Jurnal Sistem Komputer dan Informatika (JSON)
Volume 2, Nomor 2, Januari 2021
e-ISSN 2685-998X
DOI 10.30865/json.v2i2.2535

Perancangan Kriptografi Block Cipher Menggunakan Pola Logo Media Sosial

Thea Thiranadya Mardita Bulamey*, Hendry

Fakultas Teknologi Informasi, Teknik Informatika, Universitas Kristen Satya Wacana, Salatiga, Indonesia
Email: [1,*]theatm10@gmail.com, [2]hendry@uksw.edu
Submitted: **11/10/2020**; Accepted: **04/01/2021**; Published: **24/01/2021**

Abstrak–Dalam penelitian ini dirancang Kriptografi Block Cipher 64 bit berbasis Pola Logo Media Sosial, perancangan ini bertujuan untuk menghasilkan sistem kriptografi yang baru, serta bertujuan untuk mengamankan sebuah data atau informasi berupa teks. Dalam perancangan kriptografi menggunakan Pola Media Sosial ini telah dilakukan uji korelasi sebanyak 24 kali sehingga menghasilkan urutan pola terbaik dengan nilai rata-rata korelasi 0,014425413 dengan pola urutan 1-2-4-3. Setelah menemukan pola terbaik maka dilakukan putaran sebanyak 10 kali putaran dimana dalam setiap putaran terdapat 4 proses yang terdiri dari 4 pola untuk proses plaintext dan 4 pola untuk proses kunci, dan disertai dengan substitusi S-Box dalam setiap proses agar avalanche effect mengalami peningkatan yang signifikan. Pada penelitian ini juga dilakukan uji avalanche effect, Dalam setiap pengujian avalanche effect menunjukkan bahwa S-Box berpengaruh didalam proses enkripsi karena dalam setiap putaran memiliki avalanche effect yang mencapai 50%. Maka dapat dikatakan bahwa ciphertext yang dihasilkan kriptografi block cipher berbasis pada pola logo media sosial memiliki hasil output yang acak sehingga, dapat digunakan untuk mengamankan data atau informasi berupa teks.

Kata Kunci: Kriptografi; Block Cipher; Korelasi; Avalanche Effect; Pola Logo Media Sosial

Abstract–In this research, 64-bit Block Cipher Cryptography was designed based on the Social Media Logo Pattern, this design aims to produce a new cryptographic system, and aims to secure data or information in the form of text. In designing cryptography using Social Media Patterns, correlation tests have been carried out 24 times so as to produce the best pattern sequence with an average correlation value of 0.014425413 with a 1-2-4-3 sequence pattern. After finding the best pattern, 10 rounds are carried out where in each cycle there are 4 processes consisting of 4 patterns for the plaintext process and 4 patterns for the key process, and accompanied by S-Box substitution in each process so that the avalanche effect has a significant increase. In this research, the avalanche effect test was also carried out. In each avalanche effect test, it shows that the S-Box has an effect on the encryption process because in each cycle it has an avalanche effect that reaches 50%. So it can be said that the ciphertext generated by block cipher cryptography based on the social media logo pattern has random output results so that it can be used to secure data or information in the form of text.

Keywords: Cryptography; Block Cipher; Correlation; Avalanche Effect; Social Media Logo Pattern

1. PENDAHULUAN

Pada era teknologi informasi saat ini, perkembangan teknologi berkembang dengan sangat pesat. Tentunya pengiriman data dan informasi di era sekarang ini bukan hal yang jarang dilakukan tetapi, sudah sering dilakukan setiap hari. Apalagi dengan adanya jaringan internet yang semakin memudahkan kita untuk bertukar informasi dengan orang lain yang ada di seluruh dunia. Akan tetapi dengan adanya kemudahan seperti ini keamanan dan kerahasiaan akan menjadi hal yang sangat penting. Karena dalam data atau informasi yang ada di dalamnya dapat berupa informasi data pribadi atau kelompok yang bersifat umum atau rahasia yang seharusnya tidak bisa diketahui oleh orang lain. Seperti yang kita ketahui, sekarang ini banyak pencurian data dan informasi melalui internet hal ini sudah sering terjadi, dan dilakukan oleh orang-orang yang tidak berkepentingan dan tidak tau bertanggung jawab.

Karena hal seperti pencurian data dan informasi sering terjadi, maka perlu adanya cara mengamankan data atau informasi tersebut dari orang-orang yang tidak dapat bertanggung jawab. Dengan cara yang sering digunakan yaitu penyandian data atau enkripsi. Enkripsi merupakan proses mengamankan sebuah data dengan membuat data tersebut tidak bisa dibaca atau dimengerti oleh orang lain. Sehingga data yang dikirimkan hanya dapat dipahami oleh orang-orang tertentu yang dapat mendeskripsikan data hasil enkripsi tersebut menjadi data sebenarnya. Media Sosial adalah suatu media untuk bersosialisasi melalui *online*, setiap manusia di era teknologi informasi saat ini tidak mungkin untuk tidak menggunakan media sosial kecuali untuk orang-orang di kalangan tertentu, media sosial ada berbagai macam seperti *Facebook*, *Twitter*, *Gmail*, *Instagram*, *Whatsapp*, Line, dan masih banyak lagi.

