Pemilihan Metode Kriptografi Menggunakan *Fuzzy* MCDM

Artikel Ilmiah

Peneliti :
Willson Mangoki (672010101)
Magdalena A. Ineke Pakereng, M.Kom.
Alz Danny Wowor, S.Si., M.Cs.

Program Studi Teknik Informatika
Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Salatiga
April 2016

Pemilihan Metode Kriptografi Menggunakan *Fuzzy*-MCDM

Artikel Ilmiah

Diajukan kepada
Fakultas Teknologi Informasi
Untuk memperoleh gelar Sarjana Komputer

Peneliti :
Willson Mangoki (672010101)
Magdalena A. Ineke Pakereng, M.Kom.
Alz Danny Wowor, S.Si., M.Cs.

Program Studi Teknik Informatika
Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Salatiga
April 2016

Lembar Pengesahan

Lembar Pengesahan

Judul Tugas Akhir	: Pemilihan Metode Kriptografi Menggunakan *Fuzzy* MCDM
Nama Mahasiswa	: Willson Mangoki
NIM	: 672010101
Program Studi	: Teknik Informatika
Fakultas	: Teknologi Informasi

Menyetujui,

Magdalena A. Ineke Pakereng, M.Kom.	Alz Danny Wowor, S.Si., M.Cs.
Pembimbing 1	Pembimbing 2

Mengesahkan,

Dr. Dharmaputra T. Palekahelu, M.Pd.	Suprihadi, S.Si., M.Kom.
Dekan	Ketua Program Studi

Dinyatakan Lulus Ujian tanggal: 21 April 2016

Penguji:

1. Hindriyanto Dwi Purnomo, S.T., MIT., Ph.D. _____
2. Evangs Mailoa, S.Kom., M.Cs. _____

Pemilihan Metode Kriptografi Menggunakan *Fuzzy* MCDM

Oleh,

Willson Mangoki
NIM : 672010101

ARTIKEL ILMIAH

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

Disetujui oleh,

Magdalena A. Ineke Pakereng, M.Kom.	Alz Danny Wowor, S.Si., M.Cs.
Pembimbing 1	Pembimbing 2

Diketahui oleh,

Dr. Dharmaputra T. Palekahelu, M.Pd.	Suprihadi, S.Si., M.Kom.
Dekan	Ketua Program Studi

FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN SATYA WACANA
SALATIGA
2016

Lembar Publish Jurnal

FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN SATYA WACANA
Jalan Diponegoro 52 – 60
Phone. (0298) 321212 (Hunting)
Fax. (0298) 321433
E-mail: fti@uksw.edu
Salatiga 50711 – INDONESIA

LEMBAR PERSETUJUAN PUBLISH JURNAL

Dengan mempertimbangkan isi dari jurnal mahasiswa :

Nama Mahasiswa : Willson Mangobi
NIM : 672010101.

Maka jurnal ini dinyatakan :

LAYAK TERBIT / ~~TIDAK LAYAK TERBIT~~

Menyetujui,

(M.A Thesa P, M.Kom.)	(Alb Dany W, M.Cs.)
Pembimbing 1	Pembimbing 2

Mengetahui,

(Hindriyanto D.P, Ph.D.)	(Evanys Mailoa, M.Cs.)
Penguji 1	Penguji 2

Lembar Pernyataan Persetujuan Akses

PERPUSTAKAAN UNIVERSITAS
UNIVERSITAS KRISTEN SATYA WACANA
Jl. Diponegoro 52 – 60 Salatiga 50711
Jawa Tengah, Indonesia
Telp. 0298 – 321212, Fax. 0298 321433
Email: library@adm.uksw.edu ; http://library.uksw.edu

PERNYATAAN PERSETUJUAN AKSES

Saya yang bertanda tangan di bawah ini:

Nama : WILLSON MANGOKI
NIM : 672010101 Email : 672010101@student.uksw.edu
Fakultas : TEKNOLOGI INFORMASI Program Studi : TEKNIK INFORMATIKA
Judul tugas akhir : PEMILIHAN METODE KRIPTOGRAFI MENGGUNAKAN FUZZY MEDM

Dengan ini 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 sebagai berikut (beri tanda pada kotak yang sesuai):

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

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

* *Hak yang tidak terbatas hanya bagi satu pihak saja. Pengajar, peneliti, dan mahasiswa yang menyerahkan hak non-eksklusif kepada Repositori Perpustakaan Universitas saat mengumpulkan hasil karya mereka masih memiliki hak copyright atas karya tersebut.*

** *Hanya akan menampilkan halaman judul dan abstrak. Pilihan ini harus dilampiri dengan penjelasan/ alasan tertulis dari pembimbing TA dan diketahui oleh pimpinan fakultas (dekan/kaprodi).*

Demikian pernyataan ini saya buat dengan sebenarnya.

Salatiga, 27 MEI 2016

WILLSON MANGOKI
Tanda tangan & nama terang mahasiswa

Mengetahui,

M. A. Indra Putra
Tanda tangan & nama terang pembimbing I

ALB DANNY WR.
Tanda tangan & nama terang pembimbing II

F-LIB-081

Lembar Persetujuan Publikasi

PERNYATAAN PERSETUJUAN PUBLIKASI
TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

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

Nama : WILLSON MANGOKI
NIM : 67201101
Program-studi : TEKNIK INFORMATIKA
Fakultas : TEKNOLOGI INFORMASI
Jenis karya : Skripsi/ ~~Tesis/ Disertasi~~ (Coret yang tidak sesuai)

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada UKSW **Hak bebas royalti non-eksklusif** ***(Non-exclusive royalty free right)*** atas karya ilmiah saya yang berjudul:

PEMILIHAN METODE KRIPTOGRAFI MENGGUNAKAN FUZZY MCDM

beserta perangkat yang ada (jika diperlukan).

Dengan hak bebas royalti non-eksklusif ini, UKSW berhak menyimpan, mengalihmedia/ formatkan, mengelola dalam bentuk pangkalan data, merawat, dan mempublikasikan tugas akhir saya, selama tetap mencantumkan nama saya sebagai penulis/ pencipta dan sebagai pemilik hak cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : SALATIGA
Pada tanggal : 30 MEI 2016

Yang menyatakan

WILLSON MANGOKI

Mengetahui,

Pembimbing I	Pembimbing II
M. A. Maylie Rakes	ALB DANNY WOWOR

Lembar Pernyataan Tidak Plagiat

PERPUSTAKAAN UNIVERSITAS
UNIVERSITAS KRISTEN SATYA WACANA
Jl. Diponegoro 52 – 60 Salatiga 50711
Jawa Tengah, Indonesia
Telp. 0298 – 321212, Fax. 0298 321433
Email: library@adm.uksw.edu ; http://library.uksw.edu

PERNYATAAN TIDAK PLAGIAT

Saya yang bertanda tangan di bawah ini:

Nama : WILLSON MANGOKI

NIM : 672010101 Email : 672010101@student.uksw.edu

Fakultas : TEKNOLOGI INFORMASI Program Studi : TEKNIK INFORMATIKA

Judul tugas akhir : PEMILIHAN METODE KRIPTOGRAFI MENGGUNAKAN FUZZY MCDM

Pembimbing : 1. MAGDALENA A INEKE PAKERENG, M.Kom

2. ALB DANNY WOWOR, S.Si., M.Cs.

Dengan ini 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.

