JOURNAL OF INFORMATICS AND COMPUTING (RANDOM)
Vol. 2, No. 1 (Tahun 2023), Hal. 39 - 47

IMPLEMENTASI ENKRIPSI UNTUK KEAMANAN SMS MENGGUNAKAN METODE CIPHER FEEDBACK (CFB) 8-BIT BERBASIS ANDROID

Siska Ayu Widiana[1,*], Iqbal Firdaus[2]

[1]Universitas Sam Ratulangi
[2]Sekolah Tinggi Ilmu Ekonomi Indonesia Banjarmasin
*Email: siskaginting@unsrat.ac.id

INFORMASI ARTIKEL

Diajukan:
25 April 2023
Direvisi:
13 Mei 2023
Diterima:
31 Mei 2023

Kata kunci:

SMS
Enkripsi
Dekripsi
CFB-8bit
Aplikasi Android

Abstrak

Celah keamanan terbesar pada layanan komunikasi SMS adalah pada saat SMS tersebut sedang dikirim melalui jaringan SMS tersebut. SMS bekerja pada jaringan nirkabel yang memungkinkan terjadinya pencurian isi pesan SMS ketika dalam proses transmisi dari pengirim ke penerima. Kasus ini disebut SMS interception. Tujuan dari penelitian ini adalah untuk mengurangi faktor-faktor yang mengancam keamanan isi pesan dengan menggunakan aplikasi enkripsi SMS dengan menggunakan mode cipher feedback 8-bit pada aplikasi android. Faktor pertama, yaitu faktor fisik adalah jika telepon selular dipegang oleh orang lain maka orang tersebut dapat membaca dan mendapatkan informasi dari pesan di dalam telepon selular. Faktor kedua adalah keamanan pesan di dalam sistem, penyebabnya karena operator selular hanya mengenkripsi pesan pada saat proses transmisi, sedangkan dalam proses penyimpanan pesan di operator selular berbentuk plainteks. Tahapan proses pada mode cipher feedback 8-bit dimulai dengan menginput SMS yang akan dikirimkan, yaitu berupa plainteks dan ditambah dengan menginput initialization vector (IV) dan kunci yang di proses melalui fungsi enkripsi menggunakan algoritma AES 128 untuk menghasilkan keystream. 8 bit awal hasil dari keystream ini lalu di exclusive or (XOR) kan dengan 8 bit awal plainteks dan hasil yang didapat akan dikembalikan lagi ke blok paling kiri dari IV awal dengan proses register geser, dan begitu pun selanjutnya sampai dihasilkan sebuah pesan yang berbentuk cipherteks yang berbentuk deretan heksadesimal. Hasil cipherteks tersebut lah yang akan dikirimkan kepada penerima pesan melalui server sehingga pesan asli yang ditujukan kepada penerima dapat dijaga kerahasiaannya. Sesuai dengan hasil diatas maka dapat disimpulkan bahwa isi pesan yang dikirimkan tidak akan bisa dibaca kecuali oleh pengirim dan penerima saja.

ENCRYPTION IMPLEMENTATION FOR SMS SECURITY USING THE ANDROID-BASED 8-BIT CIPHER FEEDBACK (CFB) METHOD

ARTICLE INFORMATION

Submitted:
25 April 2023
Received:
13 May 2023
Accepted:
31 May 2023

Abtract

The biggest security gap in the SMS communication service is when the SMS is being sent through the SMS network. SMS works on a wireless network which allows the theft of the contents of SMS messages when they are in the process of transmission from sender to recipient. This case is called SMS interception. The purpose of this research is to reduce the factors of SMS security by using SMS

p-ISSN 2986-1942
e-ISSN 2986-1187

Keywords:

