IMPLEMENTASI KRIPTOGRAFI DENGAN ALGORITMA VIGENERE CIPHER, AES 128 DAN RC 4 UNTUK APLIKASI PESAN INSTAN BERBASIS ANDROID

Rizki Prabowo[1)], Wahyu Pramusinto[2)]
[1]Program studi, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : riski.prabowo11@gmail.com[1)], wahyu.pramusinto@budiluhur.ac.id[2)]

ABSTRAK

Penggunaan teknologi telepon genggam seperti handphone sebagai alat telekomunikasi pada saat ini telah mengubah cara pandang masyarakat untuk berkomunikasi. pengiriman pesan melalui internet dengan menggunakan aplikasi chatting yang dimiliki oleh seseorang merupakan hal penting dalam pengiriman pesan teks yang dapat mengakses informasi tersebut. Salah satu yang harus benar-benar dijaga adalah pesan yang bersifat rahasia karena jika pesan tersebar maka akan berdampak buruk pada kita. Salah satu cara yang biasa digunakan adalah dengan enkripsi. Enkripsi adalah proses untuk menyamarkan atau menyandikan pesan. Untuk merahasiakan pesan instan yang dikirim, maka dalam penelitian ini akan dibuat aplikasi chatting berbasis android yang menggunakan metode Vigenere Chiper, AES 128 bit , RC4 yang diharapkan dapat mengamankan pesan antara notaris dan client agar data percakapan yang dikirimkan tidak mudah dibaca oleh pihak yang tidak berkepentingan. Aplikasi chatting yang dibuat berbasis android dengan bahasa pemrograman Java ini dapat mengamankan pesan yang disampaikan diketahui pihak yang tidak berkepentingan.

Kata kunci : Chatting, Kriptografi, Vigenere Chiper, AES 128, RC4

1. PENDAHULUAN

1.1. Latar Belakang

Penggunaan teknologi telepon genggam seperti *handphone* sebagai alat telekomunikasi pada saat ini telah mengubah cara pandang masyarakat untuk berkomunikasi. pengiriman pesan melalui internet dengan menggunakan aplikasi *chatting* yang dimiliki oleh seseorang merupakan hal penting dalam pengiriman pesan teks yang dapat mengakses informasi tersebut. Salah satu yang harus benar-benar dijaga adalah pesan yang bersifat rahasia karena jika pesan tersebar maka akan berdampak buruk pada kita. Salah satu cara yang biasa digunakan adalah dengan enkripsi. Enkripsi adalah proses untuk menyamarkan atau menyandikan pesan. Untuk memperkuat keamanan pesan yaitu dengan menggunakan kriptografi. Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ketempat yang lain.

Aplikasi chatting adalah aplikasi yang digunakan untuk berkomunikasi dalam satu jaringan lokal atau internet yang saling terhubung satu sama lain untuk mempermudah percakapan. Aplikasi chatting yang saat ini banyak berkembang pesat antara lain BBM , WhatsApp , Line, dan Telegram aplikasi tersebut memiliki keunggulan dan fitur masing – masing, karena pada dasarnya aplikasi tersebut digunakan oleh umum dan diakses dari seluruh penjuru dunia. Resiko yang timbul dari hal tersebut adalah informasi yang ada di dalam pesan tersebut dapat dicuri, diketahui, disadap oleh pihak yang tidak bertanggung jawab yang berdampak kerugian bagi penggunanya.Permasalah yang dihadapi adalah bagaimana cara mengamankan pesan text dan mengirim pesan gambar dengan mengenkrip URL gambar tersebut agar tidak dapat diketahui oleh pihak yang tidak berkepentingan. Karena jika diketahui oleh pihak yang tidak bertanggung jawab, maka sebuah percakapan yang penting dapat dicuri dan dapat menimbulkan kerugian bagi client. Dalam penelitian ini akan digunakan algoritma enkripsi RC4 , AES 128 bit untuk mengamankan pesan teks asli dan algoritma vigenere chiper untuk mengaman URL pada gambar yang kirimkan oleh user.

1.2. Permasalahan

Dengan melihat latar belakang diatas maka dapat diambil kesimpulan permasalahan yang terjadi yaitu bagaimana cara mengamankan pesan asli (*plaintext*) dan lampiran berupa gambar yang terenkripsi tanpa mengubah isi dari pesan tersebut.