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, 27 MEI 2016

WILLSON MANGOKI

Tanda tangan & nama terang mahasiswa

F-LIB-080

Pemilihan Metode Kriptografi Menggunakan *Fuzzy*-MCDM

[1]Willson Mangoki, [2]Magdalena A. Ineke Pakereng, [3]Alz Danny Wowor
Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Jl. Diponegoro 52-60, Salatiga 50771, Indonesia
Email: [1]672010101@student.uksw.edu, [2]ineke.pakereng@staff.uksw.edu,
[3]alzdanny.wowor@staff.uksw.edu

Abstract

Cryptography is a technique of data security by encrypting certain information so can be kept confidential. Lot of cryptographic techniques has been created, but does not fulfill multiple testing variables such as the avalanche effect, correlation, frequency and differentation. Each test become an important indicator to determine how good a cryptography are. This research designed a system using Fuzzy MCDM to test block cipher cryptography with multiple variable testing to be filled at once. The results of this research can be be used to determine cryptography based on testing using some criteria that already mentioned.

***Key Words**: Cryptography, Avalanche Effect, Fuzzy*-MCDM, *Block Cipher*

Abstrak

Kriptografi merupakan teknik pengamanan data dengan mengenkripsi informasi tertentu sehingga terjaga kerahasiaannya. Telah banyak teknik kriptografi yang diciptakan, namun belum memenuhi beberapa variabel pengujian seperti *avalanche effect*, korelasi, frekuensi, dan diferensiasi. Setiap pengujian menjadi indikator penting untuk mengetahui seberapa baik suatu kriptografi. Penelitian ini merancang sebuah sistem menggunakan *Fuzzy* MCDM untuk menguji kriptografi berbasis *block cipher* dengan beberapa variabel pengujian untuk dipenuhi sekaligus. Hasil dari penelitian ini dapat digunakan untuk memilih kriptografi berdasarkan pengujian dengan menggunakan kriteria-kriteria seperti yang telah disebutkan.

Kata Kunci: Kriptografi, *Avalanche Effect, Fuzzy*-MCDM, *Block Cipher*

---

[1]Mahasiswa Program Studi Teknik Informatika, Fakultas Teknologi Informasi Universitas Kristen Satya Wacana, Salatiga.
[2]Staff pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga.
[3]Staff pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga.

UNIVERSITAS KRISTEN
SATYA WACANA
1956

1. Pendahuluan

Kriptografi merupakan teknik pengamanan data dengan mengenkripsi informasi tertentu sehingga terjaga kerahasiaannya. Hal ini dimaksudkan agar tidak terjadi kebocoran informasi kepada pihak-pihak yang tidak diinginkan.

Algoritma *block cipher* menggabungkan beberapa teknik kriptografi klasik dalam eknkripsi dan dekripsinya, antara lain subtitusi, transposisi atau permutasi, ekspansi, dan kompresi. Metode lain yang digunakan yakni dengan menggunakan pola-pola tertentu sebagai proses pengacakan bit dan kunci hingga memperoleh nilai keacakan yang cukup baik untuk diimplementasikan dalam bahasa pemrograman [1]. Kriptografi telah banyak diciptakan, namun belum memenuhi beberapa variabel pengujian seperti *avalanche effect*, korelasi, frekuensi, dan diferensiasi. Setiap pengujian menjadi indikator penting untuk mengetahui seberapa optimal suatu kriptografi. Oleh karena itu perlu dilakukan sebuah penelitian untuk memenuhi pengujian-pengujian tersebut secara keseluruhan.

Tujuan dari penelitian ini adalah merancang sebuah sistem menggunakan *Fuzzy* MCDM untuk menguji kriptografi berbasis *block cipher* dengan variabel pengujian berupa *avalanche effect*, korelasi, frekuensi, dan diferensiasi untuk dipenuhi sekaligus hingga diperoleh kriptografi yang optimal.

2. Tinjauan Pustaka

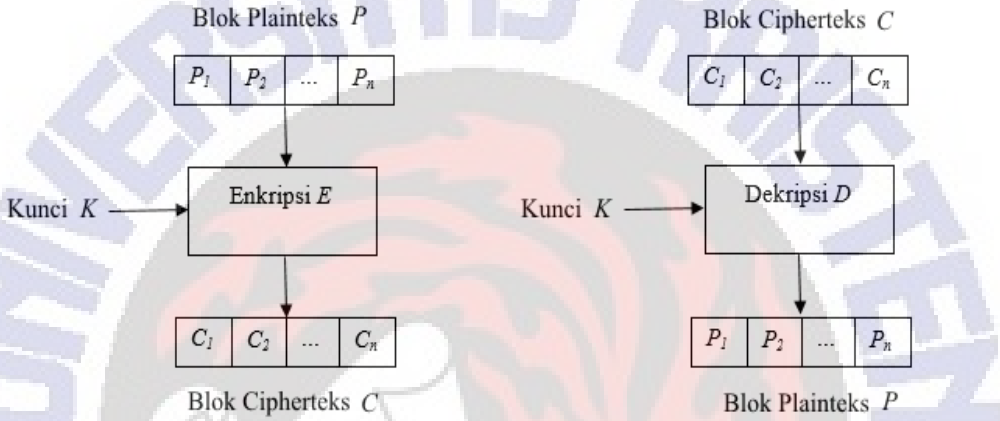
Landasan dari penelitian yang dilakukan sekarang ini merujuk pada penelitian-penelitian sebelumnya.

Penelitian pertama dengan judul "*Designing an Algorithm with High Avalanche Effect*". Dalam penelitian ini dirancang sebuah algoritma dengan menggabungkan teknik kriptografi klasik dan algoritma kriptografi modern, seperti dalam penggunaan kunci. Algoritma ini menggunakan 64-bit kunci, ataupun lebih. Pesan atau *plaintext* yang akan dienkripsi dibagi ke dalam 64-bit blok. Hasil perbandingan algoritma yang dirancang dan algoritma lainnya seperti DES, *avalanche effect* lebih tinggi 70.31 % [2]. Penelitian pertama digunakan sebagai acuan untuk pengujian *avalanche effect*.

Penelitian kedua dengan judul "Perancangan Kriptografi *Block Cipher* pada Teknik Burung Terbang". Penelitian tersebut merancang *Block Cipher* dengan mengadopsi pola ketika burung terbang berkelompok membentuk formasi "V" untuk proses pengambilan bit dari kotak 64-bit. Penelitian ini melakukan 4 putaran dimana setiap putaran melakukan proses untuk plainteks dan juga proses kunci. Hasil dari kedua proses tersebut akan dilakukan proses XOR sehingga pada putaran ke empat akan mendapatkan cipherteks Rancangan kriptografi ini membandingkan plainteks sebagai input dan cipherteks sebagai hasil ekripsi, dengan nilai keacakan -0.3193 dan nilai diferensiasi sebesar -8.8571 [3]. Penelitian ini dijadikan sebagai acuan untuk pengujian nilai diferensiasi dan nilai korelasi data antara plainteks dan cipherteks.

