IMPLEMENTASI ALGORITMA AFFINE CIPHER DAN AES-128 UNTUK PENGAMANAN PESAN DAN ONE TIME PASSWORD REGISTRASI AKUN PADA APLIKASI CHATTING BERBASIS ANDROID DI SMA HANG TUAH 1 JAKARTA

Abdul Azzam Ajhari[1)], **Windarto**[2)]
[1]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
E-mail : abdazzamajhari@gmail.com[1)], windarto@budiluhur.ac.id[2)]

Abstrak

Dunia teknologi informasi yang pertumbuhan dan perkembangannya sangat cepat membawa dampak perubahan besar dalam kehidupan manusia. Semakin banyak kegiatan yang dilakukan secara mudah dengan menggunakan teknologi mobile. Salah satu perkembangan dalam dunia teknologi mobile adalah perkembangan dari aplikasi perangkat lunak berbasis android yang sangat rentan dari segi keamanan, karena android adalah perangkat lunak open source (gratis) yang dapat di modifikasi oleh siapapun. Setiap sistem maupun aplikasi yang dibuat membutuhkan suatu database, dengan perkembangan teknologi saat ini database tidak perlu lagi disimpan dalam perangkat server lokal. Cloud database menjadi pilihan startup perusahaan dan developer baru dalam membuat aplikasi serta sistem, cloud database yang populer saat ini adalah Firebase. Firebase Cloud Database merupakan salah satu database terbaik sejak tahun 2016, dengan memanfaatkan koneksi stabil database dapat digunakan secara realtime. Ketika pertukaran informasi dituliskan dalam sebuah pesan dan dikirimkan melalui aplikasi chatting, pesan tersebut hanya sekedar disimpan untuk konsumsi pribadi. Banyaknya pengguna yang tidak peduli dengan keamanan isi pesan yang mereka kirim memberikan dampak serius dikemudian hari seperti pencurian isi pesan oleh peretas dengan teknik sniffing. Untuk itu dibutuhkan suatu aplikasi chatting yang aman dalam menyampaikan pesan dan berbagi informasi kegiatan sekolah. Tujuan utama penelitian ini adalah menyediakan keamanan chatting serta verifikasi akun dengan algoritma kriptografi Affine Cipher dan AES-128 yang menjadi suatu wadah informasi bagi siswa dan guru SMA Hang Tuah 1 Jakarta.

Kata kunci: OTP, Chatting, Kriptografi, Firebase, Android.

1. PENDAHULUAN

1.1 Latar Belakang

Semakin banyak hal dan aspek dalam kehidupan yang menggunakan teknologi *mobile* untuk mempermudah suatu aktivitas. Salah satu perkembangan yang terjadi di dunia teknologi *mobile* adalah perkembangan dari aplikasi perangkat lunak yang menggunakan sistem operasi berbasis android dan sangat rentan dari segi keamanan, karena android adalah perangkat lunak *open source* (gratis) yang dapat di modifikasi oleh siapapun. Ketika pertukaran informasi dituliskan dalam sebuah pesan dan dikirimkan melalui aplikasi *chatting* itu hanya sekedar disimpan untuk konsumsi pribadi. Isi pesan *chatting* tersebut tidak memiliki keamanan apapun. Banyaknya pengguna yang tidak peduli dengan keamanan isi pesan yang mereka kirim memberikan dampak serius dikemudian hari seperti pencurian isi pesan oleh *hacker* dengan teknik *sniffing.*

SMA Hang Tuah 1 Jakarta merupakan sekolah yang setiap tahunnya mengadakan acara besar antar sekolah. Dalam kegiatan rapat yang diadakan oleh organisasi SMA Hang Tuah 1 Jakarta, beberapa informasi hanya boleh dimiliki panitia yang memiliki hak dan guru pendamping. Pada kenyataannya, informasi yang seharusnya bersifat rahasia dan sensitif seperti informasi keuangan acara dari beberapa sponsor dan dana sekolah disalahgunakan oleh sebagian pihak yang tidak bertanggung jawab.

Aplikasi *chatting* dibutuhkan sekolah sebagai sarana para guru pendamping dan siswa untuk bertukar pesan singkat mengenai kejadian dan informasi yang dibutuhkan secara langsung. Tidak hanya bertukar pesan singkat, dengan *chatting* para guru dan siswa dapat bertukar informasi mengenai acara yang akan dibuat, dana yang dibutuhkan untuk acara tersebut dan informasi kehadiran guru masing-masing kelas. Keamanan pesan pada aplikasi *chatting* sangat dibutuhkan suatu aplikasi untuk mengamankan pesan yang dikirimkan, salah satunya dapat menggunakan metode kriptografi.

Kriptografi merupakan ilmu atau seni untuk menjaga keamanan pesan. Dalam kriptografi memiliki proses enkripsi yang bertujuan untuk mengamankan isi pesan teks menjadi pesan acak yang tidak dapat dibaca. Dan proses dekripsi yang bertujuan untuk mengembalikan pesan acak yang tidak dapat dibaca menjadi tulisan asli yang dapat dibaca. Algoritma kriptografi yang dapat digunakan dalam menjaga keamanan isi pesan *chatting* dan verifikasi akun dengan OTP (*One Time Password*) adalah algoritma Affine Cipher

dan AES-128. Prinsip yang digunakan Affine Cipher memanfaatkan teknik manipulasi bilangan bit ke bentuk-bentuk yang ditentukan seperti *hexadecimal* dengan kunci yang bisa dikustomisasi oleh pengembang. Penambahan algoritma AES-128 merupakan kombinasi yang baik, dikarenakan keamanan Affine Cipher kurang baik akan diputarkan kembali dan digabung oleh kunci yang digunakan. Setelah diputar, proses transposisi dengan perkalian matriks menjadi acuan keamanan pada AES-128.

