ISSN: 2614-6754 (print)
ISSN: 2614-3097(online)

Halaman 471-476
Volume 7 Nomor 1 Tahun 2023

Algoritma Affine Chiper pada Enkripsi dan Deskripsi untuk Keamanan Informasi Berbasis Android

Adinda Fitri[1], Cindy Sintya[2], Frihartini Ayu Salsabilah[3], Ali Ikhwan[4]

[1,2,3,4] Prodi SistemInformasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sumatera Utara

Email: adindafitri427@gmail.com[1], cindysintya2402@gmail.com[2], frihartiayus@gmail.com[3], ali_ikhwan@uinsu.ac.id[4]

Abstrak

Di era globalisasi ini perkembangan teknologi komunikasi dapat berkembang dengan pesat sehingga dapat memudahkan kita dalam mengirim dan menerima sebuah informasi melalui pesan pada teks. Namun kita juga harus waspada terhadap kejahatan pada kebocoran informasi terutama bagi sebuah perusahaan. Untuk itu perlu adanya usaha dalam mengamankan pesan informasi yang akan dikomunikasikan. Salah satu cara untuk mengamankan data atau informasi dari tindak kejahatan tersebut adalah dengan kriptografi Penelitian ini bertujuan untuk membuat algoritma guna membuat rancangan aplikasi cyssage berbasis android dalam proses Algoritma Affine Chiper pada Enkripsi dan Deskripsi Untuk Keamanan Informasi Berbasis Android.

Kata Kunci : Keamanan Data, Deskripsi, Enkripsi, Algoritma Affine Chiper

Abstract

In this era of globalization, the development of communication technology can develop rapidly so that it can make it easier for us to send and receive information via text messages. But we also have to be aware of the crime of leaking information, especially for a company. For this reason, efforts are needed to secure the information message that will be communicated. One way to secure data or information from these crimes is with cryptography. This study aims to create an algorithm to design an Android-based cyssage application in the Affine Chiper Algorithm process on Encryption and Description for Android-Based Information Security.

Keywords : Data Security, Description, Encryption, Affine Cipher Algorithm

PENDAHULUAN

Di era teknologi sekarang ini memudahkan kita dalam mengirim dan menerima sebuah informasi melalui pesan pada teks, dengan adanya ini membuat kita juga waspada terhadap kejahatan pada kebocoran informasi terutama bagi sebuah perusahaan. Untuk itu perlu adanya usaha dalam mengamankan pesan informasi yang akan dikomunikasikan[1].

Informasi yang bersifat rahasia menjadi permasalahan yang muncul bagi suatu perusahaan yang mempunyai dokumen rahasia juga data penting perusahaan. Sehingga perlu adanya keamanan untuk menjaga dokumen ataupun data tersebut agar terhindar dari gangguan orang lain. Salah satu cara untuk mengamankan data atau informasi dari tindak kejahatan tersebut dengan kriptografi[2].

Jika suatu data rahasiamudah bocor bahkandiketahui oleh pihak yang tidak berkepentingan, tentu saja menimbulkan dampak yang sangat merugikan bagi pihak yang memiliki data tersebut. Sebagai upaya mewujudkan implementasi keamanan data dengan menggunakan metode enkripsi Affine Cipher kedalam suatu aplikasi yang mudah digunakan. Aplikasi ini ditujukan untuk membantu mengatasi masalah keamanan data yang dibuat atau disimpan. Affine cipher ialah harusasan dari algoritma caesar cipher yang dihasilkan dengan

memperbanyak plainteks dengan sebuaha ngka m yang relatif prima dengan ponten perpindahan b, setelah itu hasilnya dijumlahkan dengan nilai pergeseran b[3]. Menurut Nurjamiyah , algoritma affine cipher dapat digunakan untuk menyembunyikan pesan rahasia kedalam teks dengan efektif[4]. Dengan menggunakan kriptografi klasik adalah salah satu metode penyandian pesan affine cipher.Algoritma kriptografi yang berbasis karakter dimana enkripsi dan dekripsi dilakukan pada setiap karakter pesan yang dinamakan dengan kriptografi klasik [5].