Bagian selanjutnya akan dijelaskan teori-teori atau pustaka terkait yang digunakan dalam penelitian ini.

Ilmu dan seni dari menjaga keamanan pesan adalah kriptografi, yang dilakukan oleh kriptografer. Kriptanalis adalah pelaku kriptanalisis yaitu teknik memecahkan cipherteks. Cabang matematika yang mengarahkan keduanya disebut kriptologi [4]. *Block cipher* digolongkan sebagai kriptografi moderen, input dan output dari algoritma *block cipher* berupa *block* dan setiap *block* terdiri dari beberapa bit (1 *block* terdiri dari 64-bit atau 128-bit) [5]. *Block cipher* juga merupakan algoritma kunci simetri atau kriptografi kunci private, dimana kunci untuk enkripsi sama dengan kunci untuk dekripsi [6]. Skema proses enkripsi dan dekripsi *block cipher* secara umum dapat digambarkan pada Gambar 1.



Gambar 1 Skema Proses Enkripsi dan Dekripsi Pada Block Cipher [6]

Misalkan blok plainteks (*P*) yang berukuran *m* bit dinyatakan sebagai vector [6]:

$$P = (p_1, p_2, \ldots, p_m) \quad (1)$$

yang dalam hal ini p_i adalah 0 atau 1 untuk i = 1, 2, …, *m*, dan blok cipherteks (C) adalah

$$C = (c_1, c_2, \ldots, c_m) \quad (2)$$

yang dalam hal ini c_i adalah 0 atau 1 untuk i = 1, 2, …, *m*. Bila plainteks dibagi menjadi *n* buah blok, barisan blok-blok plainteks dinyatakan sebagai

$$(P_1, P_2, \ldots, P_n) \quad (3)$$

Untuk setiap blok plainteks P_i, bit-bit penyusunnya dapat dinyatakan sebagai vektor:

$$P_i = (p_{i1}, p_{i2}, \ldots, p_{im}) \quad (4)$$

Enkripsi dan dekripsi dengan kunci *K* dinyatakan berturut-turut dengan persamaan

$$E_K(P) = C \quad (5)$$

untuk enkripsi, dan

$$D_K(C) = P \tag{6}$$

untuk dekrpsi.

Fungsi *E* haruslah fungsi yang berkoresponden satu-ke-satu, sehingga

$$E^{-1} = D \tag{7}$$

Enkripsi dilakukan terhadap *block* bit plainteks menggunakan bit–bit kunci (yang ukuranya sama dengan *block* plainteks). Algoritma enkripsi menghasilkan *block* cipherteks yang sama dengan *block* plainteks. Dekripsi dilakukan dengan cara yang serupa seperti enkripsi. Kriptografi membentuk sebuah sistem yang dinamakan sistem kriptografi. Sistem kriptografi (*cryptosystem*) adalah kumpulan yang terdiri dari algoritma kriptografi, semua plainteks dan cipherteks yang mungkin, dan kunci [6].

Korelasi merupakan suatu teknik statistik yang dipergunakan untuk mengukur kekuatan hubungan dua variabel dan juga untuk mengetahui bentuk hubungan antara dua variabel tersebut dengan hasil yang sifatnya kuantitatif. Kekuatan hubungan antara dua variabel biasanya disebut dengan koefisien korelasi dan dilambangkan dengan simbol "r". Nilai koefisien r akan selalu berada diantara -1 sampai +1 sehingga diperoleh persamaan

$$-1 \leq r \leq +1 \tag{8}$$

Berdasarkan persamaan (8) maka secara matematis nilai r dapat diperoleh dari jumlah nilai selisih perkalian antara x dan y dengan hasil perkalian jumlah total x dan y dibagi dengan hasil akar kuadrat pangkat dua untuk jumlah total x kuadrat dengan kuadrat pangkat dua untuk jumlah total x dengan selisih jumlah y kuadrat dengan kuadrat pangkat dua untuk jumlah total y dimana x sebagai plainteks dan y sebagai cipherteks sehingga diperoleh persamaan (9) [7].

$$r = \frac{n\sum xy - (\sum x)(\sum y)}{\sqrt{\{n\sum x^2 - (\sum x)^2\}\{n\sum y^2 - (\sum y^2)\}}} \tag{9}$$

Diferensiasi data adalah perbandingan selisih antara dua titik. Dalam kalkulus, metode ini sering disebut sebagai turunan atau kemiringan dari data. Jika diberikan kumpulan data ((x_1,y_1), (x_2,y_2), (x_3,y_3), …, (x_n,y_n)) dengan syarat bahwa $x_i<x_{i+1}$ dimana i=1…*n*. Data-data tersebut dapat divisualisasikan dalam koordinat Cartesius untuk setiap *x* sebagai variabel bebas dan *y* atau kadang ditulis sebagai *f(x)* variabel tak bebas. Digunakan persamaan sebagai berikut untuk menentukan diferensiasi data pada dua titik:

$$\frac{\Delta y}{\Delta x} = \frac{(y_b - y_a)}{(x_a - x_b)} \tag{10}$$

dengan (x_a,y_a) sebagai titik pertama, dan titik berikutnya adalah (x_b,y_b).

Apabila terdapat n data maka dapat ditentukan dengan rata-rata dari diferensiasi data (Rataan diferensiasi (R_d)) menggunakan Persamaan (11).

$$R_d = \frac{(y_2 - y_1)/(x_2 - x_1) + (y_3 - y_2)/(x_3 - x_2) + \cdots + (y_n - y_{n-1})/(x_n - x_{n-1})}{n-1} \quad (11)$$

Tiap teknik enkripsi memiliki kelebihan dan kelemahan. Dalam rangka menerapkan teknik yang tepat dalam aplikasi tertentu kita dituntut untuk mengetahui kekuatan dan kelemahan tersebut. Oleh karena itu analisis teknik ini adalah kritis diperlukan. Suatu hal yang diinginkan dari setiap algoritma enkripsi adalah bahwa perubahan kecil baik dalam plainteks atau kunci harus menghasilkan perubahan yang signifikan pada cipherteks. Namun, perubahan satu bit dari plainteks atau kunci seharusnya menghasilkan perubahan besar pada bit dari cipherteks. Hal ini dikenal sebagai Avalanche Effect [8]. *Avalanche Effect* dapat dihitung dengan menggunakan persamaan (12).

$$AE = \frac{No.\ of\ Flipped\ Bit\ in\ Ciphertext}{No.\ of\ Bit\ in\ Ciphertext} \times 100\% \quad (12)$$

Dimana *Avalanche Effect* diperoleh dari jumlah bit yang berganti pada *ciphertext* dibagi dengan jumlah bit ciphertext, kemudian dikalikan dengan seratus persen (100%).

