IMPLEMENTASI ALGORITMA KRIPTOGRAFI VIGENER CIPHER DAN AFFINE CIPHER UNTUK MENGAMANKAN PESAN PADA APLIKASI CHATTING BERBASIS ANDROID

Muhammad Ricky Darmawan[1)], Windarto[2)]
[1]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 1260
Telp, (021) 5853753, Fax. (021) 5866369
E-mail : rickydarmawan.rd@gmail.com[1)], windarto@budiluhur.ac.id [2)]

ABSTRAK

Pada era perkembangan ilmu pengetahuan di bidang teknologi dan informasi saat ini, komunikasi merupakan hal yang paling penting dalam komunitas global. Begitupun halnya dalam dunia pendidikan, komunikasi sudah menjadi bagian penting dalam melakukan aktivitas pembelajaran. Namun saat ini, kesibukan Wali Murid menjadi salah satu faktor kurangnya perhatian para Wali Murid terhadap anaknya di sekolah. Hal ini dikarenakan kesibukan Wali Kelas dan Wali Murid dengan pekerjaan mereka masing-masing sehingga komunikasi antara Wali Kelas dan Wali Murid sangat jarang dilakukan. Oleh karena itu, untuk menyelesaikan permasalahan tersebut dibuatlah sebuah aplikasi *chatting* sebagai media komunikasi antara Wali Kelas dengan Wali Murid sehingga Wali Kelas dan Wali Murid dapat saling berbagi informasi seputar aktivitas pembelajaran di sekolah. Untuk menjaga kerahasiaan pesan yang dikirim, digunakanlah teknik kriptografi, teknik kriptografi yang digunakan dalam penelitian ini yaitu algoritma *Vigenere Cipher* dan algoritma *Affine Cipher* Aplikasi ini dibangun untuk perangkat berbasis *Android* menggunakan bahasa pemrograman bahasa *Java Mobile* dan Firebase sebagai *web server*. Proses pengiriman akan melalui 2 kali proses enkripsi dan setelah proses enkripsi berhasil, pesan akan disimpan pada Firebase. Sementara proses penerimaan pesan akan melalui 2 kali proses dekripsi yang pada akhirnya pesan akan ditampilkan kepada penerima. Dengan adanya aplikasi *chatting* ini diharapkan dapat membantu guru untuk saling berkomunikasi antara Wali Kelas dan Wali Murid dengan tetap menjaga keamanan pesan yang dikirim sehingga terhindar dari adanya pencurian informasi.

Kata Kunci : Affine Cipher, Vigenere Cipher, *Chatting,* Firebase, Kriptografi.

1. PENDAHULUAN

1.1 Latar Belakang

Dalam bidang teknologi dan informasi saat ini, komunikasi merupakan hal yang paling penting dalam komunitas global. Perkembangan teknologi membuat pola komunikasi semakin berkembang dan muncul kebutuhan baru untuk bertukar informasi jarak jauh. Salah satu cara berkomunikasi yang paling mudah digunakan saat ini adalah dengan menggunakan e-mail maupun pesan instan (instan messaging) melalui smartphone.

Aplikasi *chatting* merupakan salah satu dampak positif dari perkembangan teknologi dan informasi yang berawal dari SMS (*Short Messsage Service).* Dengan menggunakan aplikasi chatting, manusia dapat bertukar pesan kepada teman, pasangan, maupun keluarga dengan mudah. Aplikasi *chatting* sudah menjadi hal yang dibutuhkan diberbagai macam bidang termasuk halnya di dalam dunia pendidikan. Di dalam dunia pendidikan saat ini, komunikasi antara Wali Murid dan Wali Kelas menjadi hal yang jarang dilakukan saat ini. Padahal seharusnya Wali Murid harus selalu memantau perkembangan anaknya di sekolah. Kesibukan Wali Murid menjadi salah satu faktor kurangnya perhatian para Wali Murid terhadap anaknya di sekolah, tidak terkecuali pada *Homeschooling* Al Ihsan Cilegon, dikarenakan kesibukan Wali Murid dengan pekerjaan mereka masing-masing, ataupun sebaliknya Wali Murid yang menanyakan sesuatu kepada Wali Kelas.