Supaya melindungi keamanan pesan yang bertabiat rahasia, ada teknik yang bisa dipakai, dengan menggunakan kriptografi yang mempunyai kegunaan menyembunyikan pesan selaku struktur pesan tersandi memanfaatkan metode Affine cipher, karena efisien dan efektif untuk mengamankan data, informasi, maupun dokumen-dokumen penting sehingga tidak dapat disalahgunakan oleh pihak yang tidak bertanggung jawab

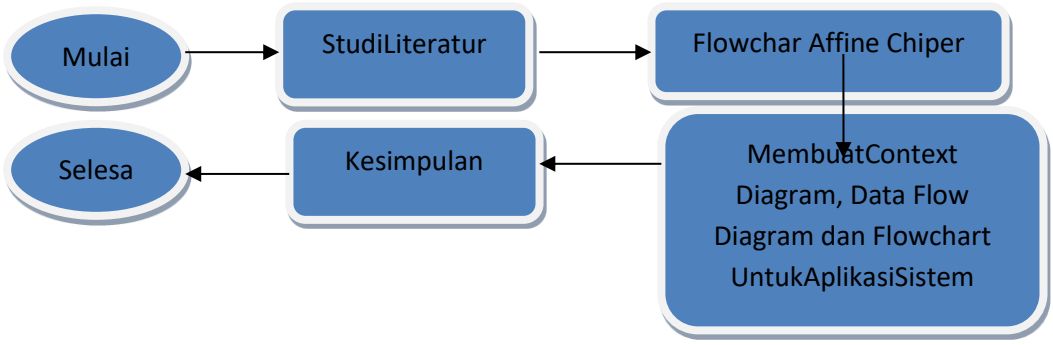
Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasian data, keabsahan data, integritas data, sertaautentikasi data[6].Adapun MenurutKatz, kriptografiialahrisetobjektif alias metodegunamengamankan data digital, negosiasi, sertakomputasi yang terdistribusi.[7].

Plaintext merupakan sebuah pesan yang akan diubah menjadi bentuk rahasia sedangkan Ciphertext merupakan pesan yang telah diubah menjadi bentuk rahasia. Enkripsi Metode untuk mengubah plaintext pesan menjadi ciphertext dengan mengubah huruf-hurufnya plainteks menggunakan transformasi dan Dekripsi adalah Proses dari kebalikan untuk mengubah ciphertext kembali keplainteks oleh penerima yang dimaksud[8].Dalam tindakkan pergantian plaintext jadi ciphertext diketahui enkripsi dan pergantian kembali dari ciphertext jadi plaintext yaitu dekripsi [9].

Metode affine yaitu teknik dari cara Caesar Cipher, yang melipatkan plainteks (P) serupa poin (a) serta jua memperbanyaknya dengan serupa pergerakan (k). P menciptakan cipherteks C diklaim atas manfaat kongruen: C=((a x P) +k) mod 26……(1) yang mana26 yaitu jumlah alphabet, persetujuan 1 dibubuhkan pada sistem enkripsi. cara dekripsi memerlukan persetujuan P=a-1(Ci-k) mod 26….(2) a merupakan potong melingkar yang relatif prima dengan 26. Melalui tutur lain great common divisior gcd(a,26) harus serupa dengan 1[10].