SMS
Encryption
Decryption
CFB-8bits
Android Application

encryption application using cipher feedback 8-bits mode on android device. The first factor, which is the physical factor, is if the mobile phone is held by another person who are not the owner of the phone. That person can read and get information from the message on that mobile phone. The second factor is the safety messages in the system, this is all because the provider of mobile phones is only encrypting the messages during the transmission process, while in the storage process in the provider of mobile phones, the messages is saved as plaintext. The step of the process on cipher feedback 8-bits mode is started from filling the SMS with plaintext and initialization vector (IV) and key. Then the encryption function will process them to produce the keystream. The early 8 bits of keystream will be exclusive-or-ed (XORed) by the early 8 bits of plaintext and the result will be sent back to left most block from early IV with shift register process, and these processes will be repeated until resulting a chipertext message filled by rows of hexadecimal. The ciphertext as a result from the system will be sent to the receiver through the server, so the real message which is addressed to the receiver will be safe. Based on the result above, it can be concluded that the message would not be read except by the sender and the receiver.

PENDAHULUAN

Telepon seluler saat ini telah menjadi salah satu kebutuhan penting manusia karena dengan telepon seluler dapat mempermudah komunikasi langsung jarak jauh antar manusia. Seiring perkembangannya, maka diikuti pula dengan perkembangan layanan komunikasi yang biasanya digunakan antara lain telepon, video call, SMS, MMS, chatting, internet, dan beberapa social media lainnya [1]. Di antara layanan komunikasi tersebut, layanan SMS yang menjadi layanan komunikasi yang masih banyak digunakan hingga saat ini karena seluruh telepon seluler menggunakan layanan komunikasi SMS. Terbukti menurut catatan ATSI (Asosiasi Telekomunikasi Seluruh Indonesia) di akhir tahun 2011 terdapat 260 miliyar SMS yang dikirim di seluruh Indonesia [2].

Kelebihan dari layanan SMS adalah ketika nomor tujuan pesan sedang tidak aktif, pesan tetap dapat di kirimkan dengan menyimpan pesan tersebut pada SMSC (Short Message Service Center) dan akan mengirimkan ketika tujuan sudah tidak sibuk ataupun aktif kembali. Namun, kelebihan ini juga menjadikan kelemahan pada SMS, dengan tersimpannya pesan pada SMSC, maka penyerang dapat mendapatkan pesan dengan melakukan penyusupan pada SMSC tersebut. Beberapa risiko juga merupakan ancaman bagi keamanan SMS yaitu SMS spoofing, SMS snooping, dan SMS interception [3].

SMS spoofing adalah pengiriman SMS dimana nomor pengirim yang tertera bukanlah nomer pengirim yang sebenarnya. Mekanisme SMS spoofing ini dimungkinkan karena lemahnya proteksi koneksi SMSC (SMS Center) – gateway [4]. Penyusup dapat merekam login dan password dari pesan yang berasal dari SMS gateway menuju SMSC. Dalam hal ini penyusup mengatur sebuah gateway palsu yang berlaku seperti gateway sesungguhnya. Gateway palsu ini dapat mengirim semua jenis pesan pendek kepada pengguna melalui SMSC [5]. Pada teknik spoofing ini pesan dikirim dengan memanipulasi nomor MSISDN (Mobile Subscriber Integrated Services Digital Network Number) asal pada field yang disediakan sehingga pesan akan tampak datang dari nomor pengirim lainnya. Kemungkinan spoofing yang lain adalah dengan membuat simulator SMSC yang berlaku seperti SMSC asli [6]. Dengan cara ini gateway akan kebanjiran pesan, sebagai contoh aplikasi bank menggunakan gateway dapat dengan mudah diperoleh informasi account bahkan dapat digunakan untuk transaksi bank tanpa proses authorisasi.

