APLIKASI *CHATTING* NOTARIS BERBASIS ANDROID DENGAN METODE KRIPTOGRAFI AES-128 DAN BLOWFISH

Zaid Fadhlurrahman[1)], **Pipin Farida Ariyani**[2)]
[1]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : zaidchrome@gmail.com[1)], pipin.faridaariyani@budiluhur.ac.id[2)]

ABSTRAK

Pada masa awalnya Instant Messaging (IM) dinamakan sebagai sarana berkomunikasi, aplikasi chatting mulai cukup dibutuhkan sebagai sarana berkomunikasi yang memumpuni. Salah satu yang sangat sering digunakan adalah SMS (Short Message Service), yang banyak digunakan untuk bertukar pesan pendek. SMS pun banyak digunakan dalam pekerjaan yang mengharuskan adanya komunikasi antara beberapa pihak, salah satunya adalah notaris. Adanya komunikasi antara notaris dengan client bertujuan untuk koordinasi dalam pengerjaan tugas seorang notaris. Semua pesan percakapan antara notaris dengan client sangatlah rahasis karena seputar dokumen-dokumen penting dan tidak boleh diketahui pihak luar yang tidak berkepentingan. Oleh karena itu dibutuhkannya aplikasi yang dapat menjaga kerahasiaan pesan antara notaris dan client sangatlah penting. Maka dari itu agar notaris dan client dapat melakukan percakapan dengan aman dan tanpa diketahui isi pesannya oleh pihak luar dibuatlah aplikasi chatting dengan fasilitas enkripsi sebagai sarana aman untuk berkomunikasi. Tujuan dari penelitian ini untuk menghasilkan suatu aplikasi chatting sebagai media komunikasi antara notaris dan client berjalan dengan baik. Dengan menerapkan Kriptografi AES-128 bit sebagai enkripsi dan dekripsi pesan dan Blowfish sebagai enkripsi dan dekripsi url gambar aplikasi dibangun berbasis android dengan menggunakan bahasa pemrograman Java Mobile dan Firebase sebagai web server. Proses pengiriman akan melalui proses enkripsi pesan yang kemudian disimpan di Firebase yang berada di cloud sedangkan proses penerimaan pesan akan melalui proses dekripsi sebelum pesan dimunculkan kepada penerima.Berdasarkan hasil pengujian, pesan dapat terbaca dengan baik oleh penerima dengan tingkat keberhasilan pengiriman pesan 100%

Kata kunci :*Android, Firebase,* Kriptografi, *AES*-128, *Blowfish*

1. PENDAHULUAN

Telepon pintar (*smartphone*) pada saat ini yang semakin banyakmembantu masyarakat dalam berkomunikasi. Banyaknya fungsi yang dimiliki telepon pintarseperti, *Sound Recorder*, *Camera*, *Chatting*, *Live Video* dan lain-lain. Pentingnya menjaga kerahasiaan data yang ada merupakan salah satu hal yang perlu diperhatikan. Salah satu cara yang bisa digunakan adalah dengan menggunakan metode enkripsi. Enkripsi adalah proses untuk menyamarkan pesan sehingga pihak luar tidak bisamengetahui pesan yang dimaksudkan. Pesan akan lebih tinggi tingkat kemanannya apabila menggunakan kriptografi. Kriptografi adalah ilmu dalam menjaga keamanan data saat proses pengiriman pesan.Aplikasi *chatting* yang berfungsi sebagai media berkomunikasi juga digunakan dalam kegiatan komunikasi pada lembaga lembaga penting. Lembaga hukum yang bekerja dalam penanganan masalah seputar pembuatan akta otentik dan kewenangan hak atas tanah dan hak kepemilikan salah satunya adalah Notaris. Notaris menangani *client* dengan data-data penting seperti akta dan data lainya yang bersifat rahasia yang perlu akan pengamanan lebih. Agar interaksi antara notaris dengan *client* nya berjalan dengan baik dan aman maka dalam penelitian ini penulis membuat aplikasi *chatting* dengan basis android menggunakan metode *Advanced Encryption Standard* (AES) 128 dan Blowfish yang diharapkan mampu mengamankan pesan antara notaris dengan *client* nya sehingga pesan antara kedua belah pihak dapat terjaga keamanannya. Enkripsi Simetris merupakan salah satu cara mengamankan data dengan menggnakan 1 kunci yang sama [1]. Metode AES ini dibuat untuk menggantikan metode *Data Encryption Standard* (DES) untuk meningkatkan aspek keamanan [2]. AES dapat digunakan secara bebas tanpa harus membayar royalti dan juga murah untuk diimplementasikan pada *smart card* yang memiliki ukuran memori kecil. Sama seperti AES, Blowfish yang sangat terkenal di dunia kriptografi, alasan utama dipilihnya adalah karena lisensinya yang bebas dan gratis. Dan komunitas open source menghargai blowfish dengan mempercayai blowfish menjadi salah satu *Open Cryptography Interface* (OCI) pada kernel Linux versi 2.5 ke atas.