1.3. Tujuan Penulisan

Adapun maksud dan tujuan dari penulisan Tugas Akhir ini adalah mengamankan pesan teks yang dikirim dari pengguna kepada pengguna lainnya. Pesan dienkripsi dengan algoritma enkripsi RC4 dan AES 128 digunakan untuk mengamankan pesan teks, algoritma enkripsi vigenere chiper digunakan untuk mengamankan URL gambar yang

dikirimkan oleh *user* sehingga pesan dapat terjaga kerahasiaannya

2. LANDASAN TEORI

2.1. Definisi 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 pengetahuan untuk memproteksi pengiriman data dengan mengubah kode tertentu dan ditunjukan kepada pengguna (user), dalam kriptografi terdapat 2 konsep utama yaitu enkripsi dan dekripsi. Enkripsi yaitu proses dimana informasi atau data yang dikirm dan diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awal dengan menggunakan algoritma tertentu. Dekripsi (plain) yaitu mengubah kembali bentuk informasi atau data tersamar tanpa merubah isi dari informasi atau data tersbut.

2.2. Vigenere Cipher

Pricilia Yulianingsih, Hamdani dan Septya Maharani (2016) Vigenere Cipher adalah suatu algoritma yang tergolong ke dalam algoritma subtitusi abjad majemuk. setiap huruf yang sama dalam plaintext tidak dipetakan atau disubtitusikan oleh satu huruf. Melainkan di subtitusikan oleh huruf yang berlainan bergantung dari kunci yang digunakan untuk melakukan enkripsi. Vigenere Cipher merupakan bentuk sederhana dari sandi substitusi polialfabetik yang sangat dikenal karena mudah dipahami dan diimplementasikan. Teknik untuk menghasilkan *chipertext* bisa meggunakan bujursangkar yang menukarkan huruf-huruf ciphertext. Bujursangkar Vigenere digunakan untuk memperoleh suatu ciphertext dengan menggunakan kata kunci. yang sudah ditentukan. Jika panjang kunci lebih pendek daripada panjang plaintext, maka kunci akan diulang penggunaannya sistem. Bila panjang kunci adalah a, maka periodenya dikatakan a

2.3. Algoritma AES

AES atau Advanced Encryption Standard merupakan algoritma enkripsi kunci simetris yang pada awalnya diterbitkan dengan algoritma Rijndael. Algoritma AES merupakan algoritma simetris yaitu menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma AES memiliki tiga pilihan kunci yaitu tipe : AES-128 bit, AES-192 bit, dan AES-256 bit. Setiap masing-masing tipe menggunakan kunci internal yang berbeda yaitu round key untuk setiap putaran yang berlangsung.

2.4. Definisi Algoritma RC4

Algoritma RC4 adalah salah satu jenis stream chiper,yaitu memproses unit atau input data. Unit atau data pada umumnya adalah sebuah byte atau bit(byte dalam RC4). Enkripsi atau dekripsi RC4 dapat dilaksanakan panjang pada sebuah variable. RC4 merupakan jens enkripsi stream simetris. Algoritma yang dipublikasikan ini sangat identik dengan implementasi algoritma RC4 pada produk resmi. RC4 digunakan secara luas pada beberapa aplikasi dan umumnya dinyatakan sangat aman. Sampai saat ini belum diketahui yang dapat memecahkan/membongkarnya, hanya saja versi ekspor 40 bitnya dapat dibongkar dengan cara "brute force" (mencoba semua kunci yang mungkin).

Kelemahan pada algoritma RC4 yaitu terlalu tinggi kemungkinan terjadi pada table S-box yang sama, hal ini sering terjadi karena kunci user diulang – ulang untuk mengisi 256 bytes, sehingga ‘bbbb’ dan ‘bbbbb’ untuk mengatasi ini maka pada setiap implementasinya mengunakan hash 160 bit SHA dari password untuk mencegah hal ini terjadi. Kekurangan lainnya dari algoritma RC4 yaitu enkripsi RC4 adalah XOR antara bytes dan pseudo-random byte stream yang dihasilkan dari kunci. Untuk mengatasinya kita menggunakan initialization vector yang berbeda – beda untuk setiap data, sehingga file yang sama akan menghasilkan chiper teks yang berbeda.

3. ANALISA MASALAH DAN PERANCANGAN PROGRAM

3.1. Analisa Masalah

Informasi yang dikirimkan seorang pengguna layanan pesan instan dapat bersifat sangat penting dan tidak boleh diketahui oleh orang lain. Oleh karena itu maka aplikasi *chatting* sangat dibutuhkan untuk sarana pertukarannya informasi berupa teks yang paling banyak digunakan oleh individu.