Di dalam sebuah aplikasi *chatting*, keamanan merupakan hal yang sangat penting yang dimana bertujuan untuk menjaga informasi yang dikirim agar terhindar dari penyalahgunaan informasi dari orang-orang yang tidak bertanggung jawab. Dalam penelitian ini penulis mencoba mengimplementasikan suatu ilmu yaitu kriptografi. Kriptografi sendiri merupakan ilmu atau seni yang dibuat untuk menjaga keamanan pesan yang mana metode yang digunakan adalah metode *Vigenere Chiper* dan *Affine Cipher.* Algoritma *Vigenere Cipher* termasuk dari bagian algoritma klasik dimana pada algoritma ini menggunakan sebuah rumus matematika. Algoritma *Vigenere Cipher* membutuhkan sebuah kunci untuk melakukan proses enkripsi dan dekripsi. *Vigenere Cipher* akan

melakukan sebuah perhitungan antara input dan kunci yang mana perhitungan angka tersebut berupa angka decimal. Setelah proses perhitungan, maka dihasilkanlah sebuah teks acak yang sulit untuk dibaca oleh seseorang.

Algoritma *Affine Chiper* merupakan metode yang mengubah teks atau file awal pengiriman yang awalnya dapat dipahami oleh manusia awam menjadi sebuah kumpulan teks yang telah dienkripsikan terlebih dahulu menggunakan metode Affine Chiper setelah itu akan dimasukan ke media penyimpanan.

1.2 Masalah

Berdasarkan latar belakang diatas, maka dapat disimpulkan permasalahan dalam penelitian tugas akhir ini adalah sebagai berikut:

a. Adanya kesulitan dalam penyampaian informasi antara Wali Kelas dengan Wali Murid.
b. Adanya ketidakamanan dalam penyampaian sebuah informasi.

1.3 Tujuan Penelitian

Berdasarkan permasalahan yang didapat sebelumnya, maka tujuan yang akan diharapkan dari penelitian tugas akhir sebagai berikut:

a. Membangun aplikasi *chatting* yang dapat memudahkan penyampaian informasi antara Wali Kelas dengan Wali Murid untuk perangkat *Android.*
b. Membangun aplikasi *chatting* yang dapat mengamankan pesan yang dikirim dengan menerapkan metode kriptografi *Vigenere Cipher* dan *Affine Chiper*.

1.4 Batasan Masalah

Adapun batasan masalah pada penelitian tugas akhir ini adalah:

a. Algoritma kriptografi yang digunakan untuk mengenkripsi dan mendekripsi pesan adalah *Vigenere Cipher* dan *Affine Cipher*.
b. Media penyimpanan menggunakan Firebase.
c. Pesan yang dapat dienkripsi dan didekripsi adalah pesan berbentuk *text.*
d. Aplikasi *chatting* ini hanya bisa digunakan oleh Wali Kelas dan Wali Murid di *Homeschooling* Al Ihsan Cilegon yang diwakili oleh 1(satu) orang.
e. Aplikasi *chatting* ini berjalan pada platform Androis

2. DASAR TEORI

2.1 Kriptografi

Pada dasarnya, kriptografi terdiri dari 2 kata yaitu kryptos yang artinya "rahasia" dan graph yang artinya "menulis". Definisi dari kriptografi adalah Ilmu yang digunakan untuk mengubah suatu informasi menjadi sebuah kata yang tidak dapat dibaca. [7]. Kriptografi ialah sebuah teknik enkripsi dengan mengubah suatu data agar data tidak dapat dibaca atau dilihat oleh seseorang yang mana pengamanan tersebut menggunakan suatu kunci enkripsi dengan menggunakan suatu algoritma dengan beberapa parameter. Untuk proses dekripsi pun dibutuhkan pula sebuah kunci agar dapat membaca data yang sebelumnya telah dienkripsi.

