ISSN 2355-3286

Perancangan Teknik Kriptografi *Block Cipher* Berbasis Pola Tarian Sajojo Papua

Dwayne Jeremy Euagellino Prihanto[1], Magdalena A. Ineke Pakereng, S.Kom.[2]
[1,2]Teknik Informatika, Universitas Kristen Satya Wacana
Jl.Dr. O. Notohamidjojo, Salatiga 50714, Indonesia
[1]dwaynejermaine96@gmail.com, [2]ineke.pakereng@staff.uksw.edu

Diterima 16 Oktober 2019
Disetujui 20 Desember 2019

***Abstract* — Cryptography is a science to maintain the security and confidentiality of an information. In this research we designed Block Cipher Cryptography 64 bit Based on Tarian Sajojo Papua Pattern to build new cryptography. In this critique is designed with 10 rounds, where each round there are 4 processes. In each round there are 4 patterns for the plaintext process and 4 patterns for the key process. In second and fourth process is transformed with S-BOX table to get a more random ciphertext. Testing is also done using Avalanche Effect and Correlation value where the average character change reaches 49,69%, so it can be used as an alternative in securing data.**

***Index* — Kriptografi adalah suatu ilmu untuk menjaga keamanan dan kerahasiaan suatu informasi. Dalam penelitian ini dirancang Kriptografi Block Cipher 64 bit Berbasis Pola Sajojo Papua guna membangun kriptografi baru. Dalam kritografi ini dirancang dengan 10 putaran, dimana setiap putaran terdapat 4 proses. Pada setiap putaran terdapat 4 pola untuk proses plaintext dan 4 pola untuk proses kunci. Di proses kedua dan keempat ditransformasikan dengan tabel S-BOX untuk mendapatkan ciphertext yang lebih acak. Pengujian juga dilakukan menggunakan Avalanche Effect dan nilai Korelasi dimana rata-rata perubahan karakter mencapai 49,69% sehingga dapat digunakan sebagai alternatif dalam mengamankan data.**

I. PENDAHULUAN

Enkripsi secara eksplisit dapat diartikan sebagai suatu proses untuk mengubah pesan (informasi) sehingga tidak dapat dilihat tanpa menggunakan kunci pembuka rahasia. Teknologi ini sudah digunakan sejak lama oleh kalangan militer dan intelejen. Saat ini, teknologi enkripsi dengan beberapa modifikasi sudah diaplikasikan untuk kepentingan umum, dalam aktivitas digital seperti merahasiakan data-data penting milik perorangan maupun perusahaan. Hasil statistik dari Breach Level Index (BLI) membuktikan, sepanjang 2016 telah terjadi 1.378.509.261 kehilangan atau pencurian data di seluruh dunia, atau sama dengan 3.776.738 data per hari, dan 157,364 per jam. Dari keseluruhan pelanggaran data di 2016 hanya 4 persen pembobolan data dianggap tidak berhasil karena data yang dicuri sudah terlebih dulu di enkripsi oleh perusahaan [1].

Maka dari itu, dapat dikatakan bahwa keamanan dalam proses pemindahan informasi sangat diperlukan. IT infrastruktur mulai gencar dalam merancang dan membangun untuk mengamankan informasi. Kriptografi hadir sebagai ilmu untuk menjaga kerahasiaan pesan/mengamankan informasi. Informasi yang dapat dibaca dan dipahami dengan bahasa tertentu diubah ke dalam bentuk sandi tertentu yang berstruktur huruf/kata/kalimat yang susah dipahami dari segi bahasa apapun. Salah satu algoritma nya adalah menggunakan algoritma Kriptografi Block Cipher. Block Cipher menggunakan kumpulan bit dengan panjang tetap yang disebut sebagai block dan kemudian dioperasikan dengan cipher kunci untuk nantinya ditransformasikan. Seiring kemajuan teknologi, makin banyak pula cara untuk memecahkan algoritma ini. Untuk itu salah satu cara untuk membuat data atau informasi menjadi lebih aman adalah dengan membuat pola atau algoritma baru untuk memodifikasi algoritma yang sudah ada.

Penelitian ini merupakan kriptografi Block cipher dengan menggunakan pendekatan pola Tarian Sajojo Papua. Dari pola-pola tersebut akan dicari korelasi terbaik yang kemudian akan digunakan sebagai proses enkripsi dan dekripsi pesan plaintext. Beberapa gerakan-gerakan dalam tarian sajojo papua dijadikan pola pertukaran kode bit di dalamnya. Sehingga kemanan data menjadi lebih kuat dan data dapat digunakan sebagaimana mestinya.

II. TINJAUAN PUSTAKA

Penelitian sebelumnya berjudul Perancangan Kriptografi Block Cipher Berbasis pada Teknik Formasi Permainan Bola. Penelitian ini membahas mengenai perancangan kriptografi berbasis pada Teknik formasi permainan bola dapat melakukan proses enkripsi dan dekripsi dan telah memenuhi 5-tuple dari kriptosistem [3].

Penelitian sebelumnya berjudul Perancangan Kriptografi *Block Cipher* Berbasis Pola Gerakan Lempeng Tektonik Divergensi dan Konvergensi. Penelitian ini membahas mengenai perancangan

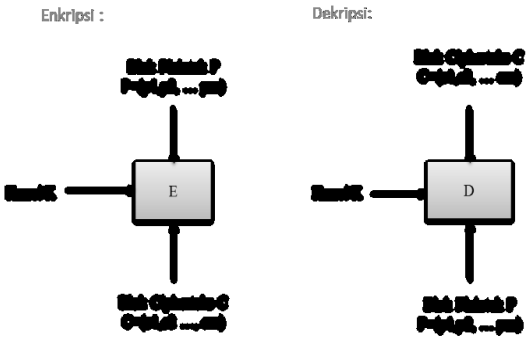
kriptografi *Block Cipher* berbasis pada pola gerakan lempeng tektonik divergensi dan konvergensi, dimana pola divergensi dijadikan dalam pertukaran kode bit pada *plaintext* sedangkan pola konvergensi digunakan pada pertukaran kode bit kunci [5].

Penelitian sebelumnya berjudul Perancangan Kriptografi *Block Cipher* dengan Langkah Permainan Engklek. Penelitian ini membahas mengenai ekperimen perancangan *Block Cipher* untuk diimplementasikan menjadi sebuah aplikasi yang dapat digunakan secara otomatis melakukan enkripsi dan dekripsi, dan penelitian ini menunjukkan bahwa permainan tradisional dari Indonesia juga dapat dijadikan alur algoritma [7].