Beberapa aplikasi *chatting* yang paling sering digunakan saat ini hanya terdapat fitur keamanan seperti *user password* pada menu *login*, tidak ada fitur keamanan untuk isi pesan yang telah disimpan pada *database server* aplikasi *chatting* tersebut. Maka apabila server diretas, seluruh isi percakapan pengguna dapat dibaca dengan mudah oleh *hacker* sehingga dapat terjadi pencurian serta manipulasi data.

3.2. Penyelesaian Masalah

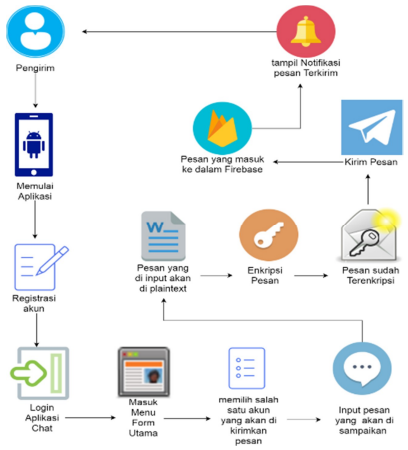
Untuk mengantisipasi permasalahan yang telah diuraikan, dibutuhkanlah sebuah aplikasi *chatting* yang memiliki fitur keamanan dalam pengiriman pesan teks. Untuk membuat aplikasi tersebut, digunakanlah teknik yang disebut kriptografi. Pada kriptografi terdapat dua proses yaitu enkripsi dan dekripsi. Proses enkripsi berfungsi untuk mengubah pesan teks yang berisi *plaintext* atau teks biasa yang terbaca menjadi *ciphertext* atau teks acak yang tak terbaca. Sedangkan proses dekripsi berfungsi untuk mengembalikan *ciphertext* tersebut menjadi plaintext seperti semula. Maka dengan penerapan kriptografi pada aplikasi ini, *hacker* pun tidak mempunyai kesempatan untuk mengetahui informasi pada pesan dalam aplikasi *chatting* ini. Seluruh akun pengguna dan isi percakapan yang terenkripsi antara pengirim dan penerima akan disimpan pada Firebase console.

Aplikasi Chatting ini menggunakan beberapa algoritma yaitu algoritma Vigenere chiper, AES 128 bit, dan RC4. Algoritma ini termasuk dalam jenis algoritma Kriptografi yang sifatnya simetris, jadi kunci yang digunakan pada enkripsi sama dengan dekripsi.

3.2. Skema Proses Keseluruhan Aplikasi

Untuk menyelesaikan masalah diatas, maka diuraikanlah skema proses keseluruhan aplikasi *chatting*. Berikut adalah tahapan dan *rich picture* pada proses pengiriman pesan :

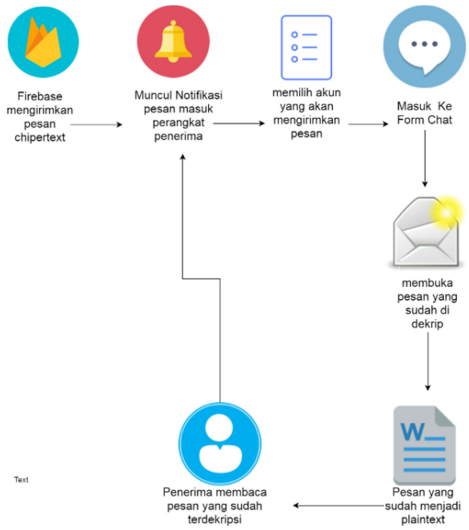
1) Untuk menggunakan aplikasi *chatting* ini , langkah pertama instal aplikasi di perangkat android.
2) Apabila pengirim belum memiliki akun aplikasi ini, pengirim dapat membuat akun baru dengan melakukan *register*. Pengirim harus mengisi data berupa *username, email, password.*
3) Bila pengirim sudah mendaftar sebagai user, pengirim dapat melakukan proses *login* dengan *email* dan *password* yang sudah terhubung ke internet.
4) Setelah *login* pada aplikasi *chatting* dan berhasil masuk. Maka pengirim masuk ke dalam *form* utama dan pengirim memilih salah satu akun penerima yang sudah tersedia untuk melakukan proses pengiriman pesan enkripsi. Lalu setelah memilih akun untuk dikirimkan pesan enkripsi, pengirim masuk ke *form chat*. Setelah itu pengirim meng-input isi pesan yang ingin dikirim ke penerima yang sudah di pilih.
5) Pada saat proses pengiriman, aplikasi akan melakukan proses enkripsi terlebih dahulu.
6) Pesan teks yang di-input akan dirubah menjadi *chipertext* dengan menggunakan kunci yang sudah diatur oleh sistem.
7) Setelah proses enkripsi selesai, pesan dikirim ke *Firebase* lalu diteruskan ke akun penerima pesan dan ditampilkan didalam *form chat* penerima.
8) Pengirim akan mendapatkan notifikasi berupa laporan pengiriman bahwa pesan berhasil terkirim atau tidak.
9) *Chipertext* yang telah dikirim akan ditampilkan pada *form chat* penerima.
10) *Chipertext* yang telah dikirim akan ditampilkan pada form chat penerima.



