi pesan terjadi didalam menu chat.
f. Dimana nantinya proses enkripsi akan berlangsung apabila pesan yang sudah diketik langsung dikirimkan kepada users lainnya.
g. System yang digunakan pada enkripsi yaitu terlebih dahulu diamankan dengan menggunakan ROT 13 lalu diamankan dengan menggunakan Vigenere cipher. Dimana kunci yang digunakan telah ditentukan oleh system.

Pada bab ini akan dijelaskan tampilan hasil dari aplikasi yang telah dibuat, yang digunakan untuk memperjelas tentang tampilan – tampilan yang ada pada perancangan Aplikasi *chat* berbasis *Android*. Sehingga hasil implementasinya dapat dilihat sesuai dengan hasil program yang telah dibuat. Dibawah ini akan

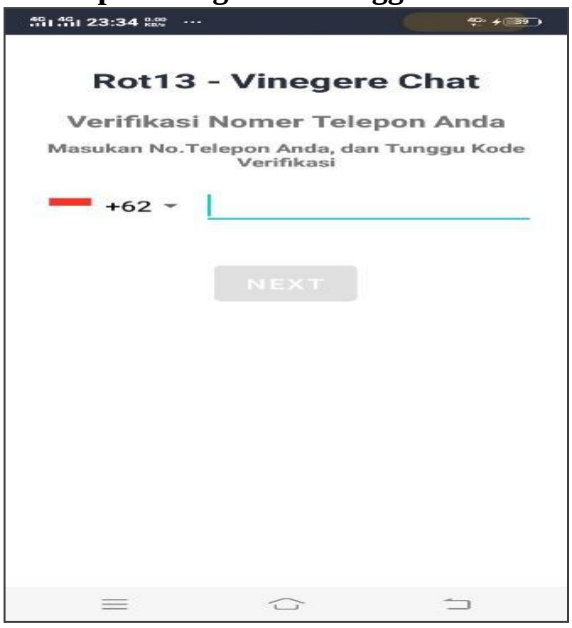
dijelaskan tiap tiap tampilan yang ada pada aplikasi:

1. Tampilan *Splash Screen*

Gambar 3. Tampilan *Splash Screen*

Tampilan *Splash Screen* adalah merupakan tampilan yang akan muncul setiap kali aplikasi dipergunakan, tampilan ini adalah merupakan tampilan pembuka dari aplikasi, tampilan ini akan secara otomatis menghilang setelah beberapa detik dan akan membuka halaman tampilan berikutnya.

2. Tampilan Registrasi Pengguna



Gambar 4. Tampilan Registrasi Pengguna

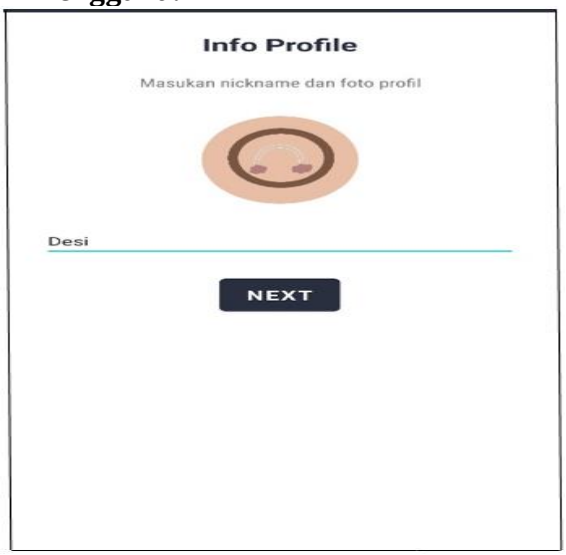
Pada tampilan halaman ini pengguna yang belum terdaftar harus melakukan proses pendaftaran terlebih dahulu, proses pendaftaran akun pada aplikasi menggunakan verifikasi nomer telepon yang aktif, hal ini bertujuan agar pengguna dapat menerima kode OTP (*One Time Password*) verifikasi yang akan dikirimkan via SMS.

3. Tampilan Kode OTP

Gambar 5. Tampilan Verifikasi Kode OTP

Setelah pengguna memasukan nomer telpon dengan benar selanjutnya akan ditampilkan halaman verifikasi kode OTP, kode OTP yang dikirimkan akan secara otomatis mengisi *form* yang telah disediakan, jika nomer telepon yang dipergunakan berada di perangkat yang sama, namun jika nomer telepon yang dipergunakan berda pada perangkat lain, maka pengguna harus mengisikan secara manual kode OTP yang dikirim. Jika proses verifikasi kode OTP gagal dilakukan maka pengguna harus meminta ulang pengiriman kode OTP dengan meng-klik pada tombol kirim ulang sms.