Penelitian terkait Kriptografi dengan berbagai metode telah dilakukan. Salah satunya adalah penelitian yang berjudul "Perancangan Teknik Kriptografi Block Cipher Berbasis Pola Batik Ceplok Yogyakarta". Dalam penelitian ini dapat disimpulkan bahwa kriptografi block cipher 64 bit berbasis pola batik ceplok Yogyakarta dapat dikatakan sebagai sistem kriptografi. Dalam proses enkripsi, rancangan kriptografi block cipher berbasis pola batik ceplok Yogyakarta ini menghasilkan output yang acak sehingga dapat digunakan sebagai alternatif dalam pengamanan data. Dalam pengujian avalanche effect yang dilakukan pun menunjukkan bahwa proses enkripsi di setiap putaran memiliki rata-rata perubahan yang mencapai 47,656% yang berarti algoritma kriptografi ini berhasil dan termasuk ke dalam kategori yang baik. Walaupun termasuk ke dalam kategori yang baik, penelitian ini masih kurang baik apabila dibandingkan dengan penelitian terdahulu yang kebanyakan mempunyai nilai rata-rata avalanche effect lebih mendekati angka 50% yang berarti algoritma kriptografinya termasuk sangat baik [1]

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 2, Nomor 2, Januari 2021
e-ISSN 2685-998X
DOI 10.30865/json.v2i2.2535

Penelitian yang berjudul "Perancangan Kriptografi Block Cipher Berbasis Pola Tarian Denok Deblong". Dalam penelitian ini menggunakan Pola Tarian Denok Deblong untuk merancang algoritma, berdasarkan penelitian yang telah dilakukan enkripsi Block Cipher memiliki kelemahan yaitu apabila data yang sama di enkripsi menggunakan kunci yang sama maka akan menghasilkan cipherteks yang sama, namun hal tersebut dapat diatasi dengan menggunakan ukuran blok yang lebih besar, misalnya 256 bit, sehingga walaupun blok data yang sama di enkripsi menggunakan kunci yang sama maka cipherteks yang dihasilkan akan berbeda. Dalam proses enkripsi, rancangan Kriptografi Block Cipher berbasis pola Tarian Denok Deblong ini menghasilkan output yang sangat acak sehingga memungkinkan untuk digunakan sebagai alternatif dalam pengamanan data. Berdasarkan pengujian terlihat bahwa dengan menambahkan S-BOX Pola tarian Denok Deblong ini dapat menghasilkan output enkripsi yang random. Selain itu, Dalam pengujian Avalance Effect yang dilakukan dengan menggunakan plaintext Yuana123 mendapatkan hasil yang baik, dengan rata-rata dari 10 putaran adalah 49,844% [2].

Penelitian yang berjudul "Perancangan Teknik Kriptografi Block Cipher Berbasis Pola Permainan Tradisional Rangku Alu" dalam penelitian ini algoritma yang dikembangkan berdasarkan prinsip pada block cipher dengan ukuran block sebanyak 64 bit, alur pola yang digunakan (nilai korelasi 0,011), metode untuk meningkatkan keacakan (menambahkan metode XOR), serta berapa putaran yang digunakan (menggunakan total 20 putaran). Kemudian berdasarkan penelitian yang dilakukan, dapat disimpulkan bahwa Kriptografi Block Cipher 64 bit berbasis pola permainan tradisional Rangku Alu ini menghasilkan output yang acak sehingga dapat digunakan sebagai alternatif dalam pengamanan data. Dalam pengujian Avalanche Effect yang dilakukan, menunjukkan bahwa proses enkripsi di setiap putaran memiliki perubahan yang mencapai 49,38% yang berarti masuk ke dalam kategori yang sangat baik [3].

Dari penelitian-penelitian di atas dapat disimpulkan bahwa dari ketiga penelitian tersebut memiliki beberapa perbedaan yaitu dari pola yang digunakan untuk merancang kriptografi, serta proses pengambilan. Berdasarkan penelitian-penilitian terkait kriptografi simetris, maka akan dilakukan penelitian tentang "Perancangan Kriptografi Block Cipher Menggunakan Pola Logo Media Sosial". Metode yang digunakan dalam penelitian ini merupakan metode baru yang dibuat berdasarkan pola logo media sosial, yang diharapkan dapat menambah koleksi teknik kriptografi untuk keamanan data.

Algoritma yang digunakan dalam penelitian ini yaitu, algoritma *Block Cipher* 64 bit dengan menggunakan pola logo media sosial. Pola logo media sosial digunakan untuk proses pengambilan bit dari *plaintext* kemudian dimasukkan ke dalam blok matriks, pola logo media sosial ini merupakan pola yang sangat unik dimana tidak ada yang dapat menebak bahwa akan tercipta sebuah perancangan untuk mengamankan data dengan menggunakan pola logo media sosial ini.