Analisis frekuensi memanfaatkan salah satu kelemahan *cipher* subtitusi yakni tidak bisa menyembunyikan hubungan statistik antara huruf-huruf plainteks dengan cipherteks. Huruf yang paling sering muncul di plainteks akan sering muncul pula di cipherteksnya [6].

Matriks perbandingan berpasangan adalah matriks berukuran n x n dengan elemen a_{ij} merupakan nilai relatif tujuan ke-i terhadap tujuan ke-j. Berikut diberikan matriks perbandingan berpasangan:

$$A = \begin{array}{c} \\ O_1 \\ \vdots \\ \vdots \\ O_j \\ \vdots \\ O_n \end{array} \begin{array}{c} \begin{array}{ccccc} O_1 & \cdots & O_j & \cdots & O_n \end{array} \\ \begin{bmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & a_{ii} & \vdots & a_{ik} & \vdots \\ a_{j1} & a_{ji} & a_{jj} & a_{jk} & a_{jn} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & \cdots & a_{nj} & \cdots & a_{nn} \end{bmatrix} \end{array}$$

Jika A adalah matriks konsisten, maka A dapat berupa matriks:

$$\begin{array}{c} \\ O_1 \\ O_2 \\ \vdots \\ O_n \end{array} \begin{array}{c} \begin{array}{cccc} O_1 & O_2 & \cdots & O_n \end{array} \\ \begin{bmatrix} \frac{w_1}{w_1} & \frac{w_1}{w_2} & \cdots & \frac{w_1}{w_n} \\ \frac{w_2}{w_2} & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ \frac{w_2}{w_2} & \frac{w_n}{w_2} & \cdots & \frac{w_n}{w_n} \end{bmatrix} \end{array}$$

dimana $w_i > 0$, i= 1,…,n adalah bobot tujuan ke- i. Secara umum vektor bobot $w=\{w_1,w_2,\ldots,w_n\}$ untuk n tujuan dapat diakomodasi matriks A dengan mencari solusi (non-trivial) dari himpunan n persamaan dengan n variable yang tidak diketahui sebagai berikut:

$$(A)(w^T)=(v)(w^T) \quad (13)$$

Jika A adalah matriks perbandingan tidak konsisten, maka vektor bobotnya:

$$(A)(w^T)=(n)(w^T) \quad (14)$$

dapat didekati dengan cara:

a. menormalkan setiap kolom j dalam matriks A, sedemikian hingga:

$\sum_i a_{ij} = 1$, disebut sebagai A’ (15)

b. untuk setiap baris i dalam A’, dihitung nilai rata-ratanya dengan:

$$w_i = \frac{1}{n}\sum_j a_{ij} \quad (16)$$

dengan w_i adalah bobot tujuan ke-i dari vektor bobot.

Untuk A adalah matriks perbandingan berpasangan, dan w adalah vektor bobot, maka konsistensi dari vektor bobot w dapat diuji sebagai berikut:

a. menghitung: $(A)(w^T)$

b. menghitung: $t = \frac{1}{n}\sum_{i=1}^{n}\left(\frac{elemen\ ke-i\ pada\ (A)(w^T)}{elemen\ ke-i\ pada\ w^T}\right)$

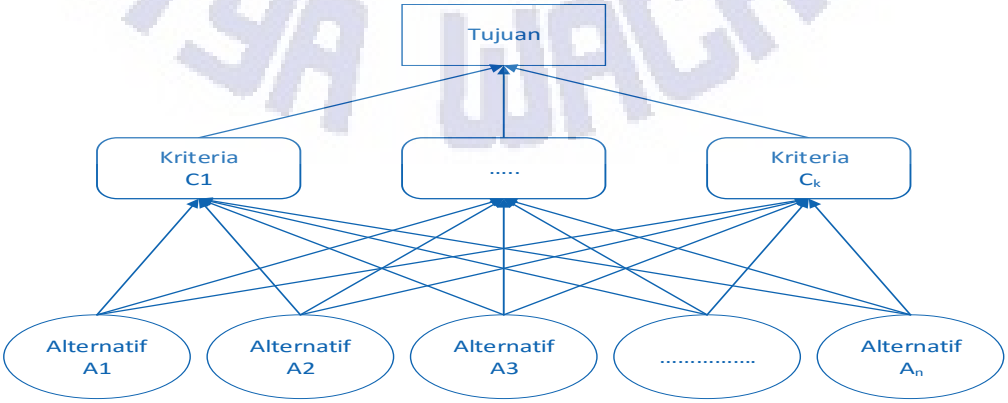
c. mengitung indeks konsistensi: $CI = \frac{t - n}{n - 1}$

d. jika CI=0 maka A konsisten, jika $\frac{CI}{RI_n} \leq 0.1$ maka A cukup konsisten; dan jika $\frac{CI}{RI_n} \geq 0.1$ maka A sangat tidak konsisten.

Indeks random RI_n adalah nilai rata-rata CI yang dipilih secara acak pada A dan diberikan sebagai:

n	2	3	4	5	6	7	⋯
RI_n	0	0.58	0.9	1.12	1.24	1.32	⋯

Fuzzy Multi Criteria Decision Making (MCDM) dikembangkan untuk membantu pengambil keputusan dalam melakukan pengambilan keputusan terhadap beberapa alternatif keputusan untuk mendapatkan suatu keputusan yang akurat dan optimal. Logika *fuzzy* adalah salah satu cabang dari AI (*Artificial Intelligence*). Logika *fuzzy* merupakan modifikasi dari teori himpunan dimana setiap anggotanya memiliki derajat keanggotaan yang bernilai kontinu antara 0 sampai 1. Sejak ditemukan pertama kali, logika *fuzzy* telah digunakan pada lingkup domain permasalahan yang cukup luas, seperti kendali proses, klasifikasi dan pencocokan pola, manajemen dan pengambil keputusan, riset operasi, ekonomi dan sebagainya. Sejak tahun 1985, terjadi perkembangan yang sangat pesat pada logika *fuzzy*, terutama dalam hubungan yang bersifat *non-linear*, *ill-defined*, *time-varying* dan situasi-situasi yang sangat kompleks. Metode ini membantu pengambil keputusan dalam melakukan pengambilan keputusan terhadap beberapa alternatif keputusan yang harus diambil dengan beberapa kriteria yang akan menjadi bahan pertimbangan [9]. Dalam kaitannya dengan pengambilan keputusan dari beberapa alternatif dengan banyak kriteria, pada penelitian ini digunakan *Fuzzy* MCDM.



Gambar 2. Diagram Representasi Masalah [10]

Berikut merupakan langkah-langkah yang dilakukan dalam merepresentasikan masalah berdasarkan Gambar 2.

a. Identifikasi tujuan keputusan, direpresentasikan dengan bahasa numeris sesuai dengan karakteristik dari masalah tersebut.

b. Identifikasi kumpulan alternatif keputusannya, jika ada n alternatif, maka dapat ditulis sebagai $A=\{A_i \mid i=1,2,...,n\}$.

c. Identifikasi kumpulan kriteria. Jika ada k kriteria, maka dapat ditulis $C=\{C_t|t=1,2,..,k\}$.

d. Membangun struktur hirarki masalah.