1.2 Masalah

Berikut ini adalah permasalahan yang ditemukan pada SMA Hang Tuah 1 Jakarta, antara lain :

a. Isi pesan pada *chatting* masih rentan dicuri pada saat pengiriman pesan dengan koneksi internet.
b. Kurang terjaminnya keamanan isi pesan *chatting* yang tersimpan pada *database*.
c. Kurang terjaminnya keamanan *privacy* akun pengguna yang tersimpan pada *database*.
d. Siswa dan guru masih mengalami kesulitan dalam mengakses informasi yang ada di *website* melalui *handphone*.

1.3 Tujuan Penelitian

Tujuan penelitian ini adalah mengamankan pesan *chatting* dan verifikasi pada akun dengan menerapkan algoritma Affine Cipher dan AES-128 pada aplikasi. Ketika pesan *chatting* dikirimkan melalui jaringan yang tidak aman, pesan tersebut tersimpan di *cloud database firebase* dengan terenkripsi Affine Cipher dan AES-128. Sedangkan, keamanan akun hanya dapat diakses oleh pemilik *email* yang terdaftar dikarenakan ketika registrasi mengharuskan pemilik akun memverifikasi akunnya dengan kode OTP yang dikirimkan pada *email*.

1.4 Batasan Masalah

Agar tidak menyimpang dari pokok pembahasan maka penulis perlu membatasi masalah yang akan dibahas, yaitu :

a. Pengamanan isi pesan *chatting* hanya dapat berupa teks.
b. Algoritma yang digunakan pada pengamanan adalah Affine Cipher dan AES-128.
c. Sistem *chatting* hanya dapat digunakan oleh semua guru, siswa yang menjadi panitia acara, dan sebagian staff administrasi sekolah.
d. Media yang digunakan untuk implementasi adalah telepon seluler dengan sistem operasi Android dengan koneksi yang stabil.
e. Media penyimpanan menggunakan *Cloud Database* Firebase yang dimiliki oleh perusahaan Google.
f. Informasi mengenai sekolah akan ditampilkan pada aplikasi dengan *mobile services* menggunakan tampilan *WebView* dari website sekolah yang sudah ada.
g. Menggunakan menu *login* dengan *username* dan *password* untuk mengakses aplikasi *chatting*.
h. Untuk verifikasi akun diharuskan memasukkan kode OTP ketika registrasi yang dikirimkan melalui *email*.
i. Sistem pendaftaran acara akan mendapatkan informasi melalui *email* ketika sukses.

2. DASAR TEORI

2.1. Firebase Chatting Messenger

Firebase merupakan penyedia layanan *cloud* dengan *backend* sebagai servis yang berasal dari San Fransisco, California. Perusahaan ini membuat sejumlah produk untuk pengembangan aplikasi *mobile* ataupun web. Firebase didirikan oleh Andrew Lee dan James Tamplin pada tahun 2011 dan diluncurkan dengan *cloud database* secara *realtime* di tahun 2012. Produk utama dari Firebase yakni suatu *database* yang menyediakan API untuk memudahkan para pengembang menyimpan dan mensinkronisasi data melalui *multiple client*. Pada Oktober 2014, perusahaan ini diakusisi oleh Google. Suatu aplikasi layanan yang memungkinkan pengembang membuat API untuk disinkronisasikan untuk *client* yang berbeda – beda dan disimpan pada *cloud* Firebase.

a. Firebase Realtime Database

Firebase *Realtime Database* adalah basis data yang menyimpan data di *cloud*. Data yang disimpan pada cloud terbentuk sebagai JSON dan disinkronisasi secara langsung ke setiap produk aplikasi yang terhubung. Ketika *developer* membangun aplikasi lintas-*platform* dengan iOS, Android, dan JavaScript SDK, semua klien berbagi satu *instance Realtime Database* dan secara otomatis menerima pembaruan dengan data terbaru. [1] *Realtime Database* merupakan sebuah basis data NoSQL yang memiliki optimalisasi dan fungsionalitas yang berbeda dibandingkan dengan basis data relasional. *Realtime Database* API didesain hanya untuk memperbolehkan operasi data yang bisa dieksekusi dengan cepat. Hal ini memungkinkan *developer* untuk membangun pengalaman *realtime*

yang bisa melayani jutaan pengguna tanpa mengorbankan daya respons. [2]

2.2. Kriptografi

a. Pengertian Kriptografi

Kata Kriptografi berasal dari Yunani, yang terdiri dari kata *crypto* yang memiliki arti rahasia dan *graphia* yang memiliki arti tulisan. Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan ketika pesan dikirimkan dari suatu tempat ke tempat lain. [3]

b. Pengertian Enkripsi

Enkripsi adalah suatu proses untuk mengubah sebuah pesan, data atau informasi (biasa disebut *plaintext*), sehingga informasi tersebut tidak dapat dibaca oleh orang yang tidak bertanggung jawab. [4] Jadi *plaintext* adalah informasi yang dapat dimengerti dan *ciphertext* adalah informasi yang tidak dapat dimengerti atau dibaca.

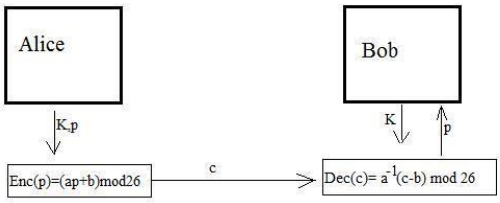
c. Pengertian Dekripsi

Dekripsi adalah suatu proses mengubah sebuah pesan, data atau informasi yang tidak dapat dibaca menjadi sebuah informasi yang dapat dimengerti dan dapat dibaca. Secara umum, kriptografi ialah mengenai mengkonstruksi dan menganalisis protokol komunikasi yang dapat memblokir lawan. [4] Berbagai aspek dalam keamanan informasi yang merupakan bagian pusat dari kriptografi modern seperti data rahasia, integritas data, autentikasi, dan non-repudansi. Terjadinya titik temu antara disiplin ilmu matematika, ilmu komputer, dan teknik elektro. Aplikasi dari kriptografi termasuk ATM, password komputer, dan E-commerce membentuk pemahaman Kriptografi Modern.

