IMPLEMENTASI ALGORITMA HASH SHA-1 DISERTAI TEKNIK KRIPTOGRAFI METODE AFFINE CIPHER DAN AES-256 PADA APLIKASI CHATTING BERBASIS ANDROID

Deditian Nurhadid[1], Noni Juliasari[2]
[1,2)]Teknik Informatika,Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
E-mail :[1]1411503509@student.budiluhur.ac.id, [2]nonijuliasari@budiluhur.ac.id

ABSTRAK

Chatting dahulu bermula dari SMS (Short Message Service) yang merupakan salah satu tipe Instant Messaging (IM) yang memungkinkan pengguna untuk bertukar pesan singkat, walaupun user sedang melakukan sambungan data atau suara. Pada studi kasus penelitian di Laboratorium ICT, kebutuhan akan aplikasi chatting adalah untuk menunjang fasilitas pendukung jalannya perkuliahan. Salah satu untuk kebutuhan dosen menginformasikan kelas pengganti, pemberian tugas atau pengiriman naskah UAS/UTS. Pengembangan aplikasi chatting pada penelitian ini akan ditujukan salah satunya untuk permasalahan tersebut. Dengan menerapkan Kriptografi Affine Cipher sebagai enkripsi dan dekripsi pesan dan AES-256 sebagai enkripsi dan dekripsi file yang berupa format .pdf 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 tetapi pada fasilitas enkripsi file bisa dipakai atau tidak enkripsinya, sedangkan proses penerimaan pesan akan melalui proses dekripsi sebelum pesan dimunculkan kepada penerima. Pengujian dilakukan dengan mengirim 8(delapan) pengiriman pesan dengan menggunakan 2(dua) akun yang berbeda, satu dosen dan satu mahasiswa (supervisor) yang terkoneksi dengan internet yang stabil melalui tahap enkripsi dekripsi pesan dan file. Berdasarkan hasil pengujian, pesan dan file dapat terbaca dengan baik oleh penerima dengan tingkat keberhasilan pengiriman pesan dan file 100%. Diharapkan aplikasi yang diimplementasikan ini dapat lebih mempermudah proses perkuliahan di Laboratorum ICT.

Kata kunci : AES-256, Affine Cipher, Chatting, Ekripsi, Dekripsi

1. PENDAHULUAN

Melalui aplikasi *chatting*, manusia bisa berbagi informasi kepada teman, sahabat, maupun keluarga. Begitu juga di Universitas Budi Luhur, terutama di Laboratorium ICT Terpadu di kalangan dosen dan mahasiswa yang menjabat sebagai *supervisor*. Aplikasi chatting sudah menjadi hal yang biasa digunakan untuk berbagi informasi, namun ketika dosen me-*request* jam mata kuliah harus menggunakan 2(dua) opsi untuk *input* kelas pengganti yaitu melalui *web* atau bisa langsung mendatangi Laboratorium ICT Terpadu untuk mengisi dan menunggu persejutuan kelas pengganti oleh mahasiswa yang menjabat sebagai *supervisor*. Maka dari itu, kami ingin membuat suatu aplikasi chatting berbasis android yang tidak hanya sekedar untuk *chatting*, namun sebagai media komunikasi antara dosen yang ingin melakukan *request* kelas pengganti dengan mahasiswa *supervisor* dengan mudah oleh aplikasi *chatting* ini, yang akan langsung disejutui atau tidak oleh mahasiswa *supervisor*. Disetujui karena tidak ada jadwal yang sama pada waktu pelaksanaan atau tidak disejutujui dikarnakan jadwal yang sama. Pesan *chatting* tersebut harus aman dari pencurian. Salah satu teknik menjaga keamanan informasi yaitu dengan metode kriptografi. Pada aplikasi *chatting* berbasis *android* ini, penulis menggunakan media penyimpanan dengan konsep *real-time* yaitu menggunakan Firebase.

