Perancangan Kriptografi *Block Cipher* 64 *bit* Berbasis Pola Permainan Tradisional Bentengan Jawa Barat

Nanda Choirul Anam
Informatika, Universitas Kristen Satya Wacana
Jl. Diponegoro No.52-60, Salatiga, Salatiga
anamnanda@gmail.com

Abstract*— Cryptography is a technique of securing data. To improve the security level, cryptography needs to be developed. Block Cipher Cryptography based on Traditional Game Pattern in West Java Bentengan is designed to create a new cryptography. This cryptography is designed by using 4 process and 10 rounds. Testing is also done by using Avalanche Effect where the character changes reach up to 51,563%, so it can be used as an alternative in securing data.

Intisari— Kriptografi adalah teknik mengamankan data. Untuk meningkatkan keamanannya, kriptografi perlu dikembangkan. Kriptografi *Block Cipher* Berbasis Pola Permainan Tradisional Bentengan Jawa Barat ini dirancang untuk membuat kriptografi baru. Kriptografi ini dirancang menggunakan 4 proses 10 putaran. Pengujian juga dilakukan menggunakan *Avalanche Effect* dimana terjadi perubahan karakter mencapai 51,563%, sehingga dapat digunakan sebagai alternatif dalam mengamankan data.

***Kata Kunci*— *Block Cipher*, Kriptografi, Pola Permainan, Bentengan**

I. PENDAHULUAN

Kriptografi sangat berhubungan dengan pengaman informasi, untuk itu menurut terminologinya kriptografi merupakan ilmu dan seni untuk menjaga sistem pengaman pesan untuk dikirim dari suatu tempat ketempat yang lain. Keamanan dan kerahasiaan dalam komunikasi data sangat diperlukan, sehingga dapat menjamin keamanan dan kerahasiannya dalam berkomunikasi. Algoritma kriptografi memiliki karakter dan spesifikasi yang berbeda-beda. Salah satunya adalah *block cipher*, algoritma ini melakukan enkripsi dan dekripsi berdasarkan ukuran blok, yang biasanya ditentukan berdasarkan banyak karakter atau banyak *bit* dari blok tersebut. *Block cipher* merupakan kriptografi yang banyak digunakan sebagai Teknik pengamanan di internet, sebagai contoh *DES (Data Encryption Standard)* dan *AES (Advanced Encryption Standard)* yang menjadikan standar keamanan untuk transfer data, transaksi keuangan, dan juga dalam berkomunikasi. Selain itu juga Teknik ini digunakan karena secara matematis tidak memerlukan operasi yang kompleks dan algoritmanya lebih mudah untuk diimplementasi di berbagai *platform*. *Block cipher* juga secara algoritma prosesnya memerlukan waktu dan memori yang sedikit dibandingkan dengan kriptografi jenis lainnya [1].