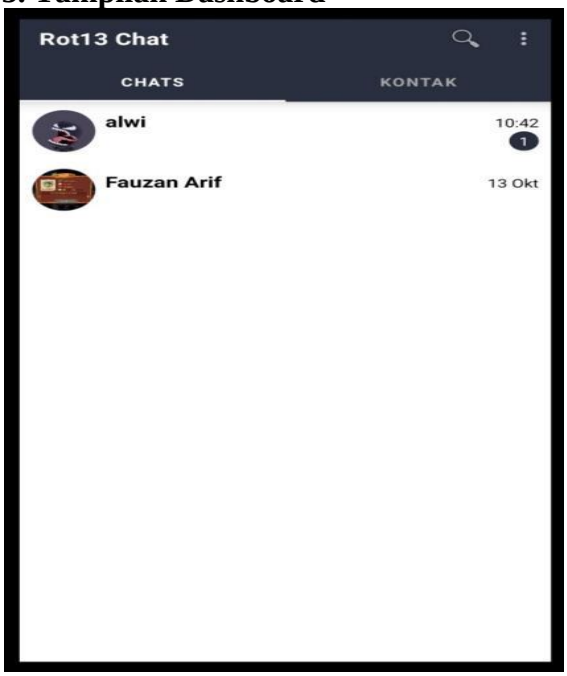
4. Tampilan Halaman Setting Profil Pengguna.



Gambar 6. Tampilan Setting Profil Pengguna

Pada *form* ini pengguna dapat mengatur gambar profil dengan meng-klik pada logo *image*, yang terletak di atas form isian nama profile.

5. Tampilan Dashboard

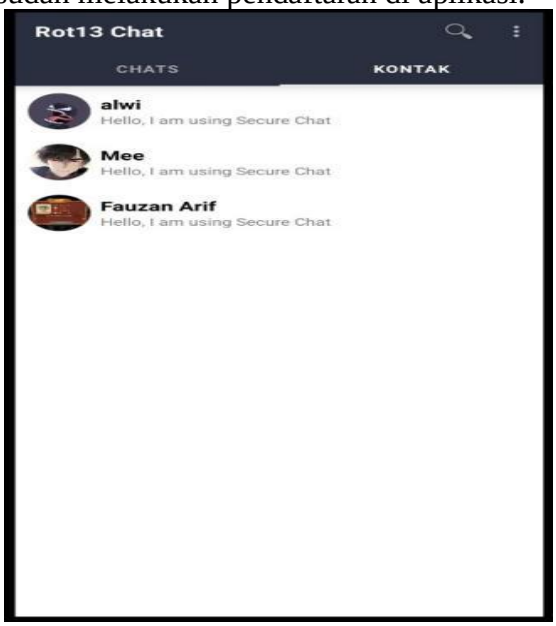


Gambar 7. Tampilan Dashboard

Pada bagian ini akan tampilkan semua *chat* yang sudah pernah dilakukan oleh pengguna.

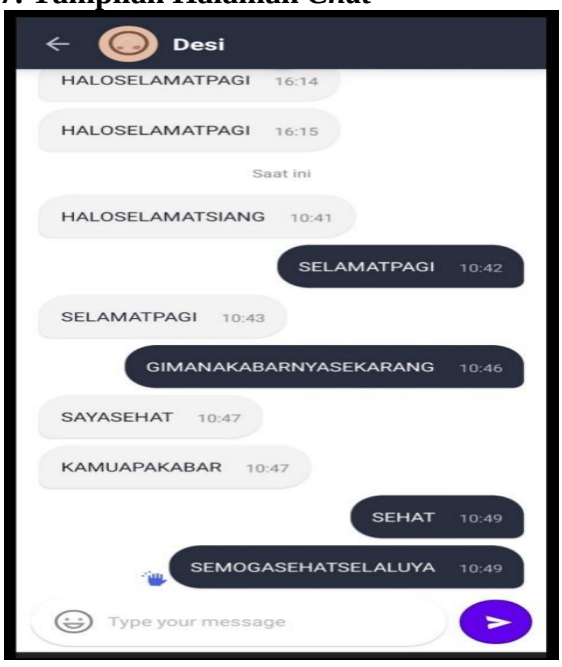
6. Tampilan Kontak

Tampilan halaman ini berfungsi untuk menampilkan seluruh kontak yang sudah melakukan pendaftaran di aplikasi.



