p-ISSN : 2443-2210
e-ISSN : 2443-2229

Perancangan Teknik Kriptografi *Block Cipher* Berbasis Pola Permainan Tradisional Rangku Alu

http://dx.doi.org/10.28932/jutisi.v5i2.1714

Perdana Bagas Tirta Kumbara ✉ #1, Magdalena A. Ineke Pakereng *2

[1,2]*Prodi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana*
Jl.Dr. O. Notohamidjojo, Salatiga 50714, Indonesia
[1]kumbaraperdana@gmail.com
[2]ineke.pakereng@uksw.edu

Abstract — ***Data security is one of the most important factors in the world of Information Technology today. One way to secure data is by Block Cipher Cryptography technique. However, some cryptographic techniques have been successfully solved by the cryptanalysis so that new cryptographic algorithms need to be created. The design of Cryptography algorithms based on traditional game patterns of Rangku Alu from East Nusa Tenggara is a design of Cryptographic Block Cipher algorithms that operate in the form of bits designed with 10 rounds where each cycle contains four processes. In each round, there are four patterns for the plaintext process and four patterns for the key. The fourth process is transformed with an S-Box table to get a more random ciphertext. Tests were also carried out using Avalance Effect which reached 49,38% and the correlation value where there was a change in character reached 73,44%. So the result designing Cryptographic algorithms can be used for encryption and description in text files.***

Keywords— ***Cryptography, Block Cipher, S-BOX, Tarian Sajojo Papua Pattern, Correlation, Avalanche Effect.***

I. PENDAHULUAN

Pengaruh teknologi informasi kini berperan hampir di setiap aspek kehidupan baik dalam pemerintahan, pendidikan, kesehatan, perbankan, bahkan dalam bidang militer sekalipun. Dengan semakin berkembangnya teknologi informasi, kini setiap orang dapat mengakses dan bertukar informasi atau data dengan mudah menggunakan internet baik yang bersifat publik maupun pribadi. Berkaitan dengan hal tersebut, tentunya tingkat keamanan data sangat diperlukan. Hal tersebut dilakukan agar data yang dikirimkan dapat sampai ke tujuan dengan aman serta guna mengantisipasi penyalahgunaan data oleh pihak yang tidak bertanggung jawab atau pihak yang tidak memiliki hak.

Oleh karena itu dikembangkan sebuah cabang ilmu yang mempelajari tentang keamanan informasi atau data yang disebut dengan Kriptografi. Kriptografi adalah ilmu yang mempelajari tentang teknik enkripsi data dimana data diacak dengan sebuah kunci sehingga menghasilkan data hasil enkripsi dan hanya dapat didekripsi oleh orang yang memiliki kunci dekripsi tersebut [1]. Namun dengan diterapkannya algoritma Kriptografi *Block Cipher*, bukan berarti hal tersebut merupakan jaminan sebuah data akan menjadi aman. Karena seiring dengan perkembangan teknologi, sudah banyak Algoritma Kriptografi *Block Cipher* yang sudah berhasil dipecahkan. Dengan demikian tentunya perlu dilakukan sebuah pengembangan algoritma baru agar polanya lebih sulit untuk dipecahkan.

Berdasarkan latar belakang masalah tersebut, maka dilakukan penelitian tentang perancangan Kriptografi menggunakan algoritma *Block Cipher* dengan memanfaatkan pola permainan tradisional Rangku Alu dari daerah Nusa Tenggara Timur (NTT) yang di dalamnya dikombinasikan dengan tabel S-*Box*. Rangku Alu merupakan permainan tradisional yang menggunakan bambu sebagai alat permainannya, Rangku Alu dapat dijadikan sebagai sarana edukasi dan pembentukan diri. Cara memainkannya adalah dengan membagi pemain menjadi dua kelompok, yaitu kelompok yang bermain dan kelompok yang menjaga. Kelompok yang menjaga menggerak-gerakkan bambu (empat orang berjongkok membentuk bidang persegi dan memegang dua bambu) sambil menyayi. Kelompok pemain yang mendapat giliran bermain akan melompat di sela-sela bambu. Mereka harus menghindari jepitan bambu. Penari akan masuk dalam bidang persegi dan melompat-lompat sesuai irama buka-tutup bambu. Ketika bermain, bambu yang digerakkan menghasilkan irama yang berpola. Permainan tersebut dapat lebih menarik lagi dengan menyanyi bersama-sama mengikuti pola irama suara bambu [2]. Berdasarkan permainan Rangku Alu tersebut, pola pergerakan pemain dan pola pergerakan bambu diadopsi untuk diterapkan ke dalam perancangan Kriptografi. Pola permainan Rangku Alu dipilih karena memiliki keunikan dimana pergerakan polanya menyebar terstruktur. Pembuatan algoritma kriptografi baru dengan pola permainan Rangku Alu bertujuan untuk menciptakan suatu kriptografi *block chiper* yang baru, sehingga dapat membantu memperbaiki dan memperbarui kriptografi yang ada agar lebih bervariatif.

Kriptografi berkembang dengan sedemikian rupa sehingga melahirkan bidang yang berlawanan yaitu kriptanalisis. Kriptanalisis adalah ilmu dan seni untuk memecahkan *chipertext* menjadi plainteks tanpa mengetahui kunci yang digunakan [3]. Dengan menggunakan kombinasi dari pergerakan pemain dan alat permainannya, menggabungkan dua hal yang ada dalam permainan tradisional Rangku Alu dapat membuat kriptanalis semakin sulit untuk memecahkan algoritma tersebut. Sehingga dengan digunakannya pola tersebut, dapat menghasilkan sebuah nilai korelasi dari pola yang digunakan dalam proses enkripsi dan dekripsi berdasarkan pesan asli atau *plaintext* yang ada.

II. TINJAUAN PUSTAKA

Penelitian yang pertama berjudul "Perancangan Kriptografi *Block Cipher* Berbasis pada Formasi Permainan Bola", penelitian ini membahas mengenai perancangan Kriptografi berbasis pada teknik formasi permainan bola yang dapat melakukan proses enkripsi dan dekripsi serta telah memenuhi 5-*tuple* dari Kriptosistem [4].