Secara umum, Proses enkripsi ialah proses untuk mengubah “kata asli” atau biasa disebut plaintext menjadi sebuah “kata acak” atau disebut ciphertext sehingga seseorang biasa akan sulit membaca apabila tidak memiliki kunci untuk melakukan dekripsi. Proses Enkripsi yang baik menghasilkan kata acak yang memerlukan waktu yang cukup lama. Untuk dapat membaca kata acak agar dapat menjadi kata asli yaitu dengan menerka kunci dekripsi yang telah dibuat, proses inilah yang menjadi suatu hal yang sulit dilakukan oleh orang awam. Kata acak tersebut pastinya dapat didekripsikan oleh seseorang yang mempunyai kunci dekripsi untuk mendapatkan kembali kata asli. [6]

2.2 Vigenere Cipher

Proses Enkripsi dan Dekripsi pada *Vigenere Cipher* bekerja dengan membaca kata per karakter, dimana apabila pesan yang dikirim melebihi panjang kunci yang digunakan, maka kunci akan diulang kembali sampai pesan yang dikirim tersebut mendapatkan kunci masing-masing. *Vigenere Cipher* dapat menggunakan sebuah tabel untuk menengkripsikan sebuah plaintext yang mana terdiri dari 26 baris dan kolom alphabet, dan tiap barisnya akan digeser satu huruf ke kiri.

Rumus yang digunakan dalam proses Enkripsi Vigenere Cipher sebagai berikut :

$Ci = (Pi + Ki) \bmod 26$

Sedangkan untuk proses dekripsi adalah :

$Pi = (Ci - Ki) \bmod 26$ jika $Ci-Ki > 0$

$Pi = ((Ci - Ki)+26) \bmod 26$ jika $Ci-Ki < 0$

Keterangan :

C = *Ciphertext* (Pesan Acak)
P = *Plaintext* (Pesan Asli)
K = Kunci

2.3 Affine Cipher

Enkripsi yang diciptakan oleh Julis Caesar ini menggunakan sebuah transformasi yang disebut Shift Transformation. Shift Transformation ini rawan akan terjadinya

analisa frekuensi. Untuk mempersulit hal tersebut, digunakanlah sebuah affine transformation yang memiliki rumus :

$C = aP + b \pmod n$

Sedangkan untuk proses dekripsi adalah :

$P = a^{-1}C ¡ a^{-1}b \pmod n$

Artinya, pada saat melakukan enkripsi, affine memiliki dua buah parameter yaitu a dan b. Sementara pada saat dekripsi, a harus memiliki inverse a^{-1} yang mana a harus mematuhi gcd(a;n) = 1

3. ANALISA MASALAH DAN RANCANGAN PROGRAM

3.1 Analisa Permasalahan

Komunikasi yang baik antara Wali Kelas dan Wali Murid sangat diperlukan dalam kegiatan belajar mengajar di *Homeschooling* Al Ihsan. Dengan adanya komunikasi yang baik, tentu segala macam bentuk penyampaian informasi antara Wali Kelas dengan Wali Murid dapat berjalan dengan lancar. Sayangnya hal tersebut cukup sulit dilakukan dikarenakan berbagai macam faktor, salah satunya dikarenakan Wali Murid memiliki kesibukan masing-masing menyebabkan kurangnya waktu untuk berkunjung menemui wali kelas untuk menyampaikan informasi ataupun masukan kepada Wali Kelas. Disamping hal tersebut, keamanan dalam penyampaian sebuah informasi pun sangat dibutuhkan karena banyaknya pencurian informasi yang dilakukan oleh pihak yang tidak bertanggung jawab.