Oleh sebab itu penulis memilih metode AES 128 dan Blowfish sebagai algoritma kriptografi pada aplikasi *chatting* yang ditujukan sebagai sarana komunikasi antara notaris dengan *client* agar pesan penting dan data rahasia dapat terjaga keamannya.

2. METODE PENELITIAN

Penelitian harus berasal dari sumber data yang lengkap dan terpercaya, karena dibutuhkan untuk dokumentasi penulisan karya ilmiah dan menentukan analisa penelitian pemecahan masalah yang ingin diselesaikan. Pengumpulan data ini menggunakan proses pencarian data dengan cara mencari *literature review*, jurnal ilmiah, buku-buku dan bacaan-bacaan yang berhubungan dengan judul penelitian ini. Berikut metode penelitian yang penulis gunakan dalam penelitian ini, yaitu :

a. Metode Kepustakaan, ini dilakukan dengan cara mempelajari jurnal jurnal dan buku buku sebagai referensi sebagai sumber pembahasan mengenai enkripsi, aplikasi *chatting*, dan hal lain yang dibutuhkan [3].
b. Metode Analisis, dilakukan dengan mencoba aplikasi *chatting* yang sudah ada. Serta melakukan wawancara ke pihak Notaris untuk memahami prosesnya.
c. Metode Perancangan Aplikasi

1) Analisa Kebutuhan Perangkat Lunak**,** Dalam tahap ini diperlukan adanya analisa terhadap kebutuhan sistem, cara pencarian jurnal ilmiah, buku-buku dan sumber referensi lainnya yang berkaitan dengan penulisan penelitian ini untuk mengumpulkan data dan menyelesaikan masalah yang terkait ini.
2) Desain**,** tahapan desain bertujuan untuk menentukan spesifikasi detail dari komponen-komponen program seperti manusia, perangkat keras, perangkat lunak, jaringan, data dan produk-produk informasi lainnya yang sesuai dengan hasil tahapan analisis, sehingga dapat dijelaskan dengan detail setiap fungsi dan kebutuhan yang diinginkan dari pembuatan aplikasi chatting kriptografi AES 128 dan Blowfish yang berbasis android. Pada langkah selanjutnya butuh adanya perancangan tampilan aplikasi agar mudah dimengerti oleh pengguna sesuai kebutuhan dan fungsi perangkat lunak.
3) *Coding* dan implementasi**,** menggunakan bahasa Java pada penerapan pemrograman sebagai bahasa pemrogramannya.
4) Pengujian**,** setelah pada tahap pembuatan program dan algoritma selesai, maka ditahap selanjutnya adalah pengujian aplikasi yang sudah dibuat [3].
5) Kesimpulan, membuat kesimpulan pembanding dari *output* program dengan perancangan pada jurnal dan referensi.

3. RANCANGAN SISTEM DAN APLIKASI

3.1 Analisa Masalah

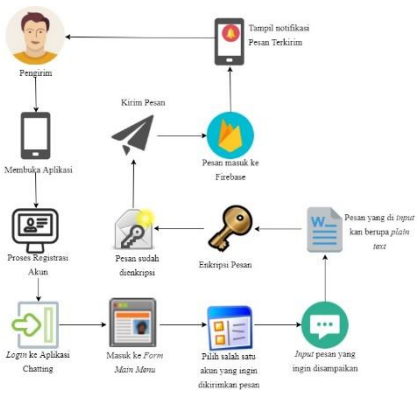
Agar komunikasi berjalan dengan baik, sarana percakapan tersebut baiknya mudah digunakan sehingga dalam proses komunikasi dan bertukar pesan pengguna tidak kesulitan menggunakannya. Serta pentingnya bagaimana untuk mengantisipasi agar pihak luar tidak dapat mencuri pesan dan data penting yang bersifat rahasia. Informasi umum mengenai pihak yang berkomunikasi pun akan perlu untuk ditampilkan agar berjalannya percakapan dapat lebih baik dengan adanya beberapa informasi dari pihak lainnya