Ancaman SMS lainnya adalah SMS snooping. SMS snooping lebih sering terjadi karena kelalaian pengguna telepon seluler. Contohnya ketika seseorang meminjamkan telepon selulernya pada orang lain untuk menggunakan telepon selulernya. Pada saat itu orang tersebut dapat dengan sengaja atau tidak

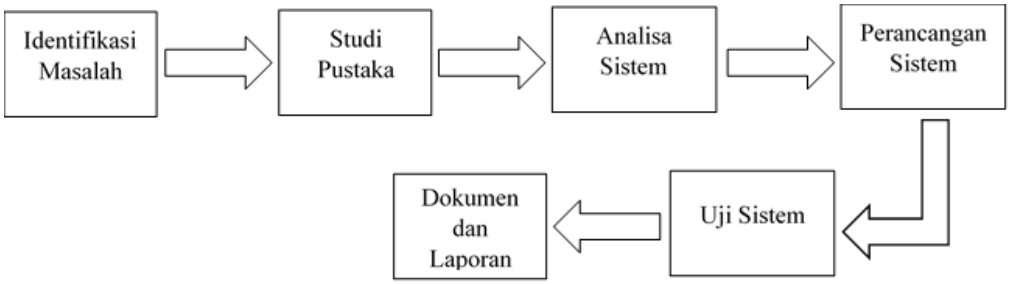
membuka isi pesan yang ada pada inbox SMS. Pesan yang bersifat personal atau rahasia dapat dibaca dengan mudah oleh orang lain melalui cara ini [7].

Celah keamanan terbesar pada layanan komunikasi SMS adalah pada saat SMS tersebut sedang dikirim melalui jaringan SMS tersebut. SMS bekerja pada jaringan nirkabel yang memungkinkan terjadinya pencurian isi pesan SMS ketika dalam proses transmisi dari pengirim ke penerima. Kasus ini disebut SMS interception [8].

Karena ancaman-ancaman SMS diatas, maka dibutuhkannya sebuah sistem pada layanan SMS yang mampu mengurangi risiko yang ditimbulkan dari kelemahan yang terdapat pada layanan SMS tersebut. Salah satu cara penanggulangannya adalah dengan dilakukannya proses penyandian (enkripsi dan dekripsi) terhadap data yang akan dikirimkan yang diimplementasikan dengan aplikasi yang menggunakan mode Cipher Feedback (CFB) yaitu dengan blok dienkripsi seperti halnya stream cipher pada satuan sesuai dengan mode CFB yang digunakan, sehingga ukuran blok plain teks tidak perlu diperbesar. Enkripsi dilakukan pada saat pengiriman dengan cara mengubah data asli menjadi data rahasia. Jadi data yang dikirimkan selama proses pengiriman adalah data rahasia, sehingga data asli tidak dapat diketahui oleh pihak yang tidak berkepentingan. Metode Cipher Feedback adalah metode yang digunakan dalam sistem keamanan File Dokumen tersebut. Metode Cipher Feedback menggunakan sistem Shift Register, dimana yang diproses terlebih dahulu adalah Initialization Vector dalam algoritma Enkripsi dengan Kunci. Dalimuthe (2019) menggunakan Metode Cipher Feedback pada Kriptografi Modern dapat diimplementasikan pada sebuah sistem informasi. Aspek kerahasiaan pada pengamanan File Dokumen, terletak pada penyandian pesan yaitu password [9]. Satyanegara (2011) mengaplikasikan algoritma kriptografi dalam sistem keamanan layanan SMS banking [10]. Oleh karena itu digunakan metode Cipher Feedback sebagai metode enkripsi keamanan SMS menggunakan Android sebagai media platformnya.

METODE PENELITIAN

Metode yang digunakan dalam pengumpulan data adalah sebagai berikut:

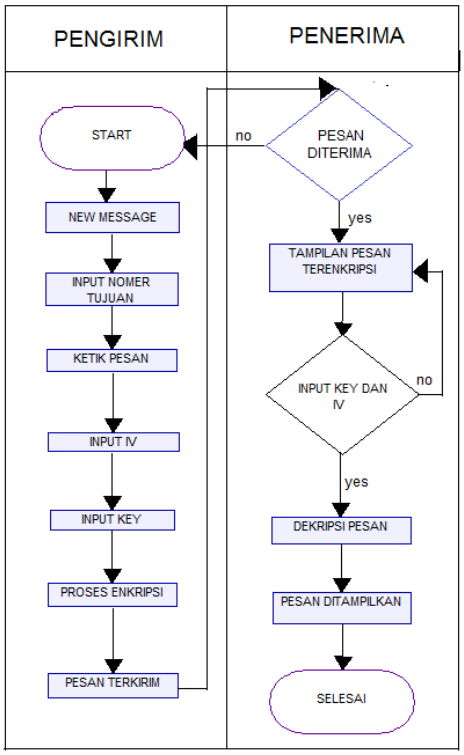


Gambar 1. Tahapan Penelitian

1. Identifikasi Masalah
   Identifikasi masalah merupakan tahap awal yang dilakukan oleh penulis untuk melakukan penelitian, di mana penulis mencari permasalahan terkait dengan sistem keamanan pada SMS di platform android dengan enkripsi menggunakan algoritma CFB 8-bit.
2. Studi Pustaka
   Setelah melakukakan identifikasi masalah maka tahap selanjutnya adalah studi pustaka dimana penulis mencari jurnal – jurnal dan buku yang berkaitan dengan penelitian untuk melengkapi pengetahuan dasar yang dimiliki peneliti, sehingga peneliti dapat menyelesaikan penelitian ini.
3. Analisa Sistem
   Pada tahap ini, semua informasi dan data untuk kebutuhan sistem diseleksi. Setelah itu barulah penulis melakukan analisa terhadap data yang digunakan, proses-proses yang terjadi dalam kegiatan penyeleksian, melakukan perhitungan serta menganalisa kebutuhan data yang digunakan serta dokumentasi yang dihasilkan dari tahap ini.
4. Perancangan Sistem
   Pada tahap perancangan sistem di uraikan proses perancangan sistem yang akan dibuat meliputi perancangan penulisan pesan teks, kotak masuk, pengiriman pesan dan laporan informasi yang akan di hasilkan oleh sistem, serta rancangan tampilan untuk pengguna sistem.
5. Uji Sistem

Pada tahap ini dilakukan pembutan aplikasi enkripsi menggunakan algoritma CFB untuk mengenkripsi isi SMS dalam transmisi pengiriman pada android. Setelah itu dilakukan proses pengujian aplikasi agar output / luaran dapat didekripsi sesuai dengan desain yang dibuat.

6. Dokumen dan Laporan
   Tahap akhir yang dilakukan penulis adalah melakukan dokumentasi dan membuat laporan penelitian.



Gambar 2. Activity Diagram Pada Proses Enkripsi Dan Dekripsi

Pada activity diagram proses enkripsi dan dekripsi pengiriman sampai penerimaan pesan adalah dimulai oleh aktor pengirim dengan tahap pertama adalah mulai program, lalu pilih menu new message. Aktor penerima memulai input nomor tujuan, pesan, kunci dan inizialization vector. Setelah semua input terpenuhi maka dimulai proses enkripsi dan selanjutnya mengirim pesan. Selanjutnya aktor penerima menerima pesan, jika tidak menerima maka aktor pengirim memulai aktifitasnya dari awal, jika aktor menerima maka sistem akan menampilkan pesan yang terenkripsi. Untuk membaca pesan tersebut maka aktor pengirim menginput kunci dan initialization vector. Jika inputan salah maka aktor pengirim harus menginput kembali kunci dan initialization vector. Jika input benar maka pesan hasil dekripsi akan ditampilkan.

