KRIPTOGRAFI DENGAN KOMPOSISI *CAESAR CIPHER* DAN *AFFINE CIPHER* UNTUK MENGUBAH PESAN RAHASIA

Muhammad Lutfi Wijaya [1)], Kartika Yulianti [2)], Husty Serviana Husain [3)]

[1), 2), 3)] Departemen Pendidikan Matematika FPMIPA UPI

*Surel: muluwi@yahoo.co.id

ABSTRAK. Kriptografi *caesar cipher* dan *affine cipher* adalah kriptografi yang sederhana dan mudah dipecahkan. Salah satu cara agar pesan menjadi sulit dipecahkan yaitu dengan cara mengkomposisi kedua *cipher* tersebut. Komposisi kriptografi *caesar cipher* dan *affine cipher* dengan cara dua kali enkripsi dan dua kali dekripsi secara berurutan. Penelitian ini dikaji konsep matematika yang terdapat pada kriptografi komposisi *caesar cipher* dan *affine cipher* dan pembuatan program. Hasil dalam penulisan penelitian ini berupa program aplikasi untuk mempermudah enkripsi dan dekripsi komposisi *caesar cipher* dan *affine cipher* yang dibuat menggunakan bahasa pemrograman Delphi 7. Hasil yang diperoleh dari pengujian program dan pengujian manual adalah sama, menunjukan bahwa aplikasi telah sesuai dengan yang diinginkan.

Kata kunci: program aplikasi, *caesar cipher, affine cipher*

ABSTRACT. Cryptography caesar cipher and affine cipher is a simple cyrptography and easily solved. One way for a message to becomes difficult to resolve that is by composing the both cipher. Composition cryptography caesar cipher and affine cipher is to double encryption and decryption sequentially. This paper examines the mathematical concepts contained in the composition cryptography caesar cipher and affine cipher and making program. The results of writing of this form of application programs to simplify encryption and decryption composition caesar cipher and affine cipher that by programming language Delphi 7. The results obtained from the testing program and manual are the same, this indicates that the application has been as expected.

Keywords: application program, caesar cipher, affine cipher

1. PENDAHULUAN

Kita ketahui bahwa zaman abad 21 sudah menjadi era digital. Hal tersebut dapat dilihat dengan banyaknya orang yang menggunakan internet dari penggunaan *e-mail*, media sosial, jual beli *online*, dan masih banyak lagi. Orang-orang berkomunikasi atau bertukar informasi menggunakan jaringan internet. Karena sifat jaringan komputer yang menggunakan konsep sistem terbuka, maka orang lain dapat dengan mudah masuk ke jaringan tersebut, sehingga pengiriman pesan menjadi tidak aman dan dapat dimanfaatkan oleh orang lain untuk mengambil atau mengubah informasi pesan tersebut di tengah jalan.

Keamanan merupakan aspek penting dalam pengiriman pesan melalui jaringan, terlebih lagi untuk pesan – pesan yang bersifat rahasia atau penting. Misalnya untuk mengirimkan soal Ujian Nasional (UN) dari pusat ke daerah akan lebih cepat dan efisien jika menggunakan *e-mail*. Supaya pesannya tidak mengalami kebocoran maka diperlukan suatu kode agar pesan tersebut masih bersifat rahasia.

Ilmu yang membuat kode atau sandi yaitu Kriptografi. Kriptografi berasal dari bahasa Yunani: *cryptos* dan *graphein*. *Cryptos* artinya rahasia, sedangkan *graphein* artinya tulisan. Jadi, kriptografi berarti tulisan rahasia. Sedangkan definisi kriptografi adalah suatu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, integritas suatu data, serta otentifikasi data (Menezes, 1996 : 4). Menurut (Kromodimoeljo, 2009 : 5) kriptografi adalah ilmu mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi data yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi. Proses enkripsi dilakukan menggunakan suatu algoritma dengan beberapa parameter. Secara garis besar, proses enkripsi adalah proses pengacakan pesan yang dapat dibaca “naskah asli” (*plaintext*) menjadi pesan yang sulit dibaca “naskah acak” (*ciphertext*). Tentunya naskah acak harus dapat didekripsi oleh seseorang yang mempunyai kunci dekripsi untuk mendapatkan kembali pesan asli. Orang yang tidak memiliki kunci dekripsi akan sulit mendapatkan kembali pesan asli yang telah diubah menjadi naskah acak.

Dalam kriptografi klasik, teknik enkripsi yang digunakan adalah enkripsi simetris dimana kunci dekripsi sama dengan kunci enkripsi. Untuk *public key cryptography*, diperlukan teknik enkripsi asimetris dimana kunci dekripsi tidak sama dengan kunci enkripsi. Enkripsi, dekripsi dan pembuatan kunci untuk teknik enkripsi asimetris memerlukan komputasi yang lebih intensif dibandingkan enkripsi simetris, karena enkripsi asimetris menggunakan bilangan-bilangan yang sangat besar.