3.2 Penyelesaian Masalah

Untuk menyelesaikan masalah yang telah diuraikan di atas, dibuatlah sebuah aplikasi *chatting* yang memiliki fitur keamanan dalam pengiriman pesan teks dan gambar. Dalam membuat aplikasi *chatting* tersebut, digunakan sebuah metode yang disebut kriptografi. Pada metode kriptografi terdapat dua proses yaitu enkripsi dan dekripsi. Enkripsi fungsinya adalah mengubah pesan teks yang berisi *plaintext* atau pesan teks biasa yang dirubah menjadi *chipertext* atau teks acak yang tidak bisa dibaca [4]. Proses dekripsi fungsinya untuk mengembalikan *chipertext* tesebut menjadi *plaintext* seperti semula. Penerapan kriptografi pada aplikasi ini diharapkan pihak yang tidak berkepentingan tidak memiliki kesempatan untuk mengetahui informasi pada pesan yang dikirimkan dari aplikasi *chatting* ini. Semua akun *user* dan isi percakapan yang dienkripsi antara pengirim dan penerima akan disimpan pada *Firebase Console.*

3.3 Skema Proses Pengiriman Pesan

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



Gambar 1. Skema Proses Pengiriman Pesan

1) Untuk menggunakan aplikasi *chatting* ini, pengirim harus membuka aplikasi yang telah di*instal* 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. Lalu setelah memilih akun, pengirim masuk ke *form chat.*
5) Setelah itu pengirim meng*input* isi pesan yang ingin dikirim ke penerima yang sudah dipilih.
6) Pada saat proses pengiriman, aplikasi akan melakukan proses enkripsi terlebih dahulu.
7) Pesan teks yang di*input* akan dirubah menjadi *chipertext* dengan menggunakan kunci yang sudah dibuat oleh sistem.
8) Setelah proses enkripsi selesai, pesan dikirim ke Firebase Console lalu diteruskan ke akun penerima dan ditampilkan di dalam *form* chat penerima.

3.4 Skema Proses Penerimaan Pesan

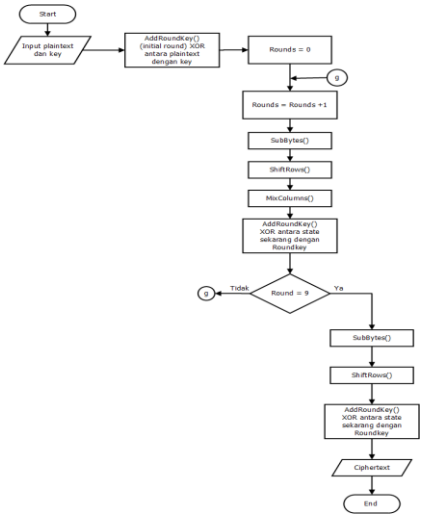
Gambar 2. Skema Proses Penerimaan Pesan

Setelah proses pengiriman pesan, berikut ini adalah proses penerimaan pesan :

1) Penerima mendapatkan notifikasi berupa pesan masuk dari pengirim.
2) Setelah itu penerima memilih salah satu akun yang mengirimkan pesan yang ditampilkan di *form main* dan membuka isi pesan tersebut. Setelah pesan dibuka maka penerima akan masuk ke *form chat.*
3) Ketika *form chat* dibuka, maka pesan yang ditampilkan pada *form chat* penerima akan langsung didekripsi.
4) *Chipertext* yang secara otomatis telah didekripsi akan berubah menjadi *plaintext* atau teks biasa.
5) *Plaintext* ditampilkan pada *form chat* penerima yang isinya adalah pesan asli yang dikirim oleh pengirim.