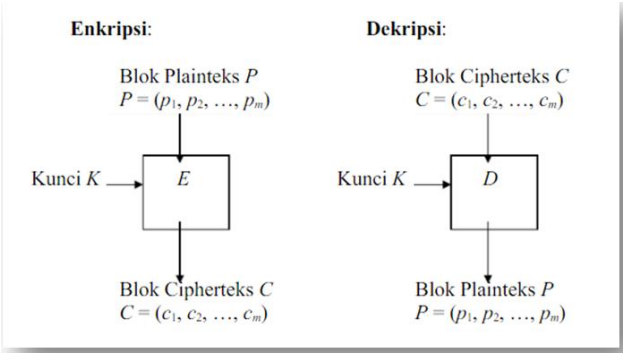
Penelitian yang kedua berjudul "Perancangan Kriptografi *Block Cipher* Berbasis Pola Formasi Futsal 1-2-1", penelitian ini membahas mengenai Kriptografi *Block Cipher* 256 bit berbasis formasi futsal 1-2-1 yang dapat menunjukkan ciri khas dari sebuah permainan futsal dalam sebuah tema sehingga dapat menyembunyikan kerahasiaan data dengan lebih baik [5].

Penelitian yang ketiga 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 [6].

Penelitian yang keempat berjudul "Perancangan Kriptografi *Block Cipher* Berbasis Pola Ikan Berenang, penelitian ini membahas mengenai teknik Kriptografi dengan menggunakan pola ikan berenang" dimana merupakan pola yang unik. Dan apabila dilihat, ikan berenang memiliki pola yang menenangkan hati. Di sini jarang orang yang memperhatikan pola ini, maka akan sulit mengetahui dasar dari pola enkripsinya [7].

Penelitian yang kelima berjudul "Perancangan Kriptografi *Block Cipher* dengan Langkah Permainan Engklek", penelitian ini membahas mengenai eksperimen perancangan *Block Cipher* untuk diimplementasikan menjadi sebuah aplikasi yang dapat digunakan secara otomatis dengan melakukan enkripsi dan dekripsi. Pada penelitian ini juga menunjukkan bahwa permainan tradisional dari Indonesia dapat dijadikan dalam bentuk alur algoritma [8].

Berdasarkan penelitian-penelitian sebelumnya terkait perancangan Kriptografi *Block Cipher*, dengan tuntutan dewasa ini maka dilakukan penelitian tentang perancangan *Block Cipher* dengan memanfaatkan pola permainan tradisional Rangku Alu dari daerah Nusa Tenggara Timur (NTT). Diharapkan dengan menggunakan pola tersebut maka didapatkan pola yang lebih acak dengan mencari korelasi terbaik yang kemudian akan digunakan sebagai proses enkripsi dan dekripsi dari pesan *plaintext*.



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

Skema proses enkripsi dan dekripsi berdasarkan Gambar 1 dapat diuraikan seperti di bawah ini.

Block Plaintext (P) yang berukuran m bit dinyatakan sebagai :

$$P = (P_1, P_2, \dots P_n) \quad (1)$$

Block Ciphertext (C) dinyatakan sebagai :

$$C = (C_1, C_2, \dots C_n) \quad (2)$$

Kunci / *Key* (K) dinyatakan sebagai :

$$K = (K_1, K_2, \dots K_n) \quad (3)$$

Proses enkripsi adalah :

$$E_k(P) = C \quad (4)$$

Proses dekripsi adalah :

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

Syarat Kriptografi adalah dapat memenuhi lima-tupel (*five-tuple*) (P, C, K, E_k, D_k) dengan kondisi [10] :

1. P adalah himpunan berhingga dari *plaintext*. Pada rancangan Kriptografi ini menggunakan *plaintext* yang ekuivalen dengan karakter ASCII *printable*. Maka himpunan *plaintext* pada perancangan Kriptografi ini adalah himpunan berhingga.
2. C adalah himpunan berhingga dari *ciphertext*. *Chipertext* dihasilkan dalam elemen heksadesimal (1,2,….,9,A,….,F), maka himpunan *chipertext* yang dihasilkan merupakan elemen terbatas.
3. K Merupakan ruang kunci (*Keyspace*), adalah himpunan berhingga dari kunci.
4. Untuk setiap k $\in$ K, maka ada $D_k \in$ E dan berkorespondensi dengan aturan dekripsi $D_k \in$ D. Setiap e_k : P $\rightarrow$ C dan d_k : C $\rightarrow$ P adalah fungsi sedemikian hingga $d_k(e_k(x))$ = x untuk setiap *plaintext* x $\in$ P.

   E = Enkripsi

D = Dekripsi

Untuk mencapai hasil yang maksimum dari nilai yang acak, maka dalam pengujian ini menggunakan korelasi yang merupakan teknik statistik untuk mengukur kekuatan hubungan antara dua variabel dan untuk mengetahui bentuk hubungan antara dua variabel tersebut dengan hasil yang bersifat kuantitatif. Kekuatan hubungan antara dua variabel itu disebut dengan koefisien korelasi. Untuk mengetahui tingkat hubungan kuat atau lemahnya nilai korelasi, dapat menggunakan acuan dari Tabel I.

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 dilihat 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 inputnya kriptoanalis tidak tahu, bisa jadi input yang dihasilkan adalah 1 atau 0. Dasar tersebut digunakan untuk melakukan kriptografi *block cipher*.

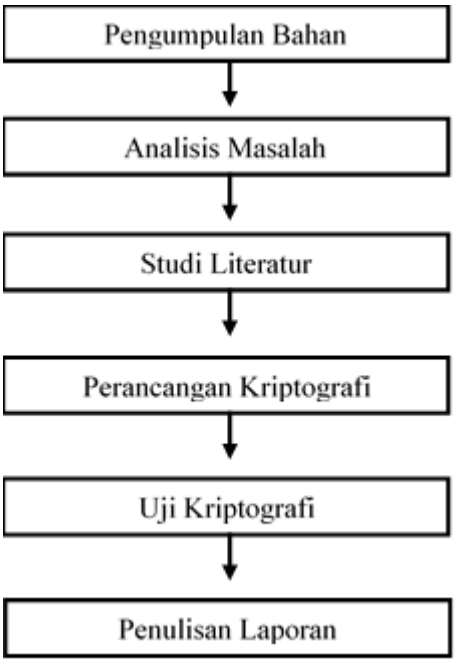
Kemudian S-*Box* (*Substitution Box*) merupakan salah satu prinsip dalam perancangan *block cipher* dimana proses s-*box* itu sendiri adalah mengganti karakter inputan dengan karakter yang sudah menjadi ketetapan pada sebuah tabel dimana ditunjukkan pada Gambar 2.. Secara teoritis, S-*Box* adalah satu-satunya 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 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 DAN PERANCANGAN SISTEM

Dalam penelitian teknik perancangan Kriptografi dengan algoritma *Block Cipher* menggunakan pola permainan tradisional Rangku Alu dari Nusa Tenggara Timur (NTT) terdapat enam tahapan penelitian, yaitu : (1) Pengumpulan Bahan, (2) Analisis Masalah, (3) Studi Literatur, (4) Perancangan Kriptografi, (5) Uji Kriptografi, (6) Penulisan Laporan.