Pada penelitian ini akan digunakan kriptografi *caesar cipher* dan *affine cipher* yang merupakan kriptografi sandi simetris. *Caesar cipher* dan *affine cipher* adalah kriptografi sederhana. Dengan pengenkripsian satu kali pada pesan asli tidak cukup untuk membuat pesan itu menjadi aman sehingga pesan tersebut akan mudah dipecahkan oleh orang ketiga. Salah satu cara agar pesan menjadi sulit dipecahkan yaitu dengan cara mengkomposisikan kedua *cipher*. Dengan dua kali enkripsi sederhana dari *caesar cipher* dan *affine* cipher akan meningkatkan keamanan (membuat enkripsi menjadi kuat/sulit dipecahkan). Karena menggunakan dua *cipher* maka ada dua cara mengenkripsiannya, yaitu diawali dengan *caesar cipher* terlebih dahulu kemudian diikuti dengan *affine cipher* atau sebaliknya yaitu mengenkripsi pesan dengan *affine cipher* terlebih dahulu kemudan dilanjut dengan enkripsi *caesar cipher*.

Berkaitan dengan kriptografi *caesar cipher* dan *affine cipher* tersebut, penulis tertarik untuk membuat program aplikasi dari komposisi kriptografi klasik dengan memperhatikan konsep matematika yang berhubungan dengan kriptografi tersebut. Berdasarkan hal tersebut, judul penelitian ini adalah "Kriptografi dengan Komposisi *Caesar Cipher* dan *Affine Cipher* untuk Mengubah Pesan Rahasia".

2. TINJAUAN PUSTAKA

1. Keterbagian

a. Definisi: Pembagian (Kromodimoeljo, 2009, hlm. 24)

Untuk setiap pasangan bilangan bulat *a* dan *b*, jika terdapat bilangan bulat *q* sehingga $a = q$, maka *b* membagi *a*, dan *b* disebut pembagi (*divisor* atau faktor) dari *a* dengan notasi *b*|*a*. Notasi $b \nmid a$ digunakan jika *b* bukan pembagi *a*.

b. Teorema: Pembagian (Burton, 2007, hlm. 17)

Untuk setiap pasangan bilangan bulat *a* dan *b* dengan $b > 0$, terdapat pasangan unik bilangan bulat q dan r yang memenuhi persamaan:

$$a = q \ + r \text{ dengan } 0 \leq r < b.$$

Bilangan q disebut hasil bagi (*quotient*) dan r disebut sisa (*residue*) dari pembagian a oleh b.

c. Definisi: *Greatest Common Divisor* (Burton, 2007, hlm. 21)

Diberikan $a, b \in \mathbb{Z} \neq 0$. Bilangan asli d disebut GCD (*greatest common divisor*) dari a dan b atau ditulis $d = \gcd(a, b)$ jika:

1. $d|a$ dan $d|b$,
2. Untuk setiap bilangan asli c dengan $c|a$ dan $c|b$ haruslah berlaku $c|d$.

2. Algoritma Euclid

Cara untuk mendapatkan $\gcd(a, b)$ adalah dengan membuat semua daftar faktor dari a dan b kemudian mencari faktor terbesar yang ada dalam kedua daftar. Akan tetapi, jika bilangannya sangat besar untuk membuat semua daftar faktor tidaklah mudah. Ada cara yang lebih efisien yaitu dengan menggunakan algoritma Euclid.

a. Teorema: Algoritma Euclid (Kromodimoeljo, 2009, hlm. 25)

Jika $a = q \quad + r$ maka $\gcd(a, b) = \gcd(b, r)$.

b. Teorema: Algoritma Euclid (Kromodimoeljo, 2009, hlm. 27)

Untuk setiap pasangan bilangan bulat *a* dan *b*, kecuali $a = b = 0$, terdapat pasangan bilangan bulat *u* dan *v* yang memenuhi:

$$\gcd(a, b) = a \quad + b \ .$$

c. Teorema: (Kromodimoeljo, 2009, hlm. 29)

Untuk setiap pasangan bilangan bulat a dan b kecuali $a = b = 0$ dengan d = $\gcd(a, b)$ dan bilangan bulat c, persamaan:

$$c = a \quad + b \quad \text{dengan } (x, y \in \mathbb{Z})$$

mempunyai solusi jika dan hanya jika c merupakan kelipatan d.

d. Definisi: Relatif Prima (Kromodimoeljo, 2009, hlm. 29)

Dua buah bilangan bulat *a* dan *b* dikatakan relatif prima jika $\gcd(a, b) = 1$.

e. Teorema: Relatif Prima (Kromodimoeljo, 2009, hlm. 29)

Pasangan bilangan bulat *a* dan *b* relatif prima jika dan hanya jika ada pasangan bulat *x* dan *y* yang memenuhi persamaan:

$$a \quad + b \quad = 1$$

f. Definisi: Modulo (Munir, 2004, hlm. 4)

