# Perancangan Kriptografi Kunci Simetris Menggunakan Fungsi Bessel dan Fungsi Legendre

## Artikel Ilmiah

**Diajukan kepada**
**Fakultas Teknologi Informasi**
**untuk memperoleh Gelar Sarjana Komputer**


**Peneliti:**
**Fhelesia E. Gomies (672008177)**
**Alz Danny Wowor, S.Si., M.Cs**

**Program Studi Teknik Informatika**
**Fakultas Teknologi Informasi**
**Universitas Kristen Satya Wacana**
**Salatiga**

**September 2013**

# Perancangan Kriptografi Kunci Simetris Menggunakan Fungsi *Bessel* dan Fungsi *Legendre*

Oleh,

**Fhelesia Gomies**
**NIM : 672008177**

Artikel Ilmiah

Diajukan Kepada Program Studi Teknik Informatika, Fakultas Teknologi Informasi guna memenuhi sebagian dari persyaratan untuk mencapai gelar Sarjana Komputer

Disetujui oleh,

Alz Danny Wowor, S.Si., M.Cs.
Pembimbing

Diketahui oleh,

Dr. Dharmaputra T. Palekahelu, M.Pd.
Dekan

Dian W. Chandra, S.Kom., M.Cs.
Ketua Program Studi

**FAKULTAS TEKNOLOGI INFORMASI**
**UNIVERSITAS KRISTEN SATYA WACANA**
**SALATIGA**
**2013**

# Lembar Pengesahan

| | |
|---|---|
| Judul Tugas Akhir | : Perancangan Kriptografi Kunci Simetris Menggunakan Fungsi *Bessel* dan Fungsi *Legendre* |
| Nama Mahasiswa | : Fhelesia Gomies |
| NIM | : 672008177 |
| Program Studi | : Teknik Informatika |
| Fakultas | : Teknologi Informasi |

Menyetujui,

Alz Danny Wowor, S.Si., M.Cs.
Pembimbing

Mengesahkan,

Dr. Dhamaputra T. Palekahelu, M.Pd.
Dekan

Dian W. Chandra, S.Kom., M.Cs.
Ketua Program Studi

Dinyatakan Lulus Ujian tanggal: 13 September 2013

Penguji:

1. M. A. Ineke Pakereng, M.Kom.
2. Indrastanti R. Widiasari, M.T.

# Pernyataan

Laporan penelitian yang berikut ini:

Judul : Perancangan Kriptografi Kunci Simetris Menggunakan Fungsi *Bessel* dan Fungsi *Legendre*.

Pembimbing : Alz Danny Wowor. S.Si., M.Cs.

adalah benar hasil karya saya:

Nama : Fhelesia E. Gomies

NIM : 672008177

Saya menyatakan tidak mengambil sebagian atau seluruhnya dari hasil karya orang lain kecuali sebagaimana yang tertulis pada daftar pustaka. Pernyataan ini dibuat dengan sebenarnya sesuai dengan ketentuan yang berlaku dalam penulisan karya ilmiah.

Salatiga, September 2013

(Fhelesia E. Gomies)

PERPUSTAKAAN UNIVERSITAS
UNIVERSITAS KRISTEN SATYA WACANA
Jl. [illegible]
Jawa Tengah, Indonesia
Telp. 0298 – [illegible], Fax. 0298 [illegible]
[illegible]

## PERNYATAAN TIDAK PLAGIAT DAN PERSETUJUAN AKSES

Sebagai sivitas akademik Universitas Kristen Satya Wacana, saya yang bertanda tangan di bawah ini:

Nama : Fhelecia. E. Gomies

NIM : 672008177 Email : Gomie-1825@yahoo.com

Fakultas : TI Program Studi : Teknik Informatika

Judul tugas akhir : Perancangan kriptografi kunci simetris menggunakan fungsi bessel dan fungsi legendre

Dengan ini menyerahkan karya tersebut di atas untuk disimpan dalam Koleksi Digital Perpustakaan Universitas dengan ketentuan akses tugas akhir elektronik sebagai berikut (beri tanda pada kotak yang sesuai):

☑ a. Saya mengijinkan karya tersebut diunggah ke dalam aplikasi Koleksi Digital Perpustakaan Universitas, dan/atau portal GARUDA

☐ b. Saya tidak mengijinkan karya tersebut diunggah ke dalam aplikasi Koleksi Digital Perpustakaan Universitas, dan/atau portal GARUDA. *

* *poin b harus dilampiri dengan surat dari Dekan/ Kaprodi atau pembimbing TA dengan diketahui oleh pimpinan fakultas yang menjelaskan alasan pilihan. Yang akan ditampilkan adalah halaman judul + abstrak*

Dengan ini saya juga menyatakan bahwa:

1. Hasil karya yang saya serahkan ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar kesarjanaan baik di Universitas Kristen Satya Wacana maupun di institusi pendidikan lainnya.
2. Hasil karya saya ini bukan saduran/ terjemahan melainkan merupakan gagasan, rumusan, dan hasil pelaksanaan penelitian/ implementasi saya sendiri, tanpa bantuan pihak lain, kecuali arahan pembimbing akademik dan narasumber penelitian.
3. Hasil karya saya ini merupakan hasil revisi terakhir setelah diujikan yang telah diketahui dan disetujui oleh pembimbing.
4. Dalam karya saya ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali yang digunakan sebagai acuan dalam naskah dengan menyebutkan nama pengarang dan dicantumkan dalam daftar pustaka.
5. Saya menyerahkan hak non-eksklusif kepada Perpustakaan Universitas – Universitas Kristen Satya Wacana untuk menyimpan, mengatur akses serta melakukan pengelolaan terhadap karya saya ini dengan mengacu pada ketentuan akses tugas akhir elektronik di atas dan norma hukum yang berlaku.

Pernyataan ini saya buat dengan sesungguhnya. Apabila di kemudian hari terbukti ada penyimpangan dan ketidakbenaran dalam pernyataan ini maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya saya ini, serta sanksi lain yang sesuai dengan ketentuan yang berlaku di Universitas Kristen Satya Wacana.

