Jurnal Informatika dan Rekayasa Perangkat Lunak ISSN 2656-2855
Vol. 5, No. 1, Maret 2023, Hal. 13-20 e-ISSN 2685-5518

Implementasi Algoritma Advance Encryption Standard dan Caesar Cipher pada Pesan Terenkripsi

Aditiya Hermawan[1*], **Anton Halim**[2], **Dera Susilawati**[3], **Intan Anjali Putri**[4]
[1,2,3,4] Jurusan TEKNIK INFORMATIKA , Fakultas SAINS DAN TEKNOLOGI, Universitas Buddhi Dharma
[*]Email: aditiya.hermawan@ubd.ac.id

Abstrak

Perkembangan teknologi informasi membuat banyak orang dapat melakukan komunikasi setiap saat dengan berbagai media, salah satunya adalah pertukaran pesan. Namun banyak tidak disadari adanya celah keamanan yang digunakan oleh pihak yang tidak bertanggung jawab untuk melakukan kejahatan seperti kejahatan pencurian pesan, penyadapan pesan, dan perubahan isi pesan. Salah satu teknik untuk mengamankan pesan adalah dengan kriptografi. Kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain. Beberapa metode kriptografi yang dapat digunakan adalah Advanced Encryption Standard dan Caesar Cipher, karena metode Advanced Encryption Standard memiliki keamanan yang tinggi terhadap keamanan pesan sedangkan metode Caesar Cipher mempunyai kelebihan cepat dalam perhitungan. Gabungan dua algoritma tersebut dalam membuat pesan rahasia di implementasikan dalam bentuk aplikasi berbasis mobile untuk memudahkan penguna membuat pesan rahasia. Hasil pesan enkripsi yang terbentuk sulit untuk dilakukan dekripsi karena melalui 2 tahap proses enkripsi sehingga isi pesan penting dapat dijamin kerahasiaanya.

***Kata kunci**: AES, Caesar Cipher, Kriptografi, Pesan Terenkripsi*

Abtract

The development of information technology allows many people to communicate at any time with various media, one of which is the exchange of messages. However, many people do not realize that there are security holes that are used by irresponsible parties to commit crimes such as theft of messages, intercepting messages, and changing the contents of messages. One technique for securing messages is cryptography. Cryptography is the science and art of keeping messages secure when messages are sent from one place to another. Several cryptographic methods that can be used are Advanced Encryption Standard and Caesar Cipher, because the Advanced Encryption Standard method has high security for message security while the Caesar Cipher method has the advantage of being fast in calculations. The combination of these two algorithms in making secret messages is implemented in the form of a mobile-based application to make it easier for users to make secret messages. The results of the encrypted messages formed are difficult to decrypt because they go through 2 stages of the encryption process so that the contents of important messages can be guaranteed confidentiality.

***Key Word** : AES, Caesar Cipher, Cryptography, Encrypted Messaging*

PENDAHULUAN

Penggunaan smartphone untuk berkomunikasi sudah menjadi kebiasaan sehari-hari. Baik itu komunikasi melalu pesan suara ataupun pesan text. Pengiriman pesan melalui smartphone tersebut mempunyai celah keamanan yang bisa saja dimanfaatkan pihak yang tidak bertanggung jawab melakukan kejatan dengan menyadap pesan dan juga melakukan perubahan isi pesan tersebut untuk tujuan yang tertentu.

Kejahatan penyadapan dapat dimanfaatkan untuk melalukan penipuan melalui penyamaran identitas orang tersebut, kemudian melakukan pencarian informasi lebih lanjut untuk mengumpulkan data-data lainnya yang dapat digunakan untuk penyamaran atau lainnya. Dengan mempunyai data dan informasi dari hasil penyadapan dapat memudahkan untuk

menyakinkan korban bahwa pelaku kejatahan adalah orang dekat sehinga memudahkan melakukan penipuan seperti meminta mengirimkan uang dengan alasan tersentu. Contoh lainnya misalkan saat mengirimkan email yaitu reply, reply adalah pengambilan pesan dan mengembalikannya kepada alamat si pengirim, pelaku menentukan alamat e-mail balasan dari pengirim ke penerima, sehingga ketika penerima ingin membalas pesan, maka pesan tersebut masuk ke e-mail pelaku (Murhada and Giap, 2011). Disamping itu layanan pesan singkat yang terdapat pada Smartphone berupa teks terbuka yang tidak terproteksi dan juga pesan yang dikirim tidak secara langsung karena melewati *Short Message Service Center* (Atmojo, Isnanto and Kridalukmana, 2016).