Misalkan *a* adalah bilangan bulat dan *n* adalah bilangan bulat positif. Operasi *a* mod *n* (dibaca "*a* modulo *n*") memberikan sisa *r* jika *a* dibagi dengan *n* dengan notasi

$$a \bmod n = r$$

Sedemikian sehingga $a = n \quad + r$, dengan $0 \leq r < n$.

g. Definisi: Kongruen (Kromodimoeljo, 2009, hlm. 32)

Untuk setiap pasangan bilangan bulat *a* dan *b*, *a* kongruen dengan *b* modulo *n*, dengan notasi

$$a \equiv b \pmod{n}$$

jika *a* dan *b* mempunyai sisa yang sama jika dibagi oleh *n*.

h. Teorema: Inverse (Kromodimoeljo, 2009, hlm. 35)

Suatu bilangan *a* mempunyai *inverse* modulo *n* jika dan hanya jika $\gcd(a, n) = 1$

3. Fungsi

Fungsi adalah suatu aturan korespondensi (padanan) yang menghubungkan setiap obyek x dalam satu himpunan, yang disebut daerah asal, dengan sebuah nilai tunggal $f(x)$ dari suatu himpunan kedua. Himpunan nilai yang diperoleh secara demikian disebut daerah hasil fungsi (Purcell, Varberg, Rigdon, 2003: 39).

a. Definisi: Fungsi Satu-Satu (Injektif) (Arifin, 2000)

Pemetaan (fungsi) $f: A \to B$ dikatakan satu-satu atau injektif, jika untuk setiap unsur x_1 dan x_2 di yang dipetakan sama oleh f, yaitu $f(x_1) = f(x_2)$ berlaku $x_1 = x_2$.

b. Definisi: Fungsi Pada (Surjektif) (Arifin, 2000)

Pemetaan (fungsi) $f: A \to B$ dikatakan pada atau surjektif, jika untuk setiap unsur $y \in B$ terdapat unsur $x \in A$ yang memenuhi $f(x) = y$.

c. Definisi: Fungsi Bijektif (Satu-Satu dan Pada)

Pemetaan (fungsi) $f: A \to B$ dikatakan bijektif, jika f adalah fungsi satu-satu dan fungsi pada.

4. Grup

Definisi Grup (Kromodimoeljo, 2009, hlm. 19)

Suatu grup G dengan operasi biner $*$ adalah suatu himpunan dengan struktur aljabar sebagai berikut:

1. Jika $a, b \in G$ maka $(a * b) \in G$ (tertutup).
2. $a * (b * c) = (a * b) * c$, $\forall\, a, b, c \in G$ (asosiatif).
3. Terdapat elemen $e \in G$ dimana $a * e = a = e * a$ untuk setiap $a \in G$ (identitas).
4. Untuk setiap $a \in G$ terdapat $b \in G$ dengan $a * b = e = b * a$ (invers).

5. Caesar Cipher

Julius Caesar menukar setiap huruf dalam naskah asli dengan huruf lain dalam naskah acak. Besar atau kecil huruf dipertahankan dalam naskah acak. Dengan kata lain huruf besar ditukar dengan huruf besar, huruf kecil ditukar dengan huruf kecil tetapi spasi, titik, koma dan tanda lainnya tidak ditukar. Cara yang dilakukan oleh Julius Caesar dalam mengubah naskah asli tersebut dikenal dengan *caesar cipher* (Kromodimoeljo, 2009, hlm. 9).

Caesar cipher adalah jenis enkripsi yang disebut *simple substitution cipher* dimana setiap huruf dalam naskah asli ditukar dengan huruf lain dalam naskah acak. Julius Caesar menukar huruf dengan cara *shift transformation*. Dengan rumus enkripsi *caesar cipher* adalah sebagai berikut:

$$C = \begin{cases} P + b_c, & \text{jika } P + b_c < n \\ P + b_c - n, & \text{jika } P + b_c \geq n \end{cases}$$

dimana, C adalah kode bilangan karakter acak, P adalah kode bilangan karakter asli, b_c adalah besarnya *shift*, n adalah besarnya perbendaharaan karakter (dengan kode 0 sampai $n-1$).

Rumus untuk enkripsi sesuai dengan relasi ekuivalen:

$$C \equiv P + b_c \ (m \quad n), \quad \infty \leq b_c \leq \infty$$

Berdasarkan rumus enkripsi rumus dekripsi untuk *caesar cipher* adalah

$$P = \begin{cases} C - b_c, & \text{jika } C \geq b_c \\ C - b_c + n, & \text{jika } C < b_c, \end{cases}$$

yang sesuai dengan relasi ekuivalen:

$$P \equiv C - b_c (\text{mod n}), \quad \infty \leq b_c \leq \infty$$

Julius Caesar sendiri menggunakan huruf "A" sampai "Z" (dengan kode 0 sampai 25) sebagai perbendaharaan karakter untuk enkripsi (karakter selain huruf tidak dienkripsi).