Salatiga, 25, September 2013
*Tanggal penyerahan*

*Tanda tangan & nama terang mahasiswa*
Fhelecia. E. Gomies

Mengetahui,

[illegible] M.Cs.
*Tanda tangan & nama terang pembimbing I*

*Tanda tangan & nama terang pembimbing II*

# Perancangan Kriptografi Kunci Simetris Menggunakan Fungsi Bessel dan Fungsi Legendre

**[1)]Fhelesia E. Gomies, [2)]Alz Danny Wowor**
Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Jln. Diponegoro 52-60, Salatiga 50771, Indonesia
Email: [1)] 672008177@student.uksw.edu, [2)] alzdanny.wr@gmail.com

**Abstract**

Cryptography is a technique for hiding the text / writing in the encoding process, so that the cryptography used as a technique for data security. But now, many cryptographic could discryptanalysizing, so the data can be accessed by people or the confidentiality of the data is not guaranteed. The purpose of the study to design a symmetric key cryptography using Bessel functions and Legendre functions which generate decimal fractions. Decimal fractions are unique as it has result of divide. Additionally ciphertext is designed in the form of bits which makes it difficult for the cryptanalyst can cryptanalysizing secret message. This result can be an alternative design in which many cryptographic be discryptanalysized

**Keywords**: Cryptographic, Cryptanalyze, Bessel Function, Legendre function, Symmetric key

**Abstrak**

Kriptografi merupakan teknik untuk menyembunyikan teks/tulisan dalam proses penyandian, sehingga kriptografi digunakan sebagai teknik untuk pengamanan data. Tetapi saat ini, banyak kriptografi yang dapat dikriptanalisis, sehingga data dapat diakses oleh pihak lain atau kerahasian data tidak terjamin. Tujuan dari penelitian ini yaitu merancang sebuah kriptografi kunci simetris menggunakan fungsi Bessel dan fungsi Legendre yang menghasilkan bilangan pecahan desimal. Bilangan pecahan desimal memiliki keunikan tersendiri karena memiliki sisa bagi. Selain itu ciphertext dirancang dalam bentuk bit sehingga mempersulit kriptanalis untuk dapat mengkriptanalisis pesan rahasia. Hasil rancangan ini dapat menjadi alternatif dimana banyak kriptografi yang dapat dikriptanalisis.

**Kata Kunci**: Kriptografi, Kriptanalisis, Fungsi Bessel, Fungsi Legendre, Kunci Simetris.

## 1. Pendahuluan

Kemajuan software dan hardware pada teknologi komputer, mendukung kemajuan kriptografi. Pada sisi lain juga menyokong kemajuan kriptanalisis. Hal tersebut awalnya diraih oleh kriptografi Rijndael yang menjadi pemenang kontes Advanced Encryption Standard (AES) yang diadakan oleh NIST (National Institute of Standards and Technology) di Amerika Serikat dengan lama proses seleksi mencapai lima tahun.

Tidak lama kemudian, prestasi Rijndael tersebut memiliki kelemahan yang diidentifikasi oleh Elad Barkan dan Eli Biham pada tahun 2002 [1]. Setelah itu, kembali lagi Eli Biham dan Nathan Kilier dari Technion University Israel, berhasil menunjukkan kriptanalisis untuk Rijndael [2]. Kemajuan ini menjadi contoh bahwa sebuah kriptografi yang handal sekalipun, masih memiliki peluang untuk dapat dibobol. Sehingga, secara berkesinambungan diperlukan adanya modifikasi terhadap teknik kriptografi yang sudah ada ataupun menciptakan teknik kriptografi baru yang semakin rumit/kompleks sehingga mempersulit kriptanalisis untuk memecahkannya.

Kriptografi yang dibuat selama ini, menggunakan kunci simetris maupun asimetris yang menggunakan kunci bilangan bulat atau hasil konversi bilangan bulat ke bit. Bilangan pecahan desimal merupakan rasionalitas dari bilangan pecahan yang kadang masih mempunyai sisa pembagian. Hal ini yang membuat para kriptografi tidak menggunakannya sebagai kunci, karena hasil perhitungannya menjadi tidak menghasilkan sebuah bilangan bulat. Banyak fungsi khusus matematika yang dapat menghasilkan bilangan pecahan desimal, seperti Bessel dan Legendre.

Oleh karena itu, dalam penelitian ini dilakukan perancangan sebuah kriptografi kunci simetris menggunakan kunci dengan bilangan pecahan desimal yaitu fungsi Bessel dan fungsi Legendre untuk proses enkripsi-dekripsi suatu data. Penelitian ini, diharapkan dapat menambah perbendaharaan teknik kriptografi dengan kunci simetris.

## 2. Tinjauan Pustaka

Penelitian sebelumya dengan judul Kriptografi Kunci Simetris Dengan Menggunakan Algoritma Crypton menganalisis kinerja algoritma crypton dengan melakukan simulasi pada Personal Computer (PC) yang bertujuan untuk meningkatkan keamanan data. Hasil yang didapat dari penelitian tersebut adalah penambahan ukuran file tidak selalu sama dengan file yang lainnya [3].

Penelitian lainnya dengan judul Rancangan Algoritma Kriptografi Simetri Dengan Menggunakan Derivasi Algoritma Klasik Subtitusi. Penelitian ini membahas mengenai rancangan algoritma kriptografi kunci simetris dengan menggunakan derivasi algoritma kriptografi klasik, yaitu algoritma subtitusi abjad-tunggal dan algoritma Caesar Cipher. Algoritma ini diharapkan dapat menambah tingkat keamanan dari algoritma kriptografi klasik, yang sangat rentan terhadap exhaustive key search, pendekatan analisa frekuensi dan metode Kasiski, terutama jika pesan yang disandikan adalah pesan panjang. Selain bertujuan untuk

meningkatkan keamanan, algoritma ini juga dirancang sedemikian sehingga faktor kesederhanaan dari algoritma subtitusi klasik tetap terjaga, sehingga praktis dan mudah diaplikasikan [4].