Tidak hanya kriptografi Affine Cipher saja yang dipakai pada aplikasi ini namun terdapat kriptografi AES untuk enkripsi file dokumen dengan format ekstensi .pdf dikarenakan kebutuhan akan adanya kirim file sangat membantu ketika ada momentum yang penting dari dosen untuk mahasiswanya seperti, diberikan tugas, UTS dan UAS ketika dosen ada halangan untuk tidak masuk atau sedikit keterlambatan masuk ke kelas.

2. STUDI LITERATUR

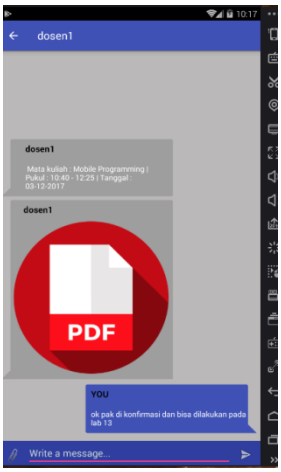
Implementasikan algoritma Affine Cipher bisa mengubah pesan berupa teks yang dapat mengamankan informasi secara aman[1**]**. Maka dari pada itu penerapan metode affine kriptografi untuk membuat aplikasi kriptosistem dalam suatu teks rahasia dapat dibutuhkan agar setiap pesan yang kita miliki tidak dapat dibaca oleh pembajak[2].

Mempelajari langkah pada modifikasi AffineCipher yang diperkuat dengan *Vigenere cipher* untuk meningkatkan keamanan pesan atau informasi dan mengetahui syarat yang harus dimiliki oleh penerima pesan (*receiver*) yang akan melakukan deskripsi[3]. Informasi digital yang bersifat pribadi tentunya, memiliki kerahasiaan data yang harus tetap dijaga. Solusi pengamanan informasi yang digunakan adalah salah satu teknik pengamanan data menggunakan kriptografi yang digabungkan dengan (Rivest Code 4) RC4 [4]. Hal volume (*terabyte* ke *petabyte*) suatu bagian yang menjadi lebih kompleks didunia digital, kondisi (terstruktur dan tidak terstruktur), dan kecepatan (3G ke 4G). Begitu juga dengan data. Semakin lama data akan semakin banyak dan makin sulit untuk memprosesnya. Big data menjadi solusinya. Era baru dari big data yaitu *NoSQLDatabase*(*Not Only SQL*)[5]. Pengambilan data, tidak memiliki hak akses dan penyadapan adalah dampak dari tindakan negatif Agar data tersebut aman maka dibuatlah Aplikasi Pengamanan Data dengan teknik kriptografi AES (Advanced Encryption Standard) serta fungsi Hash SHA-1 [6]. Kriptografi mempunyai tiga unsur penting yaitu pembangkitan kunci, enkripsi dan deskipsi. Dalam kriptografi dikenal algoritma *blockcipher* yang didalamnya terdapat AES (Anvanced Encyption Standard) merupakan bagian dari *Modern Symmetric Key Cipher*, algoritma ini menggunakan kunci yang sama pada saat proses enkripsi dan deskripsi sehingga data yang kita miliki akan sulit dimengerti maknanya[7].

3. HASIL DAN PEMBAHASAN

3.1. Tampilan Chatting Mahasiswa

Pada tampilan ini diberikan fasilitas berupa input pesan, upload gambar dari kamera serta mengupload file dari penyimpanan internal. Tampilan bisa dilihat pada Gambar 1:



Gambar1 : Tampilan Chatting Mahasiswa

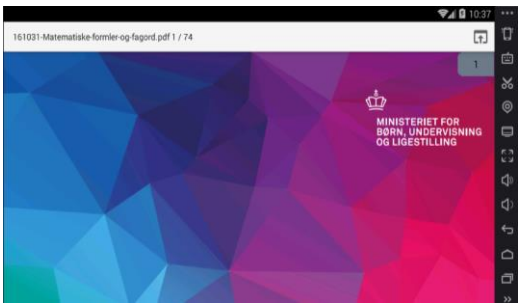
3.2. Tampilan Chatting Dosen

Pada tampilan ini diberikan fasilitas berupa input pesan, upload gambar dari kamera, mengupload file dari penyimpanan internal dan menginput pesan kelas pengganti kepada mahasiswa. Tampilan bisa dilihat pada Gambar 2 :