Gambar 1 *Rich picture* proses pengiriman pesan

Setelah proses pengiriman, berikut ini adalah tahapan dan *rich picture* pada proses penerimaan pesan :

1) Penerima memilih salah satu akun pada *form main*. Setelah itu penerima akan masuk *form chat*.
2) Pesan berbentuk c*iphertext* akan ditampilkan pada *form chat. Ciphertext* yang ditampilkan pada *form chat* berasal dari *firebase console*.
3) *Ciphertext* akan melalui dekripsi otomatis.
4) *Ciphertext* yang telah didekripsi akan berubah menjadi *plaintext* atau teks murni yang isinya sama saat pesan tersebut dikirim oleh pengirim pesan.
5) *Plaintext* ditampilkan pada form chat milik penerima



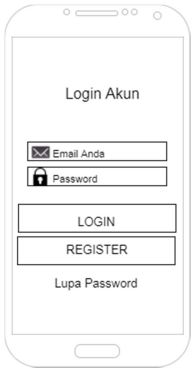
Gambar 2 *Rich picture* proses penerimaan pesan

3.3 Rancangan Layar

Rancangan layar sangat penting dalam membuat suatu program. Oleh karena itu rancangan layar harus bersifat *user friendly* atau mudah dipahami oleh user sehingga user tidak akan kebingungan dan kesulitan dalam menggunakan aplikasi. Aplikasi ini akan digambarkan rancangan layar meliputi *form login*, *register*, *main*, dan *chat*. Berikut rancangan layar pada masing-masing *form* tersebut.

a. Rancangan Layar *Form Login*

Ketika aplikasi dibuka, maka pengguna akan masuk ke *form login* dimana akan ada pilihan untuk *login* atau memilih *register* jika belum terdaftar sebagai *user*. *User* dapat masuk ke dalam aplikasi jika telah memiliki akun aplikasi ini.

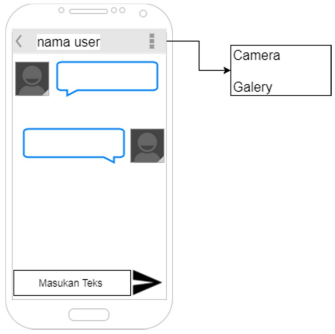


Gambar 3 Rancangan Layar *Form Login*

b. Rancangan Layar *Form Chat*

Form chat adalah *form* yang digunakan untuk melakukan aktivitas *chat* atau percakapan dengan user lain yang sudah terdaftar dan dipilih dari *form Main Menu*.

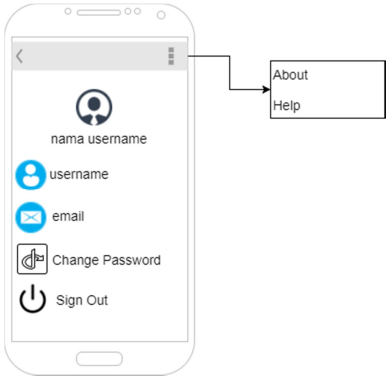
Pesan percakapan yang kita kirim ke user lain akan di enkripsi dengan menggunakan metode RC4, AES 128 bit dan enkripsi vigenere chiper untuk enkripsi *link* pada gambar, Semua pesan selama pengiriman akan aman karena telah terenkripsi. Pada saat pesan masuk ke perangkat android penerima pesan, maka pesan yang semula terenkripsi akan langsung didekripsi pada *form chat* penerima agar dapat langsung dibaca.