Perbedaan penelitian ini dengan penelitian sebelumnya adalah merancang sebuah teknik kriptografi yang baru dengan menggunakan fungsi Bessel dan fungsi Legendre pada kunci simetris dalam proses Enkripsi dan Dekripsi, serta perancangan sistem tersebut memanfaatkan aplikasi Maple yang bertujuan untuk pengamanan data.

Kriptografi (Cryptography) berasal dari bahasa Yunani yaitu dari kata Cryptos yang artinya tersembunyi dan Graphein yang artinya menulis. Kriptografi dapat diartikan sebagai suatu ilmu ataupun seni yang mempelajari bagaimana sebuah data dikonversi ke bentuk tertentu yang sulit untuk dimengerti [5]. Kriptografi bertujuan untuk menjaga kerahasiaan informasi atau data supaya tidak dapat diketahui oleh pihak yang tidak berhak (unauthorized person).

Berdasarkan kunci yang dipakai, algoritma kriptografi dapat dibedakan atas dua jenis yaitu algoritma simetrik (symmetric) dan asimetrik (asymmetric). Kriptografi kunci simetris disebut juga kunci rahasia yang menggunakan satu kunci untuk proses enkripsi dan dekripsi. Sedangkan kriptografi kunci asimetri disebut juga kunci publik yang menggunakan dua kunci, yaitu kunci public yang bisa diketahui oleh pihak lain sedangkan kunci privat tidak diketahui pihak lain [3].

Perancangan teknik kriptografi ini merupakan kriptografi kunci simetris yang menggunakan fungsi Bessel dan fungsi Legendre. Fungsi Bessel merupakan solusi kanonik y(x) dari persamaan diferensial Bessel. Perancangan ini menggunakan fungsi Bessel jenis pertama orde ke-n. Secara umum diberikan pada Persamaan 1 [6].

$$J_n(x) = x^n \sum_{m=0}^{\infty} \frac{(-1)^m x^{2m}}{2^{2m+n} \cdot m!(n+m)!} \text{ untuk setiap } n \geq 0 \quad (1)$$

Fungsi kedua yang digunakan dalam perancangan ini menggunakan Polinomial Legendre derajat-n dinotasikan sebagai $P_n(x)$ yang secara umum diberikan pada Persamaan 2 [4].

$$P_n(x) = \sum_{m=0}^{M} (-1)^m \frac{(2n-2m)!}{2^n m!(n-m)!(n-2m)!} x^{n-2m} \quad (2)$$

dimana $M = n/2$ atau $(n-1)/2$ adalah bilangan bulat.

Perancangan Kriptografi melibatkan banyak proses perhitungan, selain menggunakan kedua kunci pada Persamaan (1) dan Persamaan (2) juga digunakan Convert Between Base (CBB) yang secara umum diberikan pada definisi sebagai berikut:

Definisi 1. Konversi sembarang bilangan positif $s$ berbasis 10 ke basis β. Secara umum notasinya [7],

$$Konv\ (s, base\ \beta\ ) \quad (3)$$

Definisi 2. Konversi dari urutan bilangan (list digit) $\ell$ dalam basis $\alpha$ ke basis $\beta$. Secara umum dinotasikan [7],

$$Konv\ (\ell, \alpha\ base\ \beta\ ) \tag{4}$$

Dengan jumlahan urutan bilangan (jumlahan $\ell$) mengikuti aturan,

$$\sum_{k=1}^{nops\ (\ell)} I_k . \alpha^{k-1} \tag{5}$$

dimana nops ($\ell$) adalah nilai terakhir dari urutan bilangan $\ell$.

- $0 \leq I_k \leq \alpha$ dan $\ell$ adalah bilangan positif.
- Nilai yang diperoleh merupakan kumpulan urutan bilangan dalam basis $\beta$.

Untuk merancang sebuah kriptografi harus memenuhi 5 tuple yaitu [8].

- **P** adalah himpunan behingga dari plainteks
- **C** adalah himpunan behingga dari cipherteks
- **K** merupakan ruang kunci/keyspace, adalah himpunan berhingga dari kunci
- Untuk setiap $k \in K$, terdapat aturan enkripsi $e_k \in \boldsymbol{E}$ dan berkorespodensi dengan aturan dekripsi $d_k \in \boldsymbol{D}$. Setiap $e_k: P \longrightarrow C$ dan $d_k: C \longrightarrow P$ adalah fungsi sedemikian hingga $d_k(e_k(x)) = x$ untuk setiap plainteks $x \in P$

## 3. Metode dan Perancangan Kriptografi

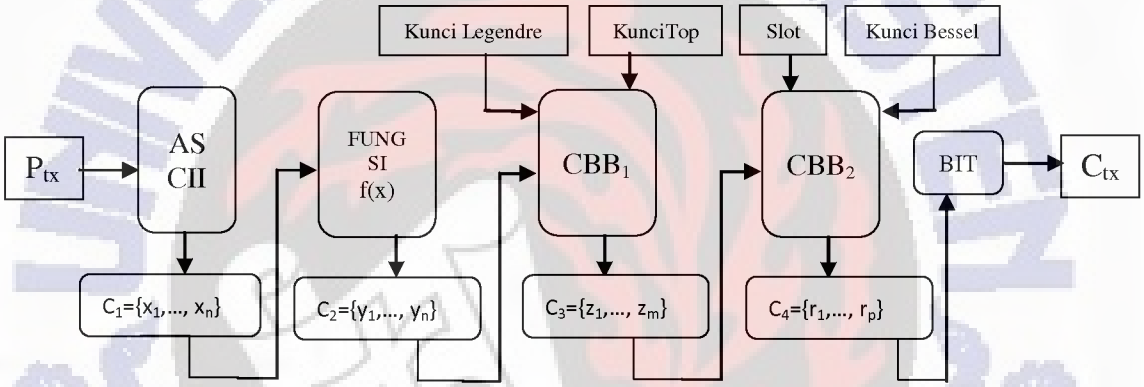
Dalam perancangan kriptografi kunci simetris menggunakan fungsi bessel dan fungsi legendre ini dibutuhkan tahap-tahap dalam menyusunan penelitian. Tahap-tahap yang dibutuhkan adalah Pengumpulan Bahan, Analisis Kebutuhan, Perancangan Kriptografi Simetris, Implementasi, Uji Hasil Perancangan, dan Laporan Penelitian seperti ditunjukkan pada Gambar 1.