Penelitian yang membahas teknik kriptografi *block cipher* banyak dilakukan. Salah satunya yaitu tentang Perancangan Kriptografi *Block Cipher* dengan Langkah Kuda. Tulisan ini membahas tentang penggunaan algoritma langkah kuda dalam kriptografi *block cipher* yang kemudian diimplementasikan ke dalam aplikasi untuk mengenkripsi dan mendekripsi data. Pada prosesnya digunakan fungsi *padding* (penambahan jumlah byte) pada proses enkripsi dan fungsi *unpadding* (pengurangan jumlah byte) pada kunci [2]. Pada penelitian kedua adalah Kriptografi Kunci Simetris Dengan Menggunakan Algoritma Crypton. Crypton adalah *Block Cipher* 128 *bit* dimana tiap blok data direpresentasikan ke dalam *array* berukuran 4 x 4 byte. Tiap blok data tersebut diproses dengan menggunakan rangkaian putaran transformasi. Keamanan enkripsi dan dekripsi dengan menggunakan kunci simetris pada dasarnya terletak pada kuncinya sendiri, artinya bahwa kunci yang digunakan untuk mengenkripsi dan dekripsi adalah kunci *private key*, dimana kunci tersebut tidak boleh dipublikasikan kepada umum. Tiap putaran transformasi terdiri dari empat tahap yaitu: substitusi byte, permutasi bit, transposisi byte dan penambahan kunci. Crypton hanya menggunakan operasi sederhana diantaranya *AND*, XOR dan *shift* [1]. Penelitian ketiga yaitu tentang Perancangan Kriptografi *Block Cipher* Menggunakan Pola Melempar Batu Ke Dalam Air. Penelitian ini membahas perancangan kriptografi *block cipher* dengan menggunakan pola membuang batu kedalam air untuk membentuk gelombang yang menyerupai lingkaran yang berbasis pada *block cipher*. Kemudian dari pola yang terbentuk akan digunakan untuk proses enkripsi dan dekripsi *plaintext* [3]. Penelitian keempat tentang Perancangan Algoritma pada Kriptografi *Block Cipher* dengan Teknik Langkah Kuda dalam Permainan Catur. Tulisan ini membahas tentang penggunaan teknik langkah kuda dalam permainan catur sebagai algoritma yang digunakan dalam proses pemasukan dan pengambilan bit. Penelitian ini menggunakan 4 putaran pada blok bit berukuran 8x8 (64-bit) dimana setiap putaran mempunyai dua proses yaitu proses pemasukan bit dan pengambilan bit yang dilakukan baik pada *plaintext* maupun pada kunci. Hasil dari putaran ini akan di XOR sehingga akan mendapatkan *Ciphertext* pada proses yang terakhir [4]. Berdasarkan penelitian-penelitian yang terkait dengan algoritma *block cipher* tersebut, digunakan sebagai acuan dalam merancang penelitian tentang implementasi *Block Cipher* menggunakan Pola Permainan Tradisional Bentengan Jawa Barat yang berdasarkan gerakan seperti penelitian [2], penelitian [4] dan menggunakan metode penelitian [1], penelitian [3]. Pada penelitian ini dilakukan proses enkripsi dan dekripsi dimana setiap putaran terdapat permutasi, kombinasi, transposisi,

substitusi, dan permutasi 8 pola terbaik dari pola Permainan Bentengan untuk proses *plaintext* maupun proses kunci (*key*). Hasil dua kali dari proses *plaintext* akan di-Xor dengan kunci yang selanjutnya disubstitusikan dengan S-Box, hasil substitusi S-Box akan di-Xor-kan dua kali dengan pola yang ada untuk menghasilkan *Ciphertext*. S-Box yang digunakan dalam penelitian ini adalah S-Box algoritma *AES (Advanced Encryption Standard).*

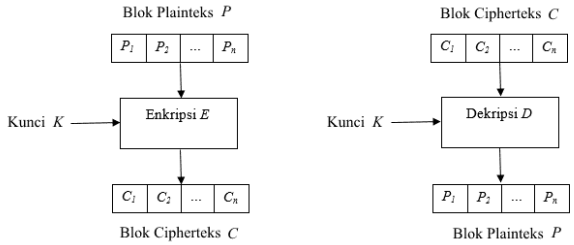
II. LANDASAN TEORI

A. Kriptografi

Kriptografi merupakan ilmu untuk menjaga keamanan data [6]. Bagian dari kriptografi yaitu *plaintext* dan *ciphertext*. *Plaintext* adalah pesan yang dapat dimengerti maknanya, sedangkan *ciphertext* merupakan pesan yang sudah dirubah sehingga tidak dapat dimengerti maknanya [7]. Bagian lain yang terdapat pada kriptografi adalah enkripsi dan dekripsi. Enkripsi adalah proses dimana *plaintext* dirubah menjadi *ciphertext*, dan dekripsi adalah kebalikan dari enkripsi yaitu mengembalikan *ciphertext* menjadi *plaintext*.