2.3. Affine Cipher

Affine Cipher adalah perluasan dari Caesar Cipher yaitu sistem persandian klasik berbasis substitusi yang sederhana. Enkripsi dan dekripsi pada sistem persandian Caesar menggunakan operasi *shift*. Operasi *Shift* adalah mensubtitusi suatu huruf menjadi huruf pada daftar alfabet berada di-k sebelah kanan atau kiri huruf itu. [5]

p, c ∈Z¬26 K=|(a,b) ∈Z^*26|



Huruf Asli	Rumus	Kode Acak	Huruf Acak
A	0.7 + 12 (mod 26)	12	M
Z	25.7 + 12 (mod 26)	5	F
Z	25.7 + 12 (mod 26)	5	F
A	0.7 + 12 (mod 26)	12	A
M	12.7 + 12 (mod 26)	18	S

Gambar 1 : Skema sandi Affine [5]

a. Enkripsi Affine Cipher

Secara sistematis enkripsi *plaintext* P lalu menghasilkan C dinyatakan dengan fungsi kongruen :

$$C = aP + b \pmod n$$

Berdasarkan persamaan diatas, maka *plaintext* dapat dihitung sebagai berikut:

Plaintext = AZZAM | n = 26
(total huruf a-z) , a = 7, b = 12

Dari hasil yang didapat, maka cipherteks dari kata AZZAM adalah MFFAS.

b. Dekripsi Affine Cipher

Dalam melakukan dekripsi diperlukan m-1, jika syarat terpenuhi maka dekripsi dilakukan dengan persamaan :

$$P= a^{-1} (C - b) \pmod n$$

Huruf Acak	Rumus	Kode Asli	Huruf Asli
M	15(12 - 12)(mod 26)	0	A
F	15(5 - 12)(mod 26)	25	Z
F	15(5 - 12)(mod 26)	25	Z
A	15(12 – 12)(mod 26)	0	A
S	15(18 - 12)(mod 26)	12	M

Untuk mengembalikan cipherteks yang telah dienskripsi menjadi pesan rahasia dapat dilakukan pendekripsian, pertama-tama dapat dihitung 7-1 (mod 26), yang dapat dihitung dengan memecahkan kekongruenan lanjar.

$$7x = 1 \pmod{26}$$

Untuk dekripsi dengan hasil 1 maka solusinya adalah x =15 (mod 26) dikarenakan 7.15 = 105 mod 26 menghasilkan = 1.

Cipherteks :
MFFAS | n = 26, a = 7, b = 12, $a^{-1} = 15$

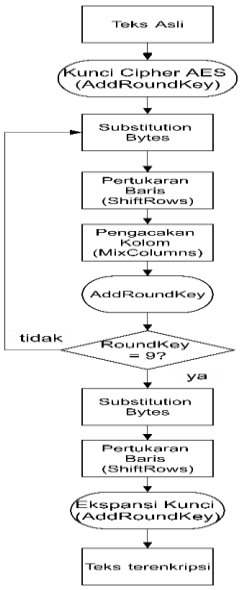
Dari hasil yang didapat, maka *plaintext* dari kata MFFAS adalah AZZAM.

2.4. AES-128

Advanced Encryption Standard (AES) dipublikasikan oleh NIST *(National Institute of Standard and Technology)* pada tahun 2001. AES merupakan kode blok simetris untuk menggantikan DES *(Data Encryption Standard)* yang sudah ditinggalkan. DES terbukti menjadi algoritma enkripsi yang aman didunia selama puluhan tahun. Pada tahun 1990 panjang kunci DES dianggap terlalu pendek dan terbukti pada tahun 1998, 70 ribu PC di internet berhasil membobol satu kunci DES dalam tempo 96 hari, tahun 1999 dalam tempo 22 hari. Karena sudah berhasil dipecahkan, maka dibuatlah mesin khusus untuk memecahkan algoritma DES yang mampu memecahkan 25% kunci DES dalam waktu 2,3 hari dan dapat memcahkan seluruh kunci DES dalam waktu rata-rata 4,5 hari. Karena alasan tersebut maka kemudian diadakan kompetisi oleh NIST untuk mengganti algoritma DES. Melalui seleksi yang ketat, maka pada 2 Oktober 2000 terpilih algoritma Rijndael atau yang dikenal sekarang algoritma AES sebegai pemenang. AES mempunyai kunci 128, 192 dan 256 bit sehingga berbeda dengan panjang dari putaran rijndael.

a. Enkripsi AES-128

Proses enkripsi algoritma AES terdiri dari 4 jenis transformasi bytes, yaitu *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*. Awal proses enkripsi, state akan mengalami transformasi byte *AddRoundKey*. Setelah itu *state* akan mengalami transformasi *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* secara berulang sebanyak Nr. Proses ini disebut juga sebagai *round function.* Pada *Round* terkahir, proses berbeda dari sebelumnya dimana *state* tidak mengalami transformasi *MixColumns*.



Gambar 2 : Proses Enkripsi AES-128 [7]

Plaintext = AZZAM | n = 26
(total huruf a-z) , a = 7, b = 12
hasil enkripsi = MFFAS.

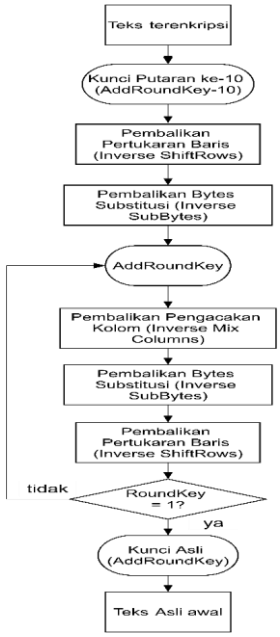
Cipherteks : MFFAS | contoh kunci : 12345 akan di enkripsi dengan algoritma AES-128:

hex	9d	5f	75	3e	7e	5f	7c	e1	58	c0	1f	c2	cc	30	6c	64
teks	□	_	u	>	~	_	|	Á	X	À	.	Â	Ì	0	l	d

Hasil enkripsi perubahan dari cipherteks Affine Cipher MFFAS dengan kunci 12345 diatas adalah □ _ u > ~ _ | á X À Â Ì 0 l d.

b. Dekripsi AES-128

Pembalikan dalam mentransformasi *cipher* dan mengimplementasikannya ke arah yang berlawanan untuk menghasilkan *inverse cipher* yang mudah dipahami untuk algoritma AES. Transformasi byte yang digunakan pada *invers cipher* adalah *InvShiftRows,InvSubBytes,InvMixColumn,* dan *AddRoundKey*.