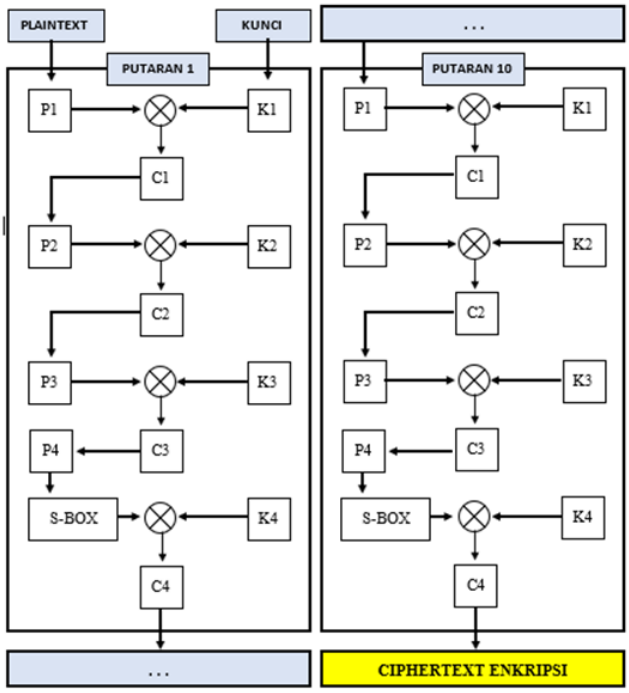


Gambar 3. Tahapan Penelitian

Tahap penelitian dari Gambar 3 dapat dijelaskan sebagai berikut : (1) Pengumpulan Bahan : yang menentukan pola untuk kriptografi baru dalam perancangan algoritma Kriptografi dengan pendekatan *block cipher* serta mengumpulkan referensi pendukung seperti artikel, cara bermain, video dari *youtube*, jurnal, (2) Analisa Masalah : tentang informasi keamanan menggunakan algoritma Kriptografi *block cipher* yang kemudian maksimal delapan karakter *plaintext* dan kunci,serta berapa bit yang digunakan,

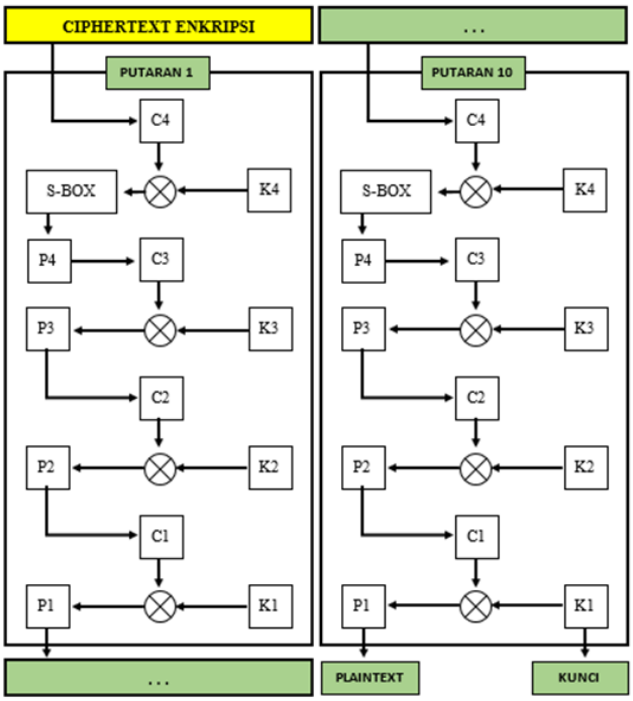
(3) Studi Literatur : dengan membaca berbagai sumber berkaitan dengan pola Kriptografi *block cipher* maka dapat di bandingkan dan mencari tingkat keacakan dari pola yang akan di buat, (4) Perancangan Kriptografi : Mulai melakukan perancangan Kriptografi *block cipher* 64-bit dengan pola permainan Rangku Alu, (5) Uji Kriptografi : setalah perancangan selesai kemudian dilakukan uji coba dari Kriptografi yang telah dibuat, pengujian meliputi hasil dari enkripsi dan dekripsi apakah sudah sesuai, serta mencari tau nilai *Avalanche Effect*, dan (6) Penulisan Laporan Penelitian : penulisan penelitian yang sudah dilakukan dalam bentuk laporan.

Dalam perancangan Kriptografi menggunakan algoritma *Block Cipher* pada pola permainan tradisional Rangku Alu ini dilakukan proses enkripsi dan proses dekripsi dimana dilakukan sebanyak 10 putaran. Masing-masing putaran terdiri dari proses empat pola.