3.5. FlowchartProses Enkripsi Algoritma AES 128 *bit*

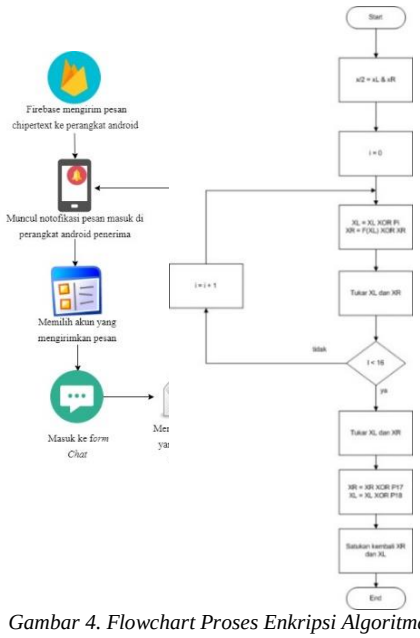
Flowchart ini menjelaskan apa saja yang terjadi pada proses enkripsi menggunakan algoritma AES 128 *bit.* Seperti yang dijelaskan pada gambar berikut :



Gambar 3. Flowchart Proses Enkripsi Algoritma AES 128 bit

3.6. Flowchart Proses Enkripsi Algoritma Blowfish

Flowchart ini menjelaskan apa saja yang terjadi pada proses enkripsi menggunakan algoritma Blowfish.Blowfish sendiri menggunakan kunci simetris dimana kunci untuk enkripsi dan dekripsi sama [5].Seperti yang dijelaskan pada gambar berikut :



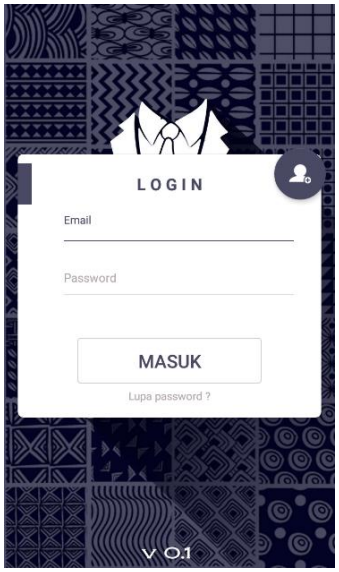
Gambar 4. Flowchart Proses Enkripsi Algoritma Blowfish

4. HASIL DAN PEMBAHASAN

4.1 Tampilan Layar

a. Tampilan Layar *Login*

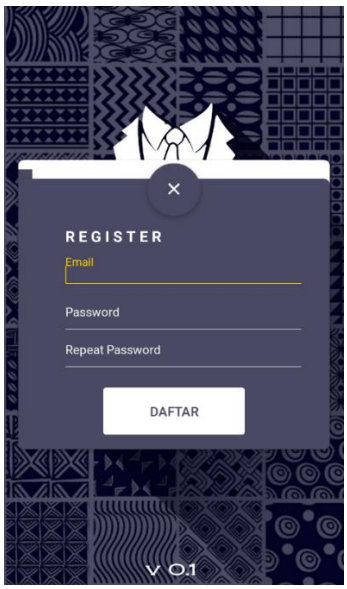
Tampilan layar *formlogin* merupakan layar yang akan tampil pertama kali ketika aplikasi dijalankan yang menjadi penghubung ke *form main*. *User* dapat mengisi *field email* dan *password* akun yang telah dibuat sebelumnya. Akun aplikasi ini tersimpan pada *Firebase Console*. Berikut adalah gambar tampilan layar *form login*.



Gambar 5. Tampilan Layar Login

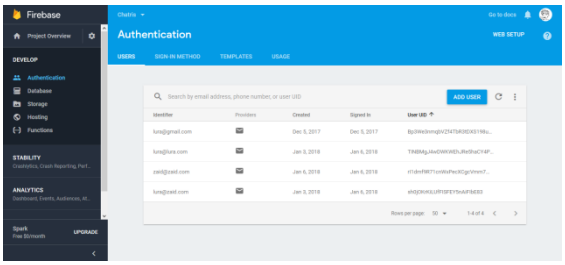
b. Tampilan Layar *Register*

Tampilan layar *form Register* merupakan tampilan layar, jika *user* belum memiliki akun aplikasi ini, maka *user* dapat memilih tombol *register* yang terdapat pada *form login* ini berikut tampilan layar *register*