Gambar 3 : Proses Dekripsi AES-128 [7]

3. ANALISA MASALAH DAN RANCANGAN DAN RANCANGAN PROGRAM

3.1. Analisa Permasalahan

Dalam proses belajar-mengajar di sekolah khusunya di SMA Hang Tuah 1 Jakarta, hubungan antara guru dan siswa perlu dijaga dengan baik. Dengan hubungan yang baik siswa akan lebih mengenal guru dan sebaliknya, terutama ketika siswa dan sekolah akan membuat sebuah acara. Namun, dikarenakan kesibukan yang dimiliki oleh guru pada jam pengajaran, siswa menjadi lebih sulit untuk mendapatkan informasi dan menghubungi guru tersebut. Pada posisi ini siswa biasanya akan mencoba menghubungi guru yang bersangkutan dengan mencari informasinya di kantor guru. Karena guru yang sibuk dan terdapat acara yang mendadak seperti rapat, terkadang informasi sering kali tidak tersampaikan kepada siswa, namun guru yang sedang berjaga selalu menuliskan informasi mengenai guru pada papan tulis di ruang guru. Tidak hanya itu, informasi berita mengenai prestasi sekolah sering tidak dilakukan pembaharuan di *website* sekolah.

3.2. Penyelesaian Masalah

Dari permasalahan diatas dapat disimpulkan bahwa masalah yang terjadi sebenarnya adalah bagaimana menjaga hubungan komunikasi antara guru dan siswa agar berjalan dengan baik, dan memudahkan siswa bertukar informasi kepada guru dengan cepat dan aman. Oleh karena itu, dibuat sebuah aplikasi *chatting* berbasis android dengan keamanan ganda menggunakan metode algoritma Affine cipher dan AES-128 yang memberikan keamanan informasi. Tidak hanya *chatting* aplikasi ini juga sebagai media komunikasi serta portal berita informasi antara kegiatan sekolah dan guru dengan siswanya menjadi lebih baik dan lancar. Guru yang tidak memiliki kegiatan dapat membuat informasi artikel pada *website* mengenai guru yang tidak hadir, izin, sakit maupun saat rapat sehingga aplikasi memberikan notifikasi kepada *smartphone* siswa.

3.3. Perancangan Aplikasi

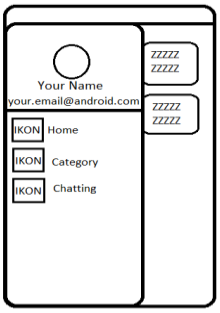
Aplikasi yang akan dikembangkan adalah sistem chatting dan artikel dengan teknologi cloud dengan mengimplementasikan algoritma kriptografi AES 128 terhadap isi pesan dan Affine Cipher untuk verifikasi OTP keamanan akun yang akan masuk ataupun keluar dalam sistem cloud. Aplikasi yang dikembangkan akan mendukung guru dan organisasi OSIS untuk menginformasikan kegiatan sekolah di website yang akan diterima oleh siswa SMA Hang Tuah 1 pada handphone dengan sistem operasi Android.

Aplikasi yang dikembangkan berbasis web dan mobile yang akan disimpan dalam sebuah hosting dan cloud database Firebase sehingga tidak perlu diinstall. Aplikasi dikembangkan menggunakan bahasa pemrograman PHP dan menggunakan database MYSQL serta Cloud database Firebase.

3.4. Rancangan Layar

a. Rancangan Menu Utama

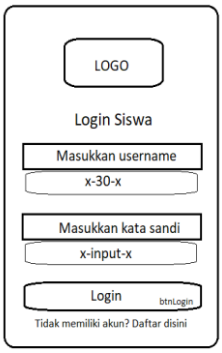
Rancangan menu dibuat untuk menganalisa menu yang terdapat pada bagian-bagiannya, sehingga ketika terdapat masalah pada menu tersebut dapat kita telusuri dalam perbaikan aplikasi. Menggunakan tampilan halaman *react native* dengan menggunakan API website untuk mengambil data berita ke dalam aplikasi dengan responsif dan cepat.



Gambar 4 : Layar Menu Utama

b. Rancangan Layar Login Chatting

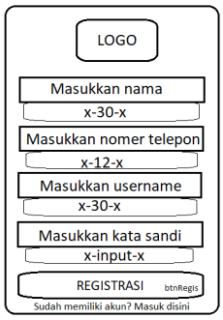
Rancangan awal aplikasi chatting ini adalah pada saat pengguna belum melakukan login. Hak akses pada pengguna diberikan level yang berbeda yaitu Guru dan Siswa.



Gambar 5 : Layar Login Chatting

c. Rancangan Layar Registrasi

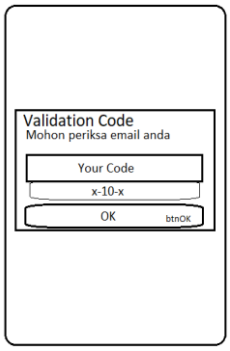
Rancangan layar registrasi adalah tahap yang apabila guru atau siswa belum melakukan pendaftaran sebelumnya pada aplikasi ini terlebih dahulu harus mengisi registrasi pada layar registrasi. Di dalam registrasi ini terdapat 4 *edittext* yaitu "Masukkan *username*" untuk mengisi *username* email, "Masukkan nama" untuk mengisi nama, "Masukkan nomer telepon" untuk mengisi Nomer telepon dan "Masukkan kata sandi" untuk mengisi *password* serta terdapat 1 *button* yaitu "Registrasi" untuk melakukan registrasi.