METODOE

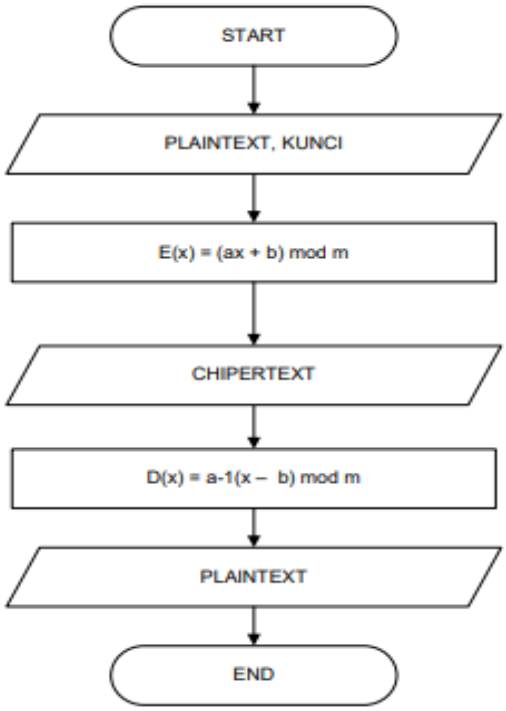
Penelitian ini disusun menggunakan studi literature berdasarkan pengumpulan bahan-bahan referensi seperti jurnal penelitian sebelumnya, buku, artikel dari websait dan juga data-data yang terkait dengan penelitian ini mengenai algoritma affine chiper, deskripsi, enkripsi, serta teknik deskripsi dan enkripsi pada affine chiper. Adapun alur dari tahapan penelitian ini yaitu sebagai berikut :



Gambar 1. Tahapan Alur Penelitian

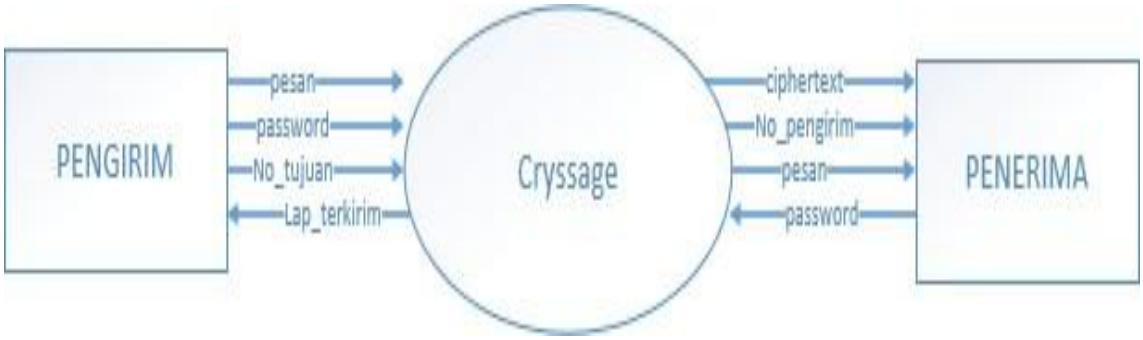
HASIL DAN PEMBAHASAN

Dalam affine chiperterdapat flowchart yang digunakan oleh pengirim untuk mengenkripsi dan mendeskripsikan plainteks sehingga nmendapatkan chiperteks. Adapun tampilan flowchartnya yaitu :