3.2 Penyelesaian Masalah

Berdasarkan masalah diatas disimpulkan bahwa masalah yang terjadi adalah adanya kesulitan dalam penyampaian sebuah informasi antara Wali Kelas dan Wali Murid serta adanya ketidakamanan pada sebuah informasi yang disampaikan. Oleh karena itu, diperlukan sebuah metode yang dapat membantu dalam penyampaian sebuah informasi dan juga dapat mengamankan informasi yang disampaikan antara Wali Kelas dan Wali Murid, yang mana metode yang digunakan adalah *Vigenere Cipher* dan *Affine Cipher*. Metode tersebut akan diimplementasikan pada sebuah aplikasi *chatting* berbasis *android* dimana aplikasi *chatting* ini dapat dipakai oleh Wali Kelas dan Wali Murid untuk saling berkomunikasi. Aplikasi *chatting* ini akan menerapkan metode tersebut yang digunakan untuk mengamankan pesan yang dikirim sehingga pesan yang dikirim aman dari pencurian yang dilakukan oleh pihak yang tidak bertanggung jawab. Dengan adanya aplikasi *chatting* ini diharapkan dapat mempermudah Wali Kelas dan Wali Murid untuk saling berkomunikasi yang mana aplikasi *chatting* tersebut juga tetap dapat menjaga keamanan informasi yang dikirim.

3.3 Perancangan Aplikasi

Aplikasi yang akan dikembangkan adalah Aplikasi *chatting* yang digunakan sebagai media komunikasi antara Wali Kelas dan Wali Murid dengan mengimplementasikan algoritma kriptogragi *Vigenere Cipher* dan *Affine Cipher* sebagai keamanan data. Pesan yang dikirim akan dienkripsikan terlebih dahulu sebelum nantinya akan tersimpan di database.

Aplikasi yang dikembangkan akan mendukung Wali Kelas untuk membuat sebuah *room* baru yang mana *room* tersebut diberi judul sesuai dengan topik yang ingin dibahas, sedangkan Wali Murid dapat masuk kedalam *room* yang telah dibuat oleh Wali Kelas sebelumnya. Didalam *room* tersebut Wali Kelas dan Wali Murid dapat saling berinteraksi baik menyampaikan informasi ataupun sekedar berbincang.

Dengan menerapkan algoritma kriptografi *Vigenere Cipher* dan algoritma kriptografi *Affine Cipher* pada aplikasi *chatting* ini resiko terjadinya pencurian informasi dapat dicegah karena pesan yang dikirim akan dienkripsi sehingga sulit untuk dibaca oleh orang awam. Aplikasi yang dikembangkan berbasis Android dan disimpan dalam Firebase.

3.4 Rancangan Layar

a. Rancangan Layar Form Menu Utama

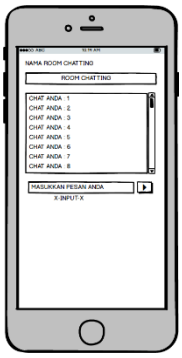
Form Menu Utama akan menampilkan pilihan Login sebagai Wali

Kelas atau Wali Murid. Dalam form ini Wali Kelas akan memilih untuk login sebagai Wali Kelas dan Wali Murid akan memilih sebagai Wali Murid.

Gambar 1 : Rancangan Layar Form Menu Utama

b. Rancangan Layar Form Chat Room

Form Chat Room digunakan untuk Wali Kelas dan Wali Murid untuk dapat berkomunikasi. Wali Kelas dan Wali Murid nantinya saling mengirimkan pesan satu sama lain didalam Chat Room tersebut.