Untuk mengatasi hal tersebut terdapat beberapa cara diatantarnya dengan mengunakan metode pesan yang terenkripsi agar ketika pesan tersebut disadap tidak menimbulkan hal yang dapat disalahgunakan. Salah satu cara untuk mengamankan pesan dan memastikan pesan tersebut diterima orang yang tepat adalah dengan menggunakan Kriptografi.

Kriptografi merupakan teknik menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain. Kriptografi merupakan teknik alternatif untuk memungkinkan pertukaran pesan yang tidak dapat dibaca oleh yang tidak berhak dengan cara megnubah pesan menjadi pesan sandi (Muharram 2018).Dalam kriptografi terdapat proses enkripsi dan dekripsi. Enrkipsi adalah proses mengubah pesan asli menjadi pesan yang terlingdungi (pesan dengan sandi), sedangkan dekripsi merupakan proses pengembalikan pesan tersandi menjadi pesan asli (Prameshwari and Sastra, 2018).

Terdapat beberapa teknik untuk menyamarkan pesan terdapat banyak cara atau metode, diataranya adalah metode Advanced Encryption Standard (AES) dan Caesar Cipher. Metode AES memiliki keamanan yang tinggi terutama untuk keamanan pesan karena karakter yang diinput menghasilkan output yang berbeda (Fitriani and Utomo, 2020), penambahan metode Caesar Cipher pada AES ialah membuat keamanan pesan menjadi lebih sulit untuk dilakukan dekripsi. Proses algoritma Caesar Cipher yang cepat dalam perhitungan sehingga sesuai jika AES dibuat berlapis dengan Caesar Cipher.

TINJAUAN PUSTAKA

Terdapat beberapa penelitian yang sudah dilakukan menggunakan algoritma AES untuk membuat pesan rahasia. Penelitian yang dilakukan Fredianto dkk (Fredianto, Kusyanti and Amron, 2018) menggunakan Algoritma *Advance Encryption Standard* (AES) untuk enkripsi Short message Service pada Android untuk menganggulangi masalah keamanan pada pengiriman pesan melalui SMS yang mana pesan SMS dapat terbaca dan disimpan pada *Short message service Center* (SMSC). pada penelitian ini dilakukan perbandingan antara AES 128 bit, 192 bit dan 256 bit untuk enkripri pesan. Hasil yang didapatkan adalah waktu proses enkripsi dan dekrip[si berbading lurus dengan panjangnya pesan yang diproses.

Penelitian lain dilakukan oleh Marsiani dkk (Marsiani, Setiadi and Cahyo, 2021) yang menggunakan metode AES 256-bit untuk melakukan pengamanan Data Pribadi. Pada penelitian ini, data peribadi dapat diamankan dengan algoritma AES karena algoritma tersebut melakukan pengamanan dan penyandian yang berlapis.

Penelitian dari Nuareni (Nuraeni, Agustin and Purnama, 2020) menggunakan metode ceasar cipher dan Advance Encryption Standard (AES) untuk pengamaman data Pajak Bumi dan Bangunan yang merupakan data confidential dan berpotensi menimbulkan masalah apabila diakses oleh yang tidak berwenang. Penggunaan Algorima AES yang di kombinasi dengan caesar cipher menghasilkan nilai avalache effect yang lebih baik dibandingkan dengan algortima AES saja.