**Gambar 1** Tahapan Penelitian

Tahapan penelitian pada Gambar 1 dapat dijelaskan sebagai berikut: Tahap pertama: analisis kebutuhan, yaitu menganalisis kebutuhan apa saja yang diperlukan dalam memulai penelitian perancangan kunci simetris dengan menggunakan fungsi bessel dan fungsi legendre; Tahap kedua: pengumpulan bahan, yaitu melakukan pengumpulan bahan yang berkaitan dengan penelitian

yang akan dilakukan terhadap permasalahan yang ada misalnya mendapatkan data dan literatur yang terkait dengan proses enkripsi dan dekripsi pada data teks menggunakan kunci simetris, fungsi bessel dan fungsi legendre melalui dokumen dan referensi yang ada; Tahap ketiga: perancangan kriptografi simetris, yaitu merancang kriptografi menggunakan kunci simetris dengan menggunakan fungsi bessel dan fungsi legendre yang akan digunakan dalam proses enkripsi dan dekripsi; Tahap keempat: uji hasil perancangan, apabila perancangan teknik kriptografi sudah selesai, maka akan dilakukan pengujian serta analisis terhadap perancangan kriptografi; Tahap kelima: laporan penelitian, yaitu mendokumentasikan proses penelitian yang sudah dilakukan dari tahap awal hingga akhir ke dalam tulisan yang nantinya akan menjadi laporan hasil penelitian.

Berdasarkan skema diagram pada Gambar 2, dijelaskan sebagai berikut:




**Gambar 2.** Skema Diagram Enkripsi

Gambar 2 merupakan proses enkripsi pada perancangan yang dilakukan. Tahap persiapan dan langkah-langkah dalam proses enkripsi dan dekripsi perancangan kriptografi pembangkit kunci dijelaskan sebagai berikut :

a) Menyiapkan plainteks.
b) Fungsi linier

$$f(x) = ax + b$$

c) Menyiapkan fungsi bessel jenis pertama orde-n

$$J_n(x) = x^n \sum_{m=0}^{\infty} \frac{(-1)^m x^{2m}}{2^{2m+n}.m!(n+m)!} \text{ untuk setiap } n \geq 0$$

d) Menyiapkan fungsi legendre menggunakan polinomial legendre derajat-n dinotasikan sebagai $P_n(x)$

$$P_n(x) = \sum_{m=0}^{M} (-1)^m \frac{(2n-2m)!}{2^n m!\,(n-m)!\,(n-2m)!} x^{n-2m}$$

dimana $M = n/2$ atau $(n-1)/2$ adalah bilangan bulat.

e) KunciTop :

$$(\xi_1 + \xi_2 + \ldots + \xi_q) \,.\, \alpha$$

$(\xi_{i\,;i=1\ldots q})$

$\alpha \in \mathbb{R}$ adalah bilangan dari ASCII

f) Kunci Slot :

Slot = $k^t$ ; $t, k > 0$

Dibawah ini dijelaskan langkah-langkah secara garis besar dalam proses enkripsi:

a) Plainteks ($P_{tx}$) dikonversi ke dalam kode ASCII, diperoleh Persamaan 3

$$C_1 = \{x_1, x_2, \ldots, x_n\} \quad (3)$$

b) Diambil $f(x) = ax + b$ sebagai FUNGSI. Selanjutnya mengecek $f(x)$ mempunyai invers, maka fungsi tersebut dapat digunakan. Dimisalkan hasil subtitusi ($C_1$) yang disubstitusikan kedalam fungsi, diperoleh Persamaan 4

$$C_2 = \{y_1, y_2, \ldots, y_n\} \quad (4)$$

c) Hasil dari Persamaan (4) diambil sebagai ($\ell$) yang akan dilakukan proses Convert Between Base tahap 1, dinotasikan ($CBB_1$). Dimana KunciTop dan KunciLegendere sebagai kunci, diperoleh Persamaan 5

$$C_3 = \{z_1, z_2, \ldots, z_m\} \quad (5)$$

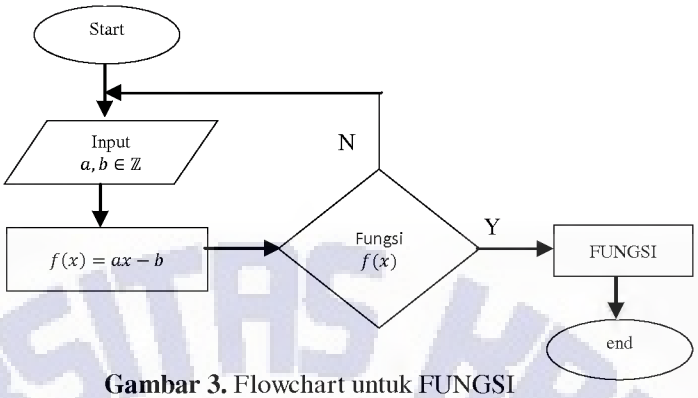
d) Konversi yang diperoleh dari $C_3$, selanjutnya juga dilakukan konversi tahap 2 ($CBB_2$), dengan slot dan KunciBessel diperoleh Persamaan 6

$$C_4 = \{r_1, r_2, \ldots, r_p\} \quad (6)$$

e) Bilangan-bilangan di $C_4$ dikonversi dalam bilangan bit (binary digit), sehingga dihasilkan cipherteks diperoleh dari Persamaan 7