HASIL DAN PEMBAHASAN

Dari hasil pengamatan, didapatkan sebuah permasalahan yang dihadapi oleh pengguna SMS yaitu keamanan isi pesan yang disebabkan oleh beberapa faktor yaitu faktor fisik dan faktor sistem. Faktor pertama, yaitu faktor fisik adalah jika telepon selular dipegang oleh orang lain, maka orang tersebut dapat membaca dan mendapatkan informasi dari pesan di dalam telepon selular. Faktor kedua adalah keamanan pesan di dalam sistem, contoh yang sering terjadi adalah pada kasus korupsi ataupun yang berkaitan dengan hukum dimana isi pesan dalam telepon selular tersangka kasus tersebut dapat dibaca dan digunakan oleh lembaga hukum sebagai bukti. Seperti yang telah dijelaskan pada bab dua, penyebabnya karena operator selular hanya mengenkripsi pesan pada saat proses transmisi, sedangkan dalam proses penyimpanan pesan di operator selular berbentuk plainteks sehingga pesan dapat dilihat oleh admin maupun orang-orang yang terlibat dalam sistem penyimpanan pesan di operator selular tersebut, ada kemungkinan jika pesan tetap terbuka maka informasinya digunakan oleh orang yang tak berhak. Dari masalah-masalah yang diuraikan diatas, maka disimpulkan bahwa dibutuhkan sebuah sistem yang dibangun berdasarkan sistem keamanan yang menjadi standar keamanan internasional untuk mengamankan suatu informasi dalam SMS.

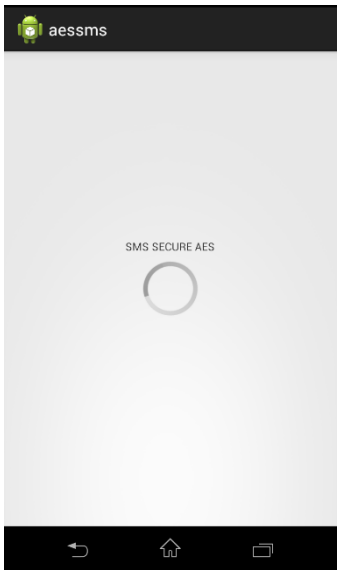
Perancangan sistem enkripsi sms serta proses awal sistem yang terdiri dari enkripsi dan dekripsi pada SMS agar pengoperasian suatu pesan dapat terjaga kerahasiaan, kutuhan, dan keasliannya. Proses enkripsi dan dekripsi tersebut dilakukan dengan menggunakan aplikasi sms berbasis android. Aplikasi sms ini tentunya telah terhubung dengan aplikasi SMS di telepon seluarnya. Proses enkripsi dimulai pada saat user mengirim pesan, dimana sebelumnya telah dimasukan kunci untuk mengenkrisi pada saat proses penulisan pesan yang kemudian hasil pesan terenkripsi tersebut dikirimkan melalui server provider, seperti pengiriman SMS biasa. Data yang telah diterima server dalam bentuk chiperteks, kemudian akan di dekripsi di dalam telepon selular yang dituju dan dlakukan oleh penerima pesan.

Tahap implementasi merupakan tahap dimana sistem siap untuk dioperasikan. implementasi itu sendiri dilakukan berdasarkan analisis dan perancangan yang telah dibuat. Tujuan dari tahap implementasi ini adalah untuk mengkonfirmasi modul-modul dari sistem yang dirancang sehingga pengguna dapat memberi masukan dalam pengembangan sistem. Seluruh program yang digunakan pada aplikasi "enkripsi SMS berbasis android dengan menggunakan mode CFB 8-bit" menggunakan bahasa pemrograman java berbasis android.

Pada penelitian kali ini akan dicoba mengimplementasikan algoritma cipher block, yaitu CFB 8-bit dengan menggunakan fungsi enkripsi dan dekripsi algoritma AES 128-bit. Alasan penggunaan kedua algoritma ini adalah terletak pada kekuatan sandi yang dihasilkan. Kekuatan sandi CFB 8-bit terletak pada initialization vector yang digunakan serta adanya antrian yang telah diproses yang akan di umpan balik untuk proses selanjutnya. Selain itu dengan mode CFB ini menghasilkan sebuah kunci internal yang berubah-ubah dan berkelanjutan untuk proses selanjutnya sehingga cipherteks yang dihasilkan akan lebih beragam dan kompleks.