Gambar 6 : Layar Registrasi Chatting

d. Rancangan Layar Validation Code

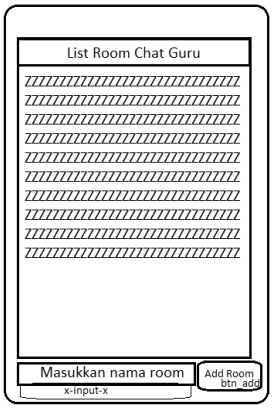
Rancangan layar aplikasi akan tampil ketika semua data yang berada di registrasi guru atau siswa sudah diisi. Form validasi ini terdiri dari 1 *textview* yaitu berisi teks pemberitahuan, 1 *edittext* yaitu *form* untuk mengisi kode dan 1 *button* untuk melakukan validasi.



Gambar 7 : Layar Validation Code

e. Rancangan Layar Chat Room

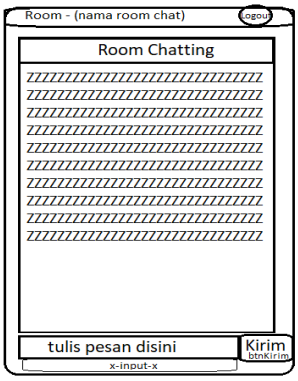
Rancangan *chat room* adalah rancangan yang akan muncul ketika guru atau siswa membuka aplikasi apabila sudah *login* dan tidak melakukan *logout*, dimana pada rancangan ini akan menampilkan *list chat room* yang telah dibuat. *Form chat room* terdiri dari 1 *edittext* berfungsi untuk memberikan nama *room*, 1 *button Add Room* yang berfungsi untuk menambahkan *room* sesuai dengan kebutuhan guru dan 1 *listview* yang berfungsi untuk melihat *room* yang telah dibuat, jika *room* dipilih juga berfungsi untuk berinteraksi dengan para siswa.



Gambar 8 : Layar Chat Room

f. Rancangan Layar Chatting Room

Rancangan layar *chatting room* ini menyediakan *listview chat* yaitu obrolan guru dan siswa. *Button "Send"* untuk mengirim pesan yang diinginkan, *edit text* untuk melihat teks yang di ketik, dan *button "LogOut"* untuk keluar dari aplikasi *chatting*.

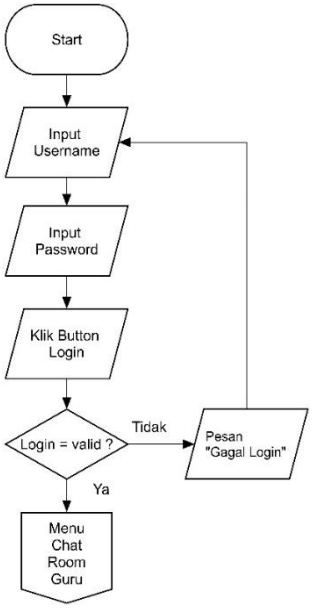


Gambar 9 : Layar Chatting Room

3.5. Flowchart

a. Flowchart Login

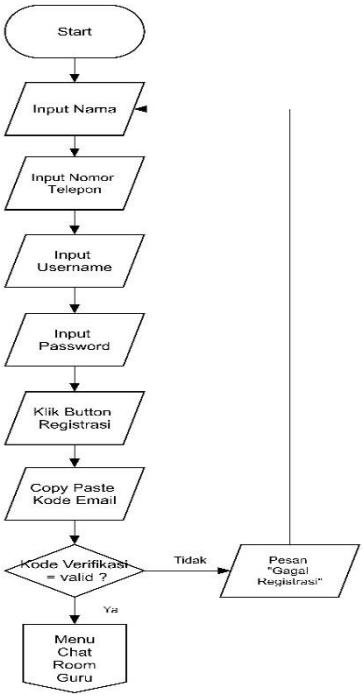
Sebelum melakukan aktifitas *chatting*, guru atau siswa dapat melihat *chat room* atau membuat *chat room*. Guru atau siswadiharapkan melakukan *login* terlebih dahulu jika sudah memiliki akun.



Gambar 10 : Flowchart Login

b. Flowchart Registrasi

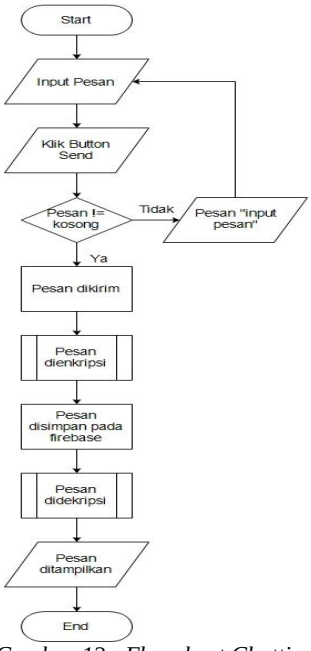
Jika guru belum mempunyai akun untuk melakukan *login* bisa registrasi pada *form login* lalu, klik sign up here maka akan diarahkan ke *form* registrasi.



Gambar 11 : Flowchart Registrasi

c. Flowchart Chatting Room

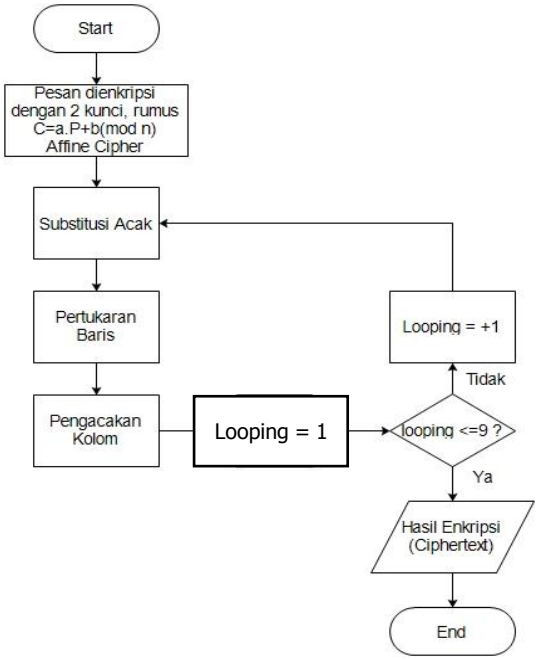
Chatting room digunakan jika ingin mengirim pesan bagi siswa maupun guru dan guru sudah membuat *room*.