$$C_{tx} = \{\ldots\ldots\} \quad (7)$$

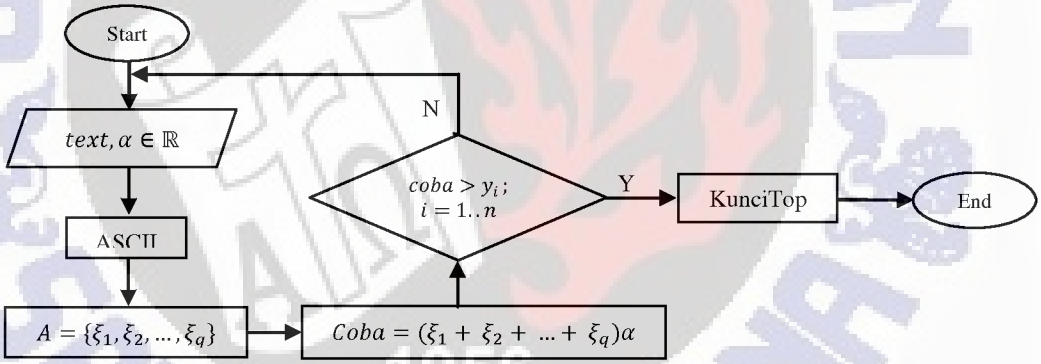
Pada Gambar 2 terdapat beberapa operasi yang perlu ditunjukkan proses kerjanya, seperti proses FUNGSI, KunciTop, KunciLegendre, Slot, dan KunciBessel. Oleh karena itu berikut akan diberikan dalam bentuk flowchart.




**Gambar 3.** Flowchart untuk FUNGSI

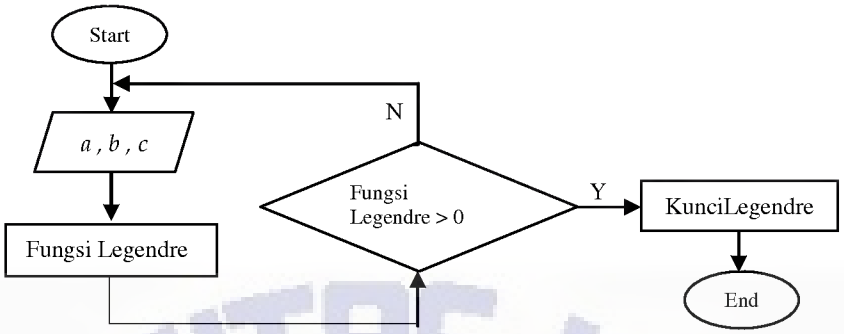
Pada Gambar 3 dapat dijelaskan alur kerja dari FUNGSI dengan input nilai $a, b \in \mathbb{Z}$ ke dalam persamaan fungsi linier. Selanjutnya jika fungsi mempunyai invers maka fungsi tersebut dapat digunakan sebaliknya jika fungsi tidak memiliki nilai invers maka proses inputan akan di ulang.

Sedangkan flowchart untuk menentukan KunciTop dan KunciLegendre ditunjukkan pada Gambar 4 dan Gambar 5.




**Gambar 4.** Flowchart KunciTop

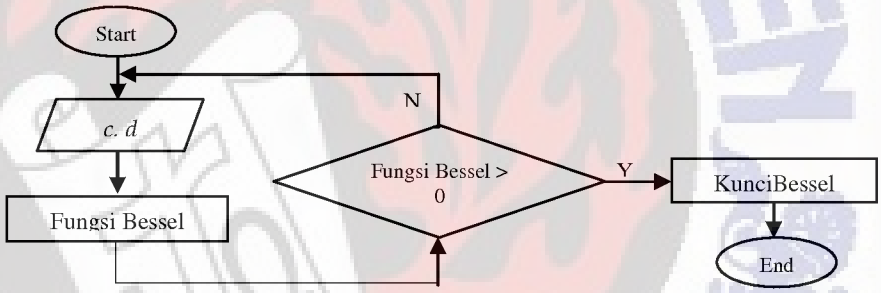
Pada Gambar 4 dapat dijelaskan alur kerja dari kunciTop dengan input nilai $text, \alpha \in \mathbb{R}$ selanjutnya teks $\xi_1 + \xi_2 + \dots + \xi_q$ ; n = banyak karakter Setelah itu setiap $\xi_{i,\ i=1\dots n}$ dikonversi ke dalam kode ASCII menghasilkan nilai $A = \{\xi_1, \xi_2, \dots, \xi_q\}$.




**Gambar 5.** Flowchart KunciLegendre

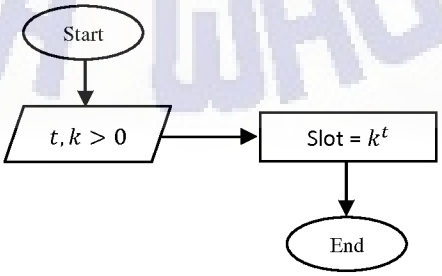
Gambar 5 merupakan alur kerja dari KunciLegendre dengan input nilai a , b , c ke dalam fungsi legendre jika nilai fungsi legendre lebih besar dari nol maka KunciLegendre tersebut dapat digunakan dan jika tidak lebih besar dari nol maka proses akan diulang.

Selanjutnya Gambar 6 dan Gambar 7 menunjukkan flowchart untuk menentukan KunciBessel dan slot.




**Gambar 6.** Flowchart KunciBessel

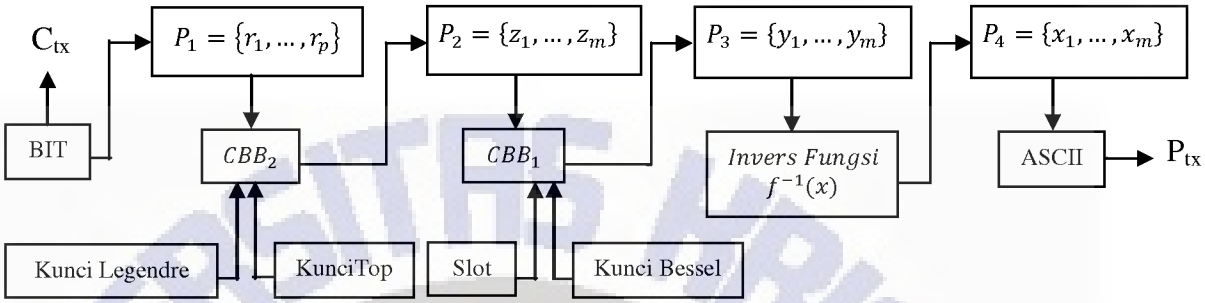
Pada Gambar 6 dapat dijelaskan alur kerja dari KunciBessel dengan input nilai c, d ke dalam fungsi bessel jika proses fungsi bessel lebih besar dari nol maka KunciBessel tersebut dapat digunakan dan jika tidak lebih besar dari nol maka proses akan diulang.