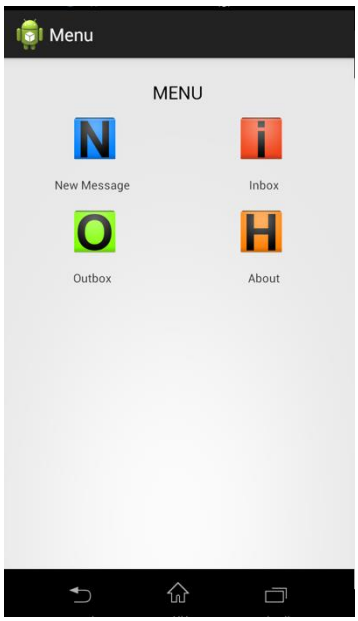
Aplikasi untuk mendekripsi pesan SMS yang sudah terenkripsi dibuat menggunakan bahasa pemograman java. Aplikasi akan diimplementasikan menggunakan smartphone berbasis android dan menggunakan server provider selular sebelum pesan yang dikirimkan sampai ke nomor yang dituju. Berikut ini akan dijabarkan cara kerja aplikasi saat enkripsi.

1. Tampilan Awal
   Tampilan ini adalah sebagai halaman awal untuk masuk ke menu utama otomatis setelah spinner berputar selama 3 detik.



Gambar 3. Tampilan Awal

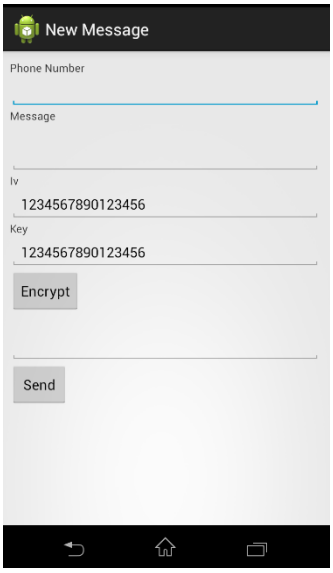
2. Menu Utama
   Menu utama menampilakan menu berupa New Message, Inbox, Outbox, dan About. Di dalam menu utama ini tidak ada tombol exit, untuk keluar aplikasi memakai tombol back yang ada dalam android.



Gambar 4. Menu Utama

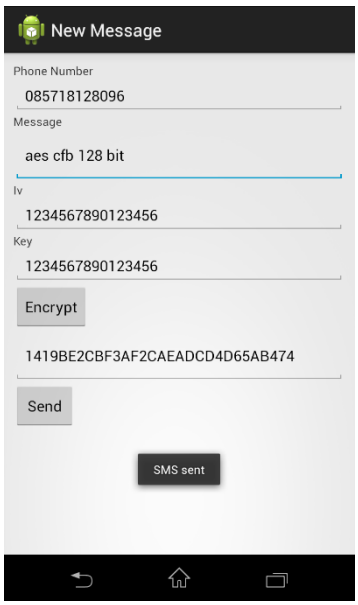
3. Halaman New Message

Halaman ini digunakan user untuk membuat pesan. Dalam halaman ini terdapat kolom phone mumber, kolom message, kolom key, kolom IV, kolom encryption, tombol encrypt dan tombol send, dimana pada saat menekan tombol encrypt, isi pesan akan otomatis terenkripsi dan ditampilkan pada kolom encryption, setelah itu akan terkirim ke nomor tujuan jika menekan tombol send. Pada halaman enkripsi ini user diminta untuk menginput kunci dan initialization vector untuk mengenkripsi teks menjadi ciphertext. Kunci dan IV yang diinput harus sama dengan kunci yang dipakai buat proses dekripsi nantinya.