Penelitian sebelumnya berjudul Perancangan Kriptografi *Block Cipher* Berbasis Pola Formasi Futsal 1-2-1. Penelitian ini membahas mengenai kriptografi Block Cipher 256-bit berbasis formasi futsal 1-2-1 dapat menunjukan ciri khas dari sebuah permainan futsal dalam sebuah team sehingga dapat menyembunyikan kerahasiaan data lebih baik [4].

Penelitian sebelumnya berjudul Perancangan Kriptografi *Block Cipher* 256-bit Berbasis pada Game SUDOKU. Penelitian ini membahas mengenai kriptografi *Block Cipher* 256-bit berbasis Game SUDOKU dapat menunjukan bahwa dari Game SUDOKU yang tersembunyi, sehingga tidak banyak orang mengira bahwa dengan Game SUDOKU ada rahasia yang tersimpan [6].

Skema proses enkripsi dan dekripsi *block cipher* secara umum digambarkan pada Gambar 1.



Gambar 1. Skema Proses Enkripsi dan Dekripsi Pada Block Cipher [9].

Misalkan blok *plaintext* (P) yang berukuran m bit dinyatakan sebagai

$P= (p_1, p_2, \dots p_n)$ (1)

Blok *ciphertext* (C) dinyatakan sebagai

$C = (c_1, c_2, \dots c_n)$ (2)

Kunci (K) dinyatakan sebagai

$K = (k_1, k_2, \dots k_n)$(3)

Sehingga proses enkripsi adalah

$EK(P) = C$ (4)

Dan proses dekripsi adalah

$DK(C) = P$ (5)

Sebuah sistem kriptografi harus memenuhi lima-tupel (*five-tuple*) (**P, C, K, E, D**) dengan kondisi [10]:

1. **P** adalah himpunan berhingga dari *Plaintext.*
2. **C** adalah himpunan berhingga dari *Ciphertext.*
3. **K** merupakan ruang kunci (*keyspace*), adalah himpunan berhingga dari kunci.
4. Untuk setiap $k \in \boldsymbol{K}$ terdapat aturan enkripsi $e_k \in \boldsymbol{E}$ dan berkorespodensi dengan aturan dekripsi $d_k \in \boldsymbol{D}$. Setiap $e_k: \boldsymbol{P} \rightarrow \boldsymbol{C}$ dan $d_k: \boldsymbol{C} \rightarrow \boldsymbol{P}$ adalah fungsi sedemikian hingga $d_k(e_k(x)) = x$ untuk setiap *plaintext* $x \in \boldsymbol{P}$.

Dalam pengujian menggunakan korelasi yang merupakan teknik statistik untuk mengukur kekuatan hubungan antar dua variabel dan untuk mengetahui bentuk hubungan antara dua variabel tersebut dengan hasil yang bersifat kuantitatif. Kekuatan hubungan antar dua variabel itu disebut dengan koefisien korelasi. Nilai koefisien akan selalu berada diantara -1 sampai +1. Untuk menentukan kuat atau lemahnya hubungan antara variabel yang diuji, dapat digunakan Tabel 1. [6].

TABEL I
KLASIFIKASI KOEFISIEN KORELASI

Interval Koefisian	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

Selain itu proses *block cipher* ini menggunakan operasi XOR dimana output yang dihasilkan dari proses enkripsi akan susah ditebak, karena apabila kita melihat dasar dari XOR seperti berikut :

- 0 XOR 0 = 0
- 0 XOR 1 = 1
- 1 XOR 0 = 1
- 1 XOR 1 = 0

Maka apabila hasil output adalah 0 untuk mendapatkan input nya kita tidak tahu, bisa jadi input yang dihasilkan adalah 1 atau 0. Dasar tersebut digunakan untuk melakukan kriptografi *block cipher*.

Kemudian *S-Box* (*Substitution Box*) merupakan salah satu prinsip dalam perancangan *block cipher* dimana proses *s-box* itu sendiri adalah mengganti karakter inputan dengan karakter yang sudah menjadi tetapan pada sebuah tabel. Secara teoritis, *S-Box*

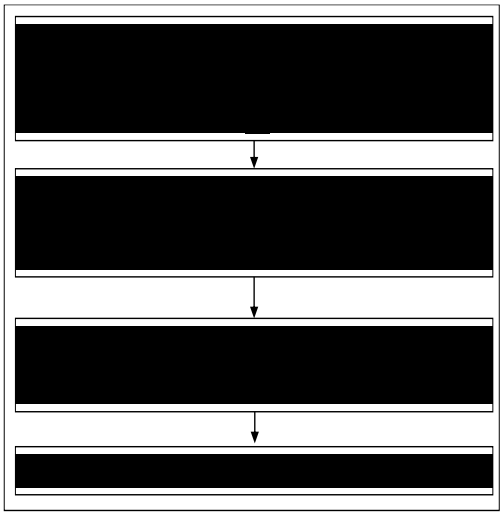
adalah satu-satunya algoritma yang mempunyai kemampuan untuk membuat hubungan yang tidak linier antara *plaintext* dan *ciphertext*. Maka dari itu, penggunaan *S-Box* ditujukan agar membuat Kriptografi *block cipher* menjadi lebih acak. Hal ini dilakukan dengan cara mensubstitusikan bilangan *hexadecimal* ke dalam tabel *S-Box* dan kemudian kita ambil output dari tabel *S-Box* berupa bilangan *hexadecimal* yang baru.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Gambar 2. Tabel S-Box

III. METODE PENELITIAN

Secara umum penelitian terbagi ke dalam 4 (empat) tahapan, yaitu: (1) tahap identifikasi masalah, (2) tahap perancangan, (3) tahap implementasi dan analisis hasil, (4) tahap pelaporan dari hasil penelitian.