Berdasarkan latar belakang masalah yang ada, maka dilakukan penelitian tentang Perancangan Kriptografi *Block Cipher* Menggunakan Pola Logo Media Sosial. Dalam penelitian ini akan digunakan 64 bit untuk menghasilkan proses enkripsi lebih baik dan memiliki 10 putaran dalam proses pengacakan data.

2. METODE PENELITIAN

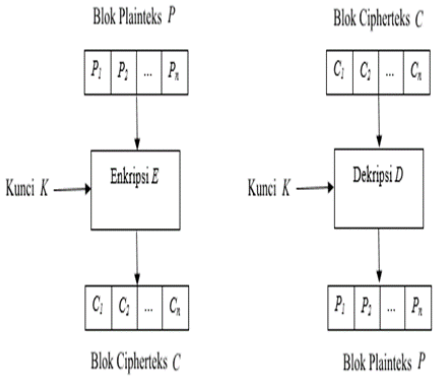
2.1 Kriptografi

Kriptografi berasal dari kata Yunani kripto (tersembunyi) dan grafia (tulisan). Secara harfiah, kriptografi dapat diartikan sebagai tulisan yang tersembunyi atau tulisan yang dirahasiakan. Tujuannya adalah supaya tulisan tersebut tidak dapat dibaca oleh setiap orang. Hanya orang-orang tertentu, yaitu orang yang mengetahui cara menyembunyikan tulisan tersebut yang dapat membacanya [4]. Proses menyandikan *plaintext* menjadi *ciphertext* disebut enkripsi (*encryption*) atau *enciphering*, Sedangkan proses mengembalikan *ciphertext* menjadi *plaintext* disebut dekripsi (*decryption*) atau *deciphering.* Bagian lain dari kriptografi adalah enkripsi dan dekripsi. Enkripsi merupakan proses pengaman data yang disembunyikan menjadi bentuk tidak dapat dibaca. Dekripsi merupakan proses mengembalikan pesan dari acak atau tidak dapat dibaca kembali menjadi pesan yang dapat dibaca atau dimengerti [5]. Algoritma Kriptografi adalah aturan untuk *enchipering* dan *dechipering*, fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Kunci adalah parameter yang digunakan untuk transformasi *enchipering* dan dechipering, sistem kriptografi atau *cryptosystem* adalah algoritma kriptografi, *plaintext, ciphertext*, dan kunci [6].

2.2 *Block Cipher*

Block Cipher merupakan rangkaian bit yang dibagi menjadi blok-blok yang panjangnya sudah ditentukan sebelumnya [7] Berikut merupakan skema proses enkripsi-dekripsi *block cipher* secara umum dapat digambarkan pada Gambar 1.

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 2, Nomor 2, Januari 2021
e-ISSN 2685-998X
DOI 10.30865/json.v2i2.2535



Gambar 1. Proses Enkripsi dan Dekripsi

Suatu proses kriptografi dapat dikatakan teknik kriptografi bila melalui uji kriptosistem terlebih dahulu yaitu diuji dengan metode Stinson. Sebuah sistem akan dikatakan sebagai sistem kriptografi jika memenuhi lima tupel (*Five tuple*):

P adalah himpunan berhingga dari *plaintext*,
C adalah himpunan berhingga dari *ciphertext*,
K merupakan ruang kunci (*keyspace*), adalah himapunan berhingga dari kunci.
Untuk setiap $k \in \mathbf{K}$, terdapat aturan enkripsi $e_k \in \mathbf{E}$ dan berkorespodensi dengan aturan dekripsi $d_k \in$ D. Setiap $e_k : \boldsymbol{P} \longrightarrow \boldsymbol{C}$ dan $d_k : \boldsymbol{C} \longrightarrow \boldsymbol{P}$ adalah fungsi sedemikian hingga $d_k(e_k(x)) = x$ untuk setiap *plaintext* $x \in \boldsymbol{P}$ [6].

Untuk menguji nilai algoritma yang dirancang memiliki hasil *ciphertext* yang acak dari *plaintext* maka digunakan Persamaan 1, dimana *variable* X merupakan *plaintext* dan Y merupakan *ciphertext*.

$$r = \frac{n\Sigma xy - (\Sigma x)(\Sigma y)}{\sqrt{\{n\Sigma x^2 - (\Sigma x)^2\}\{n\Sigma y^{2\,2} - (\Sigma y)^2\}}} \quad (1)$$

Dimana:
n = Banyaknya pasangan data X dan Y
Σx = Total jumlah dari variabel X
Σy = Total jumlah dari variabel Y
Σx^2 = Kuadrat dari total jumlah variabel X
Σy^2 = Kuadrat dari total jumlah variabel Y
Σxy = Hasil perkalian dari total jumlah variabel X dan variabel Y

Acuan dalam menentukan koefisien korelasi di tampilkan pada Tabel 1.

Tabel 1. Klasifikasi Koefisien Korelasi.