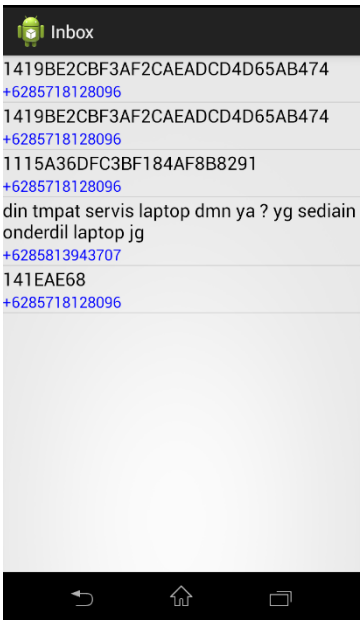
Gambar 5. Tampilan New Message

Jika IV tidak sesuai atau tidak berjumlag 16 bytes, maka message box yang tampil adalah tulisan “IV must be 16 bytes long”. Sedangan jika key yang diinput tidak berjumlah 16 bytes atau lebih maka akan akan keluar message box dengan teks :”Key length not 128”. Sehingga jika terjadi kesalahan pada input IV atau Key yang tidak sesuai atau tidak 16 bytes maka program tidak bias mengenkripsi pesan. Jika pesan memenuhi syarat maka pesan dapat di enkrip dan dapat di kirim. Saat di tekan button send, maka akan muncul notifikasi “SMS sent” jika pesan telah terkirim.



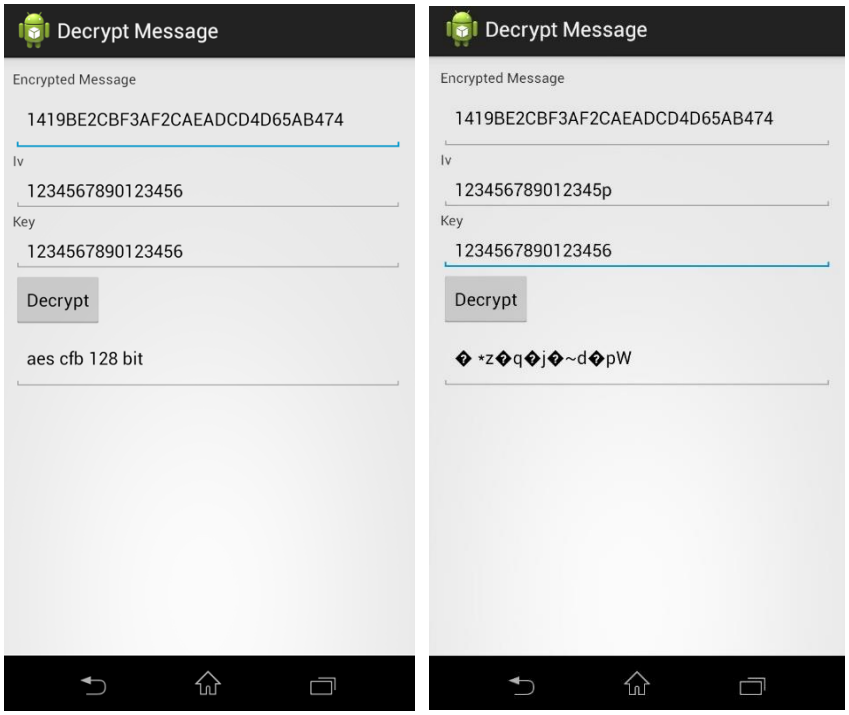
Gambar 6. Notifikasi Saat Pesan Terkirim

4. Halaman Inbox
   Halaman Inbox adalah halaman dimana pengguna dapat melihat SMS masuk. Di halaman ini pula SMS yang akan di dekrip hanya tinggal dipilih saja, maka akan masuk ke tampilan dekripsi selanjutnya.



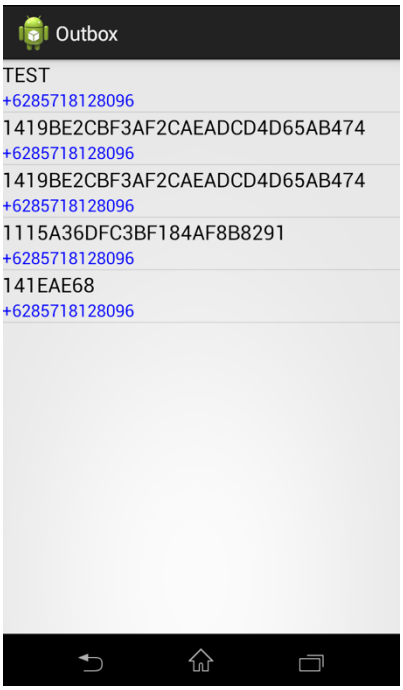
Gambar 7. Notifikasi Saat Pesan Terkirim

5. Halaman Decryption Message
   Halaman digunakan untuk memproses SMS yang berbentuk cipherteks untuk diubah menjadi plainteks, dengan menginput IV dan key yang sama dengan IV dan key yang digunakan untuk mengirim pesan tersebut.