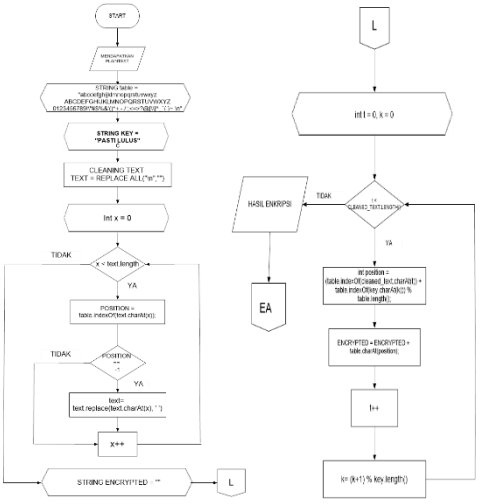


Gambar 2 : Rancangan Layar Form Chat Room

3.5 Flowchart

a. Flowchart enkripsi Vigenere Cipher

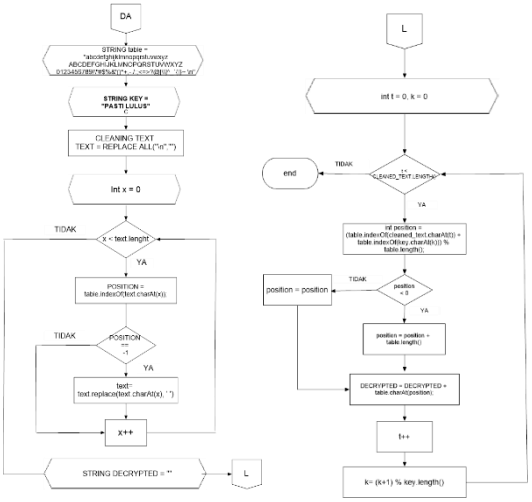
Dibawah ini flowchart yang dipakai pada saat proses mengenkripsi pesan yang dikirim.



Gambar 3 : Flowchart Enkripsi Vigenere Cipher

b. Flowchart dekripsi Vigenere Cipher

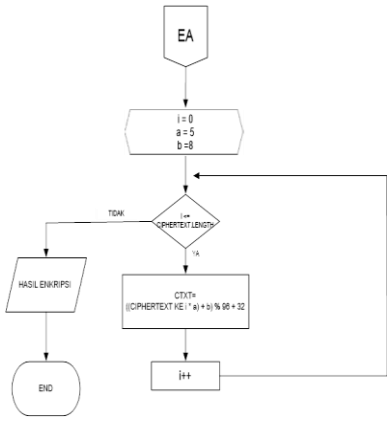
Dibawah ini flowchart yang dipakai pada saat proses pesan agar dapat dibaca oleh user.



Gambar 4 : Flowchart Dekripsi Vigenere Cipher

c. Flowchart enkripsi Affine Cipher

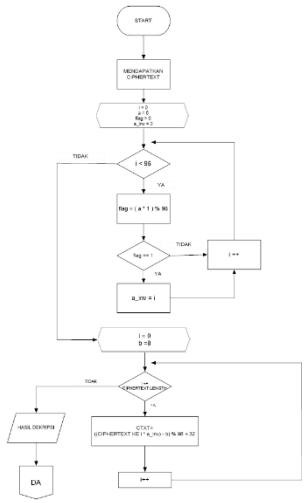
Dibawah ini flowchart yang dipakai pada saat proses mengenkripsikan pesan setelah sebelumnya telah dienkripsi menggunakan algoritma Vigenere Cipher.



Gambar 5 : Flowchart Enkripsi Affine Cipher

d. Flowchart dekripsi Affine Cipher

Berikut *flowchart* yang digunakan untuk mendekripsikan pesan menggunakan algoritma Affine Cipher.



Gambar 6 : Flowchart Dekripsi Affine Cipher

4. IMPLEMENTASI DAN ANALISIS HASIL UJI COBA PROGRAM

4.1 Implementasi Program

Dalam proses membangun Aplikasi Chatting ini digunakan hardware dan software sebagai berikut:

a. Spesifikasi Hardware
   1) Processor : AMD A8-6410 APU @ 2.0 GHz
   2) Installed Memory (RAM) : 8.00 GB
   3) Harddisk : 500GB

b. Spesifikasi Software
   1) Microsoft Windows 10
   2) Android Studio 2.3
   3) NoxPlayer 6.0.1.1 sebagai emulator *Android*

4.2 Tampilan Layar

a. Tampilan Layar Form Menu Utama

Form menu utama menampilkan form untuk login sebagai Wali Kelas atau Wali Murid.