Interval Koefisien	Tingkat Hubungan
0,00 – 0,199	Sangat Rendah
0,20 – 0,399	Rendah
0,40 – 0,599	Sedang
0,60 – 0,799	Kuat
0,80 – 1,000	Sangat Kuat

2.3 Pola Media Sosial

Media Sosial adalah suatu media untuk bersosialisasi melalui online, setiap manusia di era teknlogi informasi saat ini tidak mungkin untuk tidak menggunakan media sosial kecuali untuk orang-orang dikalangan tertentu, media sosial ada berbagai macam seperti Facebook, Twitter, Gmail, Instagram, Whatssapp, Line, dan masih banyak lagi. Pada peneletian yang berjudul "Perancangan Kriptografi *Block Cipher* Menggunakan Pola Logo Media Sosial" menggunakan *block cipher* dengan ukuran 64 bit atau 8x8 *block* bit, dimana *plaintext* dan kunci menggunakan Pola Logo Media Sosial.

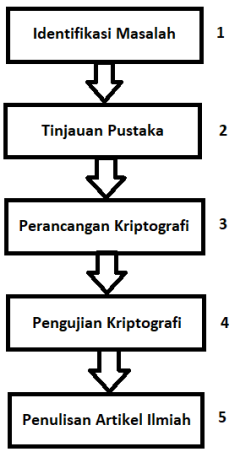
2.4 *Avalanche Effect*

Perubahan satu buah bit dalam *Block Cipher* dapat menghasilkan perubahan lebih dari satu *bit* setelah satu putaran, dan lebih banyak lagi yang akan berubah untuk putaran berikutnya. Hasil dari perubahan ini yang disebut *Avalanche Effect*, jika satu buah bit input mengalami perubahan berarti sudah memenuhi kriteria *Avalanche Effect*. *Avalanche Effect*, adalah satu karateristik yang selalu menjadi acuan untuk menentukan baik atau tidakmya algoritma kriptografi.

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 2, Nomor 2, Januari 2021
e-ISSN 2685-998X
DOI 10.30865/json.v2i2.2535

2.5 Tahapan Penelitian

Tahapan penelitian yang digunakan dalam penelitian ini dapat dibagi ke dalam 5 (lima) tahap yaitu : (1) Identifikasi Masalah, (2) Tinjauan Pustaka, (3) Perancangan Kriptografi, (4) Pengujian Kriptografi, (5) Penulisan Laporan.



Gambar 2. Tahapan Penelitian.

Tahapan penelitian pada Gambar 2 dapat dijelaskan sebagai berikut:

Tahapan pertama: Identifikasi masalah merupakan tahap awal dalam melihat permasalahan keamanan informasi yang berkaitan dengan kriptografi untuk digunakan sebagai perumusan masalah dan tujuan pada penelitian ini. Adapun rumusan masalah yang akan di bahas pada penelitian perancangan kriptografi *block cipher* dengan pola logo media sosial yaitu:

2.1 Plaintext dan kunci dibatasi maksimal 8 karakter
2.2 Blok-blok menggunakan blok 8x8 (64-bit)
2.3 Dalam perancangan penelitian kali ini menggunakan pola logo media sosial sebagai pengambilan bit *pada plaintext.*

Tahapan kedua: Tinjauan pustaka dilakukan dengan mengumpulkan referensi dari buku, jurnal atau sumber lain yang berguna dalam perancangan kriptografi

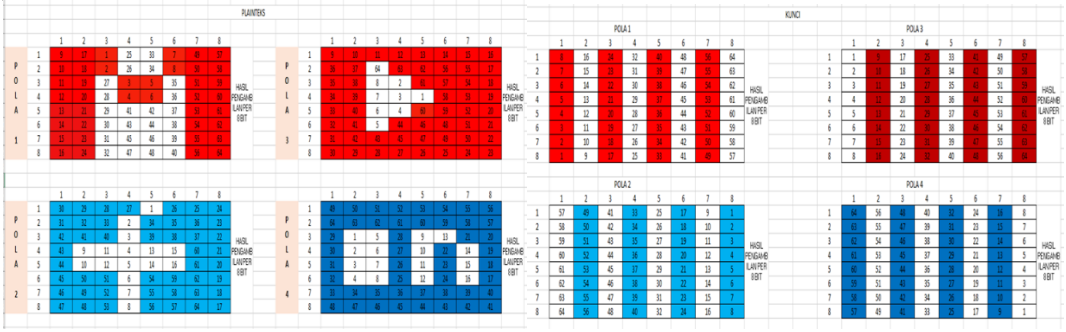
Tahapan ketiga: Merancang algoritma kriptografi *Block Cipher* 64 Bit dengan pola logo media sosial. Menerapkan pola kedalam *block cipher* dengan ukuran 8x8

Tahapan keempat: Setelah pola atau rancangan kriptografi dibuat dibutuhkan pengujian algoritma. Pengujian digunakan dengan cara manual dimana *plaintext* diubah ke dalam bit untuk melakukan proses enkripsi;

Tahapan kelima: Penulisan artikel ilmiah dari hasil penelitian yang dilakukan mengenai proses perancangan algoritma kriptografi 64 bit dengan menggunnakan pola logo media sosial.