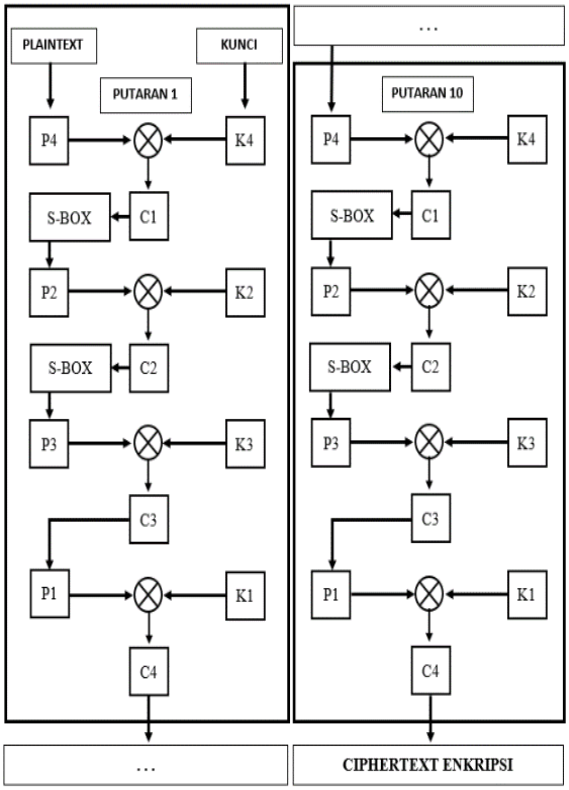


Gambar 3. Tahapan Penelitian

Tahapan penelitian tersebut dapat dijelaskan sebagai berikut.

1. Identifikasi Masalah: pada tahap ini dilakukan analisis terhadap permasalahan yang ada, yaitu perancangan kriptografi *block cipher* menggunakan pola Tarian Sajojo Papua.
2. Perancangan: tahapan selanjutnya adalah perancangan kriptografi *block cipher* dengan menggunakan pola Tarian Sajojo Papua.
3. Implementasi dan Analisis Hasil: setelah perancangan selesai kemudian dilakukan uji coba dan analisis dari kriptografi yang telah dibuat.
4. Laporan Hasil Penelitian: tahap terakhir adalah penulisan penelitian yang sudah dilakukan dalam bentuk laporan.

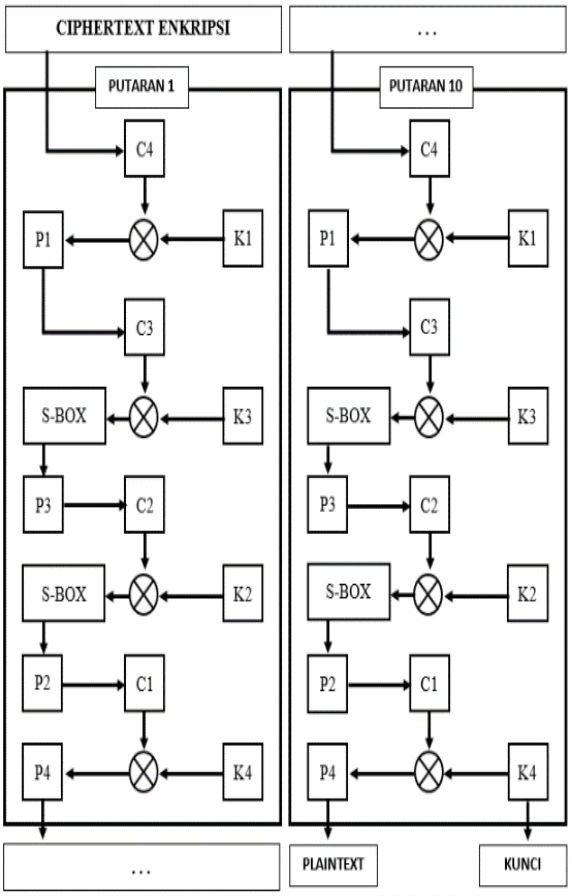
Dalam perancangan kriptografi *block cipher* pada pola Tarian Sajojo Papua ini dilakukan dua proses yaitu enkripsi dan proses dekripsi. Enkripsi dan dekripsi itu sendiri dilakukan dalam 10 putaran. 10 putaran untuk enkripsi dan 10 putaran untuk dekripsi. Di setiap putaran terdapat 4 proses.



Gambar 4. Proses Alur Enkripsi

Langkah-langkah proses enkripsi dapat dijabarkan sebagai berikut: a) Menyiapkan plaintext; b) Mengubah plaintext menjadi biner sesuai dalam tabel ASCII; c) Dalam proses enkripsi, *plaintext* dan kunci akan melewati empat proses pada setiap putaran, yaitu : 1) Putaran pertama *Plaintext* 1 (P1) melakukan transformasi dengan pola tarian Sajojo Papua dan di XOR dengan Kunci 1 (K1) menghasilkan *Ciphertext* 1 (C1); 2) *Plaintext* 2 (P2) melakukan transformasi dengan pola tarian Sajojo Papua dan di XOR dengan Kunci 2 (K2) menghasilkan *Ciphertext* 2 (C2), dan tahapan tersebut akan berlanjut sampai empat proses yang menghasilkan *Ciphertext* 4 (C4) ; 3) *Ciphertext* 4 (4) masuk pada putaran kedua dengan alur proses yang sama dengan putaran pertama, dan tahapan tersebut

akan berlanjut sampai putaran ke-20 yang menghasilkan *Ciphertext* Akhir.



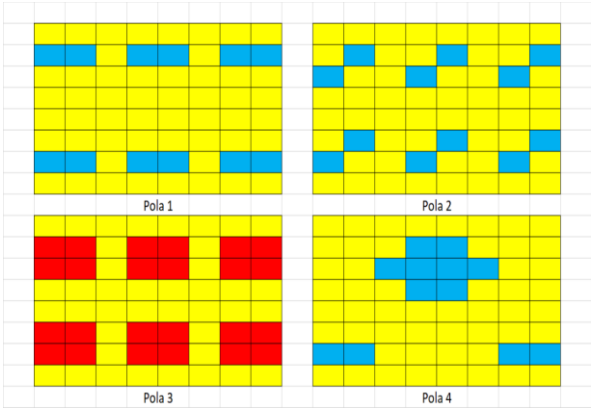
Gambar 5. Proses Alur Deskripsi

Gambar 5 menunjukan alur proses dekripsi, langkah-langkah proses dekripsi tersebut dijelaskan sebagai berikut: a) Menyiapkan *ciphertext* dan kunci; b) Mengubah *ciphertext* dan kunci menjadi biner sesuai dalam tabel ASCII; c) dalam perancangan dekripsi, *ciphertext* dan kunci akan melewati empat proses pada setiap putaran; d) Putaran pertama *Ciphertext* (C) diproses dengan pola dan di XOR dengan Kunci 4 (K4) dari putaran 20, menghasilkan P4; d) P4 tersebut kemudian menjadi C3 di putaran 20; e) Masuk pada putaran dua, C3 diproses dengan pola dan di XOR dengan Kunci 3 (K3) dari putaran 20, menghasilkan P3; Proses tersebut berlanjut sampai ke putaran 10 sehingga menghasilkan *Plaintext* akhir.