Gambar 2 : Tampilan Chatting Dosen

3.3. Perbandingan Dokumen

Pada bagian ini akan membuktikan apakah aplikasi *chatting* bisa mengenkripsi atau tidak, kami akan membandingkan file yang sudah terenkripsi dan yang belum terenkripsi. Pertama, *file* asli (contoh menggunakan 161031-*Matematiske-formler-og-fagord.pdf*) yang akan dienkripsi terlihat pada Gambar 3 :

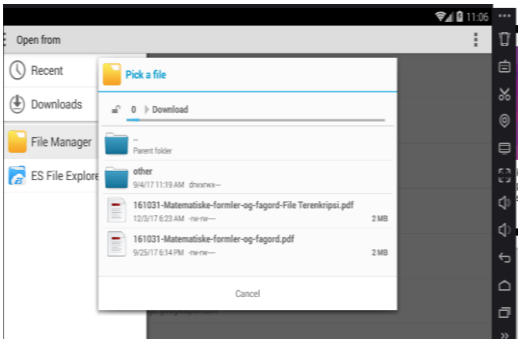


Gambar3 : File Asli

Apabila *file* tersebut sudah terenkripsi akan tetap bisa dibuka namun isinya tidak dapat terbaca oleh aplikasi dan nama *file* yang dienkripsi tidak bisa dibaca. Hasil enkripsi file tersebut dapat dilihat pada Gambar 4 :

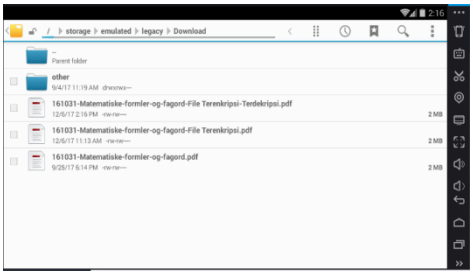
Gambar 4 : File Terenkripsi Terbuka

Bukti sudah dilakukan enkripsi file yang mengubah isi dan menambahkan kata "Terenkripsi" *pada* bagian akhir dokumen.Lokasi file yang terenkrip sama lokasi dengan file yang aslinya. *File* beserta nama *file* bisa dilihat pada Gambar 5 :



Gambar 5 : File Lokasi Terenkripsi

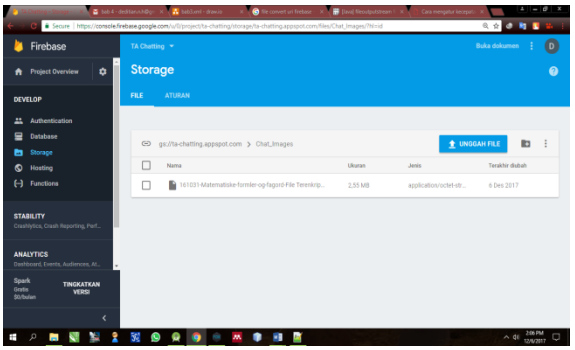
File yang sudah dikirim dan diambil melalui firebase ketika ingin membuka *file* yang di firebase harus melalui tahap dekripsi di aplikasi ini sehingga file yang ingin dibuka bisa terbaca di aplikasi *open pdf*. Tampilan bisa dilihat pada Gambar 6 :



Gambar 6 : File Terdekripsi

3.4. Tampilan Penyimpanan File Di Firebase

File yang telah terenkripsi dan sebelumnya sudah tersimpan di internal *storage* pada android kemudian dikirim ke penyimpanan *cloud* yaitu *firebase*. Berikut tampilan penyimpanan file di *firebase* pada Gambar 7 :