3. HASIL DAN PEMBAHASAN

Algoritma Perancangan Kriptografi *block cipher* 64 berbasis pola media sosial berdasarkan awal hingga akhir. Pada percangan pola yang digunakan adalah pola dari logo media sosial itu sendiri untuk *plaintext* sedangkan untuk pola kunci menggunakan pola pengambilan baris dan kolom.

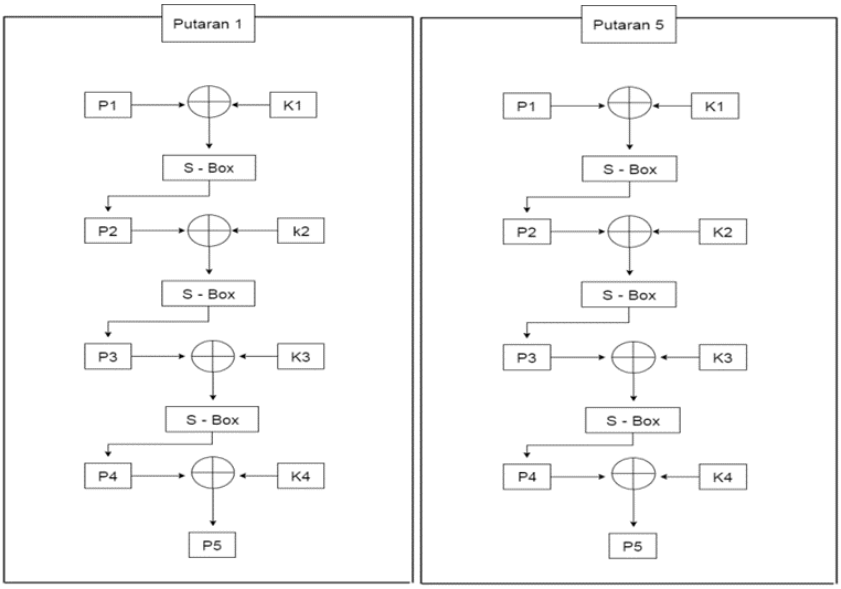


Gambar 3. Pola Plainteks dan Kunci

Gambar 3 adalah contoh pola pengambilan dan pemasukan biner dengan acuan pola logo media sosial pada p*laintext* dan pola baris kolom pada kunci, untuk mempermudah pengambilan dalam setiap kotak bit sudah terisi nomor urutannya. Berdasarkan pola yang sudah dirancang, dilakukan pengujian korelasi antara *plaintext* dan kunci dengan kombinasi urutan pola bertujuan mendapat rata-rata korelasi terbaik. Pengujian dilakukan satu kali dengan:

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 2, Nomor 2, Januari 2021
e-ISSN 2685-998X
DOI 10.30865/json.v2i2.2535

Plaintext: Salatiga, kunci: Semarang
Berdasarkan hasil pengujian korelasi, maka hasil rata-rata terbaik digunakan sebagai acuan perancangan.



Gambar 4. Rancangan Alur Enkripsi

Gambar 3 merupakan rancangan alur proses enkripsi. Langkah-langkah alur proses enkripsi dapat jelaskan: a) Membuat *Plaintext*; b) Mengubah *plaintext* menjadi bilangan biner; c) Melakukan proses enkripsi dengan meng xor *plaintext* dengan kunci akan melewati 4 proses pada setiap putarannya 1) Pada putaran pertama *Plaintext* 1 melakukan transformasi dengan pola logo media sosial dan di-XOR dengan kunci 1, hasil XOR ditransformasikan dengan *table* subtitusi *S-Box* sehingga menghasilkan *Plaintext* 2, kemudian tahapan tersebut diulang sampai proses ke-3; 2) hasil *Plaintext* 4 kemudian di-XOR dengan kunci 4 akan menghasilkan *Plaintext* 5; 3) *Plaintext* 5 akan masuk pada putaran kedua dengan proses yang sama dengan putaran pertama dan tahapan tersebut akan sampai dengan putaran ke-5 sehingga akan menghasilkan *Ciphertext*.

Tabel 1. Klasifikasi Koefisien Korelasi

KORELASI POLA DAN KUNCI			
1-2-3-4	-0,07995316	3-1-2-4	0,114264849
1-2-4-3	0,014425413	3-1-4-2	0,043622991
1-3-2-4	-0,124135556	3-2-1-4	0,175241267
1-3-4-2	-0,110471377	3-2-4-1	-0,067105712
1-4-2-3	-0,390023856	3-4-1-2	0,030999654
1-4-3-2	-0,080334143	3-4-2-1	-0,342650365
2-1-3-4	-0,098527408	4-1-2-3	-0,052867175
2-1-4-3	-0,316780514	4-1-3-2	0,12819299
2-3-1-4	-0,060876234	4-2-1-3	0,364849288
2-3-4-1	-0,119848998	4-2-3-1	0,290049705
2-4-1-3	0,022439357	4-3-1-2	-0,140527818
2-4-3-1	-0,187023366	4-3-2-1	0,137149393