IV. HASIL DAN PEMBAHASAN

Dalam bagian ini akan membahas tentang algoritma perancangan kriptografi block cipher 64bit berbasis pola Tarian Sajojo Papua secara lebih rinci.

Dalam algoritma ini pola yang terdapat pada contoh Tarian Sajojo Papua digunakan sebagai proses pemasukan dan pengambilan bit. Pola tersebut ditunjukan pada Gambar 5.



Gambar 6. Tahapan Penelitian

Pada Gambar 6 menunjukan empat pola yang berbeda, dimana pola-pola tersebut menunjukan pola-pola yang terdapat pada tarian Sajojo Papua. Berdasarkan pola-pola yang sudah dirancang, dilakukan pengujian korelasi dengan mengkombinasikan urutan pola untuk menemukan nilai korelasi terbaik. Pengujian dilakukan menggunakan contoh plaintext "GWENNI01" menggunakan kunci "DAPHNE06".

Berdasarkan hasil pengujian korelasi, maka hasil terkecil yang akan digunakan sebagai acuan perancangan dalam proses enkripsi dan dekripsi.

TABEL II
HASIL KORELASI SETIAP KOMBINASI POLA TARIAN SAJOJO PAPUA

RATA-RATA NILAI KORELASI			
POLA	**RATA-RATA**	**POLA**	**RATA-RATA**
1-2-3-4	0,009425450	3-1-2-4	0,161300639
1-2-4-3	0,017899859	3-1-4-2	0,170749096
1-3-2-4	0,090862916	3-2-1-4	0,582125035
1-3-4-2	0,207041609	3-2-4-1	0,645915328
1-4-2-3	0,220356177	3-4-1-2	0,591970156
1-4-3-2	0,180880160	3-4-2-1	0,556334151
2-1-3-4	0,361258097	4-1-2-3	0,429722001
2-1-4-3	0,313262995	4-1-3-2	0,506564942
2-3-1-4	0,038877346	4-2-1-3	0,146680735
2-3-4-1	0,659971578	4-2-3-1	0,006651533
2-4-1-3	0,130867750	4-3-1-2	0,046562621
2-4-3-1	0,502260685	4-3-2-1	0,490564999

Tabel 2 menunjukan hasil kombinasi pola dan mendapatkan nilai korelasi terbaik pada kombinasi pola 4-2-3-1. Kombinasi ini yang akan digunakan untuk melanjutkan proses enkripsi hingga putaran ke-10 untuk menghasilkan ciphertext.

Telah dijelaskan bahwa perancangan kriptografi ini dilakukan sebanyak 10 putaran, dan disetiap putaran memiliki 4 proses untuk mendapatkan hasil akhir yaitu ciphertext. Proses pertama plaintext dan kunci diubah kedalam bentuk ASCII kemudian diubah lagi

kedalam biner. Kemudian bit-bit *plaintext* diproses dengan pola pemasukan dan pengambilan kedalam kolom matriks 8x8 menggunakan bagian dari pola tarian yang berbeda-beda pada setiap proses. Kemudian di setiap proses dilakukan X-OR dari Plaintext (P) dan kunci (K) menghasilkan ciphertext (C) sampai proses keempat di setiap putaran. Kemudian diulang terus sampai putaran ke-10 dan hingga menghasilkan Ciphertext akhir.

Untuk menjelaskan secara detail proses pemasukan bit dalam matriks maka diambil proses 1 pada putaran 1 sebagai contoh. Misalkan angka 1 merupakan inisialisasi setiap bit yang merupakan hasil konversi plaintext maka urutan bit adalah sebagai berikut 1, 2, 3, 4, ….64.

1	2	3	4	36	35	34	33
8	7	6	5	37	38	39	40
9	10	11	12	44	43	42	41
16	15	14	13	45	46	47	48
17	18	19	20	52	51	50	49
24	23	22	21	53	54	55	56
25	26	27	28	60	59	58	57
32	31	30	29	61	62	63	64

Pola Kunci 1

1	8	9	16	17	24	25	32
2	7	10	15	18	23	26	31
3	6	11	14	19	22	27	30
4	5	12	13	20	21	28	29
61	60	53	52	45	44	37	36
62	59	54	51	46	43	38	35
63	58	55	50	47	42	39	34
64	57	56	49	48	41	40	33

Pola Kunci 2

33	34	35	36	29	30	31	32
40	39	38	37	28	27	26	25
41	42	43	44	21	22	23	24
48	47	46	45	20	19	18	17
49	50	51	52	13	14	15	16
56	55	54	53	12	11	10	9
57	58	59	60	5	6	7	8
64	63	62	61	4	3	2	1

Pola Kunci 3

33	40	41	48	49	56	57	64
34	39	42	47	50	55	58	63
35	38	43	46	51	54	59	62
36	37	44	45	52	53	60	61
29	28	21	20	13	12	5	4
30	27	22	19	14	11	6	3
31	26	23	18	15	10	7	2
32	25	24	17	16	9	8	1

Pola Kunci 4

Gambar 7. Pola Pemasukan Kunci

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	37
16	17	18	19	20	21	38	39
22	23	24	25	26	40	41	42
27	28	29	30	43	44	45	46
31	32	33	47	48	49	50	51
34	35	52	53	54	55	56	57
36	58	59	60	61	62	63	64

Gambar 8. Pola Ambil Semua Kunci

13	20	27	34	39	44	51	58
14	21	28	1	2	45	52	59
15	22	3	4	5	6	53	60
16	23	29	7	8	46	54	61
17	24	30	35	40	47	55	62
18	25	31	36	41	48	56	63
9	10	32	37	42	49	11	12
19	26	33	38	43	50	57	64

Gambar 9. Pola Pemasukan Plaintext dari Pola 4 Untuk Proses 1 di Setiap Putaran

58	57	44	43	34	33	20	19
59	56	45	8	7	32	21	18
60	55	3	4	5	6	22	17
61	54	46	2	1	31	23	16
62	53	47	42	35	30	24	15
63	52	48	41	36	29	25	14
12	11	49	40	37	28	10	9
64	51	50	39	38	27	26	13

Gambar 10. Pola Pengambilan Plaintext dari Pola 4 Untuk Proses 1 di Setiap Putaran

Gambar 9 merupakan pola masuk dari pola 4 yang digunakan untuk memasukkan setiap 8 bit dari karakter plaintext, kemudian pola tersebut diimplementasikan ke dalam excel. Dari pola tersebut kemudian diambil bitnya sesuai pola ambil pada Gambar 10 sehingga menghasilkan bit bit yang nantinya akan di XOR kan dengan kunci yang sebelumnya sudah dimasukkan ke pola masuk seperti pada Gambar 7 dan sudah diambil menggunakan pola ambil seperti Gambar 8, sehingga menghasilkan Ciphertext 1.