Membuat ContextDiagram

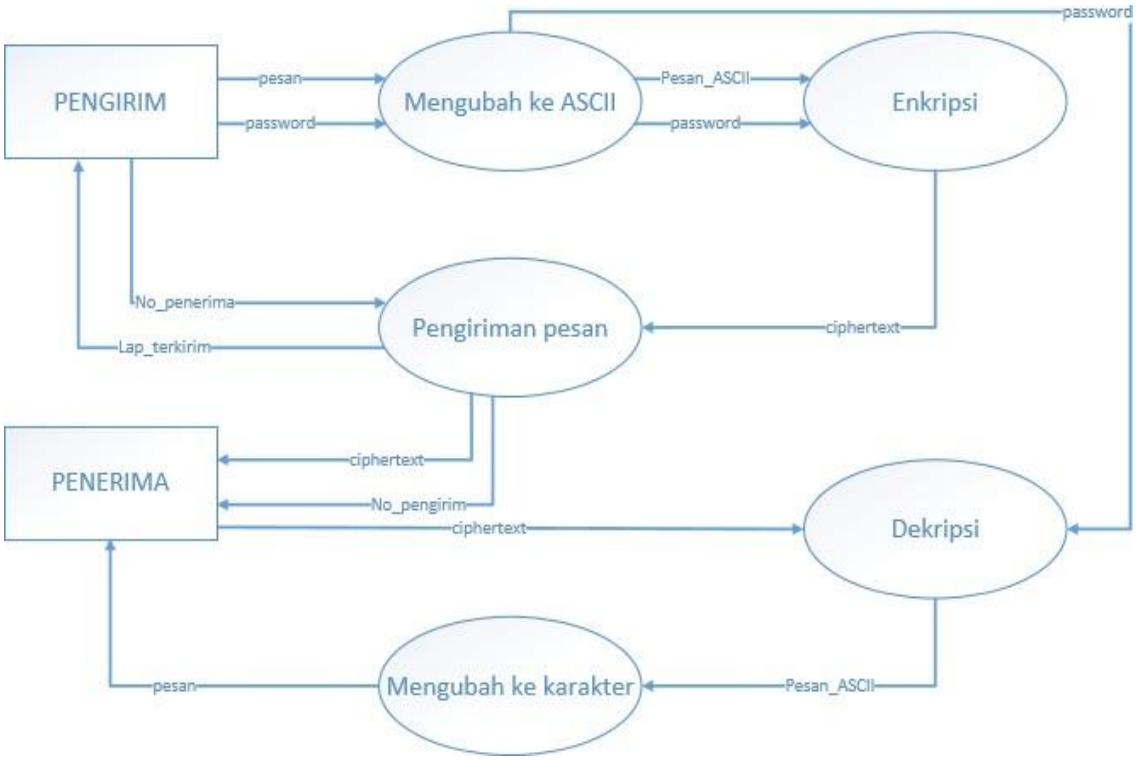
Adapun diagram context daripemodelandariEnkripsiDeskripsiAlgoritma Affine Chiherdigambarkan pada Gambar



Gambar 2. Context Diagram

Pada gambar 2 menjelaskan pengirim dapat menginput (memasukkan) pesan, password dan nomor tujuan pada sistem.Kemudian sistem bakal menciptakan output berwujud informasi moral terkirim pada pengirim.Serta gk anak septor menerima ciphertext serta nomor pengirim.Dimana buat mampu membaca moral, pemeroleh mampu menginput(memasukkan) password pada sistem dan sistem memberikan output berwujud moral pada pemeroleh[11].