Gambar 7 : Tampilan Layar Form Menu Utama

b. Tampilan Layar Form List Chat Room

Form list chat room menampilkan room yang sudah dibuat oleh Wali Kelas ataupun Wali Kelas ingin membuat sebuah room baru dengan topik baru.

Gambar 7 : Tampilan Layar Form List Chat Room

c. Tampilan Layar Form Chat Room

Form chat room menampilkan form dimana Wali Kelas dan Wali Murid dapat saling mengirimkan pesan satu sama lain.

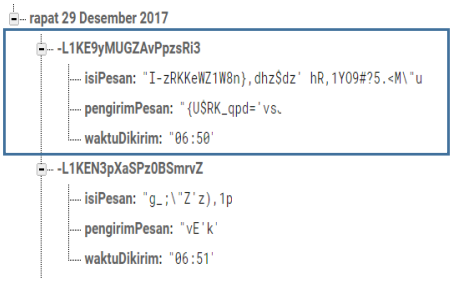
Gambar 8 : Tampilan Layar Form Chat Room

4.3 Pengujian Program

Pengujian program dilakukan untuk mengetahui kesalahan yang terdapat pada program serta menjamin program dapat bekerja sebagaimana mestinya.

a. Hasil Enkripsi Pesan Wali Kelas

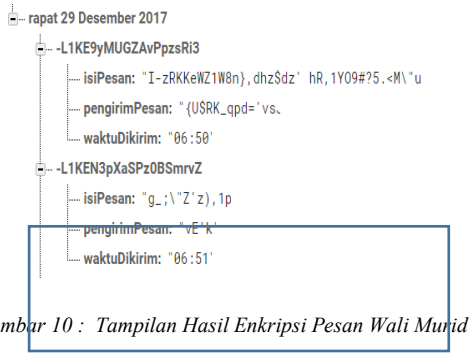
Wali Kelas mengirimkan sebuah pesan kemudian pesan akan dienkripsi dengan algoritma Vigenere Cipher dan Affine Cipher sehingga menghasilkan kata acak yang sulit dimengerti.



Gambar 9 : Tampilan Hasil Enkripsi Pesan Wali Kelas

b. Hasil Enkripsi Pesan Wali Murid

Wali Murid mengirimkan sebuah pesan kemudian pesan akan dienkripsi dengan algoritma Vigenere Cipher dan Affine Cipher sehingga menghasilkan kata acak yang sulit dimengerti.



Gambar 10 : Tampilan Hasil Enkripsi Pesan Wali Murid

c. Tabel Pengujian Enkripsi Pesan

Tabel 1 : Tabel Pengujian Enkripsi Pesan

No	Pesan	Hasil enkripsi	Keterangan
1	homeschooling	[sa@M-GuJfMbK	Berhasil
2	al	8d	Berhasil
3	ihsan	`P ,6	Berhasil
4	rapat	v-p,R	Berhasil
5	tanggal	-fJsh[	Berhasil
6	4	2	Berhasil

4.4 Kelebihan dan kekurangan Program

a. Kelebihan Program

1) Aplikasi chatting ini dapat digunakan dan juga dapat diakses kapanpun dan dimanapun.
2) Aplikasi *chatting* ini dilengkapi dengan algoritma *affine cipher* dan *vigenere cipher* untuk proses enkripsi dan dekripsi pesan sehingga keamanannya lebih terjamin.
3) Tampilan aplikasi sederhana sehingga mudah dimengerti
4) Wali Kelas dan Wali Murid dapat saling berkomunikasi tentang apapun, baik mengenai pembelajaran, acara, atau hanya berbincang-bincang dengan tetap menjaga keamanan pesan.

b. Kekurangan Program

1) Aplikasi *chatting* ini hanya dapat melakukan enkripsi berbentuk teks.
2) Tidak terdapatnya sistem validasi yang digunakan untuk mengetahui email tersebut ada atau tidak.
3) Tidak ada sistem pembuatan *password* untuk pembuatan *room* bagi Wali Kelas yang ingin membuat *room.*
4) Proses *login* dan registrasi yang cukup memakan waktu karena proses melakukan login dan registrasi bergantung kecepatan internet saat itu.