13	24	25	38	39	52	53	64
14	2	26	37	4	51	54	6
1	23	27	3	40	50	5	63
15	22	28	36	41	49	55	62
16	21	29	35	42	48	56	61
17	11	30	34	9	47	57	7
12	20	31	10	43	46	8	60
18	19	32	33	44	45	58	59

Gambar 11. Pola Pemasukan Plaintext dari Pola 2 Untuk Proses 2 di Setiap Putaran

59	58	45	44	33	32	19	18
60	8	46	43	10	31	20	12
7	57	47	9	34	30	11	17
61	56	48	42	35	29	21	16
62	55	49	41	36	28	22	15
63	5	50	40	3	27	23	1
6	54	51	4	37	26	2	14
64	53	52	39	38	25	24	13

Gambar 12. Pola Pengambilan Plaintext dari Pola 2 Untuk Proses 2 di Setiap Putaran

Gambar 11 merupakan pola masuk dari pola 2 yang digunakan untuk memasukkan setiap 8 bit dari karakter plaintext, kemudian pola tersebut diimplementasikan ke dalam excel. Dari pola tersebut kemudian dilakukan proses S-BOX lalu hasilnya dalam bentuk biner diambil sesuai pola ambil pada Gambar 12 sehingga menghasilkan bit bit yang nantinya akan di XOR kan dengan kunci yang sebelumnya sudah dimasukkan ke pola masuk seperti pada Gambar 7 dan sudah diambil menggunakan pola ambil seperti Gambar 8, sehingga menghasilkan Ciphertext 2.

25	26	27	28	29	30	31	32
1	2	34	5	6	33	9	10
4	3	35	8	7	36	12	11
44	43	42	41	40	39	38	37
45	46	47	48	49	50	51	52
13	14	54	17	18	53	21	22
16	15	55	20	19	56	24	23
64	63	62	61	60	59	58	57

Gambar 13. Pola Pemasukan Plaintext dari Pola 3 Untuk Proses 3 di Setiap Putaran

57	58	59	60	61	62	63	64
4	3	56	8	7	55	12	11
1	2	53	5	6	54	9	10
52	51	50	49	48	47	46	45
37	38	39	40	41	42	43	44
16	15	36	20	19	35	24	23
13	14	33	17	18	34	21	22
32	31	30	29	28	27	26	25

Gambar 14. Pola Pengambilan Plaintext dari Pola 3 Untuk Proses 3 di Setiap Putaran

Gambar 13 merupakan pola masuk dari pola 3 yang digunakan untuk memasukkan setiap 8 bit dari karakter plaintext, kemudian pola tersebut diimplementasikan ke dalam excel. Dari pola tersebut kemudian diambil bitnya sesuai pola ambil pada Gambar 14 sehingga menghasilkan bit bit yang nantinya akan di XOR kan dengan kunci yang sebelumnya sudah dimasukkan ke pola masuk seperti pada Gambar 7 dan sudah diambil menggunakan pola ambil seperti Gambar 8, sehingga menghasilkan *Ciphertext* 3.

13	14	15	16	17	18	19	20
1	2	22	3	4	21	5	6
23	24	25	26	27	28	29	30
38	37	36	35	34	33	32	31
39	40	41	42	43	44	45	46
54	53	52	51	50	49	48	47
7	8	55	9	10	56	11	12
64	63	62	61	60	59	58	57

Gambar 15. Pola Pemasukan Plaintext dari Pola 1 Untuk Proses 4 di Setiap Putaran

57	58	59	60	61	62	63	64
12	11	56	10	9	55	8	7
47	48	49	50	51	52	53	54
46	45	44	43	42	41	40	39
31	32	33	34	35	36	37	38
30	29	28	27	26	25	24	23
6	5	21	4	3	22	2	1
20	19	18	17	16	15	14	13

Gambar 16. Pola Pengambilan Plaintext dari Pola 1 Untuk Proses 4 di Setiap Putaran

Gambar 15 merupakan pola masuk dari pola yang digunakan untuk memasukkan setiap 8 bit dari karakter plaintext, kemudian pola tersebut diimplementasikan ke dalam excel. Dari pola tersebut kemudian dilakukan proses S-BOX lalu hasilnya dalam bentuk biner diambil bitnya sesuai pola ambil pada Gambar 16 sehingga menghasilkan bit bit yang nantinya akan di XOR kan dengan kunci yang sebelumnya sudah dimasukkan ke pola masuk seperti pada Gambar 7 dan sudah diambil menggunakan pola ambil seperti Gambar 8, sehingga menghasilkan Ciphertext 4.

Proses enkripsi putaran 1 telah selesai, kemudian dilakukan proses yang sama secara terus-menerus hingga putaran ke-10 untuk mendapatkan ciphertext akhir. Di semua putaran dilakukan proses transformasi dengan menggunakan Tabel *S-BOX* pada *Plaintext* 2 dan *Plaintext* 4.