Gambar 12 : Flowchart Chatting Room

d. Flowchart Enkripsi

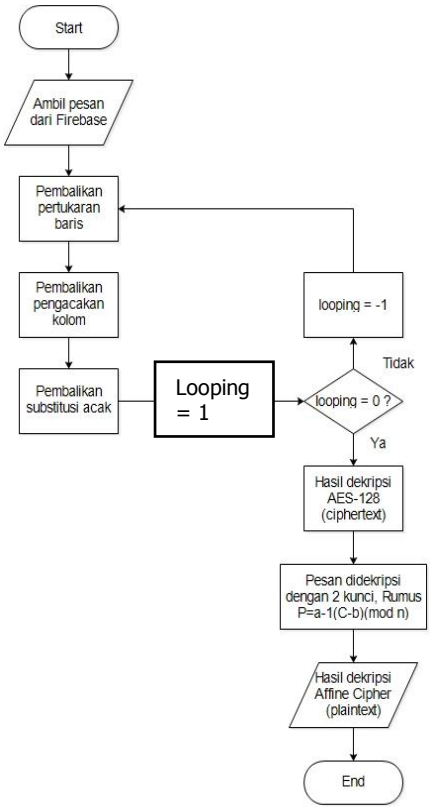
Proses enkripsi ini bekerja saat pesan yang sudah terkirim akan di enkripsi menggunakan algoritma Affine Cipher yang menggunakan 2 kunci dengan rumus C = a.P+b(mod n). Setelah C memiliki hasil berupa *ciphertext*, dilakukan kombinasi dengan bentuk ke dalam hexadecimal dan perputaran sebanyak 9x dengan subtitusi acak AES-128. hasil dari kombinasi Affine dan AES-128 yang berupa ciphertext akan disimpan pada Firebase.



Gambar 13 : Flowchart Enkripsi

e. Flowchart Dekripsi

Proses dekripsi ini bekerja saat ada pesan baru yang berada di Firebase. Pesan ini berupa *ciphertext* yang diambil oleh program dan didekripsi menggunakan algoritma AES-128 diputar hingga 9 putaran dan dilakukan substitusi acak, pertukaran baris dan pengacakan kolom. Kemudian dilakukan penguraian dengan Affine Cipher yang menggunakan 2 kunci dengan rumus $P = a^{-1} (C-b)(\text{mod } n)$, hasil dari P yang berupa plaintext akan ditampilkan pada *chatting room*.



Gambar 14 : Flowchart Dekripsi

4. IMPLEMENTASI DAN ANALISIS HASIL UJI COBA PROGRAM

4.1 Implementasi Program

Pada lingkungan percobaan akan dijelaskan mengenai spesifikasi dalam membuat aplikasi dan menjalankan aplikasi sesuai kebutuhan dengan spesifikasi minimum pada tahapan sebagai berikut :

a. Spesifikasi Hardware
   1) Processor i3 *Quad-Core* dengan minimum 1.80 Ghz (*Giga Hertz) clock.*
   2) RAM (*Random Access Memory)* minimum 8 GB (*Giga Byte*).
   3) VGA (*Video Graphics Array*) minimum 1 GB (*Giga Byte*).

b. Spesifikasi Software
   1) Sistem operasi Android minimum 5.0 Lollipop dengan RAM 512 MB (*Mega Byte).*
   2) Memori internal dibutuhkan minimal 70 MB (*Mega Byte).*
   3) Android Studio 2.2.3.
   4) Java Development Kit (JDK) versi jdk-7u71 dan jdk-8u45.
   5) Microsoft Windows 10 64-bit.

4.2 Tampilan Layar

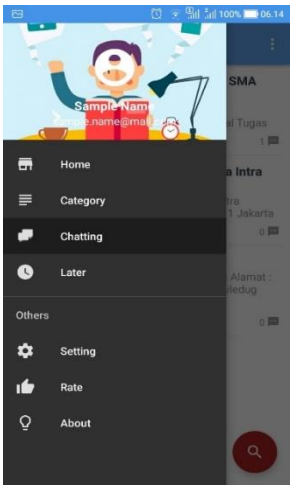
a. Tampilan Menu Utama

Pada menu ini pengguna dapat melihat berita-berita yang ada di *website* dan dapat berkomentar dalam setiap artikel sehingga

pengguna dapat berinteraksi secara langsung. Tampilan ini merupakan tampilan menu utama, pengguna tidak perlu registrasi untuk melihat informasi berita yang ada pada *website* organisasi sekolah.

Gambar 15 : Tampilan Menu Utama

b. Tampilan Navigation Bar Menu Utama
Terdapat *navigation bar* untuk melihat menu-menu yang tersembunyi ketika kita membuka aplikasi, pada *navigation bar* ini kita dapat menggunakan menu yang dibutuhkan. Salah satu menu yang menjadi penelitian adalah menu *chatting*.



Gambar 16 : Tampilan Navigation Bar Menu Utama

c. Tampilan Menu Artikel
Pada menu ini semua pengguna dapat mengakses tanpa harus melakukan *login* untuk melihat berita terbaru yang ada pada *website* dengan menggunakan aplikasi.

Gambar 17 : Tampilan Menu Artikel

d. Tampilan Menu Komentar Artikel
Tidak hanya untuk melihat artikel, pengguna juga dapat melihat komentar yang dikirimkan oleh pengguna lain secara langsung. Sehingga informasi yang didapatkan cepat dan akurat.