METODE PENELITIAN

3.1 Metode *Advanced Encryption Standard* (AES)

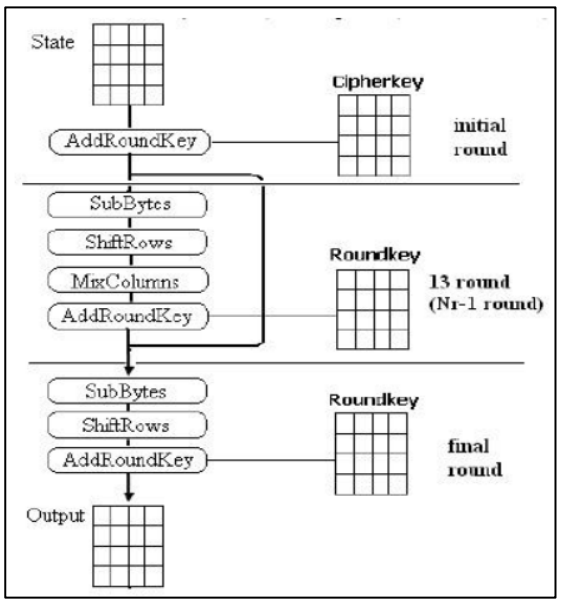
Algoritma AES merupakan algortima kriptografi modern simetris dengan menggunakan ukuran blok khusus dalam proses enkripsi dan dekripsinya. Kunci Kriptografi yang digunakan pada Algoritma AES adalah 128,192, dan 256 bit untuk melakukan proses enkripsi dan dekripsi data pada blok 128bits (Nuraeni, Putra and Hendriyani, 2019). Perbedaan dari ketiga urutan tersebut adalah panjang kunci yang mempengaruhi jumlah round (perputaran) yang dapat ditunjukkan pada Tabel 1 (Prameshwari and Sastra, 2018)

Tabel 1. Urutan data AES

	Panjang kunci	Panjang Blok	Jumlah Putaran
AES-128	4	4	10
AES-129	6	4	12
AES-256	8	4	14

Berdasarkan Tabel 1. AES 128 *bit* menggunakan panjang kunci Nk = 4 *word* (kata) yang setiap katanya terdiri dari 32 *bit* sehingga total kunci 128 *bit*, ukuran blok teks asli 128 *bit* dan memiliki 10 putaran.

Pada Gambar 1 terdapat empat jenis transformasi yang digunakan pada proses enkripsi algoritma AES yaitu *SubBytes*, *ShiftRows*, *Mixcolumns*, dan *AddRoundKey*. Pertama, inputan yang telah di-*copy* ke dalam *state* akan mengalami transformasi *byte AddRoundKey*. Kemudian *state* akan mengalami transformasi *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* secara berulang-ulang sebanyak Nr. *Round* yang terakhir sedikit berbeda dengan sebelumnya dimana pada *round* terakhir, state tidak mengalami transformasi *MixColumns* (Gumelar and Pramusinto, 2018).



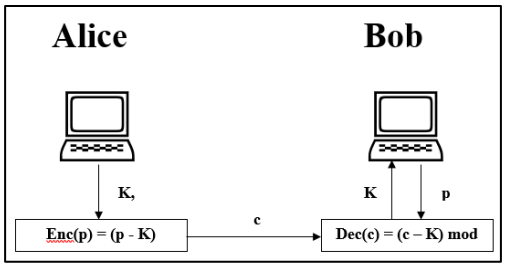
Gambar 1. Proses Algortima AES

3.2 Metode *Caesar Chipher*

Sandi *Caesar Cipher* merupakan sistem persandian klasik berbasis substitusi yang sederhana yaitu enkripsi dan dekripsi pada sistem persandian *Caesar Cipher* menggunakan operasi *shift* seperti yang ditunjukkan pada Gambar 2 (Rifki, 2012).