TABEL III
TABEL PERUBAHAN P2 DAN P3 SETIAP PUTARAN SETELAH DILAKUKAN PROSES S-BOX

Putaran	**Plaintext**	**Hexa Sebelum Proses S-BOX**	**Hexa Sesudah Proses S-BOX**
1	P2	D7C260575AE8A4B7	0DA890DA46C81D20
	P3	3A8B0414462B9658	A2CE309B980B355E
2	P2	9B2CAAFCF856C993	E8426355E1B91222
	P3	4418925676728EBA	863474B90F1EE6C0
3	P2	ABCC8FA4EB545531	0E27731D3CFDED2E
	P3	287616759DD1095F	EEOFFF3F75514084
4	P2	3B7B018CF82E6EB0	490309F0E1CC345FC
	P3	62D72F3FD21AD212	AB0D4E257F437F39
5	P2	FF6E056DFB3B156A	7D4536B363492F58
	P3	48038E1BDF34653F	D4D5E644EF28BC25
6	P2	C93BC52B54E0E92D	1249070BFDA0EBFA
	P3	CE4C6C0D1ED78E5A	EC5DB8F3E90DE646
7	P2	3538F08290DC36AB	D97617119693240E
	P3	8979F330CA6380B3	F2AF7E0810003A4B
8	P2	ED9A12C38B376BAF	53373933CEB2051B
	P3	29F13D8A1D614C01	4C2B8BCFDED85D09
9	P2	761638DDFF01159F	0FFF76C97D092F6E
	P3	5B381E358DF4BD46	5776E9D9B4BACD98
10	P2	04E184A4299BD7CF	30E04F1D4CE80D5F
	P3	104348FAD6F6A669	7C64D4144AD6C5E4

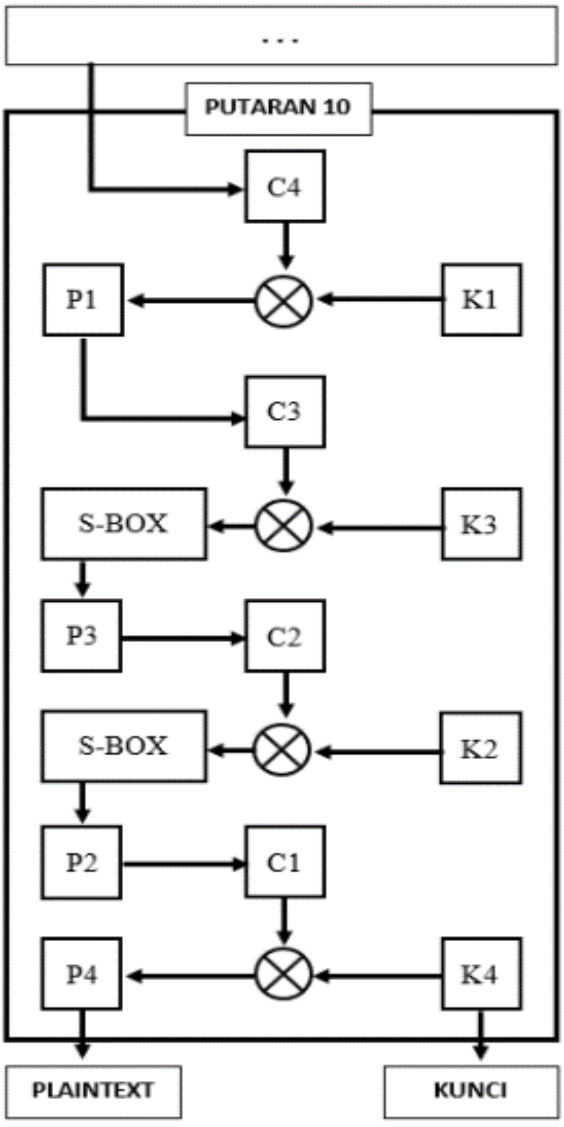
Tabel 3 merupakan hasil dari proses S-BOX yang dilakukan pada setiap putaran untuk proses Plaintext 2 dan Plaintext 3. Proses S-BOX dilakukan agar Chipertext yang dihasilkan pada setiap akhir putaran menjadi lebih acak.

Untuk pengujian algoritma dilakukan dengan mengambil contoh plaintext GWENNI01 dan kunci adalah DAPHNE06. Kemudian dilakukan proses enkripsi sebanyak 10 putaran, dan disetiap putaran enkripsi akan mendapatkan ciphertext (C) berupa char dan konversi hexadesimal. Hasil enkripsi dari putaran ke 10 adalah final ciphertext ditunjukan pada Tabel 4.

TABEL IV
HASIL CIPHERTEXT SETIAP PUTARAN PADA PROSES ENKRIPSI

Putaran	Hasil Hexadesimal	Hasil Char
1	F147964FA14D0BA	ñG–úÐº
2	5ABE15AEF08410BA	Z¾®ð„º
3	963A369D4E63CCA	c£iÔæ<Ê
4	AAF663585EC479B7	ªöcX^Äy·
5	4A12A1A9128BDDF8	J¡©‹Ýø
6	99B4DA29896B65E8	™´Ú)‰keè
7	96251D2AFD13FDA6	–%*ýý¦
8	1CB74C7C73E3A6E	·ÇÇ>:n
9	2EC1B0F0CAFEE755	.Á°ðÊþçU
10	EA14FD29794750ED	êý)yGPí

Kemudian masuk ke proses dekripsi. Proses dekripsi adalah proses merubah ciphertext menjadi plaintext awal. Dekripsi dilakukan sama seperti enkripsi, tetapi dekripsi dimulai dari putaran ke-10 menuju putaran ke-1 untuk mendapatkan *plaintext* awal.



Gambar 17. Skema Proses Dekripsi

Gambar 17 menjelaskan alur dekripsi. Pola pengambilan pada proses enkripsi akan menjadi pola pemasukan pada proses dekripsi, sedangkan pola pemasukan pada enkripsi akan digunakan sebagai pola pengambilan pada dekripsi. Proses dekripsi dimulai dari memasukkan ciphertext ke kolom matrik 8x8 C4 kemudian di-XOR dengan K1 pada proses keempat menghasilkan P1. Kemudian P1 akan digunakan sebagai C3 kemudian di XOR dengan K3 dan menghasilkan P3. P3 kemudian dilakukan proses S-BOX lalu akan digunakan sebagai C2 pada proses berikutnya. Setelah itu, C2 di-XOR dengan K2 menghasilkan P2. Kemudian P2 dilakukan proses S-BOX lalu akan digunakan sebagai C1 pada proses selanjutnya. C1 kemudian di-XOR dengan K4 menghasilkan P4, proses itu dilakukan berulang-ulang sebanyak 10 putaran sesuai dengan banyaknya putaran enkripsi dan hasil akhir dari dekripsi putaran ke-10 adalah *plaintext* awal.