Gambar 18 : Tampilan Menu Komentar Artikel

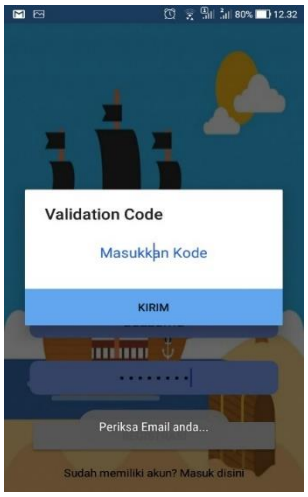
e. Tampilan Menu Login Chatting
Ketika siswa atau guru ingin melakukan *chatting* pada aplikasi diharapkan melakukan *login* terlebih dahulu. Ada 2 *edit text* yang disediakan di tampilan menu dengan *hint* "Masukkan *username*" untuk mengisi *username* yang sudah didaftarkan dan *hint* "Masukkan kata sandi" untuk mengisi kata sandi.

Gambar 19 : Tampilan Menu Login Chatting

f. Tampilan Menu Registrasi Siswa
Pada menu ini terdapat 4 *edit text* yang dimana untuk mengisi nama, nomer telepon, *username* dan kata sandi serta satu tombol untuk menampilkan menu validasi apakah pengguna tersebut terdaftar di sekolah.

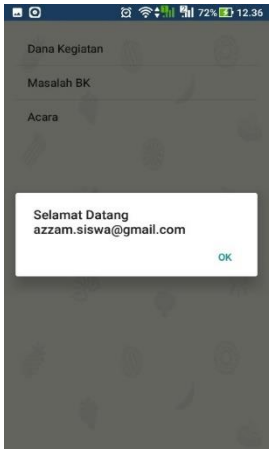
Gambar 20 : Tampilan Menu Registrasi Chatting

g. Tampilan Validation Code OTP
Proses pengiriman pesan akan selesai apabila pesan sudah berhasil terkirim ke *email* siswa.



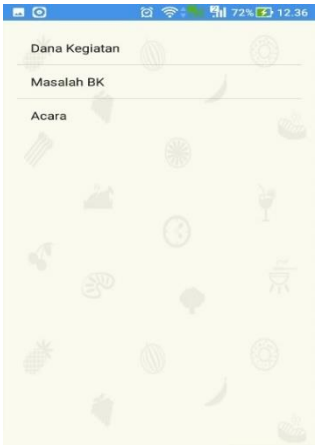
Gambar 21 : Tampilan Validation Code OTP

h. Tampilan Chat Room
Setelah masuk ke *chat room*, siswa atau guru akan mendapatkan notifikasi selamat datang dengan *username* berupa *email* yang terdaftar.



Gambar 22: Tampilan Chat Room

i. Tampilan Chat Room
Chat Room berisi daftar ruangan untuk melakukan *chatting* dengan ketentuan hanya dapat melihat tanpa bisa menambahkan atau membuat *Chat Room.*



Gambar 23 : Tampilan Chat Room

j. Tampilan Chatting Room

Setelah siswa atau guru memilih *listview Chat Room* maka akan diarahkan ke tampilan *Chatting Room* yang telah disediakan.

Gambar 24 : Tampilan Chatting Room

4.3 Analisa Hasil Uji Coba Program

Tabel 1 : Tabel Pengujian

No	Proses	Lokasi	Jaringan	Ukuran (byte) 1 char = 1 byte	Waktu (milidetik)			Kecepatan (Mbps)
					Proses	Enkripsi	Dekripsi	
1.	Login	Di dalam gedung	Wi-Fi	13 byte	3,135	-	5,213	Unggah : 2,6 Unduh : 2,5
2.	Login	Di luar gedung	Wi-Fi	13 byte	7,025	-	8,512	Unggah : 1,8 Unduh : 0,9
3.	Login	Di dalam gedung	Paket Data	13 byte	1,235	-	1,879	Unggah : 2,77 Unduh : 9,29
4.	Login	Di luar gedung	Paket Data	13 byte	0,465	-	0,921	Unggah : 7,84 Unduh : 15,36
5.	Registrasi	Di dalam gedung	Wi-Fi	13 byte	0.649	0,182	-	Unggah : 2,6 Unduh : 2,5
6.	Registrasi	Di luar gedung	Wi-Fi	13 byte	1,529	0,891	-	Unggah : 1,8 Unduh : 0,9
7.	Registrasi	Di dalam gedung	Paket Data	13 byte	0,206	0,102	-	Unggah : 2,77 Unduh : 9,29
8.	Registrasi	Di luar gedung	Paket Data	13 byte	0,101	0,83	-	Unggah : 7,84 Unduh : 15,36
9.	Pesan	Di dalam gedung	Wi-Fi	13 byte	0,500	0,500	0,500	Unggah : 2,6 Unduh : 2,5
10.	Pesan	Di luar gedung	Wi-Fi	13 byte	0,830	0,830	0,830	Unggah : 1,8 Unduh : 0,9
11.	Pesan	Di dalam gedung	Paket Data	13 byte	0,325	0,325	0,325	Unggah : 2,77 Unduh : 9,29
12.	Pesan	Di luar gedung	Paket Data	13 byte	0,100	0,100	0,100	Unggah : 7,84 Unduh : 15,36
13	Rata-rata			13 byte	1.342	0.47	2.285	-

Tabel 2 : Tabel Pengujian Enkripsi Pesan

No	Pesan	Hasil enkripsi	Waktu (milidetik)	Keterangan
1	Sma hang tuah 1	Gi-hP-nKh,1-Ph]	0.705	Berhasil
2	Hang	p-nK	0.193	Berhasil
3	Tuah	L1-P	0.215	Berhasil
4	Satu	G-,1	0.190	Berhasil
5	Jakarta	z-_-\",-	0.256	Berhasil
6	Seskoal	GA'_s-d	0.302	Berhasil
7	Abdul	M2<1d	0.214	Berhasil
8	Azzam	MJJ-i	0.202	Berhasil
9	Ajhari	MZP-\"U	0.209	Berhasil
10	Abdul Azzam Ajhari	M2<1dhMJJ-ihMZP-\"U	0.659	Berhasil

Dari 10 kali percobaan pengiriman pesan, 10 pesan itu masuk dengan menggunakan 2 akun yang berbeda dengan melalui tahap enkripsi dan dekripsi pesan. Dengan demikian, dapat disimpulkan pesan dapat terkirim dengan tingkat keberhasilan 100 %.