Tabel 2 kombinasi pola dengan rata-rata korelasi yang terbaik terdapat pada “1-2-4-3”. Kombinasi ini nantinya akan menjadi pola proses enkripsi sampai putaran ke 10 untuk menghasilkan *ciphertext.*

Perancangan algoritma kriptografi *Block Cipher* 64 bit berbasis pola media sosial hanya dilakukan dalam 10 putaran untuk mendapatkan *ciphertext* dan didalam setiap putaran terdapat proses. Proses pertama *plaintext* dan kunci dikonversi menjadi ASCII kemudian diubah ke bilangan biner, kemudin plaintext dimasukkan kedalam kolom 8x8 menggunakan pola pengambilan bit dan dilakukan dengan pola media sosial yang berbeda-beda ditiap proses. Hasil proses XOR kemudian ditransformasikan dengan tabel susbstitusi S-Box untuk menghasilkan plaintext berikutnya samapai 10 kali putaran.

Tabel 2. Tabel Subtitusi *S-Box*

TABEL S-BOX			
INPUT	XOR-4	S-BOX	S-BOX INVERSE
00	0	63	52
01	1	7C	09

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 2, Nomor 2, Januari 2021
e-ISSN 2685-998X
DOI 10.30865/json.v2i2.2535

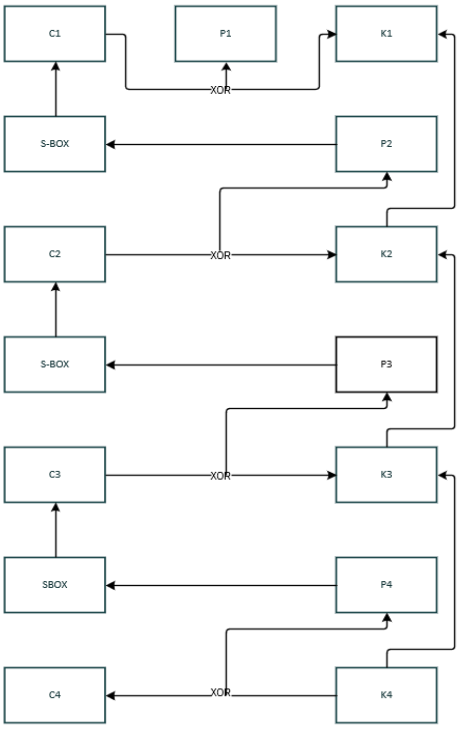
TABEL S-BOX			
INPUT	XOR-4	S-BOX	S-BOX INVERSE
02	2	77	6A
03	3	7B	D5
04	4	F2	30
05	5	6B	36
06	6	6F	A5
07	7	C5	38
08	8	30	BF
09	9	01	40
0A	A	67	A3
0B	B	2B	9E
0C	C	FE	81

Tabel 3 adalah tabel substitusi S-Box yang digunakan dalam proses enkripsi dan dekripsi. S-Box ini digunakan karena lebih mudah dipahami. Misalnya di-*input*-kan *hexadecimal* dengan *variable* "01" maka hasil yang dikeluarkan "7c". untuk algortma dilakukan dengan mengambil *plantext* "Salatiga" dan kunci "Semarang". Setelah melalui proses enkripsi maka mendapatkan ciphertext yang telah dikonversi ke nilai *hexadecimal*.

Tabel 3. Hasil *Ciphertext* Setiap Putaran

HASIL CIPHERTEXT	
PUTARAN 1	0559DA6DE2EE1035
PUTARAN 2	0BA060C28E342263
PUTARAN 3	99C9C4AF55E326CF
PUTARAN 4	A7DFC5AD18D371CD
PUTARAN 5	5CCD7E67E5593C5D
PUTARAN 6	1CDA6BDA9FDE69E9
PUTARAN 7	5C6FB239DDCD7451
PUTARAN 8	430D91CE49CFD974
PUTARAN 9	9115453F4AEB28BE
PUTARAN 10	6A3644037668AF71

Tabel 4 merupakan hasil *ciphertext* dari setiap putaran. Hasil putaran 10 merupakan *final ciphertext.* Gambar 5 memberikan penjelasan bagaimana alur proses pengembalian *ciphertext* ke *plaintext*. Pola yang digunakan sebagai pola pengambilan bit pada proses enkripsi akan digunakan sebagai pola pemasukan pada proses dekripsi. Sebaliknya pola pemasukan yang digunakan pada proses enkripsi akan digunakan sebagai pola pengambilan proses dekripsi sehingga dapat dikatakan pola logo media sosial digunakan sebagai pola pemasukan bit pada proses dekripsi.