Evaluasi Himpunan *Fuzzy*, dimana dilakukan dengan menggunakan aturan sebagai berikut [10]

a. Memilih himpunan *rating* untuk bobot-bobot kriteria, dan derajat kococokan setiap alternatif dengan kriterianya. Himpunan *rating* terdiri atas 3 elemen, yaitu: 1) variabel linguistik (x) yang merepresentasikan bobot kriteria, dan derajat kecocokan alternatif dengan kriterianya; 2) Fungsi keanggotaan yang berhubungan dengan setiap elemen dari T(x). Fungsi keanggotaan untuk setiap *rating* ditentukan dengan menggunakan fungsi segitiga.

b. Mengevaluasi bobot-bobot pada setiap kriteria dan derajat kecocokan dari setiap alternatif terhadap kriteria.

c. Mengagregasi bobot-bobot kriteria, dan derajat kecocokan setiap alternatif dan kriterianya dengan metode mean. Penggunaan operator mean, Fi dirumuskan pada persamaan (13) sebagai berikut:

$$F_i = \left(\frac{1}{k}\right)\left[(S_{i1} \otimes W_1) \oplus (S_{i1} \otimes W_2) \oplus \ldots \oplus (S_{ik} \otimes W_k)\right] \quad (18)$$

dengan cara mensubtitusikan S_{it} dan W_t dengan bilangan *fuzzy* segitiga, yaitu $S_{it}=(o, p, q)$; dan $Wt=(at,bt,ct)$; maka F_t dapat didekati sebagai:

$$F_i \cong \left(\frac{1}{k}\right)\sum_{t=1}^{k}(o_{it}\, a_i) \quad (19)$$

$$Q_i = \left(\frac{1}{k}\right)\sum_{t=1}^{k}(p_{it}\, b_i) \quad (20)$$

$$Z_i = \left(\frac{1}{k}\right)\sum_{t=1}^{k}(q_{it}\, c_i) \quad (21)$$

Seleksi alternatif yang Optimal dilakukan dengan tahapan sebagai berikut:

a. Memprioritaskan alternatif keputusan berdasarkan hasil agregasi. Prioritas dari hasil agregasi dibutuhkan dalam rangka proses perangkaian alternatif keputusan. Misalkan F adalah bilangan *fuzzy* segitiga, F=(a,b,c) maka total nilai integral dapat dirumuskan sebagai berikut:

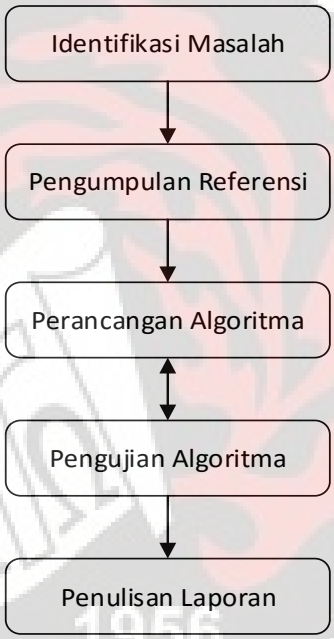
$$I_T^{\alpha}(F) = \frac{1}{2}(ac + b + (1-\alpha)a) \quad (22)$$

b. Nilai a adalah indeks keoptimisan yang merepresentasikan derajat keoptimalan bagi pengambil keputusan $0 \leq x \leq 1$ apabila nilai a semakin besar.

c. Memilih alternatif keputusan dengan prioritas tertinggi sebagai alternatif yang optimal.

3. Metode Penelitian

Tahapan-tahapan yang dibutuhkan yaitu: (1) Identifikasi Masalah, (2) Pengumpulan Referensi, (3) Perancangan Sistem, (4) Pengujian, dan (5) Penulisan Laporan.



Gambar 3. Tahapan Penelitian

Tahapan penelitian berdasarkan Gambar 3 dapat dijelaskan sebagai berikut.

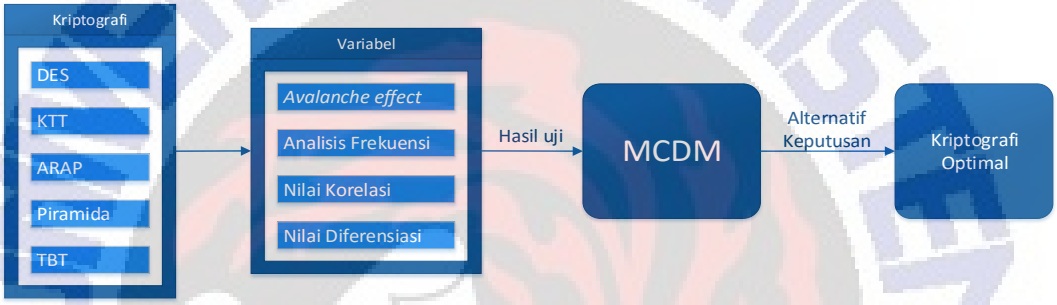
Identifikasi Masalah, meliputi apa saja yang diperlukan untuk menyelesaikan penelitian, dalam hal ini yaitu data yang akan digunakan dan metode yang sesuai untuk mencari kriptografi yang optimal.

Pengumpulan referensi, berupa penelitian-penelitian sebelumnya yang mendukung optimasi kriptografi. Terdapat lima penelitian sebelumnya yang digunakan berkaitan dengan perancangan kriptografi *block cipher* dengan menggunakan pola pada proses pengambilan dan pemasukan bit serta pengujian yang dilakukan. Penelitian terdahulu yang lainnya berkaitan dengan kriteria pengujian yang akan digunakan, serta metode untuk mencapai tujuan penelitian ini.

Perancangan algoritma, berupa rancangan algoritma pengujian yang akan digunakan pada kriptografi berbasis *block cipher* yang kemudian menjadi inputan pada *fuzzy-MCDM*. Pada tahap ini juga ditentukan kriptografi *block cipher* yang akan diuji. Pengujian menggunakan empat variabel antaralain: *avalanche effect*, analisis frekuensi, nilai korelasi, dan nilai diferensiasi.

Pengujian algoritma, menggunakan keempat kriteria yang telah ditentukan sebelumnya pada masing-masing alternatif kriptografi. Hasil pengujian digunakan sebagai inputan pada *fuzzy-MCDM* untuk mendapatkan alternatif kriptografi yang paling optimal.

Tahap terakhir yaitu mendokumentasikan proses penelitian yang sudah dilakukan dari tahap awal hingga akhir ke dalam bentuk tulisan yang kemudian menjadi laporan hasil penelitian.