Gambar 8. Tampilan Decryption Message dan Hasil dekripsi Jika Key atau IV Berbeda Dengan Key atau IV Saat Pesan Dikirim

6. Halaman Outbox
   Halaman Outbox adalah halaman dimana pengguna dapat melihat SMS masuk yang sudah terenkripsi menggunakan metode CFB 8-bit.



Gambar 9. Tampilan Outbox

KESIMPULAN

1. Dengan adanya program aplikasi Android ini membuat pengiriman SMS yang dikirimkan menjadi lebih aman dikarenakan pada aplikasi ini menggunakan metode enkripsi yaitu CFB 8-bit.
2. Secara umum, algoritma block-cipher pada mode CFB 8- bit dapat diimplementasikan dan berhasil berjalan dengan baik pada perangkat Android. Melalui pengujian ditunjukkan bahwa aplikasi dapat berjalan dengan baik pada berbagai jenis perangkat Android.

3. File yang mampu dijalankan oleh program aplikasi ini secara optimal enkripsi maupun kompresinya file tersebut harus bertipe Text ataupun data, dikarenakan teknik kompresi pada aplikasi ini kurang begitu optimal untuk file bertipe gambar, audio maupun video.

DAFTAR PUSTAKA

[1] S. Subhan, S. Amini, P. F. Ariyani, and R. Chiper, "Implementasi Pengamanan Data Enkripsi SMS Dengan Algoritma RC4 Berbasis Android," 2017.
[2] A. P. Sari, I. M. Seno, and W. Gunawan, "Aplikasi Enkripsi dan Dekripsi untuk Keamanan Komunikasi Data pada SMS (Short Message Service) Berbasis Android Menggunakan Algoritma Blowfish," *Format J. Ilm. Tek. Inform.*, vol. 8, no. 1, p. 34, Aug. 2019, doi: 10.22441/format.2019.v8.i1/005.
[3] A. Hidayat, K. A. Ashari, D. Setiana, and R. Rosyadi, "Perbandingan Penggunaan Memory Dan CPU Menggunakan Kriptograpi AES," vol. 6, no. 2, 2018.
[4] R. Yusuf and M. R. Suheri, "Pengamanan Sms Pada Telepon Seluler Berbasis Android Menggunakan Algoritma," *PETIR*, vol. 9, no. 1, pp. 63–70, Jan. 2019, doi: 10.33322/petir.v9i1.191.
[5] N. Gulo, "Pengamanan Short Message Service (SMS) Menggunakan Algoritma Vibranium Cipher," vol. 1, no. 5, 2021.
[6] D. D. Mavianto and A. Fadillah, "Aplikasi Enkripsi Dan Kompresi File Pada Blackberry Dengan Menggunakan Mode Cfb 8-Bit Dan 3DES," 2017.
[7] W. Fahriah and T. Febrianto, "Aplikasi Enkripsi dan Dekripsi Short Message Service di Android Menggunakan Metode Blowfish," *JISAJurnal Inform. Dan Sains*, vol. 2, no. 1, Jun. 2019, doi: 10.31326/jisa.v2i1.512.
[8] A. G. Pratama, "Implementasi Aplikasi Enkripsi Short Message Service (SMS) Berbasis Android," vol. 1, no. 1, 2015.
[9] M. F. Dalimuthe, "Perancangan Aplikasi Pengamanan File Dokumen Teks Dengan Menggunakan Algoritma Cipher Feedback," vol. 04, 2019.
[10] B. Satyanegara, "Penerapan Kriptografi dalam Sistem Keamanan SMS Banking".