Gambar 7 : Penyimpanan File Di Firebase

3.5. Tabel Pengujian

Dalam tabel pengujian ini akan dibahas tentang hasil pengujian dari aplikasi *chatting* mulai dari proses waktu proses enkrip pesan, waktu proses deskripsi pesan dan kecepatan internet. Hasil pengujian dapat terlihat dalam tabel 1 :

Tabel 1 : Tabel Pengujian Enkripsi Teks

No	Pesan	Hasil enkripsi	Waktu (detik)	Keterangan
1	universitas budi luhur	1nU6A\'"U,-'h21<Uhd1P1\"	0.51	Berhasil
2	Budi	21<U	0.19	Berhasil
3	Universitas	1nU6A\'"U,-'	0.21	Berhasil
4	Luhur	d1P1\"	0.19	Berhasil
5	fakultas teknologi informasi	F-_1d,-'h,A_nsdsKUhUnFs\"i-'U	0.30	Berhasil

Dari 5 kali percobaan pengiriman pesan, 5 pesan itu masuk dengan menggunakan 2 akun yang berbeda dengan melalui tahap enkripsi dan deskripsi pesan dengan demikian dapat disimpulkan pesan dapat terkirim dengan tingkat keberhasilan 100 % dan tidak adanya kerusakan pada pesan setelah dilakukannya enkrip dan dekrip.

Berikut ini adalah table pengujian file. Penentuan kunci tidak dilakukan oleh *user* namun sudah ditentukan terlebih dahulu didalam aplikasi sehingga *user* hanya bisa mengirim file tanpa harus kesulitan untuk mengingat kunci tersebut.

Tabel 2 : Tabel Pengujian File

No	Nama *File*	Nama File Enkripsi	Ukuran File Asli (MB)	Ukuran file Enkripsi (MB)	Waktu (detik)
1	161031-*Matematiske-formler-og-fagord*.pdf	161031-*Matematiske-formler-og-fagord*- File Terenkripsi.pdf	2	2	13
2	autocad2017winpreviewguide.pdf	autocad2017winpreviewguide-File Terenkripsi.pdf	4	4	20

3	java_tutorial.pdf	java_tutorial-File Terenkripsi.pdf	4	4	22
4	modul-belajar-desain-web-site-2.pdf	modul-belajar-desain-web-site-2-File Terenkripsi.pdf	1	1	7
5	Otomatisasi_Perkantoran.pdf	Oromatisasi_Perkantoran- File Terenkripsi.pdf	4	4	22

Dari hasil *table* pengujian *file* bisa dibuktikan bahwa proses enkrip pada *file* yang berekstensi .pdf bisa dijalankan dengan waktu pengolahan yang tergantung dari ukuran *file* itu sendiri. Ukuran *file* asli dengan ukuran *file* yang telah dienkripsi tidak merubah ukuran maka penelitian yang dilakukan tersebut dapat menjadi pertimbangan karya ilmiah.

3.6. Evaluasi Program

Berdasarkan dari tabel pengujian diatas, maka dibuatlah evaluasi program dengan maksud untuk menganalisa hasil yang telah dicapai oleh program yang dikembangkan. Aplikasi *chatting* ini tentu memiliki kelebihan dan kekurangan yang diukur berdasarkan kebutuhan pengguna dalam bermacam kondisi dan situasi. Adapun kelebihan dan kekurangan aplikasi *chatting* ini adalah sebagai berikut :

a. Kelebihan Aplikasi *Chatting*

1. Aplikasi berbasis android yang mudah digunakan dan juga dapat diakses kapanpun dan dimanapun.
2. Tampilan aplikasi sederhana namun memiliki ciri khas dari Universitas Budi Luhur.
3. Proses validasi melalui email @student.budiluhur.ac.id dan @budiluhur.ac.id yang dimiliki oleh setiap mahasiswa dan dosen.
4. Aplikasi *chatting* ini dilengkapi dengan algoritma *affine cipher* untuk proses enkripsi dan deskripsi pesan.
5. Dosen bisa melakukan *request* penjadwalan perkuliahan yang dilakukan di Laboratorium ICT Terpadu melalui aplikasi *mobile.*
6. Terdapat enkripsi dan dekripsi pesan *file* yang berguna untuk mengirim tugas atau soal-soal latihan untuk mahasiswa.