Gambar 4. Rancangan Pengujian Algoritma

Bagian ini menjelaskan secara garis besar proses perancangan pengujian algoritma berdasarkan Gambar 4. Secara umum pengujian algoritma dapat dibagi dalam dua proses utama. Pada proses pertama diambil lima kriptografi berbasis *block cipher* dari penelitian sebelumnya, yakni DES [11], Kain Tenun Timor (KTT) [12], Anyaman Rambut Papua (ARAP) [13], Piramida [14], dan Teknik Burung Terbang (TBT) [3]. Pada setiap kriptografi dilakukan pengujian empat kriteria yaitu *Avalanche Effect*, Analisis Frekuensi, Nilai Korelasi, dan Nilai Diferensiasi, dengan menggunakan parameter yang sama agar hasil uji dari kelima kriptografi tersebut dapat dibandingkan. Pada proses kedua, hasil dari pengujian yang telah dilakukan sebelumnya disesuaikan dengan *Fuzzy-MCDM*. Hasil yang diperoleh berupa kriptografi yang optimal.

Secara umum langkah-langkah dalam MCDM diberikan pada tabel 1 sebagai berikut:

Tabel 1. Penyelesaian *Fuzzy* MCDM [10]

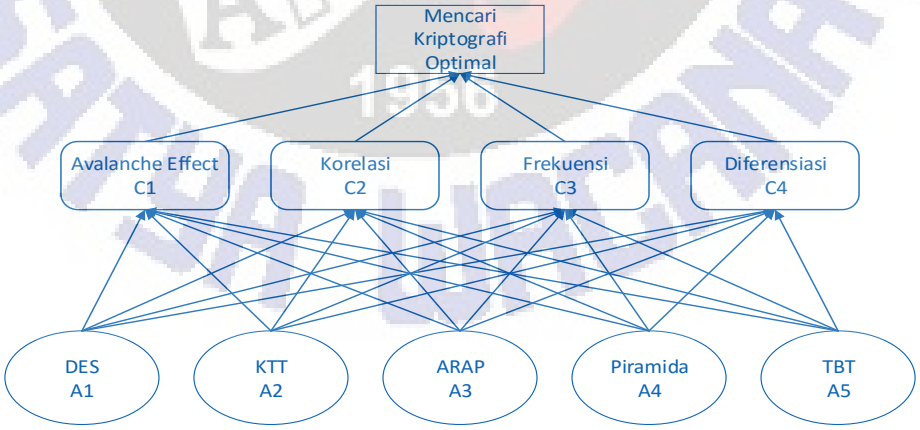
Langkah	Aktivitas	*Tool* Utama
Representasi Masalah	• Identifikasi tujuan dan kumpulan alternatif, A = {A_i | i=1, 2, …, n}. • Identifikasi kriteria, dengan C = {C_t}; t=1, 2, …, k • Membangun struktur hirarki masalah keputusan dengan beberapa pertimbangan	• Pohon Keputusan

Evaluasi himpunan fuzzy untuk alternatif-alternatif keputusan	• Memilih himpunan rating untuk bobot-bobot pada setiap kriteria dan derajat kecocokan dari alternatif-alternatif terhadap kriteria. • Mengevaluasi bobot-bobot pada setiap kriteria dan derajat kecocokan dari alternatif-alternatif terhadap kriteria. • Melakukan agregasi bobot-bobot pada setiap kriteria dan derajat kecocokan dari alternatif-alternatif terhadap kriteria.	• Variabel linguistic, bilangan fuzzy segitiga. • Operator fuzzy: Mean
Menyeleksi alternatif yang optimal	• Memprioritaskan alternatif keputusan menggunakan agregasi. • Memilih alternatif keputusan dengan prioritas tertinggi sebagai hasil alternatif optimal.	• Metode Nilai Total Integral.

4. Hasil dan Pembahasan

Representasi masalah dalam penelitian ini, dijelaskan sebagai berikut:

a. Tujuan keputusan ini adalah mencari kriptografi (DES, ARAP, TBT, Piramida, KTT) yang optimal berdasarkan kriteria pengujian (*Avalanche Effect*, Nilai Korelasi, Analisis Frekuensi, Nilai Diferensiasi).
b. Terdapat 5 alternatif kriptografi yang diberikan adalah A= {A_1, A_2, A_3, A_4, A_5}, dengan A_1= DES, A_2= ARAP, A_3=TBT, A_4= Piramida, A_5= KTT.
c. Struktur hirarki permasalahan dapat dilihat pada Gambar 5.



Gambar 5. Struktur Hirarki Permasalahan.

Untuk menentukan himpunan *fuzzy* keempat kriteria digunakan nilai statistika dari data. Nilai statistika yang digunakan adalah data terkecil (X_{min}), data terbesar (X_{max}) dan kuartil (Q_1, Q_2, Q_3) dari keseluruhan data yang diperoleh Untuk setiap kriteria. Nilai sari data digunakan untuk penentuan nilai *fuzzy* pada

setiap Himpunan. Penggunaan sari data karena secara statistika, nilai tersebut akan tersebar dalam rentangan data dari setiap kriteria.

Himpunan *fuzzy Avalanche Effect* dijelaskan sebagai berikut: SK: sangat kurang, K: kurang, C: cukup, B: baik, SB: sangat baik, yang masing-masing direpresentasikan sebagai berikut. SK= {0, 0, 0.25}, K= {0. 0.25, 0.50}, C= {0.25, 0.50, 0.75}, B= {0.50, 0.75, 1}, SB= {0.75, 1, 1}. Kurva bahu untuk bilangan *fuzzy* varibel *Avalanche Effect* dapat dilihat pada Gambar 6.

Fungsi keanggotaan untuk setiap himpunan pada variable *avalanche effect* diberikan sebagai berikut:

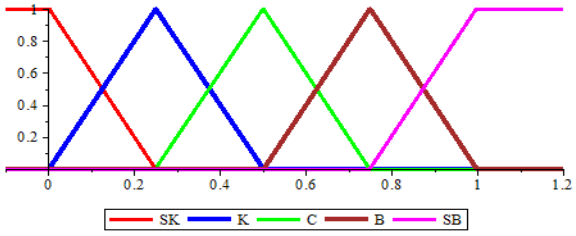
$$SK = \begin{cases} 1; & x \le 0.25 \\ \dfrac{0.25 - x}{0.25}; & 0 \le x \le 0.25 \\ 0; & x \ge 0.25 \end{cases}$$

$$K = \begin{cases} 0; & x \le 0.25 \; atau \; x \ge 0.5 \\ \dfrac{x}{0.25}; & 0 \le x \le 0.25 \\ \dfrac{x - 0.5}{0.25 - 0.5}; & 0.25 \le x \le 0.5 \end{cases}$$

$$C = \begin{cases} 0; & x \le 0.25 \; atau \; x \ge 0.75 \\ \dfrac{x - 0.25}{0.5 - 0.25}; & 0.25 \le x \le 0.5 \\ \dfrac{0.75 - x}{0.75 - 0.5}; & 0.5 \le x \le 0.75 \end{cases}$$