Gambar 8. Tampilan Halaman Utama (*Fragment Kontak*)

7. Tampilan Halaman *Chat*



Gambar 9. Tampilan Halaman Chat

Gambar 9 adalah merupakan tampilan dari halaman *chat* yang sedang dilakukan oleh pengguna, pada tampilan diatas terlihat bahwa *chat* yang dikirimkan dan diterima oleh pengguna berisikan teks yang tidak terenkripsi. Konsep yang diterapkan pada proses chat ini adalah konsep *End To End*

Encryption, yang artinya bahwa proses enkripsi dilakukan saat pengguna mengirimkan pesan *chat* kepada lawan *chat* dan dilakukan proses dekripsi saat *chat* di terima.

Skenario Pengujian

Pengujian ini bertujuan untuk memastikan bahwa aplikasi *chat* dengan menggunakan implementasi Algoritma *Rot*13 dan *Vinegere Cipher* yang telah berhasil dibangun dapat berkerja dengan baik dan tidak ada terjadi kesalahan dalam proses pengoperasiannya

Tabel 1. Pengujian Registrasi Pengguna

No	Pengujian	Target Pengujian	Pengamatan	Kesimpulan
1	Menggunakan nomor telepon yang tidak valid	Menampilkan pesan bahwa nomor yang dimasukan tidak dapat dipergunakan	Berhasil menampilkan pesan peringatan bahwa nomor yang dipergunakan tidak valid, dan kembali ke *activity* regstrasi	Hasil Pengujian Berhasil
2	Menggunakan nomor telepon yang valid	Mengarahkan pengguna ke *activity* verifikasi OTP	Berhasil mengarahkan pengguna ke halaman verifikasi OTP	Hasil Pengujian Berhasil

Tabel 2. Tabel Pengujian *Chatting*

No	Pengujian	Target Pengujian	Pengamatan	Kesimpulan
1	Pengiriman *Chat* melalui *Frament* Kontak	Memilih kontak dan melakukan *chat*	Berhasil melakukan *chat* via kontak	Hasil Pengujian Berhasil
2	Pengiriman Chat melalui *Fragment Chat*	Melakukan proses *chatting* melalui *fragment chat*	Berhasil melakukan *chat* via Fragment Chat	Hasil Pengujian Berhasil
3	*End To End Encryption*	Melakukan proses enkripsi saat mengirimkan *chat* dan menyimpan hasil enkripsi pada *Database Firebase*, mengirimkan *chat* kepada pengguna yang dituju dan melakukan proses *dekripsi* berdasarkan chat yang enkripsi pada *database*.	*Chat* enkripsi berhasil disimpan kedalam database dalam bentuk *Ciphertext*, penerima *chat* menerima pesan *chat* dalam bentuk *plainttext*	Hasil Pengujian Berhasil

Kelebihan dan Kekurangan Sistem

Setiap sistem memiliki kelebihan dan kekurangan, berikut ini adalah kelebihan dan kekurangan sistem yang telah dibuat.

Kelebihan Sistem

Kelebihan sistem ini diantaranya yaitu :

1. Tampilan dari aplikasi sederhana dan mudah dipergunakan, serta mirip dengan aplikasi *chat* yang selama ini sudah dikenal dikalangan pengguna internet.
2. Aplikasi sudah menerapkan sistem metode verifikasi dengan menggunakan nomor telepon dan kode OTP, sehingga pengguna yang menggunakan nomor telepon yang valid dapat menggunakan aplikasi ini.
3. *Chat* yang ditampilkan adalah *chat realtime*, yang artinya tidak dibutuhkan proses *refresh* halaman untuk memperoleh *chat* maupun kontak baru yang terdaftar.
4. Menggunakan penerapan algoritma enkripsi ganda yaitu ROT13 dan Vinegere *Cipher*, sehingga chat yang dikirimkan akan mengalami dua kali proses enkripsi saat dikirimkan kepada lawan chat.
5. Melakukan penerpaan konsep *End To End Encryption* sehingga hasil chat yang di kirimkan dan di terima oleh pengguna akan tetap menampilkan *plaintext*, penerapan konsep ini bertujuan untuk menghindari terjadinya penyadapan isi dari *chat* saat dikirim via jaringan intenet.