5. PENUTUP

5.1 Kesimpulan

a. Aplikasi ini ditujukan untuk Wali Kelas dan Wali Murid pada *Homeschooling* Al Ihsan yang digunakan untuk memudahkan penyampaian informasi antara Wali Kelas dan Wali Murid
b. Aplikasi ini menggunakan dua buah metode pengamanan yaitu *Affine Cipher* dan *Vigenere Cipher* yang diterapkan pada saat Wali Kelas dan Wali Murid melakukan proses Registrasi, *Login*, dan pengiriman pesan
c. Pesan yang dikirim akan tersimpan pada Firebase.
d. Pada aplikasi *chatting* ini Wali Kelas dapat membuat sebuah *room* baru bila Wali Kelas ingin membuat sebuah topik baru sesuai dengan Nama *Room* yang ditulis oleh Wali Kelas.

5.2 Saran

a. Dapat menambahkan fitur-fitur lain seperti dapat mengenkripsi gambar, video, ataupun file (pdf,doc,pptx).
b. Ditambahkan sebuah validasi untuk memastikan email pengguna benar atau tidak
c. Ditambahkan sebuah password dalam proses pembuatan *room* bagi Wali Kelas yang ingin membuat sebuah *room* baru.
d. Ditambahkan sebuah fitur *Personal Message* agar pengguna dapat berkomunikasi dengan satu akun saja.
e. Selalu memperbarui keamanan yang ada pada aplikasi chatting dikarenakan saat ini banyak peretas yang dapat membobol algoritma yang telah lama dibuat sehingga tidak dapat dipastikan algoritma yang ada apakah masih aman untuk digunakan.

DAFTAR PUSTAKA

[1] Agung, H. & Budiman, 2015. Implementasi Affine Chiper Dan RC4 Pada Enkripsi File Tunggal. *Prosiding SNATIF*, hal. 243–250.
[2] Anwar, S., Nugroho, I., dan Ahmadi, A., 2015. Implementasi Kriptografi Dengan Enkripsi Shift Vigenere Cipher Serta Checksum Menggunakan CRC32 Pada Data Text. *Jurnal Sistem Informasi*, vol. 2, hal. 51-58.
[3] Efrandi, Asnawati & Yupiyanti, 2014. Aplikasi Kriptografi Pesan Menggunakan Algoritma

Vigenere Cipher. *Jurnal Media Infotama*, 10(2), pp.120–128.

[4] Hardiyanti, S. et al., 2012. Enkripsi Affine Cipher Untuk Steganografi Pada Animasi Citra GIF. , 9(1), pp.89–100.

[5] Hidayat, Arfian. "Algoritma Kriptografi Vigenere Cipher." http://arfianhidayat.com/algoritma-kriptografi-vigenere-cipher" [diakses tanggal 10 Desember 2017]
[6] Kromodimoeljo, S., 2009. *Teori & Aplikasi Kriptografi, SPK IT Consulting*.
[7] Sutiono, A.P., 2011. Algoritma RC4 sebagai Perkembangan Metode Kriptografi : Institut Teknologi Bandung.
[8] Yulianingsih, P., Hamdani & Maharani, S., 2014. Aplikasi Chatting Rahasia Menggunakan Algoritma Vigenere Cipher. *INFORMATIKA Mulawarman*, 9(1), pp.1–4.
[9] Yatini, B., I. & Dwi Astuti, F., 2015. Analisis Performansi Kriptografi Menggunakan Algoritma Affine Cipher, Vigenere Cipher dan BASE64. *Jurnal teknik*, vol. 5, no. 1, hal. 64-70.