TABEL V
ALGORITMA ENKRIPSI DAN DEKRIPSI

No.	Proses Enkripsi	No.	Proses Dekripsi
1.	Masukkan *plaintext*	1.	Masukkan *ciphertext*
2.	*Plaintext* diubah ke DECIMAL	2.	*Ciphertext* diubah ke DECIMAL
3.	DECIMAL diubah ke BINER	3.	DECIMAL diubah ke BINER
4.	Bit BINER dimasukkan ke kolom matriks 8x8 P4 dengan pola pemasukan *plaintext*	4.	Bit BINER dimasukkan ke kolom matriks 8x8 C4 dengan pola pemasukan *plaintext*
5.	Bit pada kolom matrik diambil menggunakan pola pengambilan pola 4	5.	C4 di-XOR dengan K4 menghasilkan P1
6.	Bit pengambilan dimasukkan lagi kedalam matrik mendapatkan hasil akhir P4	6.	P1 diproses dengan pola pemasukan *plaintext*
7.	P4 di-XOR dengan K4 menghasilkan C1	7.	Hasil proses P1 dimasukkan kedalam matriks 8x8 lagi dengan pola pengambilan pola 1
8.	C1 menjadi P2 untuk proses selanjutnya	8.	P1 menjadi C3 untuk proses selanjutnya
9.	Bit pada kolom matrik diambil menggunakan pola pengambilan pola 2	9.	C3 di-XOR dengan K3 menghasilkan P3
10.	Bit pengambilan dimasukkan lagi kedalam matrik mendapatkan hasil akhir P2	10.	P3 diproses dengan pola pemasukan *plaintext*
11.	P2 dilakukan proses S-BOX.	11.	P3 dilakukan proses S-BOX
12.	P2 di-XOR dengan K2 menghasilkan C2	12.	Hasil proses P3 dimasukkan kedalam matriks 8x8 lagi dengan pola pengambilan pola 3
13.	C2 menjadi P3 untuk proses selanjutnya	13.	P3 menjadi C2 untuk proses selanjutnya
14.	Bit pada kolom matrik diambil menggunakan pola pengambilan pola 3	14.	C2 di-XOR dengan K2 menghasilkan P2
	Bit pengambilan dimasukkan lagi kedalam matrik mendapatkan hasil akhir P3	15.	P2 diproses dengan pola pemasukan *plaintext*
16.	P3 dilakukan proses S-BOX.	16.	P2 dilakukan proses S-BOX
17.	P3 di-XOR dengan K3 menghasilkan C3	17.	Hasil proses P2 dimasukkan kedalam matriks 8x8 lagi dengan pola pengambilan pola 2
18.	C3 menjadi P1 untuk proses selanjutnya	18.	P2 menjadi C1 untuk proses selanjutnya
19.	Bit pada kolom matrik diambil menggunakan pola pengambilan pola 1	19.	C1 di-XOR dengan K4 menghasilkan P4
20.	Bit pengambilan dimasukkan lagi kedalam matrik mendapatkan hasil akhir P1	20.	P4 diproses dengan pola pemasukan *plaintext*
21.	P1 di-XOR dengan K1 menghasilkan C1	21.	Hasil proses P4 dimasukkan kedalam matriks 8x8 lagi dengan pola pengambilan

			pola 4
22.	C1 diubah ke DECIMAL	22.	P4 diubah ke DECIMAL
23.	DECIMAL diubah ke CHAR untuk mendapatkan *Ciphertext* akhir.	23.	DECIMAL diubah ke CHAR untuk mendapatkan *Plaintext* awal.

Tabel 5 merupakan algoritma proses ekripsi dan dekripsi secara menyeluruh. Proses enkripsi menghasilkan Ciphertext akhir, dan proses dekripsi menghasilkan Plaintext awal.

Algoritma proses Kunci (key), dijelaskan sebagai berkut:

1. Masukkan Kunci
2. Kunci diubah ke DECIMAL
3. DECIMAL ke BINER
4. Bit BINER dimasukkan ke kolom K4 dengan pola pemasukan Kunci
5. Bit kunci diambil dengan pola pengambilan Kunci
6. BINER hasil pengambilan dimasukkan kedalam kolom matrik K4
7. K4 = K2
8. K2 dimasukkan ke kolom matrik K2 dengan pola pemasukan
9. Bit kunci diambil dengan pola pengambilan Kunci
10. BINER hasil pengambilan dimasukkan kedalam kolom matrik K2
11. K2 = K3
12. K3 dimasukkan ke kolom matrik K3 dengan pola pemasukan
13. Bit kunci diambil dengan pola pengambilan Kunci
14. BINER hasil pengambilan dimasukkan kedalam kolom matrik K3
15. K3 = K1
16. K1 dimasukkan ke kolom matrik K1 dengan pola pemasukan
17. Bit kunci diambil dengan pola pengambilan Kunci
18. BINER hasil pengambilan dimasukkan kedalam kolom matrik K1

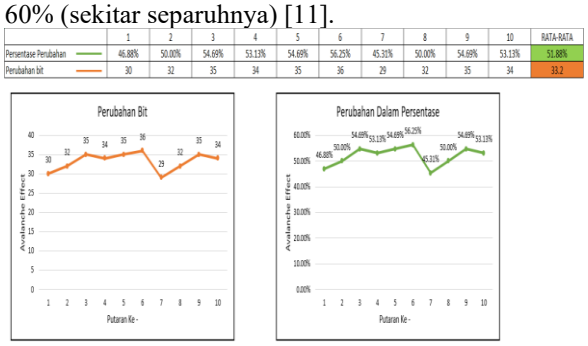
Dari setiap putaran, tentunya akan menghasilkan nilai korelasi antara *plaintext* dengan *ciphertext* yang bertujuan untuk menilai seberapa acak hasil enkripsi yang berupa *ciphertext* dengan *plaintext* awal pada masing-masing putaran. Nilai korelasi itu sendiri berkisaran 1 sampai -1 dimana jika nilai korelasi mendekati 0, maka *plaintext* dan *ciphertext* tidak memiliki nilai yang berhubungan. Akan tetapi jika nilai korelasi mendekati 1 atau -1, maka nilai dari korelasi itu sangat berhubungan.