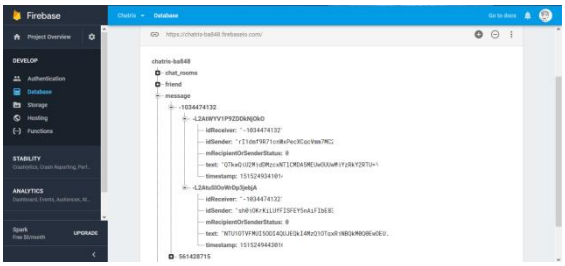
Gambar 6. Tampilan Layar Register

Bagian tampilan layar akan dijelaskan mengenai langkah-langkah penggunaan aplikasi dari tahap awal hingga akhir. Berikut adalah tampilan layar serta langkah-langkah penggunaan aplikasi kriptografi *chatting*



Gambar 7. Tampilan Akun Yang Terdaftar

Pesan yang dikirimkan secara otomatis akan disimpan kedalam database firebase console sebagai pesan yang sudah terenkripsi. Untuk lebih jelasnya bisa dilihat pada gambar berikut :



Gambar 8. Tampilan Firebase Console Dikirim dan Terenkripsi

4.1 Pengujian Proses Enkripsi

Pengujian proses enkripsi mengubah *plaintext* menjadi *ciphertext*. *Key* yang digunakan berasal dari kombinasi antara karakter yang telah ditentukan oleh sistem ditambah dengan karakter dari *Room ID User* pengirim dan penerima yang ada pada *Firebase*. Pengujian proses enkripsi aplikasi ini dibagi menjadi dua, yaitu proses enkripsi pesan teks dan proses enkripsi pesan gambar.

Tabel 1 : Pengujian proses enkripsi *teks*

No	*Key*	Ukuran (Byte)	Waktu (ms)
1	Fibbonaci101	15	0.56
2	Fibbonaci101	15	0.54
3	Fibbonaci101	21	1.03
4	Fibbonaci101	20	1.43
5	Fibbonaci101	13	0.98
Rata-rata		16.8	0.9

Tabel 2 : Pengujian proses enkripsi *url* gambar

No	***Key***	**Ukuran (Byte)**	**Waktu (ms)**
1	Fibbonaci101	224	1.94

2	Fibbonaci101	171	1.78
3	Fibbonaci101	184	1.81
Rata-rata		193	1.84

4.2 Pengujian Proses Dekripsi

Pengujian proses dekripsi merupakan pengujian untuk merubah ciphertext menjadi plaintext. Proses dekripsi bersifat otomatis sehingga user tidak perlu melakukan input apapun. Key yang digunakan untuk melakukan dekripsi ini berasal dari kombinasi antara karakter yang telah ditentukan oleh sistem ditambah dengan beberapa karakter dari ID User pengirim dan penerima yang ada pada Firebase Console. Pengujian proses dekripsi aplikasi ini dibagi menjadi dua, yaitu proses enkripsi pesan teks dan proses enkripsi pesan.

Tabel 3 : Pengujian proses dekripsi *teks*

No	*Key*	Ukuran (Byte)	Waktu (ms)
1	Fibbonaci101	44	0.56
2	Fibbonaci101	44	0.56
3	Fibbonaci101	47	0.64
4	Fibbonaci101	47	0.64
5	Fibbonaci101	45	0.59
Rata-rata		16.8	45.4

Tabel 4 : Pengujian proses dekripsi *url* gambar

No	***Key***	**Ukuran (Byte)**	**Waktu (ms)**
1	Fibbonaci101	256	1.75
2	Fibbonaci101	263	1.86
3	Fibbonaci101	247	1.69
Rata-rata		255	1.76

4.3 Kelebihan Program

Berdasarkan hasil uji coba program yang dilakukan dengan beberapa sampel, maka diperlukan adanya evaluasi terhadap program yang telah diuji. Terdapat beberapa kelebihan program dari hasil evaluasi sebagai berikut :

a. Aplikasi chatting ini dapat secara real-time mengirimkan pesan.
b. Aplikasi chatting ini dapat mengirim pesan teks dan gambar.
c. Aplikasi chatting ini secara otomatis mengatur key oleh sistem sehingga pengguna tidak perlu meng-input lagi secara manual.
d. Aplikasi chatting ini dapat mengenkripsi pesan teks dengan waktu rata-rata 0.9m/s dan 1.84m/s untuk dekripsi url gambar.
e. Aplikasi chatting ini dapat mendekripsi pesan teks dengan waktu rata -rata 06m/s dan 1.76m/s untuk dekripsi url gambar.
f. Apabila aplikasi chatting ini dalam keadaan terbuka dan terhubung ke jaringan internet, maka aplikasi akan memberikan notifikasi pesan.
g. Aplikasi kriptografi chatting dapat berjalan dengan baik selama ada koneksi internet.
h. Aplikasi ini dapat berjalan dengan baik pada sistem operasi android versi 4.4 ke atas.