Operasi shift adalah mensubstitusi huruf menjadi huruf pada daftar alfabet berada di k sebelah kanan atau sebelah kiri huruf itu. Misalnya dipilih k = 3 (ganti dengan huruf ke 3 sebelah kanan) maka "A" menjadi "D", "B menjadi "E" dan seterusnya. Bagaimana dengan "X", "Y" dan "Z". Supaya semuanya memiliki substitusi, huruf "A" dianggap disebelah kanan huruf "Z" sehingga "X" menjadi "A", "Y" menjadi "B" dan "Z" menjadi "C". Untuk dapat mengolah teks asli yang merupakan deretan simbol huruf diperlukan pemetaan dari huruf menjadi angka sehingga dapat diaplikasi operasi matematika. Misalnya huruf "A" sampai "Z" dipetakan ke angka integer dari "0" sampai "25".

Perhatikan nilai yang mungkin bagi teks asli dan teks sandi adalah 0 sampai dengan 25 dan apabila hasil pergeseran (penjumlahan) melebihi angka 26 dan nilai yang dipakai adalah sisa bagi. Oleh karena itu aritmatika\ modular Z_{26} digunakan pada sistem persandian Caesar.



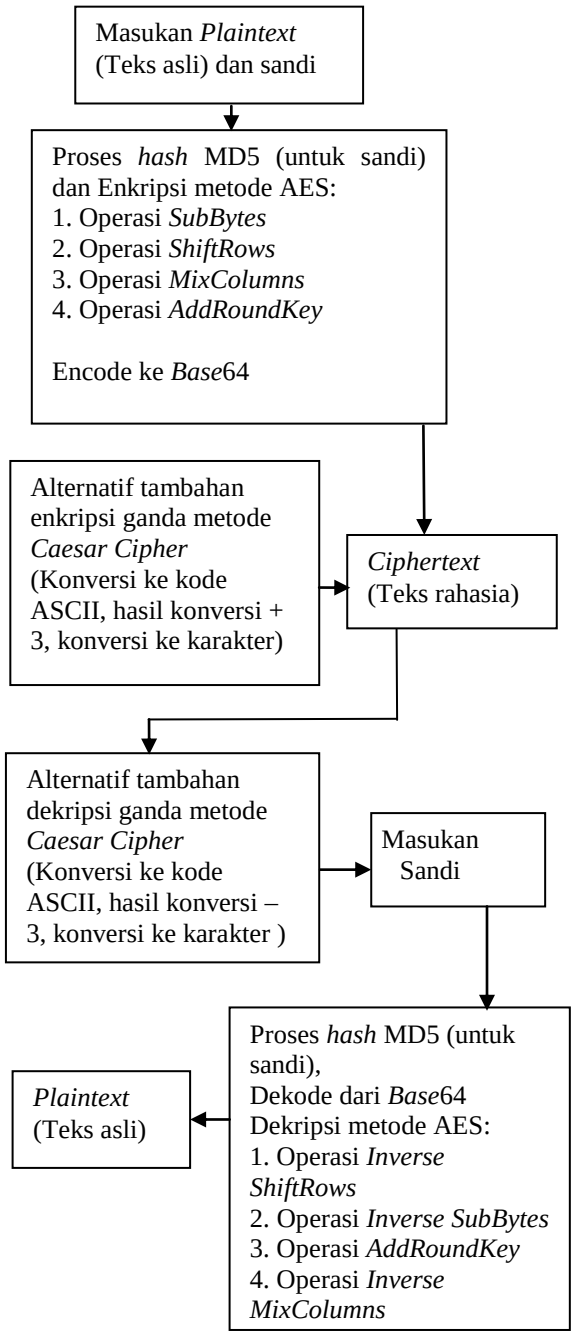
Gambar 2. Proses Enkripsi dan Dekripsi Sandi *Caesar Cipher* (Rifki, 2012)

3.3 Proses Enkripsi dan Dekripsi

Metode *AES (Advanced Encryption Standard)* dan *Caesar Cipher* digabungkan agar membentuk pesan enkripsi yang sulit di lakukan dekripsi oleh orang yang tidak seharusnya menerima pesan tersebut. Proses pengabungan algoritma tersebut ditunjukkan pada Gambar 3.