TABEL VI
NILAI KORELASI SETIAP PUTARAN

Putaran	Nilai Korelasi
1	-0.537021257
2	-0.091528429
3	0.212142943
4	0.295297477
5	0.179997713
6	0.097581066
7	0.234471714
8	-0.847113678
9	-0.610498822
10	0.104262947

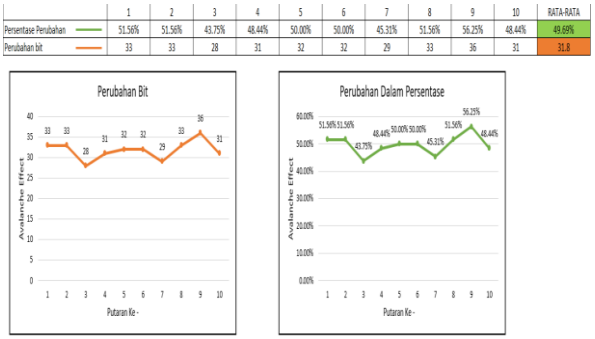
Tabel 6 menunjukkan nilai korelasi pada setiap putaran dan dapat disimpulkan bahwa algoritma Kriptografi Block Cipher berbasis pola Tarian Sajojo Papua memiliki korelasi yang lemah dan menghasilkan nilai korelasi yang acak. Kemudian pengujian Avalanche Effect dilakukan agar dapat mengetahui nilai perubahan bit yang ada ketika plaintext diubah. Pengujian dilakukan dengan mengubah karakter yang terdapat pada plaintext awal, dan tentunya akan menghasilkan perbedaan pada setiap putarannya.

Pada umunya, bit pada chipertext akan mengalami perubahan dari jumlah bit pada plaintext sebesar 50 %. Suatu Avalanche Effect dikatakan baik jika perubahan bit yang dihasilkan berkisar antara 45% - 60% (sekitar separuhnya) [11].



Gambar 18. Grafik Avalanche Effect dari Plaintext "GWENNI01"

Gambar 18 adalah hasil dari pengujian Avalanche Effect dimana plaintext awal yang digunakan adalah "GWENNI01". Pada putaran keenam perubahan bit yang terjadi tidak terlalu besar yaitu 56,25%. Dengan ini berarti terdapat perubahan bit yang baik, namun untuk nilai Avalanche Effect dapat dikatakan tidak begitu baik jika persentase jauh dari angka 50%. Berdasarkan hasil putaran pertama hingga putaran kesepuluh, dapat disimpulkan bahwa rata-rata hasil pengujian Avalanche Effect ini yaitu sebesar 51,88% yang berarti termasuk kategori sangat baik[11].



Gambar 19. Grafik Avalanche Effect dari Plaintext "VIONA997"

Pada Gambar 19 merupakan hasil dari pengujian Avalanche Effect dari plaintext awal "VIONA997", menghasilkan perubahan bit yang tidak terlalu tinggi dimana paling tinggi 56,25% pada putaran kesembilan . Nilai Avalanche Effect yang dihasilkan dari plaintext awal "VIONA997" lebih baik dibandingkan dengan plaintext awal "GWENNI01" yaitu sebesar 49,69% dengan kategori sangat baik[11].

V. SIMPULAN

Berdasarkan penelitian yang dilakukan, dapat disimpulkan bahwa kriptografi *block cipher* 64 bit berbasis pola Tarian Sajojo Papua dapat dikatakan sebagai sistem kriptografi. Dalam proses enkripsi, rancangan kriptografi *block cipher* berbasis pola Tarian Sajojo Papua 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 49,69% pada plaintext "VIONA997" dibandingkan dengan plaintext "GWENNI01" memiliki rata-rata perubahan yang mencapai 51,88% yang berarti algoritma kriptografi ini berhasil dan termasuk ke dalam kategori yang sangat baik. Penelitian ini sudah sangat baik apabila dibandingkan dengan penelitian terdahulu yang kebanyakan mempunyai nilai rata-rata *avalanche effect* sama-sama mendekati angka 50% yang berarti algoritma kriptografinya termasuk sangat baik.

VI. DAFTAR PUSTAKA

[1] Berita Satu, "Teknologi Enkripsi, Solusi Terbaik Pengamanan Data," [Online]. Available: http://www.beritasatu.com/iptek/426799-teknologi-enkripsi-solusi-terbaik-pengamanan-data.html. [Accessed 29 November 2018].

[2] Humaira, Rafiqa, dkk "Kriptanalisis dengan Metode Brute Force pada Graphics Processing Unit", Hal. 2–5, Bandung

[3] F. D. Paliama, "Perancangan Kriptografi Block Cipher Berbasis Pada Teknik Formasi Permainan Bola Perancangan Kriptografi Block Cipher Berbasis Pada Teknik Formasi Permainan Bola," Universitas Kristen Satya Wacana, 2016.

[4] N. M. Louhenapessy, "Perancangan Kriptografi Block Cipher Berbasis Pola Formasi Futsal 1-2-1," Universitas Kristen Satya Wacana, 2016.

[5] B. L. Setiyadi, " Perancangan Kriptografi Block Cipher Berbasis Pada Pola Gerakan Lempeng Tektonik Divergensi dan Konvergensi Program Studi Tenik Informatika Fakultas Teknologi Informasi Universitas Kristen Satya Wacana Salatiga Movember 2016 Perancangan Kriptografi Block, " Universitas Kristen Satya Wacana, 2016.

[6] Mahendra, Dwi Putera. 2016. Perancangan Kriptografi Block Cipher Menggunakan Pola Game SUDOKU. Universitas Kristen Satya Wacana: Salatiga.

[7] K. D. Cahyono, " Perancangan Kriptografi Block Cipher dengan Langkah Permainan Engklek, " Universitas Kristen Satya Wacana, 2016.

[8] Munir, R., 2006. Kriptografi. Bandung: Informatika.

[9] J. Leodrian, "Pengaruh Perubahan Ciphertext Terhadap Perancangan Kriptografi Block Cipher 64 Bit Berbasis Pola Ikatan Jimbe Dengan Menggunakan Kombinasi S-Box," Universitas Kristen Satya Wacana, 2016.

[10] Sugiyono. 2009. "Metode Penelitian Bisnis (Pendekatan Kuantitatif, Kualitatif, dan R&D)". Bandung : Alfabeta.

[11] Sugianto. 2016. Pengembangan Algoritma Advanced Encryption Standard pada Sistem Keamanan SMS Berbasis Android Menggunakan Algoritma Vigenere. Institut Teknologi Adhi Tama: Surabaya.