b. Kekurangan Aplikasi *Chatting*

1. Aplikasi *chatting* ini hanya dibatasi untuk meng-enkripsi teks dan *file* yang berekstensi .pdf.
2. Pada saat enkripsi dan dekripsi pesan file terdapat layar hitam yang terjadi karena proses tersebut yang mengakibatkan user mempunyai prasangka bahwa aplikasi tersebut rusak.
3. Proses login dan registrasi yang terbilang cukup lama dikarenakan menggunakan proses akses data melalui internet.
4. Waktu yang dibutuhkan untuk enkripsi dan dekripsi file tergantung dari ukuran file semakin besar ukuran file maka akan semakin lama prosesnya.

4. KESIMPULAN

Berdasarkan dari uraian yang terdapat pada bab sebelumnya terhadap masalah yang dihadapi, maka dapat ditarik kesimpulan, antara lain:

a. Aplikasi ini dapat mengirim pesan obrolan yang dapat digunakan oleh pengguna, khususnya pada Laboratorium ICT Terpadudi Universitas Budi Luhur untuk memberikan informasi kepada para mahasiswa(*supervisor*) melalui dosen kelas pengganti secara tidak langsung dengan pengamanan pesan menggunakan teknik kriptografi affine cipher yang di simpan melalui firebase yang dikembangkan oleh google.
b. Pengamanan pesan pada aplikasi *chatting* menggunakan metode affine cipher yang memiliki 2 kunci yang yang telah ditentukan dan pesan juga disimpan pada firebase yang berada di *cloud*.
c. Pada aplikasi *chatting* ini dosen dapat membuat pesan kelas pengganti yang disebut dengan (KP) yang berguna untuk memberi tahu *supervisor* bahwa ada permintaan kelas pengganti.
d. Metode sha-1 diterapkan di aplikasi *chatting* pada saat mahasiswa dan dosen melakukan registrasi. Pada proses enkripsi metode affine cipher menggunakan rumus utama yaitu, C = aP + b (mod n) dengan a dan b sebagai kunci dengan nilainya yang telah ditentukan yang juga dimodifikasi sesuai dengan kebutuhan aplikasi *chatting* yang di buat.
e. Tingkat keberhasilan pengiriman dan proses enkripsi pesan mencapai 100% dengan menggunakan 10 kali proses pengiriman pesan yang terkoneksi dengan jaringan internet.
f. Isi *file* yang telah dienkripsi merupakan benar bahwa isi

file dari *file* sumber, sehingga jika akan dilakukan proses dekripsi, maka akan kembali seperti *file* sumber semula.

5. DAFTAR PUSTAKA

[1] Wibowo, S., Nilawati, E., & Suharnawi. 2014. Implementasi Enkripsi Dekripsi Algoritma Affine Cipher Berbasis Android. *Techno.COM* 13(4): p.215–221.

[2] Septiarini, A.,& Hamdani. 2011. Sistem Kriptografi Untuk Text Message Menggunakan Metode Affine. FMIPA Universitas Mulawarman

[3] 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.

[4] Agung, H., & Budiman. 2015. Implementasi Affine Chiper Dan RC4 Pada Enkripsi File Tunggal. In Prosiding SNATIF ke-2 Tahun 2015, 243–250.

[5] Hossain, S.A., & Moniruzzaman, A. 2013. 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.

[6] Prasetyo, Ratno. 2016. Teknik Algoritma Kriptografi AES dan Fungsi Hash SHA-1 Berbasis Desktop.Universitas Budi Luhur

[7] Ibrahim, A. A. (2017) 'Perancangan Pengamanan Data Menggunakan Algoritma AES (Advanced Encyption Standard)', III(1), pp. 53–60.