**Gambar 7.** Flowchart Slot

Pada Gambar 7 dapat dijelaskan alur kerja dari Kunci slot dengan input nilai $t, k > 0$ jika nilai slot lebih besar dari nol maka ke proses selanjutnya dimana Slot = $k^t$ diperoleh

Proses dekripsi menggunakan fungsi bessel dan fungsi legendre, ditunjukkan dalam bentuk skema diagram pada Gambar 8.




**Gambar 8** Skema Diagram Dekripsi

Gambar 8 menunjukkan proses dekripsi dari perancangan kriptografi simetris ini. Proses dekripsi merupakan proses kebalikan dari proses enkripsi dimana cipherteks yang diperoleh dikonversi balik menggunakan fungsi bessel dan fungsi legendre, kuncitop dan slot kemudian disubstitusikan ke dalam invers fungsi selanjutnya diekuivalensi ke dalam kode ASCII sehingga output yang dihasilkan berupa teks yang berkorespodensi dengan cipherteks. Invers Fungsi linear yang digunakan dalam proses dekripsi yaitu :

Langkah-langkah dalam proses dekripsi berdasarkan skema diagram pada Gambar 8, dijelaskan sebagai berikut :

f) Ciphertext ($C_{tx}$) dikonversi balik, akan membentuk urutan bilangan pada Persamaan 8
$P_1 = \{r_1, r_2, \dots, r_p\}$. (8)

g) Hasil dari $P_1$, kemudian dilakukan proses $CBB_2$, dengan kunciLegendre dan kunciTop pada Persamaan 9
$P_2 = \{z_1, z_2, \dots, z_m\}$. (9)

h) Persamaan (9) diambil sebagai ($\ell$) yang akan dilakukan proses $CBB_1$. Dimana slot dan KunciBessel sebagai kunci, diperoleh Persamaan 10
$P_3 = \{y_1, y_2, \dots, y_m\}$. (10)

i) Invers fungsi dari FUNGSI dimisalkan $f^{-1}(x)$, kemudian hasil dari $P_3$ disubstitusikan kedalam $f^{-1}(x)$, diperoleh Persamaan 11
$P_4 = \{x_1, x_2, \dots, x_m\}$. (11)

j) Bilangan yang diperoleh dari $P_4$ diekuivalensi dengan ASCII maka diperoleh plainteks, yang dinotasikan pada Persamaan 12
$P_{tx} = \{\dots \dots\}$ (12)

## 4. Hasil dan Pembahasan

Untuk menguji perancangan kriptografi simetris sebagai sebuah teknik kriptografi, dilakukan proses enkripsi-dekripsi. Proses dilakukan sesuai dengan langkah-langkah yang telah dilakukan pada Gambar 1.

Berikut adalah tahap persiapan yaitu tahap yang dilakukan sebelum proses enkripsi-dekripsi dilakukan :

a) Plainteks yang digunakan adalah UKSW
b) Fungsi linier : $f(x) = 2x - 5$
c) KunciTop : $(\xi_1 + \xi_2 + \ldots + \xi_q) . \alpha$
   $(\xi_{i\,;i=1\ldots q})$
   $\alpha \in \mathbb{R}$ adalah bilangan dari ASCII
d) Fungsi Legendre sebagai kunci $(\mathbf{LegendreP}(1.2, 1.6))$ : 1826378427
e) Fungsi Bessel sebagai kunci $(\mathbf{BesselJ}(0.5, 1.5))$ : 6498380748
f) Slot sebagai kunci : Slot = $k^t$ ; $t, k > 0$

Setelah tahap persiapan kunci dilakukan, kemudian lakukan proses enkripsi-dekripsi.

1. Plainteks yang digunakan UKSW
   Dengan mengikuti Persamaan (3), plainteks tersebut dikonversi dalam bentuk ASCII sehingga memperoleh
   $C_1 = \{85, 75, 83, 87\}$ (13)
2. Selanjutnya hasil dari Persamaan (13) disubstitusikan ke dalam FUNGSI $f(x) = 2x - 5$, (sesuai dengan Pers. (4)) diperoleh
   $C_2 = \{165, 145, 161, 169\}$ (14)
3. Dari Pers. (5), dengan mengambil $\ell = C_2$, KunciLegendre = 1826378427, dan KunciTop = 646 hasil pada C2 diperoleh
   $C_3 = \{156, 184, 586, 630, 482, 270, 87, 625, 147, 223, 81\}$ (15)
4. Dengan mengikuti aturan pada Persamaan (6), dipilih
   - slot = $17^{31}$ =139288917338851014461418017489467720433.
   - KunciBesel = 6498380748.

   Sehingga diperoleh
   $C_4 = \{8916758637495456908219537258780534726 2,$
   $8776431492643895064538910645389106405754344121,$
   $\{560664979109199484643093\}$ (16)
5. Hasil dari Persamaan (16), dilakukan proses dengan Persamaan (7) diperoleh
   $C_{tx} = \{0, 1, 1\}$ (17)
   Sehingga diperoleh cipherteks adalah 0, 1, 1

Selanjutnya akan dilakukan proses dekripsi. Karena dirancang kriptografi simetris maka kunci yang digunakan adalah sama. Berikut ditunjukkan proses dekripsi.