6. Affine Cipher

Affine chiper merupakan perluasan dari metode *caesar cipher* untuk mempersulit analisa frekuensi. *Caesar cipher* menggunakan *shift transformation* yang rentan terhadap analisa frekuensi (Kromodimoeljo, 2009, hlm. 37). Untuk mempersulit analisa frekuensi, *affine cipher* menggunakan *affine transformation*, dengan rumus enkripsi :

$$C \equiv a \quad + b_a (\text{mod } n),$$

Sehingga rumus dekripsinya :

$$P \equiv a^{-1} C - a^{-1} b_a (\text{mod } n).$$

Jadi kunci untuk affine cipher terdiri dari dua parameter *a* dan b_a. Agar *a* mempunyai invers a^{-1}, *a* harus mematuhi $\gcd(a, n) = 1$.

7. Kriptografi

Kriptografi adalah ilmu pengetahuan dengan menggunakan teknik matematika untuk mengenkripsi dan dekripsi data. Data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi (Kromodimoeljo, 2009).

Kriptografi sudah digunakan sejak zaman perang untuk mengirimkan pesan. Kriptografi yang digunakan adalah kriptografi klasik dan cara menggunakannya masih manual atau belum menggunakan komputer. Kriptografi klasik adalah cara merubah pesan asli ke pesan sandi / rahasia dengan menggunakan metode subtitusi (perpindahan huruf) atau metode transposisi (pertukaran posisi), yang mengetahui operasi ini hanya kedua pihak (pengirim dan penerima) sehingga pesan akan aman apabila ada orang ketiga yang mengetahui pesan tersebut.

Di dalam kriptografi, akan sering ditemukan berbagai istilah (terminologi). Istilah-istilah yang sering kali digunakan adalah sebagai berikut:

1. Pesan : Suatu data atau informasi yang dapat dibaca dan dimengerti maknanya.
2. *Plaintext* : Pesan asli dari pengirim A yang kemudian akan disandikan dan dikirim kepada penerima B.
3. *Ciphertext* : Bentuk pesan yang tersandi. *Ciphertext* harus dapat ditransformasi kembali menjadi *plaintext*.
4. Enkripsi : Proses menyandikan *plaintext* menjadi *ciphertext*.
5. Kunci : Parameter yang digunakan untuk transformasi *enciphering* dan *deciphering*.
6. Dekripsi : Proses mengembalikan *ciphertext* menjadi *plaintext*.

Gambar 1: Proses enkripsi dan dekripsi (Kromodimoejo, 2009: 5)

Berdasarkan Gambar 1, pengirim mengirim pesan dan mengubah naskah asli (*plaintext*) tersebut dengan kunci untuk dienkripsi menjadi naskah acak (*ciphertext*) yang sulit dibaca oleh orang ketiga atau seseorang yang tidak mempunyai kunci. Naskah acak ini harus dapat didekripsi penerima yang mempunyai kunci. Enkripsi dan dekripsi ini, kunci yang digunakan pengirim dan penerima adalah kunci yang sama, disebut dengan kriptografi kunci tunggal atau simetris biasanya kriptografi ini disebut kriptografi klasik. Sedangkan pada kunci yang digunakan pada algoritma enkripsi dan dekripsi berbeda disebut kriptografi kunci publik atau asimetris biasanya kriptografi ini disebut kriptografi modern.

a. Cryptanalysis

Cryptanalysis adalah teknik untuk mencoba memecahkan enkripsi, biasanya dengan mencari kunci enkripsi. “Kriptanalisis adalah ilmu pengetahuan mengenai teknik matematika untuk percobaan menggagalkan teknik kriptografi, secara umum, layanan keamanan jaringan” (Menezes *et al*., 1996, hlm. 15). Menurut Kromodimoeljo ada tiga kategori teknik pencarian kunci yang biasanya digunakan untuk kriptografi klasik yaitu *known plaintext attack,* analisa statistik, dan *brute force search.*

Kombinasi dari teknik-teknik tersebut juga sering digunakan. Minimal pemecahan mempunyai akses ke naskah acak dan kadang juga mengetahui naskah aslinya.

8. Kode ASCII

ASCII (*American Standart Code for Information Interchange*) merupakan suatu standar internasional dalam kode huruf dan simbol seperti *Hex* dan *Unicode* tetapi ASCII lebih bersifat universal. Jumlah kode ASCII adalah 256 kode.

3. METODE PENELITIAN

Dalam penulisan ini, dikaji kriptografi *caesar cipher* dan *affine cipher* dan konsep matematika yang berhubungan dengan kriptografi tersebut. Referensi utama dalam penelitian ini adalah "Teori dan Aplikasi Kriptografi" karya Sentot Kromodimoeljo.