4.4 Kekurangan Program

Berdasarkan hasil evaluasi terhadap program yang telah diuji. Terdapat beberapa kekurangan program dari hasil evaluasi sebagai berikut :

a. Aplikasi chatting ini tidak dapat melakukan group chat, broadcast message, voice calll dan video call.
b. Aplikasi chatting ini bergantung kepada jaringan internet, maka saat koneksi ke internet tidak ada aplikasi tidak bisa menerima dan mengirim pesan.

5. KESIMPULAN

Setelah melewati beberapa tahap percobaan terhadap program, maka dapat disimpulkan bahwa :

5.1 Kesimpulan

a. Aplikasi chatting ini dapat mengirim pesan yang dapat digunakan oleh pengguna, khususnya pada Notaris untuk berkomunikasi dengan client secara tidak langsung dengan pengamanan pesan menggunakan teknik kriptografi AES-128 bit dan Blowfish dan di simpan melalui firebase yang dikembangkan oleh google.
b. Pengamanan pesan pada aplikasi chatting menggunakan metode AES-128 bit dan Blowfish yang sama-sama simetris, jadi kunci yang digunakan pada proses enkripsi sama dengan yang digunakan pada proses dekripsi dan pesan juga disimpan pada firebase yang berada di cloud.
c. Tingkat keberhasilan pengiriman dan proses enkripsi pesan mencapai 100% dengan menggunakan 8 kali proses pengiriman pesan yang terkoneksi dengan jaringan internet.
d. URL gambar yang telah dienkripsi merupakan benar bahwa dari url gambar

sebelumnya, sehingga jika akan dilakukan proses dekripsi, maka akan kembali seperti url gambar sumber semula.

5.2 Saran

Dalam penelitian ini masih terdapat banyak kekurangan dan jauh dari kata sempurna, oleh karena itu diperlukan perbaikan dan pengembangan agar aplikasi ini dapat menjadi lebih baik lagi. Berikut merupakan beberapa saran untuk pengembangan aplikasi ini pada penelitian selanjutnya :

a. Aplikasi diharapkan dapat lebih ditingkatkan lagi sehingga tidak hanya dapat mengenkripsi dan deskripsi pesan teks dan url gambar saja, namun juga dapatmengenkripsi dan deskripsi file, audio, dan video.
b. Aplikasi diharapkan dapat menyediakan fitur voice call dan video call yang akan menunjang komunikasi bagi pengguna aplikasi chatting ini

6. DAFTAR PUSTAKA

[1] M Dr. Prena, Sachdeva Abhishek, 2013. A Study of Encryption Algorithms AES, DES and RSA for Security. Global Journal of Computer Science and Technology Network, Web & Security, Volume 13 Issue 15

[2] S Indra, Suhery Drs. Cucu, B Yulrio 2017. Pengembangan Aplikasi Chat Messenger Dengan Metode Advanced Encryption Standard (Aes) Pada Smartphone. Jurnal Coding Sistem Komputer Untan, Volume 05, No. 2.

[3] Latif Agustan, 2015. Implementasi Kriptografi Menggunakan Metode Advanced Encryption Standar (Aes) Untuk Pengamanan Data Teks. Jurnal Ilmiah Mustek Anim Ha Vol. 4 No. 2.

[4] Wirdoyo Siswo, Imanullah Zaldi,F Rian 2016. Enkripsi Dan Dekripsi File Dengan Algoritma Blowfish Pada Perangkat Mobile Berbasis Android. Jurnal Teknik Elektro SETRUM Vol: 5, No. 1

[5] Prafanto, Anton, 2016. Penerapan Algoritma Blowfish Untuk Keamanan SMS Pada Android, Jurnal Teknik Informatika Stmik Antar Bangsa, VOL. III NO. 1.