Pada gambar 3, pesan asli (*Plain Text)* di proses enkripsi dengan sandi tertentu, kemudian di enkripsi dengan algoritma AES dengan beberapa tahap sampai menghasilkan pesan terenkripsi *(Cipher Text)*. Hasil pesan rahasia

output dari metode AES dapat dilakukan enkripsi tambah dengan algoritma *Caesar Cipher* sehingga menjadi Pesan terenrkipsi yang baru. Untuk proses dekripsinya tergantung pada proses enrkipsi, apakah menggunakan enkripsi ganda dengan *Caesar Cipher* atau tidak. Jika menggunakannya maka proses dekrispsi juga melalui proses dekripsi ganda dimulai dari *Caesar* Cipher kemudian masukan sandi untuk di proses pada algortima AES untuk dijadikan Pesan Asli kembali.



Gambar 3. Proses Enkripsi dan Dekripsi

HASIL dan PEMBAHASAN

4.1 Proses Enkripsi

Proses tahapan enkripsi yang dilakukan pada metode AES seperti pada gambar 4. Untuk membuat pesan enkripsi dibutuhkan *plaintext* dan *key* kemudian dilakukan prosesnya seperti berikut :

Plaintext :ANTONHALIM
Key :SEMANGATBELAJAR

Plaintext ANTONHALIM dilakukan konversi dengan tabel ASCII setelah itu dilakukan perubahan menjadi bilangan HEX menjadi 41 4E 54 4F 4E 48 41 4C 49 4D 00 00 00 00 00 00

Plaintext			
A	N	I	
N	H	M	
T	A		
O	L		

⇨

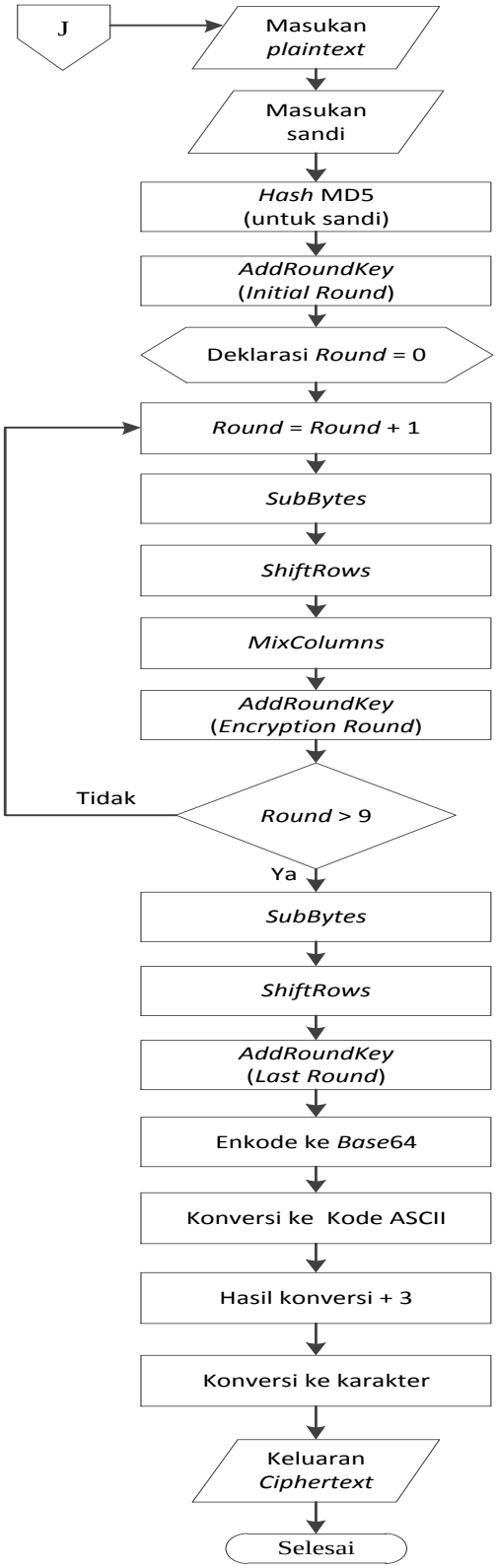
Plaintext			
41	4E	49	00
4E	48	4D	00
54	41	00	00
4F	4C	00	00