4. HASIL DAN PEMBAHASAN

1. Komposisi Kriptografi *Caesar Cipher* dan *Affine Cipher*

Salah satu cara untuk meningkatkan keamanan suatu kriptografi adalah dengan melakukan dua kali enkripsi. Hal tersebut menyebabkan semakin sulit suatu kriptografi untuk dipecahkan. Dengan menggunakan dua *chiper* yaitu *caesar cipher* dan *affine cipher* akan dibutuhkan dua kali percobaan dalam memecahkan enkripsinya. Karena menggunakan dua *cipher* maka ada dua cara pengkomposisian, yaitu diawali dengan *caesar cipher* terlebih dahulu kemudian diikuti dengan *affine cipher* atau sebaliknya yaitu mengenkripsi pesan dengan *affine cipher* terlebih dahulu kemudian dilanjut dengan enkripsi *caesar cipher*.

a. Caesar Cipher – Affine Cipher

Mengkomposisi dua *cipher* yaitu dengan melakukan *caesar cipher* diikuti dengan *affine cipher* secara matematis dapat ditulis :

$E_A \circ E_C(P) = E_A\big(E_C(P)\big) = E_A(C') = C''$ untuk enkripsi,

$D_C \circ D_A(C'') = D_C(D_A(C'')) = D_C(C') = P$ untuk dekripsi,

dimana, E_A adalah enkripsi *affine cipher*, E_C adalah enkripsi *caesar cipher*, D_A adalah dekripsi *affine cipher*, dan D_C adalah dekripsi caesar cipher.

b. Affine Cipher – Caesar Cipher

Mengkomposisi dua *cipher* yaitu dengan melakukan *affine cipher* diikuti dengan *caesar cipher* secara matematis dapat ditulis :

$E_C \circ E_A(P) = E_C\big(E_A(P)\big) = E_C(C') = C''$ untuk enkripsi,

$D_A \circ D_C(C'') = D_A\big(D_C(C'')\big) = D_A(C') = P$ untuk dekripsi.

2. Diskusi dan Pembahasan

Pada bagian ini akan diungkapkan konsep – konsep matematika yang terselubung terdapat pada metode kriptografi.

A. Akan dibuktikan bahwa kriptografi enkripsi *caesar cipher* adalah fungsi bijektif.

Misalkan $f: \mathbb{Z}_{95} \rightarrow \mathbb{Z}_{95}$ didefinisikan oleh $f(x) = x + b \ (m \quad 95)$, $\forall\, x \in \mathbb{Z}_{95}$, $\forall\, b$ elemen tetap di $\mathbb{Z}_{95}$

i. Akan ditunjukan bahwa f injektif.

Ambil sebarang $x_1, x_2 \in \mathbb{Z}_{95}$ dan $f(x_1) = f(x_2)$ sedemikian sehingga

$$f(x_1) = f(x_2)$$
$$x_1 + b \ (m \quad 95) = x_2 + b \ (m \quad 95)$$
$$x_1 + b - b \ (m \quad 95) = x_2 + b - b \ (m \quad 95)$$
$$x_1 (m \quad 95) = x_2 \ (m \quad 95)$$

Jadi, fungsi $f(x)$ adalah fungsi injektif. ■

ii. Akan ditunjukan bahwa f surjektif.

Ambil sebarang $y \in \mathbb{Z}_{95}$, pilih $x = y - b$, maka $y = f(x) = x + b$. Berdasarkan definisi maka $f(x)$ merupakan fungsi surjektif. ■

Berdasarkan (i) dan (ii) maka $f(x)$ merupakan fungsi bijektif .

B. Akan dibuktikan bahwa kriptografi enkripsi *affine cipher* adalah fungsi bijektif.

Misalkan $f: \mathbb{Z}_{95} \rightarrow \mathbb{Z}_{95}$ didefinisikan oleh $f(x) = a * x + b \ (m \quad 95)$, $\forall\, x \in \mathbb{Z}_{95}$, $\forall\, a, b \in \mathbb{Z}$.

i. Akan ditunjukan bahwa f injektif

Ambil sebarang $x_1, x_2 \in \mathbb{Z}_{95}$ dan $f(x_1) = f(x_2)$ sedemikian sehingga

$$f(x_1) = f(x_2)$$
$$a * x_1 + b \ (m \quad 95) = a * x_2 + b \ (m \quad 95)$$
$$a * x_1 + b - b \ (m \quad 95) = a * x_2 + b - b \ (m \quad 95)$$
$$a * x_1 (m \quad 95) = a * x_2 \ (m \quad 95)$$

$a * x_1 * \frac{1}{a} \ (m \quad 95) = a * x_2 * \frac{1}{a} \ (m \quad 95)$, a^{-1} ada dengan syarat $\gcd(a, n) = 1$

$$x_1 (m \quad 95) = x_2 \ (m \quad 95)$$

Jadi, fungsi $f(x)$ adalah fungsi injektif. ■

ii. Akan ditunjukan bahwa f surjektif.