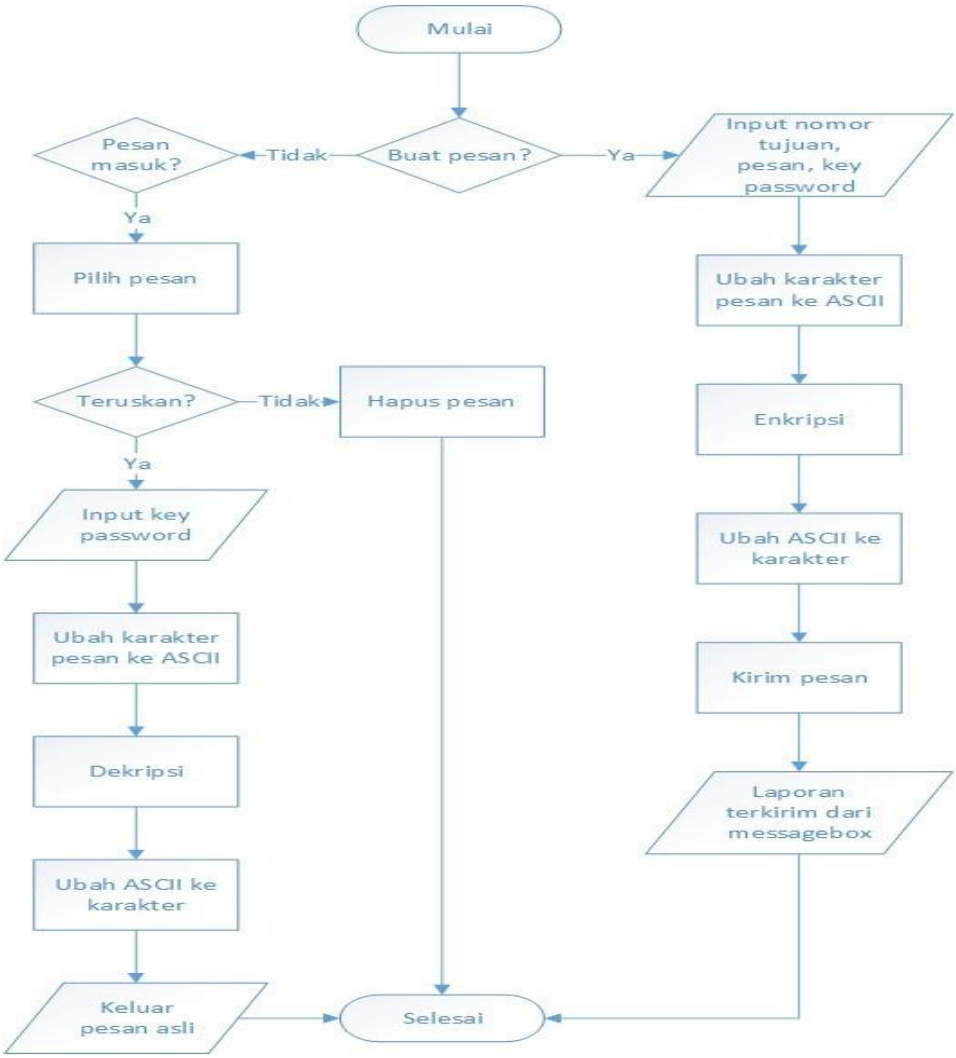
Membuat DataFlow Diagram



Gambar 3. Data Flow Diagram

Pada sketsa 3 yakni data flow gambaran mengartikan apabila sistem bakal dipecah selaku proses-proses kecil alhasil bisa mengartikan proses proses serta arus data yang mengalir dalam sistem. Proses-proses yang kedapatan pada sketsa 3 yaitu[[11]: 1. Mengalihkan ke ASCII: tata cara ini mengubah permohonan dan password kedalam tandaASCII. 2. Enkripsi: tata cara ini melaksanakan pengenkripsian permohonan mengenakan algoritma affine cipher dengan kunci/password yang diinputkan. 3. Pengiriman petaruh: tata cara ini mengirimkan permohonan yang dienkripsi dan memberikan maklumat pengiriman pengirim jikalau permohonan terkirim kenomor yang telah diinputkan. 4. Dekripsi: tata cara ini melaksanakan pendekripsian permohonan sesuai dengan password yang diinputkan. bila password pas maka ciphertext mau sebagai permohonan asli. bila password salah permohonan mau senantiasa didekripsi permohonan yang didapat bukan permohonan asli. karna key yang dipakai bakal mendekripsi ciphertext salah. 5. Mengalihkan ketabiat: tata cara ini mengubah isyarat ASCII yang ditemui dari hasil dekripsi kedalam tabia tmengenakan password.

Membuat Flowchart Aplikasi Sistem



Gambar 4. Flowchart Aplikasi Sistem

Perancangan Sistem

Perancangan sistem adalah pemberian teknik-teknik yang hendak dilaksanakan dalam suatu konsep bentuk-bentuk saat sebelum diawali pembuatan code ataupun coding. Aplikasi Cryssageada 4 kastaadalah: MainActivity, Buat Pesan, Data Pesan, serta Lihat Pesan. metode coding terbuat memanfaatkan aplikasi eclipse[11]. Kegunaan masing-masing kastaadalah:

1. MainActivity, adalah kasta pokok yang menjalin kasta yang lain serta kasta yang mula-mula ditemui kala melaksanakan aplikasi Cryssage.
2. Buat Pesan, adalah tempat terletaknya proses enkripsi dekripsi pesan serta tempat proses pengiriman amaran berlangsung.
3. Data Pesan, adalah tempat guna menyisihkan data dari pesan yang masuk serta pesan yang pergi.
4. Lihat Pesan, adalah tempat guna menunjukkan pesan yang masuk serta pesan yang pergi dengan cara khusus

SIMPULAN

Kesimpulan dari penelitian ini yaitu Perancangan aplikasi ini bertujuan untuk mengimplementasikan hasil enkripsi dan dekripsi untuk keamanan teks dimanaAlgoritma yang terbuat mengunakan campuran kunci kompleks terprediksi, hal ini diakibatkan algoritma itu

memanfaatkan campuran 2 kunci yang berselisih. Selepas itu Aplikasi Cryssage ini mampu dibubuhkan guna mengerjakan enkripsi amanat serta mengirimnya kenomor tujuan pemeroleh amanat. Serta adalah aplikasi yang terbuat sesederhana bisa jadi, akibatnya pengguna(use) bisa dengan gampang mengetahui tiap tugas melalui tombol-tombol yang dibubuhkan dalam aplikasi ini. Selepas itu Aplikasi Cryssage mampu dibubuhkan oleh user dalam lingkup lumrah yang menginginkan keamanan data dengan sms serta menghindari orang yang tidak berkenan guna mengerti data yang pernah dikirim user terhadap pemeroleh.Adapun data dari penelitian ini sejalan dengan penelitian sebelumnya yang dilakukan oleh Randytia Akbar(2013) dengan judul “Implementasi Enkripsi Deskripsi Algoritma Affine Chiper berbasis Android”.

DAFTAR PUSTAKA

A. B. Nasution, “Modifikasi Algoritma Affine Cipher untuk Mengamankan Data,” *J. Teknol. Inf.*, 2020, [Online]. Available: http://www.jurnal.una.ac.id/index.php/jurti/article/view/1742

H. Agung, “Implementasi Affine Chiper dan RC4 pada Enkripsi file Tunggal,” *jakarta Univ. Bunda Mulia*, p. 1, 2015.

R. Munir, “Kriptografi Edisi Kedua,” *Bandung Inform.*, 2019.

N. Nurjamiyah, “Implementasi Algoritma Affine Cipher untuk Keamanan Data Teks,” *Query J. Inf. Syst.*, 2020, [Online]. Available: http://jurnal.uinsu.ac.id/index.php/query/article/view/8174

Y. Permanasari, “Kriptografi Klasik Monoalphabetic,” *Mat. J. Teor. dan Terap. …*, 2017, [Online]. Available: https://ejournal.unisba.ac.id/index.php/matematika/article/view/2543

M. M. Amin, “Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks,” *Pseudocode*, vol. 3, no. 2, pp. 129–136, 2017, doi: 10.33369/pseudocode.3.2.129-136.

J. Katz and Y. Lindell, “Private Key Encryption and Pseudorandomness,” *Introd. to Mod. Cryptogr. Chapman \& Hall …*, 2007.

S. Y. Wulandari, “Cryptography: A Combination of Caesar and Affine Cipher to Conceal the Message,” *Proceeding Int. Conf. Sci. Eng.*, vol. 3, no. April, pp. 741–744, 2020, doi: 10.14421/icse.v3.595.

R. A. Mollin, *An introduction to cryptography*. taylorfrancis.com, 2006. doi: 10.1201/9781420011241.

D. Rachmawati and A. Candra, “Implementasi Kombinasi Caesar dan Affine Cipher untuk Keamanan Data Teks,” *J. Edukasi dan Penelit. Inform. …*, 2015, [Online]. Available: https://core.ac.uk/download/pdf/324174360.pdf

S. Wibowo, “Implementasi Enkripsi Dekripsi Algoritma Affine Cipher Berbasis Android,” *J. Inf. Syst.*, vol. 3, no. 1, pp. 89–99, 2018.