Key SEMANGATBELAJAR dilakukan konversi dengan tabel ASCII setelah itu dilakukan perubahan menjadi bilangan HEX menjadi 53 45 4D 41 4E 47 41 54 42 45 4C 41 4A 41 52 00

Key			
S	N	B	J
E	G	E	A
M	A	L	R
A	T	A	

⇨

Key			
53	4E	42	4A
45	47	45	41
4D	41	4C	52
41	54	41	00



Gambar 4. Proses Enkripsi Pesan Rahasia

a. Operasi *AddRoundKey*

Langkah selanjutnya operasi *AddRoundKey* (*Initial Round*) yaitu *plaintext* dan *key* konversi ke biner setelah itu dilakukan XOR. Dalam operasi AddRoundKey (Initial Round) di atas dihasilkan 12 0B 19 0E 00 0F 00 18 0B 08 4C 41 4A 41 52 00.

***AddRoundKey* (*Initial Round*)**			
12	00	0B	4A
0B	0F	08	41
19	00	4C	52
0E	18	41	00

b. Operasi *SubBytes*

Langkah selanjutnya operasi *SubBytes* merupakan suatu operasi substitusi pada setiap *byte* dengan menggunakan tabel S-box.

12	00	0B	4A
0B	0F	08	41
19	00	4C	52
0E	18	41	00

C9	63	2B	D6
2B	76	30	83
D4	63	29	00
AB	AD	83	63

c. Operasi *ShiftRows*

Langkah selanjutnya operasi *ShiftRows* yaitu melakukan rotasi pergeseran dari kiri dengan mengikuti aturan untuk baris pertama tidak terjadi rotasi, baris kedua terjadi rotasi 1 dari kiri, baris ketiga terjadi rotasi 2 dari kiri, baris keempat terjadi rotasi 3 dari kiri.

C9	63	2B	D6
2B	76	30	83
D4	63	29	00
AB	AD	83	63

C9	63	2B	D6
76	30	83	2B
29	00	D4	63
63	AB	AD	83

d. Operasi *MixColumns*

Langkah selanjutnya adalah operasi *MixColumns*, langkah pertama ialah menggunakan kolom pertama dari hasil operasi sebelumnya yaitu operasi *ShiftRows*, setelah itu melakukan perkalian matriks mengikuti aturan *Galois Field* (GF).

59	3D	B1	2A
3D	A8	FC	A6
48	B5	F7	A5
D9	D8	6B	34
D9	D8	6B	34

e. Operasi *AddRoundKey (Encryption Round)*

Langkah berikutnya operasi *AddRoundKey* (*Encryption Round*), langkah pertama ialah mencari *RoundKey*, setelah itu hasil *MixColumns* dan *RoundKey* konversi ke biner lakukan XOR. Dalam operasi AddRoundKey (Encryption Round) di atas dihasilkan 88 78 66 4E A2 AA DA 1B 6C BB D4 E9 BD A0 D4 B6, dan proses Encryption Round berulang sampai 9 putaran dari operasi SubBytes, operasi ShiftRows, operasi MixColumns, operasi AddRoundKey (Encryption Round), kemudian diteruskan ke putaran 10 (Last Round) tanpa operasi MixColumns.

Untuk Last Round pada enkripsi metode AES tidak dilakukan operasi MixColumns dan operasi terakhir enkripsi metode AES adalah operasi AddRoundKey (Last Round), dari contoh perhitungan enkripsi AES di atas dilakukan tanpa hash dan tidak dilakukan encode ke Base64 sehingga menghasilkan 24 53 DA 09 4F 85 B1 3B 85 F8 CA 6E 22 6B 38 A1 (dalam HEX), kemudian dilakukan konversi dengan tabel ASCII sehingga ciphertext menjadi **; à ° ╩ n " k 8 í**.