Gambar 4 Rancangan Layar *Form Chat*

c. Rancangan Layar *Form* Akun Anda

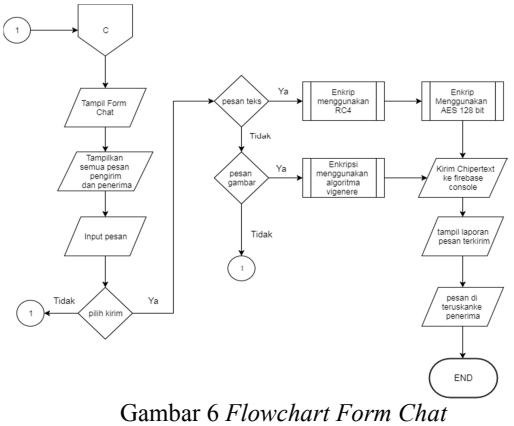
Rancangan layar *form* Akun anda merupakan form yang memberikan fitur berupa mengganti foto *Profil* kita supaya mudah dikenali user lain, mengubah *password* dan *Logout*. *Form* Akun anda akan muncul ketika kita memilih *fragment* Akun anda pada *fragment main menu.*



Gambar 5 Rancangan Layar *Form* Akun

3.4 Flowchart Program

Pada *flowchart form chat* ini *user* dapat mengirim pesan teks ke *user* lain yang sebelumnya dipilih pada *form main*. Pesan yang dikirim akan melalui proses enkripsi dan pesan yang diterima akan melalui proses dekripsi. Berikut adalah penjelasan dari *flowchart form chat*



Gambar 6 *Flowchart Form Chat*

3.5 Algoritma Alur Proses

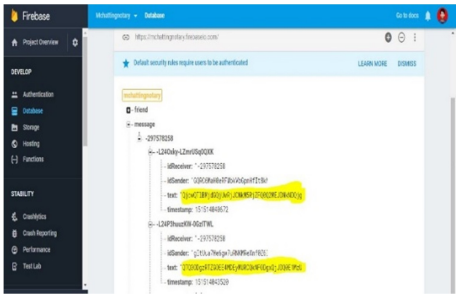
Algoritma ini menjelaskan tentang alur proses yang terjadi pada *Form chat*. Berikut adalah proses dari algoritma *Form chat*

1. Tampil Form Chat
2. Tampil semua Teks pesan Pengirim dan Penerima
3. Input Pesan
4. If Pilih Kirim then
5. If pesan "teks" then
6. Enkrip RC4
7. Enkrip AES 128 bit
8. Kirim ke Firebase Console
9. End If
10. Else if Pesan "Gambar" then
11. Enkrip Vigener chiper
12. Kirim Ke Firebase Console
13. End if
14. Tampil laporan pengiriman "Pesan Terkirim"
15. Pesan diteruskan ke Penerima
16. else
17. Kembali ke baris 1
18. EndIf

4. HASIL DAN PEMBAHASAN

4.1 Tampilan Layar

Pesan yang dikirimkan secara otomatis akan disimpan kedalam *database firebase console* sebagai pesan yang sudah terenkripsi. Dapat di lihat pada gambar 7



Gambar 7 Tampilan *Firebase Console* dikirim dan terenkripsi

4.2 Analisa Hasil Uji Coba Program

Setelah proses perangkat keras dan perangkat lunak terpenuhi,penulis melakukan uji coba program. Analisa hasil uji program sangat perlu untuk menganalisa dan mengetahui hasil dari program tersebut. Dari hasil uji coba program penulis menemukan beberapa batasan program yang dilihat dari beberapa kondisi dan situasi. Adapun batasan program pada aplikasi ini adalah :

Kelebihan Pada Program

1) Aplikasi ini mengirimkan pesan secara *real time.*
2) Pesan yang dikirim dapat berupa teks dan gambar.
3) Pengguna tidak perlu meng-input key serta melakukan penyimpanan kunci, karena sudah diatur oleh *system*.
4) Pada saat aplikasi sedang tidak dibuka, program dapat memberikan *notifikasi* pada pengguna selama koneksi tetap tersambung.
5) Aplikasi kriptografi *chatting* dapat berjalan dengan baik selama ada koneksi internet.
6) Aplikasi ini dapat berjalan dengan baik pada sistem operasi android API 19(kitkat) ke atas.