Gambar 4. Proses Enkripsi

Gambar 4 merupakan alur proses enkripsi. Tahapan-tahapan dari proses enkripsi dapat dijabarkan sebagai berikut : Menyiapkan *plaintext* dan kunci, kemudian *plaintext* dan kunci diubah menjadi biner sesuai tabel ASCII. Selanjutnya *plaintext* dan kunci akan melewati empat proses pada setiap putaran. Proses pertama yaitu *plaintext* 1 (P1) melakukan transformasi dengan pola permainan tradisional Rangku Alu dan dilakukan perhitungan XOR dengan kunci 1 (K1) yang kemudian menghasilkan *ciphertext* 1 (C1) dimana digunakan di proses selanjutnya sebagai *plaintext* 2 (P2). Proses selanjutnya adalah *plaintext* 2 (P2) melakukan transformasi dengan pola permainan tradisional Rangku Alu dan dilakukan perhitungan XOR dengan kunci 2 (K2) yang kemudian menghasilkan *ciphertext* 2 (C2) dimana digunakan di prosess selanjutnya sebagai *plaintext* 3 (P3). Langkah berikutnya adalah *plaintext* 3 (P3) melakukan transformasi dengan pola permainan tradisional Rangku Alu dan dilakukan proses perhitungan XOR dengan kunci 3 (K3) yang kemudian menghasilkan *ciphertext* 3 (C3) dimana digunakan di proses selanjutnya sebagai *plaintext* 4 (P4). Lalu *plaintext* 4 (P4) melakukan transformasi dengan pola permainan tradisional Rangku Alu kemudian dilakukan proses S-*Box* dan dilakukan perhitungan XOR dengan kunci 4 (K4) yang kemudian menghasilkan *ciphertext* 4 (C4). Setelah mendapatkan *ciphertext* 4 (C4) maka akan digunakan pada putaran kedua dengan alur proses yang sama dengan putaran pertama. Tahap tersebut akan berlanjut sampai putaran ke-10 dimana pada putaran tersebut memberikan hasil *ciphertext* enkripsi.



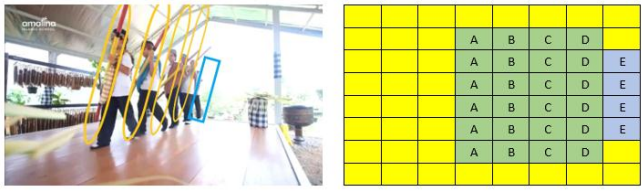
Gambar 5. Proses Dekripsi

Gambar 5 merupakan alur proses dekripsi. Tahapan-tahapan dari proses dekripsi dapat dijabarkan sebagai berikut : Menyiapkan *ciphertext* dan kunci dari proses enkripsi putaran ke-10. Kemudian *plaintext* dan kunci akan melewati empat proses pada setiap putaran. Proses pertama yaitu *ciphertext* 4 (C4) diisi oleh *ciphertext* dari enkripsi putaran ke-10. Kemudian dilakukan perhitungan XOR dengan kunci 4 (K4) kemudian hasilnya akan dilakukan proses S-*Box* untuk menghasilkan *plaintext* 4 (P4) dimana digunakan di proses selanjutnya sebagai *ciphertext* 3 (C3) untuk kemudian diproses dengan menggunakan pola dan dilakukan perhitungan XOR dengan kunci 3 (K3) dan menghasilkan *plaintext* 3 (P3) dimana digunakan di proses selanjutnya sebagai *ciphertext* 2 (C2) untuk kemudian

diproses dengan menggunakan pola dan dilakukan proses perhitungan XOR dengan kunci 3 (K2) dan menghasilkan *plaintext* 2 (P2) dimana digunakan di proses selanjutnya sebagai *ciphertext* 1 (C1) untuk kemudian diproses dengan menggunakan pola dan dilakukan perhitungan XOR dengan kunci 1 (K1) dan menghasilkan *plaintext* 1 (P1). Tahap tersebut berlanjut sampai putaran 10 dan menghasilkan *plaintext* hasil dekripsi.

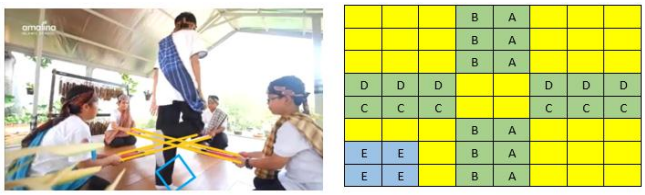
IV. HASIL DAN PEMBAHASAN

Dalam algoritma ini, pola yang diambil berasal dari permainan tradisional Rangku Alu yang kemudian digunakan sebagai proses pengambilan bit. Berikut adalah empat pola yang akan digunakan.



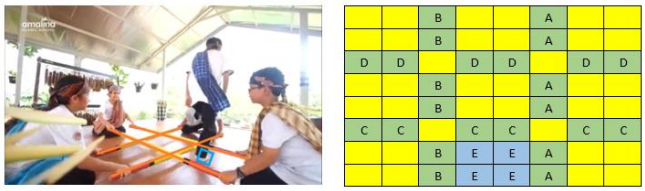
Gambar 6. Pola A dari Permainan Tradisional Rangku Alu

Pada Gambar 6 menunjukkan sebuah formasi awal dari permainan tradisional Rangku Alu, formasi ini digunakan untuk membuat Pola A dengan cara mengambil dari posisi tongkat bambu (tanda lingkaran orange) dan penarinya (tanda kotak biru). Setelah memberi tanda dan melihat formasinya, langkah berikutnya melakukan pemetaan posisinya dalam Pola A.



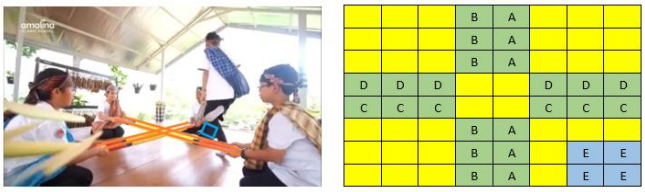
Gambar 7. Pola B dari Permainan Tradisional Rangku Alu

Pada Gambar 7 menunjukkan sebuah formasi dimana permainan mulai siap dimainkan, formasi ini yang akan digunakan untuk membuat Pola B dan caranya sama seperti cara menggambil Pola A yang berdasarkan posisi tongkat bambu dan posisi penarinya.



Gambar 8. Pola C dari Permainan Tradisional Rangku Alu

Pada gambar 8 menunjukkan posisi bambu menjadi terbuka dan pemain melompat ke posisi di antara dua bambu. Dari proses tersebut maka dapat dilakukan pemetaan yang menghasilkan C.