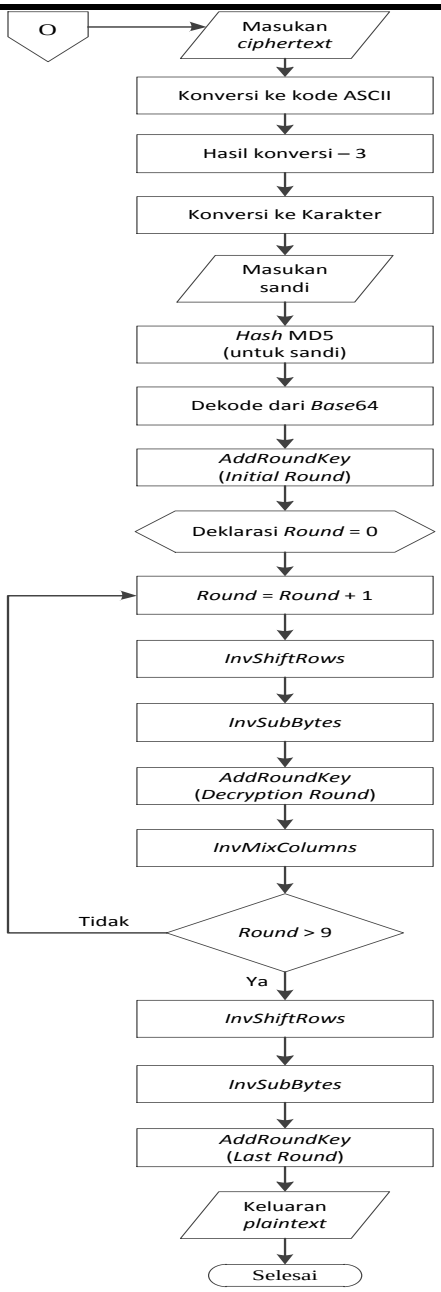
4.2 Enkripsi *Caesar Cipher*

Untuk proses Enkripsi Pada metode *caesar cipher* dilakukan pada hasil chipertext yang berbentuk Hexa pada metode AES sebelumnya, kemudian lakukan langkah sebagai berikut :

a. Konversi text ke dalam kode ASCII
   3B 85 F8 CA 6E 22 6B 38 A1
   ↓
   59 133 248 202 110 34 107 56 161
b. Hasil konversi ditambah dengan Key. (Contoh 3)
   62 136 251 205 113 37 110 59 164
c. Konversi ASCII ke dalam text untuk menghasilkan ciphertext yang baru.
   > ê √ ═ q % n ; ñ

4.3 Proses Dekripsi

Pada proses dekripsi di lakukan dengan proses kebalikan dengan enrkipsi mengikuti langkah pada Gambar 5 sehingga *chippertext* menjadi *plaintext* kembali.



Gambar 5. Proses Dekripsi Pesan Rahasia

4.4 Aplikasi Pesan Rahasia

Untuk memudahkan melakukan konversi pesan ke dalam pesan rahasia menggunakan Algoritma AES dan *caesar cipher*, maka di bangun aplikasi berbasis mobile agar dapat melakukan proses pembuatan pesan rahasia dalam komunikasi sehari-hari pada aplikasi pepesanan maka di buat aplikasi pesan rahasia berikut yang memungkinkan untuk melakuan enkripsi dan dekripsi pada pesan yang akan di kirim.

Gambar 6. Tampilan aplikasi untuk Enkripsi

Gambar 7. Tampilan aplikasi unutk proses Dekripsi

4.5 Pembahasan

Aplikasi pesan rahasia dapat membantu untuk memudahkan melakukan enkripsi pada pesan yang akan dikirim, sehingga mengurangi terjadinya kejahatan yang ditimbulkan akibat penyadapan pesan karena pesan yang di enkripsi menggunkan metode AES dan *caesar cipher* sulit untuk di baca dan di dekripsi tanpa mengetahui Kunci (*key)* dari pesan tersebut. Pesan yang dikirim hanya dapat baca oleh penerima yang mempunyai kunci untuk dimasukan kedalam aplikasi pesan rahasia tersebut.