- Dengan mengikuti aturan (f) pada Persamaan (8), sehingga diperoleh
  $P_4 = \{8916758637495456908219537258780534726 2,$
  $8776431492643895064538910640575434412 1,$
  $5606649791091994846430 93\}$ (18)

- KunciBessel dan Slot digunakan sebagai basis untuk proses $CBB_2$ dengan mengambil $\ell = P_4$ sebagai urutan bilangan, sehingga diperoleh
  $P_3 = \{156, 184, 586, 630, 482, 270, 87, 625, 147, 223, 81\}$ (19)

- Mengacu pada aturan (h), maka hasil dari Persamaan (19) dilakukan proses $CBB_1$ diperoleh
  $P_2 = \{165, 145, 161, 169\}$ (20)

- Hasil dari Persamaan (20), disubstitusikan ke dalam persamaan $f^{-1}(x) = (x + 5)/2$, maka hasilnya adalah
  $P_1 = \{85, 75, 83, 87\}$ (21)

- Tahapan akhir adalah mengekuivalensi Persamaan (21) kedalam kode ASCII diperoleh kembali plainteks UKSW.

Secara keseluruhan perancangan ini dapat melakukan proses enkripsi-dekripsi sehingga secara umum menjadi sebuah kriptografi dan memehuni syarat-syarat sebagai sistem kriptografi. Bagian selanjutnya menjelaskan secara rinci bagaimana perancangan ini memenuhi sebuah sistem kriptografi.

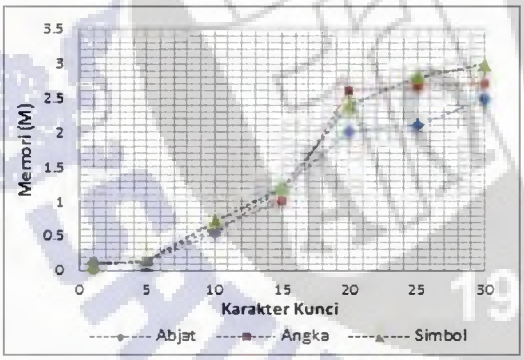
Sebuah kriptografi harus memenuhi 5 tuple **P**, **C**, **K**, **E**, **D**. Oleh karena itu akan ditunjukkan perancangan ini memenuhi kelima kondisi tersebut [8].

- **P** adalah himpunan berhingga dari plainteks. Rancangan kriptografi ini menggunakan plainteks berupa karakter yang ekuivalen dengan ASCII. Dan pada bilangan ASCII adalah sekumpulan karakter yang ekuivalen dengan sejumlah bilangan yang semuanya terbatas dalam sebuah himpunan yang berhingga. Maka dari itu jelas bahwa plainteks dari perancangan ini adalah himpunan berhingga.
- **C** adalah himpunan berhingga dari cipherteks. Cipherteks dihasilkan dalam elemen bit binner (bilangan 0 dan 1). Maka cipherteks perancangan ini juga merupakan elemen terbatas karena himpunan cipherteks hanya {0,1}, maka cipherteks kunci simetris menggunakan fungsi Bessel dan fungsi Legendre adalah himpunan berhingga [6].
- **K** merupakan ruang kunci (Keyspace), adalah himpunan berhingga dari kunci. Penggunaan kunci KunciBessel dan KunciLegendre adalah fungsi dan kunci tambahan lain seperti Slot dan KunciTop juga berupa fungsi. Maka dari itu kunci yang digunakan juga himpunan berhingga.

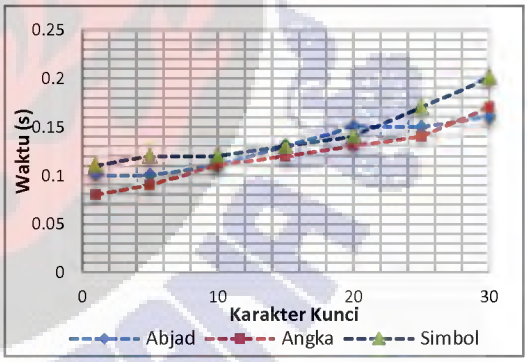
- Untuk setiap $k \in K$, terdapat aturan enkripsi $e_k \in \boldsymbol{E}$ dan berkorespodensi dengan aturan dekripsi $d_k \in \boldsymbol{D}$. Setiap $e_k: P \longrightarrow C$ dan $d_k: C \longrightarrow P$ adalah fungsi sedemikian hingga $d_k\big(e_k(x)\big) = x$ untuk setiap plainteks $x \in P$.
  Kondisi ke-4 ini secara menyeluruh, terdapat kunci yang dapat melakukan proses enkripsi sehingga merubah plainteks menjadi cipherteks. Dan dapat melakukan proses dekripsi yang merubah cipherteks ke plainteks.
  Berdasarkan penjelasan di atas, terbukti bahwa proses perancangan kriptografi kunci simetris menggunakan fungsi bessel dan fungsi legendre memenuhi syarat sebuah kriptografi.

  Kemudian akan dijelaskan mengenai penggunaan kedua fungsi tersebut sebagai kunci dalam perancangan kriptografi. Fungsi bessel dan legendre menghasilkan bilangan pecahan desimal. Bilangan pecahan desimal memiliki keunikan tersendiri karena mempunyai sisa pembagian. Hal ini yang membuat hingga saat ini tidak ada teknik kriptografi yang menggunakannya sebagai kunci. Keunikan ini yang dipilih sehingga harapannya akan mempersulit kriptanalisis dengan teknik untuk menebak kunci dan tentu juga memecahkannya.

Selanjutnya dilakukan pengujian terhadap kunciTop. KunciTop merupakan kunci yang inputannya berupa karakter, perancangan ini dapat memberikan kebebasan bagi user untuk memilih kunci yang akan digunakan. Karakter KunciTop dapat berupa abjad, angka, dan simbol.