Gambar 5. Rancangan Alur Dekripsi

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 2, Nomor 2, Januari 2021
e-ISSN 2685-998X
DOI 10.30865/json.v2i2.2535

Gambar 4, Proses dekripsi dimulai dari memasukkan *ciphertext* pada kolom matriks C4 kemudian di-XOR dengan K4 pada proses K4 menghasilkan P4. Kemudian P4 ditransformasikan kedalam S-BOX dan menghasilkan C3, C3 di-XOR dengan K3 pada proses K3 menghasilkan P3. Kemudian P3 ditransformasikan kedalam S-BOX dan menghasilkan C2, C2 di-XOR dengan K2 pada proses K2 menghasilkan P2. Kemudian, P2 ditransformasikan kedalam S-BOX dan menghasilkan C1, C1 di-XOR dengan K1 menghasilkan P1, proses tersebut dilakukan sebanyak 10 putaran sesuai dengan banyaknya putaran enkripsi sehingga hasil akhir dari dekripsi putaran ke-10 yaitu *plaintext* awal.

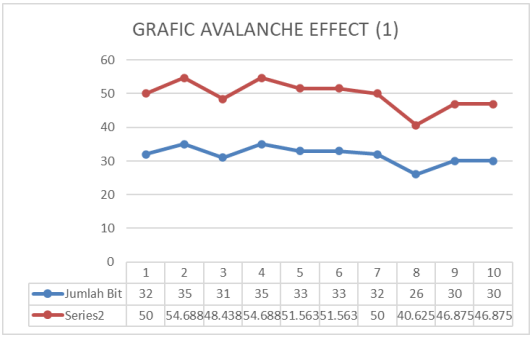
Pengujian korelasi digunakan untuk mengukur seberapa acak perbandingan antara hasil enkripsi *(ciphertext)* dan *plaintext*. Nilai korelasi itu sendiri berkisar 1 sampai -1, jika nilai korelasi tersebut mendekati angka 1 maka *plaintext* dan *ciphertext* memiliki hubungan yang sangat kuat, tetapi jika mendekati angka 0 maka *plaintext* dan *ciphertext* memiliki hubungan yang lemah atau tidak kuat.

Tabel 4. Nilai Korelasi Setiap Putaran

KORELASI HASIL PUTARAN 1-10	
PUTARAN 1	0,265307353
PUTARAN 2	-0,43864502
PUTARAN 3	-0,379588221
PUTARAN 4	-0,602875118
PUTARAN 5	0,224855162
PUTARAN 6	-0,707979855
PUTARAN 7	0,5804054
PUTARAN 8	-0,227362591
PUTARAN 9	0,097711906
PUTARAN 10	0,371877189

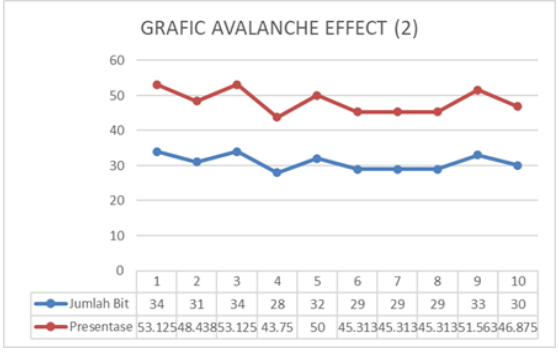
Tabel 5 menjelaskan nilai berdasarkan setiap putaran korelasi. Putaran ke 9 memiliki nilai korelasi yang baik karena nilai yang dihasilkan tingkat hubungan *plaintext* dan *ciphertext* masuk dalam kategori sangat rendah.

Pengujian *Avalanche Effect* harus dilakukan dengan tujuan untuk mengetahui berapa besar perubahan bit ketika karakter *plaintext* diubah. Pengujian dilakukan dengan tiga contoh *plaintext* yang berbeda dengan kunci yang sama dan kemudian akan diubah satu karakter pada plaintext sehingga dapat menghasilkan perbedaan *Avalanche Effect* pada setiap putaran yang dilakukan.



Gambar 6. Grafik Pengujian *Avalanche Effect* 1

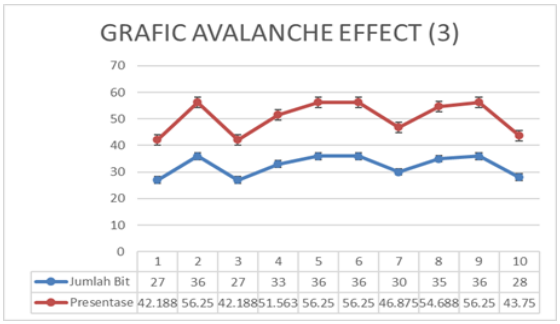
Gambar 6, menjelaskan *plaintext* yang digunakan dalam grafik *Avalanche Effect* (1) yaitu DISASTER yang diubah menjadi DISCSTER dengan kunci SRIRAMSR. Terjadi peningkatan yang besar pada putaran kedua dan selajutnya terjadi penurunan 4 bit pada putaran ketiga namun kembali meningkat pada putaran keempat dan terjadi penurunan lagi pada putaran kelima dan seterusnya.