Kekurangan Sistem

Adapun kekurangan aplikasi *chat* ini adalah sebagai berikut :

1. Fitur yang tersedia masih sangat minim, seperti tidak adanya fitur untuk melakukan *update* status maupun

mengubah profil pengguna.
2. Tidak memiliki fungsi untuk menghapus *chat* yang sudah pernah dilakukan.
3. Kontak ditampilkan adalah kontak seluruh pengguna yang terdaftar didalam aplikasi, sehingga tidak ada perbedaan isi dari kontak yang ditampilkan pada setiap pengguna.
4. Dalam melakukan proses enkripsi menggunakan algoritma Vinegere *Cipher* kunci yang pergunakan sudah ditetapkan pada *script* sehingga pengguna tidak dapat mengubah isi dari kunci.
5. Aplikasi memiliki keterbatasan karakter yang dipergunakan yaitu 26 karakter dengan huruf kecil dan 26 karakter dengan huruf besar dan tidak dapat melakukan enkripsi untuk tanda baca, spasi dan spesial karakter, keterbatasan ini dikarenakan algoritma yang dipergunakan hanya menggunakan total karakter sebanyak 26 huruf *alpabet* yang hanya terdiri dari huruf besar dan huruf kecil.

KESIMPULAN

Dari hasil penelitian yang dilakukan, maka dapat di ambil kesimpulan sebagai berikut : 1). Algoritma Rot13 dan *Vinegere Cipher* adalah merupakan algoritma klasik yang menerapkan konsep algoritma simetris, sehingga kunci yang dipergunakan saat melakukan proses *enkripsi* dan *dekripsi* adalah sama, 2). Jumlah karakter *default* yang dapat digunakan pada aplikasi ini adalah berjumlah 26 karakter *alpabet*, sehingga tidak mengenal tanda baca dan *special* karakter, 3). Agar proses yang dihasilkan dapat mengenali huruf besar dan huruf kecil, maka perlu dilakukan modifikasi terhadap jumlah karakter yang dipergunakan, dan 4). Metode *End to End Encryption* yang diterapkan pada aplikasi *chat* bertujuan untuk menghindari penyadapan data saat chat dikirimkan via jaringan *internet*.

DAFTAR PUSTAKA

Adinta, F., & Neforawati, I. (2019). Rancang Bangun Aplikasi Chatting Berbasis Web Menggunakan Docker. *JOISIE (Journal Of Information Systems And Informatics Engineering), 1*(1), 28-34.

Anwar, S., Roslina, R., & Agustin, F. (2020). Aplikasi Perbandingan Metode Vernam Dan Kombinasi OTP Dengan ROT13 Pada Wirelles Chating LAN Dan WLAN. *Jurnal Mahasiswa Fakultas Teknik dan Ilmu Komputer, 1*(1), 380-393.

Ardhianto, E., Handoko, W. T., Supriyanto, E., & Murti, H. (2021). Evolusi Cipher Vigenere dalam Peningkatan Pengamanan Informasi. *Jurnal Informatika UPGRIS, 7*(2), 202-214.

Fajri, G. R., Sembiring, E. H., & Hasan, M. A. (2020). Keamanan Data Pada Pengarsipan Surat Menggunakan Metode Kriptografi Klasik Vigenere Cipher Dan Shift Cipher. *ZONAsi: Jurnal Sistem Informasi, 2*(1), 61-72.

Khairil, A., & Hayati, R. S. (2020). Rancang Bangun Aplikasi Chatting Keluarga Menggunakan Fitur Device Location Berbasis Android. *Jurnal Mahasiswa Fakultas Teknik dan Ilmu Komputer, 1*(1), 489-498.

Kurniawan, T., & Samsudin, T. (2021). Implementasi Layanan Firebase pada Pengembangan Aplikasi Sewa Sarana Olahraga Berbasis Android. *Jurnal Informatika Universitas Pamulang, 6*(1), 13-18.

Ryan, A. R., Perdana, A., & Budiman, A. (2020). Kombinasi Algoritma Beaufort Cipher Dan Vigenere Cipher

Untuk Pengamanan Pesan Teks Berbasis Mobile Application. *Jurnal Minfo Polgan*, *9*(2), 12-17.

Situmorang, P. G., Siburian, H. K., Mesran, M., Fau, A., & Arifin, S. (2017). Perancangan Aplikasi Penyandian Pesan Chatting Client Dan Server Dengan Algoritma RC5. *KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer)*, *1*(1), 1-12.

Rosa, A. S., & Shalahuddin, M. (2018). *Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek*. Bandung: Informatika.

P-ISSN (2985-9689) & E-ISSN (2986-0687)