Beberapa hal yang perlu ditambahakan dalam pesan rahasia adalah integrasi aplikasi tersebut ke dalam aplikasi perpesanan secara otomatis sehinggai tidak perlu lagi melakukan perubahan pesan melalui aplikasi yang berbeda sehingga terkesan merepotkan dalam pengunaannya sehari-hari.

Pembuatan aplikasi yang berbasis *mobile* dengan sistem operasi android pun menjadi batasan aplikasi tersebut, karena tidak dapat digunakan oleh masyarakat luas dalam hal ini adalah pengguna *moblie phone* yang bukan android.

SIMPULAN

Penerapan Algortima AES dan Caesar Chiper pada aplikasi mobile berbasis android dapat membantu masyarakat dalam membuat dan mengirimkan pesan rahasia yang sulit dilakukan dekripsi tanpa mempunya kunci dari pesan rahasia tersebut. kedua algoritma yang digabungan ini menghasilkan pesan rahasia yang sangat berbeda dari pesan aslinya dan sulit terbaca sehingga dapat mengurangi dampak dari penyadapan pesan yang sering terjadi ketika melakukan komunikasi melalui pesan teks. Algortima AES juga dapat dicoba ditambahkan dengan algortima Blowfish untuk membuat pesan rahasia, dan dibandingkan tingat kesulitannya dengan AES dan Caesar Chiper.

DAFTAR PUSTAKA

Atmojo, W.P., Isnanto, R.R. and Kridalukmana, R. (2016) 'Implementasi Aplikasi Kriptografi Pada Layanan Pesan Singkat (SMS) Menggunakan Algoritma RC6 Berbasis Android', *Jurnal Teknologi dan Sistem Komputer*, 4(3), p. 450.

Fitriani, I. and Utomo, A.B. (2020) 'Implementasi Algoritma Advanced Encryption Standard (AES) pada Layanan SMS Desa', *JISKA (Jurnal Informatika Sunan Kalijaga)*, 5(3), pp. 153–163.

Fredianto;, Kusyanti, A. and Amron, K. (2018) 'Analisis Perbandingan Algoritma Advanced Encryption Standard Untuk Enkripsi Short Message Service (SMS) Pada Android', *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 2(10), pp. 4281–4289.

Gumelar, D.B. and Pramusinto, W. (2018) 'Implementasi Algoritma Kriptografi dengan Algoritma Caesar Cipher, Advanced Encryption Standard 256, Dan Rc6 untuk Aplikasi Chatting Berbasis Android', *SKANIKA*, 1(2), pp. 711–717.

Marsiani, E.S., Setiadi, I. and Cahyo, A. (2021) 'Implementasi Sistem Keamanan AES 256-Bit GCM Guna Mengamankan Data Pribadi', *Jurnal Rekayasa Komputasi Terapan*, 1(2), pp. 108–114.

Murhada and Giap, Y.C. (2011) *Pengantar*

Teknologi Informasi, *Mitra Wacana Media, Tangerang*.

Nuraeni, F., Agustin, Y.H. and Purnama, A.E. (2020) 'Implementasi Caesar Cipher & Advanced Encryption Standar (Aes) Pada Pengamanan Data Pajak Bumi Bangunan', *Jurnal Ilmiah Matrik*, 22(2), pp. 187–194.

Nuraeni, F., Putra, P.Y. and Hendriyani, I. (2019) 'Implementasi Kriptografi Superenkripsi Vigenere Cipher Dan Advanced Encrytion Standard (Aes) Pada Pengamanan Data Riwayat Pasien Rumah Sakit', in *Seminar Nasional Sisterm Informasi dan Teknik Informatika*, pp. 309–316.

Prameshwari, A. and Sastra, N.P. (2018) 'Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen', *Eksplora Informatika*, 8(2), p. 52.

Rifki, S. (2012) *Kriptografi Untuk Keamanan Jaringan dan Implementasi dalam Bahasa Java, CV Andi Offset, Yogyakarta*.