Tabel 3 : Database Artikel

No	Nama String / Variabel	Tipe	Keterangan
1	post_id	Integer(4)	Nomor artikel
2	Name	Varchar(30)	Nama artikel
3	Email	Varchar(30)	Email penulis artikel
4	content	Varchar(500)	Isi artikel

Tabel 4 : Database *Chatting*

No	Nama String / Variabel	Tipe	Keterangan
1	room_name	Varchar(30)	Nama ruangan chat
2	Msg	Varchar(300)	Isi pesan chat
3	Name	Varchar(30)	Nama pengguna
4	Timestamp	Date Time(20)	Waktu kirim / terima chat

4.4 Kelebihan dan Kekurangan Program

a. Kelebihan Program
   1) Aplikasi berbasis android yang mudah digunakan dan juga dapat diakses kapanpun dan dimanapun.
   2) Proses validasi mudah melalui *email* dari username.siswa@gmail.com dan username.guru@gmail.com yang dimiliki oleh setiap siswa dan guru.
   3) Aplikasi *chatting* ini dilengkapi dengan algoritma affine cipher dan AES-128 untuk proses enkripsi dan dekripsi pesan.
   4) Rata-rata waktu proses pada *chatting* yang dikirimkan 1,342 milidetik, proses enkripsi yang dibutuhkan 0,47 milidetik dan proses enkripsi yang dibutuhkan 2,285 detik.
   5) Siswa dan guru dapat saling berkomunikasi tentang apapun, dimanapun dan kapanpun yang berkaitan dengan acara yang akan dibuat sekolah atau hanya sekedar berbagi ilmu atau berbincang-bincang dengan tetap menjaga keamanan pesan.

b. Kekurangan Program
   1) Aplikasi *chatting* ini hanya dibatasi untuk mengenkripsi teks.
   2) Tidak ada *direct invite* grup sehingga semua pengguna dapat masuk ke grup *chat* manapun.
   3) Proses *login* dan registrasi memakan waktu yang cukup lama dikarenakan menggunakan proses akses data melalui internet yang harus stabil.

5. PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian dan pembahasan serta uji coba aplikasi *chatting* dapat disimpulkan sebagai berikut :

a. Akun pengguna dapat diamankan dengan verifikasi OTP (*One Time Password*) dan kombinasi algoritma Affine Cipher dan AES-128 sehingga tiap pengguna memiliki kode OTP yang berbeda.
b. Isi pesan yang tersimpan pada *cloud database* Firebase terenkripsi ganda dengan algoritma Affine Cipher dan AES-128 sehingga tidak dapat diakses oleh orang yang tidak memiliki hak.
c. Informasi kegiatan yang terdapat di *website* organisasi dapat diakses dengan mudah melalui aplikasi *handphone* pengguna yang berbasis Android.
d. Proses pengiriman waktu pesan *chatting*, proses enkripsi dan dekripsi adalah 1,342 milidetik, 0,47 milidetik dan 2,285 milidetik.

5.2 Saran

Kekurangan dalam pengembangan aplikasi yang perlu dilakukan untuk penelitian berikutnya adalah sebagai berikut :

a. Karena hanya dapat mengenkripsi pesan teks saja, diharapkan pada penelitian berikutnya, aplikasi ini dapat mengenkripsi pesan gambar, audio dan video.
b. Karena notifikasi saat pesan masuk tidak muncul, diharapkan pada penelitian berikutnya, aplikasi ini dapat dibuat notifikasi pesan *chatting* untuk memudahkan siswa dan guru dalam menerima pesan masuk.
c. Perbaikan tampilan ruang *chatting* agar lebih nyaman dilihat oleh pengguna.
d. Penambahan informasi nama ruang *chatting* agar pengguna tidak salah masuk ruang *chat*.
e. Dapat mengirim undangan untuk masuk ruang *chat* khusus.
f. Menambahkan nama ruang *chatting* dan data pengguna yang berada di ruangan tersebut.
g. Meningkatkan kapasitas *cloud database* Firebase agar pesan dikirim dan diterima lebih cepat.

DAFTAR PUSTAKA

[1] Kumar, Manoj K.N et al., 2016, IMPLEMENTING SMART HOME USING FIREBASE. Vol. 6 Issue 10, October - 2016, pp. 193~198. ISSN(O): 2249-3905, ISSN(P): 2349-6525. International Journal of Research in Engineering and Applied Sciences (IJREAS).

[2] Hossain, S.A., & Moniruzzaman, A., 1995, NoSQL Database : New Era of Databases for Big data Analytics-Classification, Characteristics and Comparison. International Journal of Database Theory and Application 6(4): p.1–13.

[3] Wijaya, Andi , 2015, SISTEM ENKRIPSI MENGGUNAKAN ALGORITMA AES-128 PADA PROTOTYPE COMMUNITY MESSENGER BERBASIS ANDROID. E-Proceeding of Engineering : Vol.2, No.2 Agustus 2015 | Page 3306, ISSN : 2355-9365.

[4] Sularsono, Eko et al., 2014, IMPLEMENTASI ALGORITMA RIJNDAEL 128 PADA APLIKASI CHATTING BERBASIS HTML5 WEBSOCKET. Jurnal INFORMATIKA Vol. 10 No. 2.

[5] Juliadi, Prihandono, B., & Kusumastuti, N., 2013, Kriptografi Klasik Dengan Metode Modifikasi Affine Cipher Yang Diperkuat Dengan Vigenere Cipher. Buletin Ilmiah Mat.Stat. dan Terapannya (Bimaster) 2(2): p.87–92.