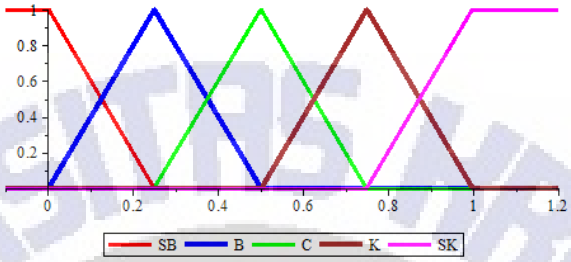
$$B = \begin{cases} 0; & x \le 0.5 \; atau \; x \ge 1 \\ \dfrac{x - 0.5}{0.75 - 0.5}; & 0.5 \le x \le 0.75 \\ \dfrac{x - 1}{0.75 - 1}; & 0.75 \le x \le 1 \end{cases}$$

$$SB = \begin{cases} 0; & x \le 0.75 \\ \dfrac{x - 0.75}{1 - 0.75}; & 0 \le x \le 0.25 \\ 1; & x \ge 1 \end{cases}$$



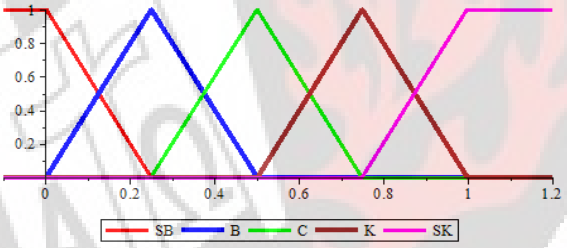
Gambar 6. Bilangan *Fuzzy* Untuk Variabel *Avalanche Effect*

Himpunan *fuzzy* Korelasi dijelaskan sebagai berikut: bilangan *fuzzy* yang digunakan adalah SK: sangat kurang, K: kurang, C: cukup, B: baik, SB: sangat baik, yang masing-masing direpresentasikan sebagai berikut. SB= {0, 0, 0.25}, B= {0. 0.25, 0.50}, C= {0.25, 0.50, 0.75}, K= {0.50, 0.75, 1}, SK= {0.75, 1, 1}. Kurva bahu untuk bilangan *fuzzy* varibel korelasi dapat dilihat pada Gambar 7.



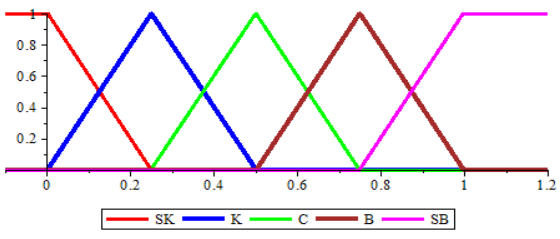
Gambar 7. Bilangan *Fuzzy* Untuk Variabel Korelasi

Himpunan *fuzzy* Frekuensi dijelaskan sebagai berikut: bilangan *fuzzy* yang digunakan adalah SK: sangat kurang, K: kurang, C: cukup, B: baik, SB: sangat baik, yang masing-masing direpresentasikan sebagai berikut. SB= {0, 0, 0.25}, B= {0. 0.25, 0.50}, C= {0.25, 0.50, 0.75}, K= {0.50, 0.75, 1}, SK= {0.75, 1, 1}. Kurva bahu untuk bilangan *fuzzy* varibel frekuensi dapat dilihat pada Gambar 8.



Gambar 8. Bilangan *Fuzzy* Untuk Variabel Frekuensi

Himpunan *fuzzy* Diferensiasi dijelaskan sebagai berikut: bilangan *fuzzy* yang digunakan adalah SK: sangat kurang, K: kurang, C: cukup, B: baik, SB: sangat baik, yang masing-masing direpresentasikan sebagai berikut. SK= {0, 0, 0.25}, K= {0. 0.25, 0.50}, C= {0.25, 0.50, 0.75}, B= {0.50, 0.75, 1}, SB= {0.75, 1, 1}. Kurva bahu untuk bilangan *fuzzy* varibel analisis frekuensi dapat dilihat pada Gambar 9. Secara fungsi, untuk variabel korelasi sama dengan varibel *avalanche effect*.



Gambar 9. Bilangan *Fuzzy* Untuk Variabel Nilai Diferensiasi

Rating kepentingan diperoleh dari penentuan tingkat kepentingan menggunakan matriks perbandingan berpasangan pada kriteria *avalanche effect*, korelasi, frekuensi, dan diferensiasi. Hasilnya kemudian disesuaikan dengan bilangan *fuzzy* pada Gambar 6, maka rating kepentingan untuk setiap kriteria diperoleh seperti yang diberikan pada Tabel 2.

Tabel 2. Rating Kepentingan Untuk Setiap Kriteria

Kriteria	*Avalanche effect*	Korelasi	Frekuensi	Diferensiasi
Rating Kepentingan	C	R	SR	SR

Sedangkan rating kecocokan diberikan pada Tabel 3, diperoleh dari data pengujian kriptografi dan keempat kriteria pengujian sesuai dengan hasil uji yang telah dilakukan, kemudian dimasukkan ke dalam bentuk variabel linguistik.

Tabel 3. Rating Kecocokan Setiap Alternatif Terhadap Kriteria

Alternatif	Kriptografi	Rating Kecocokan			
		Avalanche effect	Korelasi	Frekuensi	Diferensiasi
A1	DES	C	SK	SB	SB
A2	ARAP	SK	B	SB	SB
A3	TBT	SK	B	SB	SB
A4	Piramida	SK	B	SB	SB
A5	KTT	SK	SB	SB	SB

Evaluasi Himpunan *Fuzzy* dari alternatif-alternatif keputusan dijelaskan sebagai berikut:

Sesuai dengan teori yang sebelumnya diberikan pada *point* 2 maka selanjutnya dilakukan penentuan himpunan *fuzzy* dari setiap alternatif keputusan. Dalam mensubtitusikan indeks kecocokan *fuzzy* diambil derajat keoptimisan $\alpha=0$, $\alpha=0.5$ dan $\alpha=1$, maka diperoleh nilai integral yang kemudian digunakan untuk menentukan kriptografi yang optimal. Variabel linguistik ditentukan untuk bobot kepentingan dan kriteria keputusan, yang akan digunakan untuk menghitung nilai integral.

Variabel-variabel linguistik yang merepresentasikan bobot kepentingan untuk setiap kriteria, adalah: T (kepentingan) W = {SR, R, C, T, ST} dengan SR: sangat rendah, R: rendah, C: cukup, T: tinggi, ST: sangat tinggi, yang masing-masing direpresentasikan dengan *fuzzy* segitiga. SR = (0, 0, 0.25), R = (0, 0.25, 0.5), C = (0.25, 0.5, 0.75), T = (0.5, 0.75, 1), ST = (0.75, 1, 1). Sedangkan untuk derajat kecocokan alternatif-alternatif dengan kriteria-kriteria keputusan adalah: T(kecocokan) S = {SK, K, C, B, SB} dengan SK: sangat kurang, K: kurang, C: cukup, B: baik, SB: sangat baik, yang masing-masing direpresentasikan dengan *fuzzy* segitiga: SK = (0, 0, 0.25), K = (0, 0.25, 0.5), C = (0.25, 0.5, 0.75), B = (0.5, 0.75, 1), SB = (0.75, 1, 1).