Gambar 9. Pola D dari Permainan Tradisional Rangku Alu

Pada Gambar 9 menunjukkan adanya perubahan posisi bambu kembali saling berdekatan dan pemain melompat keujung yang satunya. Dari proses tersebut maka dap dilakukan pemetaan yang menghasilkan Pola D

Gambar 6, Gambar 7, Gambar 8, dan Gambar 9 masing-masing menunjukkan empat pola yang berbeda dimana masing-masing pola diambil merupakan pola yang berasal dari pola permainan tradisional Rangku Alu. Berdasarkan pola tersebut, dilakukanlah pengujian korelasi dengan mengkombinasikan urutan pola tersebut yang bertujuan untuk menemukan nilai korelasi terbaik. Pengujian yang dilakukan menggunakan contoh *plaintext* yaitu "DIESUKSW" dan kunci yaitu "BUDAYAKU".

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

TABEL II
RATA-RATA NILAI KORELASI

POLA	NILAI	POLA	NILAI
ABCD	0.1739066	**CABD**	0.316055506
ABDC	0.503568289	**CADB**	0.202153318
ACBD	0.011053989	**CBAD**	0.504687923
ACDB	0.097015629	**CBDA**	0.076848471
ADBC	0.337461274	**CDAB**	0.242745957
ADCB	0.749254038	**CDBA**	0.451843594
BACD	0.272551791	**DABC**	0.12415066
BADC	0.300657006	**DACB**	0.042473019
BCAD	0.670632353	**DBAC**	0.322277928
BCDA	0.1839073	**DBCA**	0.134645077
BDAC	0.587720191	**DCAB**	0.284338932
BDCA	0.445050163	**DCBA**	0.232420937

Tabel II menujukkan hasil korelasi terbaik dari kombinasi pola yang digunakan. Dimana nilai terbaiknya terdapat pada pola ACBD,yang di dapat dari proses satu kali putaran pada masing-masing kombinasi. Kombinasi inilah yang akan digunakan untuk melanjutkan proses enkripsi hingga putaran ke-10 untuk menghasilkan *ciphertext*.

p-ISSN : 2443-2210
e-ISSN : 2443-2229

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

Gambar 10. Pola Ambil Kunci A

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

Gambar 11. Pola Pemasukan Kunci A

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

Gambar 12. Pola Ambil Kunci B

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

Gambar 13. Pola Pemasukan Kunci B

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

Gambar 14. Pola Ambil Kunci C

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

Gambar 15. Pola Pemasukan Kunci C

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

Gambar 16. Pola Ambil Kunci D

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

Gambar 17. Pola Pemasukan Kunci D

Untuk Gambar 10, Gambar 12, Gambar 14, dan Gambar 16 merupakan pola dari kunci dimana nanti akan digunakan untuk mengambil data kunci yang tersedia. Sedangkan untuk Gambar 11, Gambar 13, Gambar 15, dan Gambar 17 berfungsi menyediakan bit untuk pengaplikasian perhitungan XOR dimana mengambil data dari kunci yang

sudah memiliki pola seperti pada Gambar 10, Gambar 12, Gambar 14, dan Gambar 16.

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

Gambar 18. Contoh Pengambilan Pola A

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

Gambar 19. Pola Pemasukan *Plaintext*

Gambar 18 dari permainan Rangku Alu dilihat dari atas formasi antara bambu dan penarinya digunakan untuk memasukkan ke dalam setiap blok setiap 8 bit dari karakter plainteks kedalam pola A dengan menggunakan *Microsoft Excel*. Kemudian pola yang sudah diberi angka tersebut mengambil data bit dari pola pemasukan *plaintext* sesuai Gambar 19.

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

Gambar 20. Contoh Pengambilan Pola B

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

Gambar 21. Pola Pemasukan *Plaintext*

Gambar 20 dari permainan Rangku Alu dilihat dari atas formasi antara bambu dan penarinya digunakan untuk memasukkan ke dalam setiap blok setiap 8 bit dari karakter plainteks kedalam pola B dengan menggunakan *Microsoft Excel*. Kemudian pola yang sudah diberi angka tersebut mengambil data bit dari pola pemasukan *plaintext* sesuai Gambar 21.

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

Gambar 22. Contoh Pengambilan Pola C

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

Gambar 23. Pola Pemasukan *Plaintext*

Gambar 22 dari permainan Rangku Alu dilihat dari atas formasi antara bambu dan penarinya digunakan untuk memasukkan ke dalam setiap blok setiap 8 bit dari karakter plainteks kedalam pola A dengan menggunakan *Microsoft Excel*. Kemudian pola yang sudah diberi angka tersebut mengambil data bit dari pola pemasukan *plaintext* sesuai Gambar 23.

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

Gambar 24. Contoh Pengambilan Pola D

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

Gambar 25. Pola Pemasukan *Plaintext*

Gambar 24 dari permainan Rangku Alu dilihat dari atas formasi antara bambu dan penarinya digunakan untuk memasukkan ke dalam setiap blok setiap 8 bit dari karakter plainteks kedalam pola D dengan menggunakan *Microsoft Excel*. Kemudian pola yang sudah diberi angka tersebut mengambil data bit dari pola pemasukan *plaintext* sesuai Gambar 25.

Setelah pola yang terdapat di Gambar 19 dilakukan perhitungan XOR dengan pola yang terdapat di Gambar 11, begitu juga Gambar 21 dilakukan perhitungan XOR dengan

Gambar 13, Gambar 23 dilakukan perhitungan XOR dengan Gambar 15, dan Gambar 25 dilakukan perhitungan XOR dengan Gambar 17. Serta dimana sudah disesuaikan dengan pola yang didapat dari hasil korelasi, maka proses enkripsi putaran 1 telah selesai. Kemudian dilakukan proses yang sama hingga putaran ke-10 untuk mendapatkan *ciphertext* akhir.

Setelah proses enkripsi selesai, langkah selanjutnya adalah masuk ke proses dekripsi. Proses dekripsi adalah proses merubah *ciphertext* menjadi *plaintext* awal. Untuk mendapatkan *plaintext* awal, langkah-langkahnya sama seperti proses enkripsi, namun pada proses dekripsi dimulai dari *ciphertext* yang kemudian dilakukan perhitungan XOR dengan pola kunci yang akan menghasilkan *plaintext*. Dalam proses dekripsi yang dimulai dari putaran ke-1 menuju putaran ke-10, dilakukan persis seperti dari putaran ke-10 menuju putaran ke-1 pada proses enkripsi.