Ambil sebarang $y \in \mathbb{Z}_{95}$, pilih $x = \frac{y}{a} - \frac{b}{a}$, maka $y = f(x) = a * x + b$. Berdasarkan definisi maka $f(x)$ merupakan fungsi surjektif. ■

Berdasarkan (i) dan (ii) maka $f(x)$ merupakan fungsi bijektif .

C. Selain ditemukannya bahwa *caesar cipher* dan *affine cipher* adalah fungsi bijektif, bahwa hasil komposisi dari dua buah fungsi bijektif adalah bijektif.

D. Hasil komposisi *caesar cipher* dan *affine cipher* tidak komutatif

$$c \circ a \neq a \circ c$$

E. Akan dibuktikan bahwa himpunan $\mathbb{Z}_9$ dengan operasi rumus enkripsi *caesar cipher* adalah grup, dimana operasi rumus enkripsi *caesar cipher* adalah operasi penjumlahan.

i. Ambil sebarang $a, b \in \mathbb{Z}_9$, karena $a, b \in \mathbb{Z}_9$ dan $a + b \in \mathbb{Z}_9$, maka

$$a + b \in \mathbb{Z}_9$$

Jadi $(\mathbb{Z}_9, +)$ tertutup. ■

ii. Ambil sebarang $a, b, c \in \mathbb{Z}_9$, maka $a + (b + c) = (a + b) + c$

$$a + (b + c) = a + (b + c)$$
$$a + (b + c) = a + b + c$$
$$a + (b + c) = (a + b) + c$$
$$a + (b + c) = (a + b) + c$$

Jadi $(\mathbb{Z}_9, +)$ bersifat asosiatif. ■

iii. Ada $e \in \mathbb{Z}_9$ dimana $a + e = e + a = a$

$a + e = a$	$e + a = a$
$e = a - a$	$e = a - a$
$e = 0$	$e = 0$

Jadi $(\mathbb{Z}_9, +)$ memiliki identitas yaitu 0. ■

iv. Ada $b \in \mathbb{Z}_9$ dimana $a + b = b + a = e$

$a + b = e$	$b + a = e$
$a + b = 0$	$b + a = 0$
$b = -a$	$b = -a$

Jadi $(\mathbb{Z}_9, +)$ memiliki invers yaitu $-a$. ■

Berdasarkan (i), (ii), (iii), dan (iv) maka $(\mathbb{Z}_9, +)$ merupakan grup.

F. Akan diperiksa apakah himpunan $\mathbb{Z}_9$ dengan operasi rumus enkripsi *affine cipher* adalah bukan grup.

Misalkan himpunan bilangan bulat $\mathbb{Z}_9$, didefinisikan operasi biner:

$$a * b = 2a + b$$

i. Ambil sebarang $a, b \in \mathbb{Z}_9$, karena $a, b \in \mathbb{Z}_9$ dan $2a + b \in \mathbb{Z}_9$ maka

$$a + b = 2a + b \in \mathbb{Z}_9$$

Jadi $(\mathbb{Z}_9, *)$ tertutup. ■

ii. Ambil sebarang $a, b, c \in \mathbb{Z}_9$, maka $a * (b * c) = (a * b) * c$

$$a * (b * c) = a * (2b + c)$$
$$= 2a + 2b + c$$
$$(a * b) * c = (2a + b) * c$$
$$= 2(2a + b) + c$$
$$= 4a + 2b + c$$

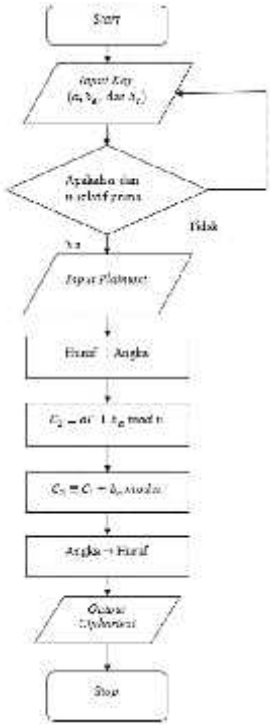
$a * (b * c) \neq (a * b) * c$ maka $(\mathbb{Z}_9, *)$ tidak bersifat asosiatif. ■

Karena (ii) tidak asosiatif maka $(\mathbb{Z}_9, *)$ bukan grup.

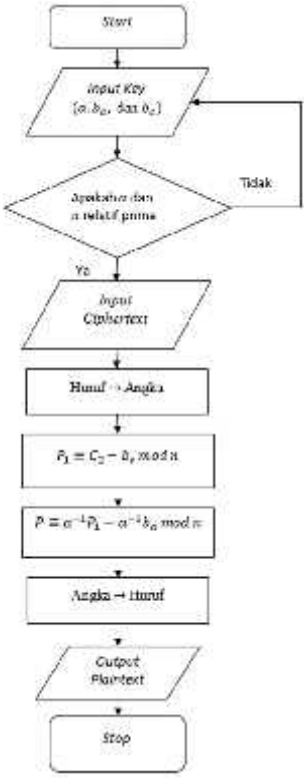
3. Pembuatan Program Aplikasi

Tahap perancangan program aplikasi meliputi perancangan *flowchart* proses enkripsi dan dekripsi, membuat program, pengujian program dan perancangan desain tampilan program aplikasi.