Bilangan *fuzzy* segitiga disubstitusikan ke setiap variabel linguistik ke dalam persamaan (19) hingga persamaan (21), sehingga diperoleh nilai kecocokan *fuzzy* seperti pada Tabel 4. Penghitungan nilai kecocokan *fuzzy* untuk alternatif A1 diberikan sebagai berikut:

$$Y = \frac{(0.25 * 0.25) + (0 * 0) + (0 * 0.75) + (0 * 0.75)}{4} = 0.0156$$

$$Q = \frac{(0.5 * 0.5) + (0.25 * 0) + (0 * 1) + (0 * 1)}{4} = 0.0625$$

$$Z = \frac{(0.75 * 0.75) + (0.5 * 0.25) + (0.25 * 1) + (0.25 * 1)}{4} = 0.2969$$

Tabel 4. Indeks Kecocokan *Fuzzy* Untuk Setiap Alternatif

Alternatif	Kriptografi	Rating Kecocokan				Indeks Kecocokan *Fuzzy*		
		C1	C2	C3	C4	Y	Q	Z
A1	DES	C	SK	SB	SB	0.0156	0.0625	0.2969
A2	ARAP	SK	B	SB	SB	0.0000	0.0469	0.2969
A3	TBT	SK	B	SB	SB	0.0000	0.0469	0.2969
A4	Piramida	SK	B	SB	SB	0.0000	0.0469	0.2969
A5	KTT	SK	SB	SB	SB	0.0000	0.0625	0.2969

Alternatif yang optimal diperoleh dengan mensubstitusikan indeks kecocokan *fuzzy* pada tabel 4 ke persamaan (22), dengan mengambil derajat keoptimisan (α)=0 (tidak optimis), α=0.5, dan α=1 (sangat optimis). Penghitungan nilai total integral untuk alternatif A1 (DES) diberikan sebagai berikut:

$$I_1^0 = \left(\frac{1}{2}\right)((0)(0.2969) + (0.0625) + (1-0)(0.0156) = 0.039$$

$$I_1^{0.5} = \left(\frac{1}{2}\right)((0.5)(0.2969) + (0.0625) + (1-0.5)(0.0156) = 0.109$$

$$I_1^1 = \left(\frac{1}{2}\right)((1)(0.2969) + (0.0625) + (1-1)(0.0156) = 0.180$$

Nilai total integral untuk α=0, α=0.5 dan α=1 dapat dilihat pada Tabel 5, Tabel 6, dan Tabel 7.

Tabel 5. Nilai Integral Untuk α=0

Alternatif	α=0
DES	0.039
KTT	0.031
ARAP	0.023
TBT	0.023
Piramida	0.023

Tabel 6. Nilai Integral Untuk α=0.5

Alternatif	α=0.5
DES	0.109
KTT	0.105
ARAP	0.098
TBT	0.098
Piramida	0.098

Tabel 7. Nilai Integral Untuk α=1

Alternatif	α=1
DES	0.180
KTT	0.180
ARAP	0.172
TBT	0.172
Piramida	0.172

Berdasarkan hasil diatas tidak dapat dipungkiri bahwa DES mendominasi algoritma kriptografi lainnya untuk derajat keoptimisan α=0, α=0.5 dan α=1. Namun pada derajat keoptimisan α=1 KTT mampu berada setara dengan kriptografi DES. Sementara untuk kriptografi ARAP, TBT, dan Piramida menghasilkan nilai total yang sama, yakni 0.023 pada derajat keoptimisan α=0, 0.098 untuk α=0.5, dan α=1 adalah 0.172.

5. Simpulan

Berdasarkan hasil dari penelitian ini maka dapat disimpulkan bahwa: 1) *Fuzzy*-MCDM dapat digunakan untuk memilih metode kriptografi berdasarkan pengujian dengan menggunakan kriteria *avalanche effect*, korelasi, frekuensi, dan diferensisasi. 2) Kriptografi *block cipher* yang optimal untuk digunakan dari kelima kriptografi berbasis *block cipher* yang diuji adalah DES dan KTT.

6. Daftar Pustaka

[1] Setiawan, E. F., & Wowor, A. D, Magdalena, A. I. P., 2015, *Perancangan Algoritma Kriptografi Block Cipher Berbasis Pola Cabang dan Ranting Pohon*, Universitas Kristen Satya Wacana, Salatiga.

[2] Ramanujam, Sriram., Karuppiah, Marimuthu., *Designing an Algorithm with High Avalanche Effect*. IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.1, January 2011

[3] Muabuay, A. W., A. N., Wowor, A. D., Magdalena, A. I. P., 2015. *Perancangan Kriptografi Block Cipher pada Teknik Burung Terbang*. Universitas Kristen Satya Wacana. Salatiga.

[4] Schneier, Bruce., 1996, *Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C*. New York: John Wiley & Sons, Inc.

[5] Ariyus, Dony. 2006. *Kriptografi Keamanan Data dan Komunikasi*. Yogyakarta: Graha Ilmu.

[6] Munir, Rinaldi, 2006, *Kriptografi*, Bandung: Informatika.

[7] Joan Daemen-Vincent Rijmen. 2001. *The Design of Rijndael AES-The Advanced Encryption Standard*. New York: Springer

[8] Agrawal, Himani., Sharma, Monisha., *Implementation and analysis of Various Symmetric Cryptosystems*., Indian Journal of Science and Technology, Vol. 3 No. 12, Dec 2010

[9] Kusumadewi, S., Guswaludin, I., *Fuzzy Multi-Criteria Decision Making*, Media Informatika, vol. 3, no. 0854-4743, Juni 2005.

[10] Kusumadewi, S., Hartati, S., Harjoko, A., & Wardoyo, R., 2006, *Fuzzy Multi-Attribute Decision Making (FUZZY MADM)*, Yogyakarta: Graha Ilmu.

[11] Minase, Nayuki, 2014, *DES cipher internals in Excel*, http://nayuki.eigenstate.org/page/des-cipher-internals-in-excel

[12] Mone, Aleksandro S., Magdalena, A. I. P., Wowor, A. D., 2015. *Penggunaan Motif Kain Tenun Timor Dan Linear Congruential Generator (LCG) Dalam Merancang Dan mengimplementasikan Algoritma Kriptografi Cipher Block*. Universitas Kristen Satya Wacana. Salatiga.

[13] Mamoba, Supyanto, Magdalena, A. I. P., Wowor, A. D., 2015. *Perancangan Kriptografi Block Cipher Berbasis Pada Anyaman Rambut Papua (ARAP).* Universitas Kristen Satya Wacana. Salatiga.

[14] Mauliku, W. M., Magdalena, A. I. P., Wowor, A. D., 2015, *Perancangan dan Implementasi Algoritma Kriptografi Cipher Block Berbasis Pada Bentuk Piramida dan Linear Congruential Generator*. Universitas Kristen Satya Wacana. Salatiga.