Untuk pengujian menggunakan algoritma tersebut, dilakukan dengan mengambil contoh *plaintext* yaitu "DIESUKSW" dan kunci yaitu "BUDAYAKU". Kemudian dilakukan proses enkripsi sebanyak 10 putaran. Dimana di setiap putaran enkripsi akan mendapatkan *ciphertext* dan konversi ke dalam bentuk Hexa. Sehingga hasil enkripsi dari putaran ke-10 adalah final *ciphertext* yang ditunjukkan seperti Tabel III di bawah ini.

TABEL III
HASIL *CIPHERTEXT* SETIAP PUTARAN PADA PROSES ENKRIPSI

Putaran	***Hexa Input***	***Hexa Output***
1	44494553554B5357	B566E43493E97CF2
2	B566E43493E97CF2	54347A0D1A82A24A
3	54347A0D1A82A24A	B6D60FFAE9969FC3
4	B6D60FFAE9969FC3	202DF0651BF3E1BC
5	202DF0651BF3E1BC	7CA4AD0B1542470B
6	7CA4AD0B1542470B	323D7F7D0DABADD8
7	323D7F7D0DABADD8	8F6D87EA59A510B1
8	8F6D87EA59A510B1	FA6921B5D004D82E
9	FA6921B5D004D82E	7019CBCB490870CB
10	7019CBCB490870CB	91CA5590ED252A90

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 IV
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 *Binary*	3.	*Decimal* diubah ke *Binary*
4.	Bit *Binary* dimasukkan ke kolom matriks 8x8 pada *plaintext* proses pertama (P1)	4.	Bit *Binary* dimasukkan ke kolom matriks 8x8 C4 dengan pola pemasukan *plaintext*
5.	Bit pada kolom matriks P1 diambil menggunakan pola A	5.	C4 di-XOR dengan K4 menghasilkan P4
6.	Bit pengembalian dimasukkan lagi ke dalam matriks mendapatkan hasil akhir P1	6.	P4 diproses dengan pola pemasukan *plaintext*
7.	P1 di-XOR dengan K1 menghasilkan C1	7.	P4 dilakukan proses S-*Box*
8.	C1 manjadi P3 untuk proses selanjutnya	8.	Hasil proses P4 yang telah melalui S-*Box* dimasukkan kedalam matriks 8x8 lagi dengan pola pengambilan pola D
9.	Bit pada kolom matrix P3 diambil menggunakan pola C	9.	P4 menjadi C2 untuk proses selanjutnya
10.	Bit pengembalian dimasukkan lagi ke dalam matriks mendapatkan hasil akhir P3	10.	C2 di-XOR dengan K2 menghasilkan P2
11.	P3 di-XOR dengan K3 menghasilkan C3	11.	P2 diproses dengan pola pemasukan *plaintext*
12.	C3 manjadi P2 untuk proses selanjutnya	12.	Hasil proses P2 dimasukkan ke dalam matriks 8x8 lagi dengan pola pengambilan pola B
13.	Bit pada kolom matriks P2 diambil menggunakan pola B	13	P2 menjadi C3 untuk proses selanjutnya
14.	Bit pengembalian dimasukkan lagi kedalam matriks mendapatkan hasil akhir P2	14	C3 di-XOR dengan K3 menghasilkan P3
15.	P2 di-XOR dengan K2 menghasilkan C2	15	P3 diproses dengan pola pemasukan *plaintext*
16.	C2 manjadi P4 untuk proses selanjutnya	16	Hasil proses P3 dimasukkan kedalam matriks 8x8 lagi dengan pola pengambilan pola C
17.	Bit pada kolom matriks P4 diambil menggunakan pola D	17	P3 menjadi C1 untuk proses selanjutnya
18.	Bit yang telah diambil kemudian diubah ke	18	C1 di-XOR dengan K1 menghasilkan P1

No	Proses Enkripsi	No	Proses Dekripsi
	Decimal		
19.	*Decimal* diubah ke *Hexa*	19.	P1 diproses dengan pola pemasukan *plaintext*
20.	Hasil *Hexa* dilakukan proses S-*Box* dan menghasilkan *Hexa* yang berbeda.	20.	Hasil proses P1 dimasukkan kedalam matriks 8x8 lagi dengan pola pengambilan pola B
21.	*Hexa* yang telah melalui proses S-*Box* diubah menjadi *Binary*.	21	Kemudian diambil bit dari P1 dan dipindah ke tabel *Binary*
22.	*Bunary* diubah ke Bit, Bit dimasukkan lagi ke dalam matriks mendapatkan hasil akhir P4	22,	*Binary* yang didapatkan diubah ke *Decimal*
23.	P4 di-XOR dengan K4 menghasilkan C4	23.	*Decimal* diubah ke *Hexa*
24.	C4 diubah ke *Decimal*	24	*Hexa* diubah ke *Char*
25.	*Decimal* diubah ke *Char* untuk mendapatkan *ciphertext* akhir.	25.	Char digabungkan dan menjadi hasil *plaintext*

Tabel IV merupakan algoritma proses enkripsi dan dekripsi secara menyeluruh. Proses enkripsi menghasilkan *chipertext* akhir, dan proses dekripsi menghasilkan *plaintext* awal.

Algoritma proses Kunci (*key*), dijelaskan sebagai berikut:

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

TABEL V
PSEUDO CODE PROSES ENKRIPSI DAN DEKRIPSI

Proses Enkripsi	**Proses Dekripsi**
{Program ini digunakan untuk melakukan proses enkripsi data 64 *bit*}	{Program ini digunakan untuk melakukan proses dekripsi data 64 *bit*}
Kamus P,K,P1,K1,P2,K2,P3,K3,P4,K4, = *integer* C,C1,C2,C3,C4 = *integer*	
Start C1 <- P1 ⊕ K1 *Input* P *Read* P P *to* ASCII ASCII *to Binary* Dari *Binary* = blok matriks P, masukkan *Binary* P menggunakan Pola pemasukan awal Dari blok matriks P = *Binary*, ambil bit P dengan Pola Permainan Tradisional Rangku Alu *Plaintext* 1 = blok matriks P1 *Output* P1 *Input* K *Read* K K *to* ASCII ASCII *to Binary* Dari *Binary* = blok matriks K, masukkan *Binary* K menggunakan Pola pemasukan awal Dari blok matriks K = *Binary*, ambil bit K dengan Pola Kunci 1 = blok matriks K *Output* K1 *Print* C1 C3 <- P3 ⊕ K3 *Input* P *Read* P P *to* ASCII ASCII *to Binary* Dari *Binary* = blok matriks P, masukkan *Binary* P menggunakan Pola	*Start* P4 <- C4 ⊕ K4 *Input* C4 *Read* C4 C4 *to* ASCII ASCII *to Binary* Dari *Binary* = blok matriks C4, masukan *Binary* *Input* K *Read* K K *to* ASCII ASCII *to Binary* Dari *Binary* = blok matriks K, masukkan *Binary* K menggunakan Pola pemasukan awal Dari blok matriks K = BINER, ambil bit K dengan Pola Kunci 4 = blok matriks K4 *Output* K4 C4 ⊕ K4 *Output* P4 Dari kolom matrik P4 = *Binary*, ambil bit P4 *Binary to* HEXA Dari HEXA = Tabel *S-Box*, masukan HEXA HEXA ditranformasi menggunakan *S-Box* Dari *Binary* P4 = kolom matrik P4, masukan *Binary* menggunakan pola pengambilan 4 *Print* P4 P2 <- C2 ⊕ K2 *Input* C2
pemasukan awal Dari blok matriks P = *Binary*, ambil bit P dengan Pola Permainan Tradisional Rangku Alu *Plaintext* 3 = blok matriks P3 *Output* P3 *Input* K *Read* K K *to* ASCII ASCII *to Binary*	*Read* C2 C2 *to* ASCII ASCII *to Binary* Dari *Binary* = blok matrik C2, masukan *Binary* *Input* K *Read* K K *to* ASCII ASCII *to Binary* Dari *Binary* = blok matriks K, masukkan

Dari *Binary* = blok matriks K, masukkan *Binary*
K menggunakan Pola pemasukan awal
Dari blok matriks K = *Binary*, ambil bit
K dengan Pola Kunci 3 = blok matriks K3
Output K3
Print C3
C2 <- P2 ⊕ K2
Input P
Read P
P *to* ASCII
ASCII *to Binary*
Dari *Binary* = blok matriks P, masukkan *Binary*
P menggunakan Pola pemasukan awal
Dari blok matriks P = *Binary*, ambil bit
P dengan Pola Permainan Tradisional Rangku Alu *Plaintext* 2 = blok matriks P2
Output P2
Input K
Read K
K *to* ASCII
ASCII *to Binary*
Dari *Binary* = blok matriks K, masukkan *Binary*
K menggunakan Pola pemasukan awal
Dari blok matriks K = *Binary*, ambil bit
K dengan Pola Kunci 2 = blok matriks K2
Output K2
Print C2
C4 <- P4 ⊕ K4
Input P
Read P
P *to* ASCII
ASCII *to Binary*
Dari *Binary* = blok matriks P, masukkan *Binary*
P menggunakan Pola pemasukan awal
Dari blok matriks P = *Binary*, ambil bit
P dengan Pola Permainan Tradisional Rangku Alu *Plaintext* 4
Binary to HEXA
Dari HEXA = Tabel *S-Box*, masukan HEXA
HEXA subtitusi menggunakan *S-Box*
HEXA *S-Box to Binary* = *Binary*
K menggunakan Pola pemasukan awal
Dari blok matriks K = BINER, ambil bit
K dengan Pola Kunci 2 = blok matriks K2
Output K2
C2 ⊕ K2
Print P2
P3 <- C3 ⊕ K3
Input C3
Read C3
C3 *to* ASCII
ASCII *to Binary*
Dari *Binary* = blok matrik C3, masukan *Binary*
Input K
Read K
K *to* ASCII
ASCII *to Binary*
Dari *Binary* = blok matriks K, masukkan *Binary*
K menggunakan Pola pemasukan awal
Dari blok matriks K = BINER, ambil bit
K dengan Pola Kunci 3 = blok matriks K3
Output K3
C3 ⊕ K3
Print P3
P1 <- C1 ⊕ K1
Input C1
Read C1
C2 *to* ASCII
ASCII *to Binary*
Dari *Binary* = blok matriks C1, masukan *Binary*
Input K
Read K
K *to* ASCII
ASCII *to Binary*
Dari *Binary* = blok matriks K, masukkan *Binary*
K menggunakan Pola pemasukan awal
Dari blok matriks K = BINER, ambil bit
K dengan Pola Kunci 1 = blok matriks K1
Output K1
C1 ⊕ K1
Print P1
Repeat
End

blok matriks P4
Output P1
Input K
Read K
K *to* ASCII
ASCII *to Binary*
Dari *Binary* = blok matriks K, masukkan *Binary*
K menggunakan Pola pemasukan awal
Dari blok matriks K = *Binary*, ambil bit
K dengan Pola Kunci 4 = blok matriks K4
Output K4
Print C4
Repeat
End

Tabel V merupakan hasil dari proses S-*Box* yang dilakukan pada setiap putaran untuk proses *plaintext* 4. Proses S-*Box* dilakukan agar *ciphertext* yang dihasilkan pada setiap akhir putaran menjadi lebih acak.

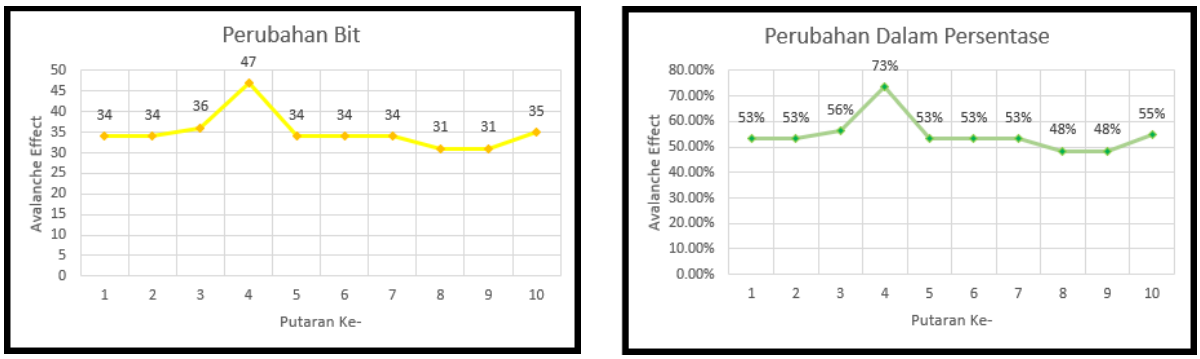
TABEL VI
NILAI KORELASI SETIAP PUTARAN

Putaran	Nilai Korelasi
1	-0.225539242
2	-0.284325633
3	0.554163168
4	0.04234029
5	-0.881122619
6	0.320165878
7	-0.025066312
8	0.130136634
9	0.222855921
10	0.18079767