Berikut adalah tahapan mengenkripsi komposisi *affine cipher – caesar cipher* dalam bentuk *flowchart* pada Gambar 2 dan Gambar 3



Gambar 2: Enkripsi Komposisi Affine Cipher – Caesar Cipher



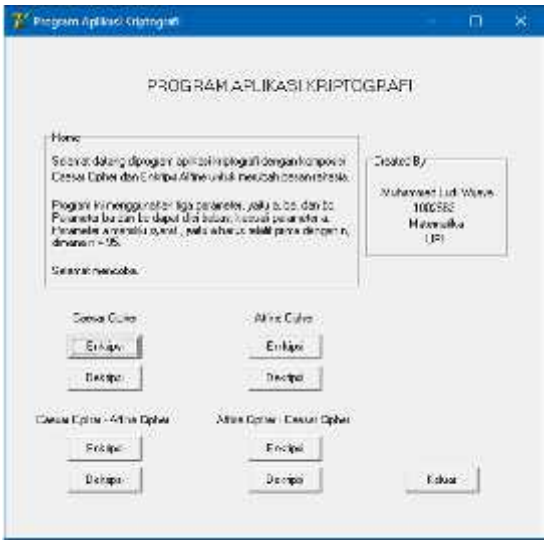
Gambar 3: Dekripsi Komposisi Affine Cipher – Caesar Cipher

Flowchart untuk enkripsi dan dekripsi komposisi *caesar cipher – affine cipher*, serupa dengan Gambar 2 dan Gambar 3. Perbedaannya hanya pada urutan rumus C_1 dan C_2.

4. Implementasi

a. Antarmuka Menu Utama

Berikut ini adalah tampilah hasil antarmuka yang telah dirancang menggunakan *software* aplikasi pemrograman Delphi 7

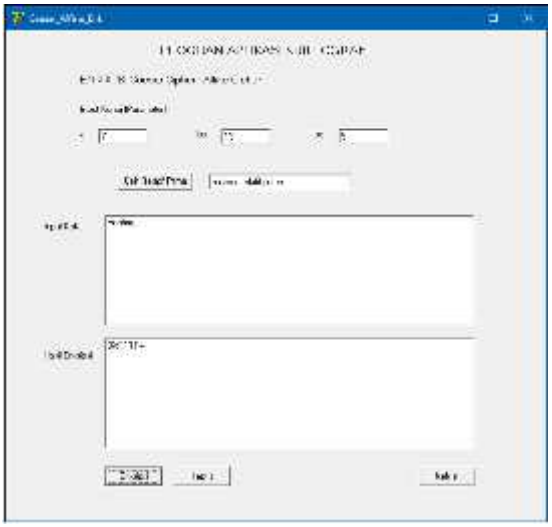


Gambar 4: Tampilan Menu Utama

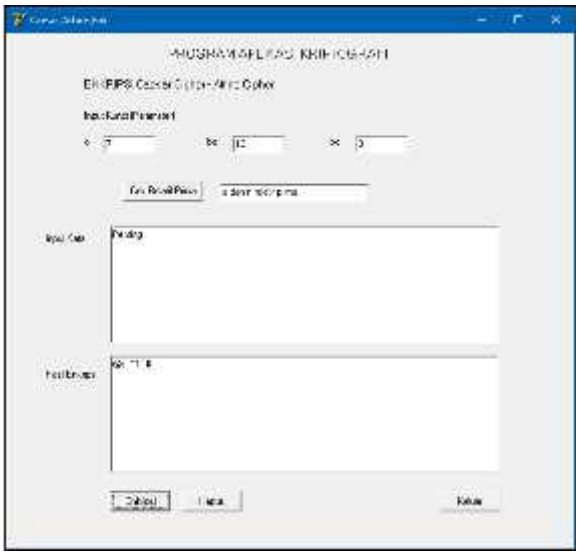
Gambar 4 adalah tampilan antarmuka Menu Utama program aplikasi kriptografi komposisi *caesar cipher* dan *affine cipher*. Terdapat penjelasan mengenai program, terdapat tombol "enkripsi" untuk memasuki halaman enkripsi, tombol "dekripsi" untuk memasuki halaman dekripsi, dan tombol "keluar" untuk keluar dari program tersebut.

b. Antarmuka Enkripsi dan Dekripsi Program

Berikut ini adalah tampilah enkripsi dan dekripsi program:



Gambar 5: Tampilan Enkripsi Program



Gambar 6: Tampilan Dekripsi Program

Gambar 5 dan Gambar 6 adalah tampilan program aplikasi kriptografi komposisi *caesar cipher dan affine cipher* untuk enkripsi dan dekripsi komposisi *caesar cipher – affine cipher*. Terdapat tombol "cek relatif prima" untuk mengecek apakah a dengan n relatif prima, tombol "enkripsi" untuk proses mengeksekusi *plaintext* menjadi *ciphertext*, tombol "dekripsi" untuk proses mengeksekusi *ciphertext* menjadi *plaintext*, tombol "hapus" untuk menghapus semua kolom yang telah terisi menjadi kosong, dan tombol keluar untuk keluar dari program tersebut.