Gambar 7. Grafik Pengujian *Avalanche Effect* 2

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 2, Nomor 2, Januari 2021
e-ISSN 2685-998X
DOI 10.30865/json.v2i2.2535

Gambar 7, plaintext yang digunakan dalam grafik Grafik *Avalanche Effect* (2) THEA2016 yang diubah menjadi THEC2016 dengan kunci SRIRAMSR, ini menunjukkan hasil yang tidak stabil karena terjadi peningkatan signifikan pada putaran pertama, namun pada putaran kedua terjadi penurunan 3 bit dan kembali meningkat pada putaran ketiga, pada putaran keempat terjadi penurunan sebanyak 4 bit dan pada putaran kelima kembali meningkat sebanyak 4 bit.



Gambar 8. Grafik Pengujian *Avalanche Effect* 3

Gambar 8, pada grafik *Avalanche Effect* (3) plaintext yang digunakan 7|-|3AMB yang diubah menjadi 7|-|3CMB dengan kunci SRIRAMSR, sama halnya dengan grafik (1) dalam grafik ini menunjukan *avalanche effect* yang tidak stabil karena terjadi peningkatan mencapai 56% pada putaran kedua kemudian mengalai penurunan hingga 42% pada putaran ketiga namun kembali mengalami peningkatan pada putaran keempat yang mencapai 51%, putaran kelima dan keenam 56%, kemudian terjadi penurunan kembali pada putaran ketujuh yang mencapai 46% meningkat lagi pada putaran kedelapan mencapai 54% dan putaran kesembilan 56%, dan mengalami penurunan kembali pada putaran kesepuluh yaitu mencapai 43%.

4. KESIMPULAN

Berdasarkan penelitian dan pengujian yang dilakukan, dapat disimpulkan kriptografi *block cipher* 64 bit berbasis pola media sosial dapat melakukan enkripsi dan telah memenuhi standart konsep 5-*tuple* Stinson dan dapat diakui sebagai sistem kriptografi. Kemudian perubahan 1 karakter dapat membuat perubahan yang siginifikan pada analisis *avalanche effect* karena adanya tabel susbstitusi *S-Box* yang dipasang dalam proses putaran pertama, kedua, dan ketiga. Adapun dilakukan pengujian korelasi setiap putaran memiliki nilai korelasi yang lemah sehingga dapat disimpulkan perancangan kriptografi *block cipher* 64 bit berbasis pola logo media sosial dapat menghasilkan *output* enkripsi yang acak. Sehingga dapat digunakan untuk mengamankan data atau informasi berupa teks. Dalam setiap pengujian *avalanche effect* menunjukkan bahwa *S-Box* berpengaruh didalam proses enkripsi karena dalam setiap putaran memiliki *avalanche effect* yang mencapai 50%.

REFERENCES

[1] A. K. Aziiz and M. A. I. Pakereng, "Perancangan Teknik Kriptografi Block Cipher Berbasis Pola Batik Ceplok Yogyakarta," *J. Sist. dan Teknol. Inf.*, vol. 8, no. 1, p. 68, 2020, doi: 10.26418/justin.v8i1.37135.
[2] J. D. No, K. Sidorejo, K. Salatiga, and J. Tengah, "Perancangan Kriptografi Block Cipher Berbasis Pola Tarian Denok Deblong," no. 52, pp. 43–51, doi: 10.21460/jutei.2018.31.146.
[3] P. B. T. Kumbara and M. A. I. Pakereng, "Perancangan Teknik Kriptografi Block Cipher Berbasis Pola Permainan Tradisional Rangku Alu," *J. Tek. Inform. dan Sist. Inf.*, vol. 5, no. 2, pp. 189–200, 2019, doi: 10.28932/jutisi.v5i2.1714.
[4] J. Diponegoro, "PADA DATA CITRA."
[5] R. Munir, "Kriptografi."
[6] D. T. Informatika, "Pengantar Kriptografi," 2004.
[7] M. A. I. Pakereng, "Perancangan Kriptografi Block Cipher Berbasis Pola Bercocok Tanam Pada Game Harvest Moon Artikel Ilmiah," no. 672013722, 2017.
[8] A. N. Setiawan, A. D. Wowor, and M. A. I. Pakereng, "Perancangan Algoritma pada Kriptografi Block Cipher dengan Teknik Langkah Kuda Dalam Permainan Catur," *Tek. Inform. Fak. Teknol. Informasi, Univ. Kristen Satya Wacana*, pp. 2–7, 2015.
[9] M. A. I. Pakereng, "Perancangan Kriptografi Block Cipher Menggunakan Pola Kabel UTP Straight dan Cross Over Artikel Ilmiah," no. November, 2016.
[10] A. Ilmiah *et al.*, "Perancangan Kriptografi Block Cipher Berbasis Pola Ikan Berenang," no. November, 2016.
[11] E. Juliansyah, M. T. Informatika, I. Pendahuluan, and R. L. Rivest, "Implementasi Algoritma Kriptografi Rc-6 Dalam," vol. 16, pp. 267–269, 2017.
[12] D. Andriani, "Perancangan Aplikasi Penyandian Teks Dengan Menggunakan Algoritma Chiper Block Chaining," *J. Tek. Inform. Unika St. Thomas*, vol. 02, no. 338, pp. 14–23, 2017.