**Gambar 9** Banyak Karakter KunciTop (abjad, angka, simbol) vs Memori




**Gambar 10** Banyak Karakter KunciTop (abjad, angka, simbol) vs Waktu.

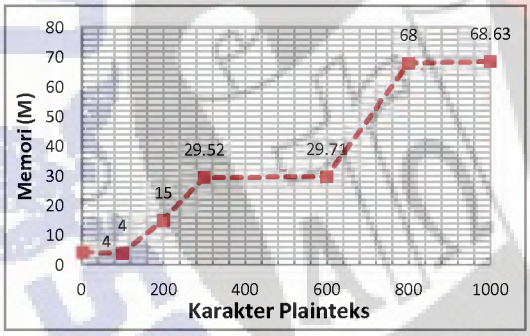
Gambar 9 maupun Gambar 10, jika dianalisa kebutuhan memory dan waktu yang diperlukan terhadap kunciTop.Yang terdiri dari tiga jenis karakter yang diinputkan antarara lain karakter abjad, angka dan simbol. Pada karakter abjad dari jumlah 1 sampai 30 adalah 2,5 M, dan waktu yang dibutuhkan 0,16s, karakter angka dari jumlah 1 sampai 30 adalah 2,7M, waktu yang dibutuhkan 0,17s sedangkan karakter simbol dari jumlah 1 sampai 30 adalah 3M, waktu yang dibutuhkan 0,2s. Rata-rata memory dan waktu yang dibutuhkan dari ketiga jenis karakter ini adalah sebesar 2,73M dan 0,17s.

Pengujian selanjutnya dilakukan pengujian peran kunci slot dalam perancangan kriptografi ditunjukkan pada Tabel 1.

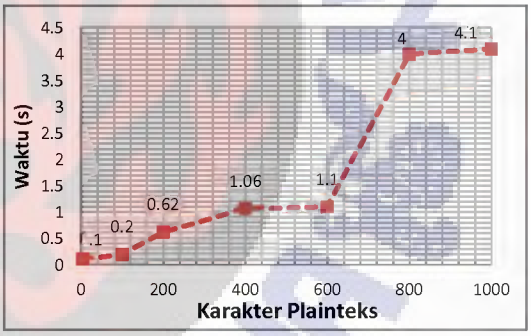
**Tabel 1** Slot vs Cipherteks

| No | Karakter Plainteks | Slot | Banyak Cipherteks |
|---|---|---|---|
| 1 | 72 | $17^{17}$ | 109 |
| 2 | 72 | $17^{32}$ | 58 |
| 3 | 72 | $17^{51}$ | 37 |
| 4 | 72 | $17^{151}$ | 13 |
| 5 | 72 | $17^{2513}$ | 1 |

Kriptografi ini, dirancang agar plainteksnya berupa bit dan elemen bit yang dihasilkan relatif sedikit. Slot memainkan peran yang besar dalam menentukan banyaknya cipherteks. Tabel 1 menunjukkan bahwa semakin besar slot digunakan sebagai kunci akan membuat karakter cipherteks semakin kecil. Relasi ini membuat kriptanalisis sulit untuk melihat hubungan antara plainteks dan cipherteks. Setelah aplikasi selesai dibuat, dilakukan pengujian banyak pesan terhadap waktu dan memory yang dibutuhkan ditunjukkan pada Gambar 11 dan Gambar 12.




**Gambar 11** Banyak Karakter Plainteks vs Memori




**Gambar 12** Banyak Karakter Plainteks vs Waktu

Hasil pada Gambar 11 dan Gambar 12, menunjukkan perbandingan karakter input memori dan waktu terhadap banyak karakter plainteks perancangan ini, seperti biasanya bahwa banyaknya karakter plainteks yang diberikan akan mempengaruhi pada kebutuhan memory dan waktu. Misalnya pada memory inputan karakter berjumlah 0 sampai 1000 maka memory yang dibutuhkan adalah 68,63 M, sedangkan pada perbandingan waktu dari inputan karakter 0 sampai 1000 maka waktu yang dibutuhkan adalah 4,1s. Rata-rata memory dan waktu yang dibutuhkan adalah sebesar 31,26 M dan 1,6s. Jadi semakin banyak karakter plainteks akan membutuhkan waktu dan ruang memori yang semakin banyak.

## 5. Simpulan

Perancangan kriptografi dengan menggunakan fungsi Bessel dan fungsi Legendre berhasil menjadi sebuah teknik kriptografi simetris, dan dapat

dikategorikan sebagai kriptografi modern karena menghasilkan cipherteks dalam elemen bit.

## 6. Daftar Pustaka


[1] Barkan, E., & Biham, E., 2002, In How Many Ways Can You Write Rijndael?, Advances in Cryptology, procigings of Asiacryp 2002, Lectture Notes in Computer Science 2501, Springer-Verlag, pp. 160-175. (http://link.springer.com/chapter/10.1007/3-540-36178-2_10), Diakses pada tanggal 3 Mei 2013.

[2] Biham, E., & Kilier, N., 2004, Cryptanalysis of Reduced Variants of Rijndael, Haifa: Computer Science Department, Technion Israel Institute of Technology. (http://madchat.fr/crypto/codebreakers/35-ebiham.pdf ), Diakses pada tanggal 3 Mei 2013.

[3] Dafid, 2006, Kriptografi Kunci Simetris Dengan Menggunakan Algoritma Crypton, Jurnal Ilmiah STIMIK GI MDP, Volume 2 Nomor 3, Oktober 2006.

[4] Putri, Sila Wiyanti, 2006, Rancangan Algoritma Kriptografi Simetri Dengan Menggunakan Derivasi Algoritma Klasik Subtitusi, Bandung: Institut Teknologi Bandung, http://informatika.stei.itb.ac.id. Diakses pada tanggal 20 Juli 2013.

[5] Bruce Schneier, 1996, AppliedCryptograp by: Protocols, Algorithms, and Source Code in C, USA: John Wiley & Sons, Inc.

[6] Spiegel, M., 1968, Mathematical Handbook of Formulas and Tables, (Schaum Series), New York: McGraw-Hill.

[7] Maplesoft, 2010, Convert/Base: Convert Between Base, Maple-14, Waterloo: Waterloo Maple Inc.

[8] Stinson, D.R., 1995, Cryptography Theory and Practice, Florida: CRC Press, Inc.