Tabel VI menunjukkan nilai korelasi pada setiap putaran dan dapat disimpulkan bahwa algoritma Kriptografi *Block Cipher* berbasis pola permainan tradisional Rangku Alu memiliki korelasi yang lemah (mendekati 0) dan menghasilkan nilai korelasi yang acak (korelasi bernilai 1 hingga -1, dan sangat lemah jika mendakati 0). 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 umumnya, 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) [12].

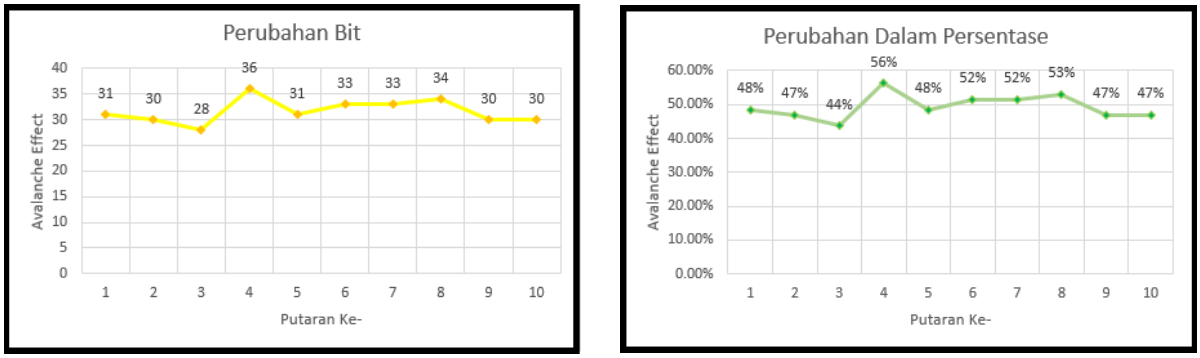
	1	2	3	4	5	6	7	8	9	10	RATA-RATA
Persentase Perubahan	53.13%	53.13%	56.25%	73.44%	53.13%	53.13%	53.13%	48.44%	48.44%	54.69%	54.69%
Perubahan bit	34	34	36	47	34	34	34	31	31	35	35



Gambar 26. Grafik *Avalanche Effect* dari *Plaintext* "DIESUKSW"

Gambar 26 adalah hasil dari pengujian *Avalanche Effect* dimana *plaintext* awal yang digunakan adalah "DIESUKSW". Pada putaran keempat perubahan bit yang tejadi cukup besar yaitu 73,44%. Dengan ini berarti terdapat perubahan bit yang baik, namun untuk nilai *Avalanche Effect* dapat dikatakan tidak begitu baik karena jauh dari angka 50%. Berdasarkan hasil putaran pertama hingga putaran ke sepuluh, dapat disimpulkan bahwa rata-rata hasil pengujian *Avalanche Effect* ini yaitu sebesar 54,69% yang berarti termasuk kategori sangat baik.

	1	2	3	4	5	6	7	8	9	10	RATA-RATA
Persentase Perubahan	48.44%	46.88%	43.75%	56.25%	48.44%	51.56%	51.56%	53.13%	46.88%	46.88%	49.38%
Perubahan bit	31	30	28	36	31	33	33	34	30	30	31.6



Gambar 27. Grafik *Avalanche Effect* dari *Plaintext* "PERDANA1"

Pada Gambar 27 yang merupakan hasil dari pengujian *Avalanche Effect* dari *plaintext* awal "PERDANA1", menghasilkan perubahan bit yang tidak terlalu tinggi dimana paling tingi hanya mencapai 56% pada putaran keempat. Nilai *Avalanche Effect* yang dihasilkan dari *plaintext* awal "PERDANA1" lebih baik dibandingkan dengan *plaintext* awal "DIESUKSW" yaitu sebesar 49,38% dengan kategori sangat baik.

V. KESIMPULAN

Enkripsi Block Cipher memiliki kelemahan mudahnya pendeteksian terutama jika ada blok-blok data yang sama di enkripsi manggunakan kunci yang sama, maka akan menghasilkan cipherteks yang sama. Kunci dalam dunia kriptografi merupakan data yang bersifat *private*, sekali data kunci telah di ketahui seorang kriptoanalis juga perlu melakukan analisa berkaitan dengan ukuran blok (dalam penelitian ini menggunakan 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.

DAFTAR PUSTAKA

[1] Tuhumury, Frellian dkk , "Perancangan Kriptografi *Block Cipher* 256 Bit Berbasis pada Pola Tuangan Air", Universitas Kristen Satya Wacana, 2016.

[2] Nanang Ajim, "Permainan Tradisional Rangku Alu", [*Online*]. *Available*: http://www.mikirbae.com/2016/05/permainan-tradisional-rangku-alu.html. [*Accessed* 12 April 2019].

[3] Humaira, Rafiqa, dkk, "Kriptanalisis dengan Metode *Brute Force* pada *Graphics Processing Unit*", Hal. 2–5, Bandung, 2015.

[4] 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.

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

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

[7] Guntoro, "Perancangan Kriptografi *Block Cipher* Berbasis Pola Ikan Berenang," Universitas Kristen Satya Wacana, 2016.

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

[9] Munir, R., "Kriptografi", Informatika, Bandung, 2006.

[10] A. 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.

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

[12] Sugiyanto and R. K. Hapsari, "Pengembangan Algoritma Advanced Encryption Standard pada Sistem Keamanan SMS Berbasis Android Menggunakan Algoritma Vigenere," Institut Teknologi Adhi Tama Surabaya, 2016.