Kelemahan Pada Program

1) Aplikasi ini tidak bisa melakukan *group chat* dan *broadcase message.*
2) Fitur pada aplikasi *chatting* ini masih sedikit, diantaranya tidak bias mengirim pesan berupa suara, dokumen dan dan tidak ada *setting* penggunaan data.
3) Aplikasi ini tidak bisa menelpon dan *video call* untuk berkomunikasi
4) Tampilan masih sangat sederhana
5) Aplikasi ini sangat tergantung pada kecepatan internet

5. KESIMPULAN

Berdasarkan analisa yang dilakukan dimulai dari pengumpulan informasi, pemecahan masalah hingga pengembangan aplikasi ini, maka dapat ditarik kesimpulan dan saran yang diperlukan untuk pengembangan sistem ketahap yang lebih kompleks.

1) Kesimpulan

Berdasarkan analisa permasalahan dan bab – bab sebelumnya, program Aplikasi *Chatting* dengan metode Advanced Encryption Standard (AES) 128, Rivest Code 4(RC4) dan mengkripsi link pada gambar dengan Vigenere Chiper berbasis Android
sangat diperlukan karena:

Dengan adanya aplikasi ini maka isi dari pesan teks terjaga kerahasiaannya dari yang tidak berkepentingan, dan yang tidak

a. berhak untuk mengetahui apa isi dari pada pesan teks tersebut.
b. Tingkat keamanan pesan setelah dienkripsi cukup terjaga, dengan kata lain pesan tidak berkurang atau mengalami kerusakan setelah proses enkripsi dan dekripsi pesan dilakukan.
c. Aplikasi ini tergolong ringan hanya 3.5 MB

2) Saran

Dengan terbatasnya waktu yang diberikan untuk menyelesaikan tugas akhir ini penyelesaian masalah yang telah dikembangkan masih jauh dari sempurna, sehingga perlu dilakukan penyempurnaan baik disisi *hardware* maupun software. Saran yang dapat dikembangkan antara lain:

a. Ditambahkannya fitur-fitur untuk melengkapi aplikasi ini seperti kirim file, penghapusan pesan, dan *voice call.*
b. Ditambahkannya kompatibilitas pada sistem operasi android dibawah versi 4.4. agar aplikasi ini dapat berjalan di seluruh versi sistem operasi android.
c. Membuat *autentifikasi* melalui email untuk mengecek email pengguna yang dimasukkan.

DAFTAR PUSTAKA

[1]. Arif, A., & Mandarani, P. (2016). REKAYASA PERANGKAT LUNAK KRIPTOGRAFI MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) 128 BIT PADA SISTEM KEAMANAN SHORT MESSAGE SERVICE (SMS) BERBASIS ANDROID. Fakultas Teknologi Industri Institut Teknologi Padang: Jurnal TEKNOIF.

[2]. Pandiangan, H., & Sijabat, S. (2016). PERANCANGAN MEDIA PENGIRIMAN PESAN TEKS DENGAN PENYANDIAN PESAN MENGGUNAKAN ALGORITMA RC4 BERBASIS WEB. Medan, Sumatera Utara : Jurnal Matik Penusa.

[3]. Priyono. (2016). PENERAPAN ALGORITMA CAESAR CIPHER DAN ALGORITVIGENERE CIPHER DALAM PENGAMANAN PESAN TEKSMA . Simpang Limun Medan: Jurnal Riset Komputer (JURIKOM), Volume : 3, Nomor: 5, Oktober 2016.

[4]. Subhan, S., Amini, S., & Ariyani, P. F. (2017). IMPLEMENTASI PENGAMANAN DATA ENKRIPSI SMS DENGAN ALGORITMA RC4 BERBASIS ANDROID. Jakarta Selatan: Seminar Nasional Inovasi Dan Aplikasi Teknologi Di Industri 2017 ITN Malang, 4 Pebruari 2017.

[5]. Wanda, P. (2016). EFISIENSI PENGAMANAN PESAN MOBILE BANKING BERBASIS ALGORITMA ADVANCED ENCRYPTION STANDARD (AES). Yogyakarta: Seminar Nasional Teknologi Informasi dan Multimedia 2016.

[6]. Yulianingsih, P., Hamdani, & Maharani, S. (2014). APLIKASI CHATTING RAHASIA MENGGUNAKAN ALGORITMA VIGENERE CIPHER. Universitas Mulawarman:INFORMATIKA Mulawarman Februari 2014