Untuk tampilan enkripsi dan dekripsi *affine cipher*, *caesar cipher*, dan *komposisi affine cipher – caesar cipher* serupa dengan Gambar 5 dan Gambar 6.

5. Pengujian Program Aplikasi

Pada pengujian program aplikasi ini, bertujuan agar program dapat berjalan dengan baik dan tidak adanya *error*. Sangat memungkinkan untuk program ini dilakukan pengembangan lebih lanjut. Sebelum pada tahap pengujian, dibahas mengenai karakter ASCII yang digunakan dalam program aplikasi kriptografi ini.

Jumlah kode ASCII adalah 256 kode tetapi kode ASCII yang digunakan dalam program hanyalah 95 kode. Kode – kode yang digunakan dalam program berupa spasi ( ), karakter khusus (!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~), abjad (A..Z), dan numerik (0..9).

Pengujian program dilakukan dengan cara membandingkan hasil manual dengan hasil pada program. Berdasarkan hasil perbandingan tersebut, hasil yang diperoleh dari keduanya sama. Hal ini menunjukan bahwa program telah sesuai dengan yang diinginkan.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian, maka dapat disimpulkan beberapa hal antara lain: (1) Kriptografi dengan cara *caesar cipher* dan *affine cipher* yaitu dengan menukar setiap huruf asli dengan huruf yang lain. Penukaran ini menggunakan cara *shift transformation* untuk *caesar cipher* dan *affine transformasion* untuk *affine cipher*. Pengkomposisian kriptografi *caesar cipher* dan *affine cipher* dengan cara dua kali enkripsi dan dua kali dekripsi secara berurutan. (2) Konsep – konsep matematika yang digunakan dalam kriptografi komposisi *caesar cipher* dan *affine cipher* yaitu fungsi komposisi, GCD, relatif prima, modulo, algoritma eulcid. Lebih lanjut lagi diperoleh suatu hubungan bahwa kriptografi enkripsi *caesar cipher* dan *affine cipher* merupakan fungsi bijektif (satu-satu dan pada), dan himpunan bilangan bulat dengan operasi rumus enkripsi *caesar cipher* adalah grup. (3) Perancangan program kriptografi komposisi *caesar cipher* dan *affine cipher* diawali dengan membuat *flowchart* enkripsi dan dekripsi, kemudian membuat desain tampilan program. Pembuatan program aplikasi kriptografi menggunakan bahasa pemrograman Delphi 7. Pengujian program dilakukan dengan cara membandingkan hasil manual dengan hasil pada program. Berdasarkan hasil perbandingan tersebut, hasil yang diperoleh dari keduanya sama. Hal ini menunjukan bahwa program telah sesuai dengan yang diinginkan.

Beberapa saran yang ditujukan untuk pengebangan program aplikasi komposisi kriptografi antara lain: (1) Mencari metode lain selain komposisi dalam memperkuat kriptografi. (2) Dapat mengembangkan karakter yang tidak terbatas hanya pada 95 karakter.

6. DAFTAR PUSTAKA

[1] Kromodimoeljo, S. (2009). *Teori & Aplikasi Kriptografi*. SPK IT Consulting.

[2] Munir, R. (2011a). *Algoritma Pemrograman dalam Bahasa Pascal dan C.* Bandung: Informatika.

[3] Munir, R. (2004b). *Bahan Kuliah ke-1: Pengantar Kriptografi.* Bandung: Departemen Teknik Informatika ITB.

[4] Munir, R. (2004c). *Bahan Kuliah ke-3:Teori Bilangan (Number Theory).* Bandung: Departemen Teknik Informatika ITB.

[5] TheAsciiCode. (2016). *ASCII Table* [Online]. Tersedia di: http://www.theasciicode.com.ar/. Diakses 7 April 2016.

[6] Kusnassriyanto. (2011). *Belajar Pemrograman Delphi*. Bandung: Modula.

[7] Menezes, A., Oorschot, P., dan Vanstone, A. (1996). *Handbook of Applied Cryptography*. USA: CRC Press.

[8] Arifin, A. (2000). *Aljabar*. ITB Bandung Press, Bandung.

[9] Bartle, Robert. G., and Donald R. Sherbert. (2000). *Introduction to Real Analysis*. New York: John Wiley & Sons.

[10] Burton, D. M. (2007). *Elementary Number Teory, Sixth Edition.* New York: McGraw-Hill.