B. *Block Cipher*

Block Cipher merupakan rangkaian *bit* yang dibagi menjadi blok-blok yang panjangnya sudah ditentukan sebelumnya [4]. Skema proses enkripsi-dekripsi Bl*ock Cipher* secara umum dapat digambarkan pada Gambar 1.



Gambar. 1. Skema Proses Enkripsi –Dekripsi *Block Cipher* [8]

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

$$P = (p_1,p_2,p_3,...,p_n) \quad (1)$$

Blok *ciphertext* (C) maka blok C adalah

$$C = (c_1,c_2,c_3,...,c_n) \quad (2)$$

Kunci (K) maka kunci adalah

$$K = (k_1,k_2,k_3,...,k_n) \quad (3)$$

Sehingga proses Enkripsi adalah

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

Proses dekripsi adalah

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

C. S-Box

Kemudian S-Box (*Substitution Box*) merupakan salah satu prinsip dalam perancangan *block cipher* dimana proses S-Box itu sendiri adalah mengganti karakter masukan 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

D. Sistem Kriptografi

Sebuah sistem kriptografi terdiri dari 5-*tuple* (*Five Tuple*) (**P,C,K,E,D**) yang memenuhi kondisi [9]:

1. **P** adalah himpunan berhingga dari *plaintext*.
2. **C** adalah himpunan berhingga dari *ciphertext*.
3. **K** merupakan ruang kunci (*Key space*), himpunan berhingga dari kunci.
4. **E** adalah himpunan fungsi enkripsi e_k: $P \longrightarrow C$
5. **D** adalah himpunan fungsi dekripsi d_k: $C \longrightarrow P$

Untuk setiap $\boldsymbol{k} \in \boldsymbol{K}$, terdapat aturan enkripsi $\boldsymbol{ek} \in \boldsymbol{E}$ dan berkorespodensi dengan aturan dekripsi $\boldsymbol{dk} \in \boldsymbol{D}$. Setiap *ek* : P $\rightarrow$ C dan d_k : C $\rightarrow$ P adalah fungsi sedemikian hingga $d_k(e_k(x)) = x$ untuk setiap *plaintext* x $\in P$.

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 [10].

JUTEI Edisi Volume.3 No.1 April 2019
ISSN 2579-3675, e-ISSN 2579-5538
DOI 10.21460/jutei.2018.31.145

TABEL I. 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

III. METODE PENELITIAN

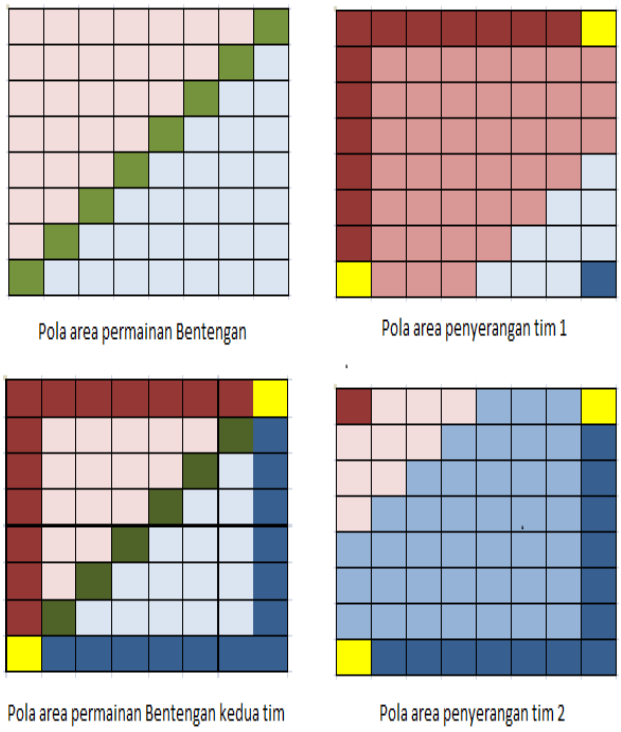
A. Prosedur Penelitian

Tahapan-tahapan penelitian yang dilakukan adalah sebagai berikut:

1. Melakukan pendefinisian dan pembatasan masalah pada perancangan yang akan dibuat.
2. Melakukan pemahaman terhadap penelitian yang berhubungan dengan kriptografi *block cipher* berbasis pola permainan Bentengan Jawa Barat.
3. Melakukan perancangan berdasarkan pola Permainan Bentengan.
4. Perancangan alur proses pencarian kombinasi dari rancangan pola Permainan Bentengan.
5. Perancangan alur proses Enkripsi dan Dekripsi.
6. Pengujian alur proses kombinasi dan melakukan analisis hasil pengujian proses enkripsi dekripsi berdasrkan kombinasi pola terbaik dari pola permainan bentengan.
7. Pengujian alur proses Enkripsi Dekripsi dan melakukan analisis hasil alur proses Enkripsi Dekripsi berdasarkan pola kombinasi terbaik dari pola permainan bentengan.
8. Pengambilan kesimpulan.

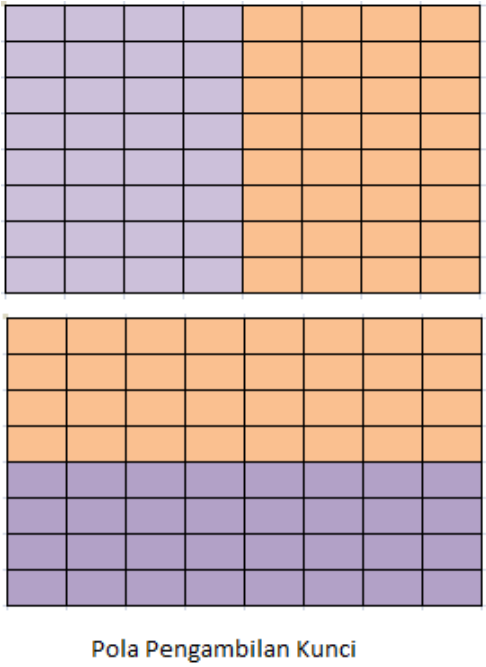
B. Perancangan Pola Permainan Bentengan

Dalam penelitian ini yang akan dirancang adalah pola dari permainan Bentengan Jawa Barat yang akan dibuat dalam bentuk *padding* 8x8 (64-bit) yang berupa pola area permainan bentengan yang kemudian akan diberi pengambilan bit pada masing-masing pola, pola area permainan bentengan kedua tim, pola penyerangan dari tim 1, pola penyerangan dari tim 2.



Gambar. 4. Pola Permainan Bentengan

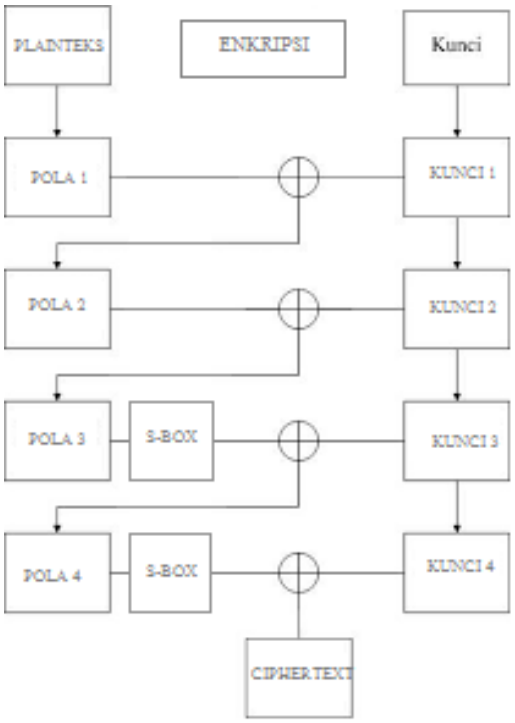
Gambar 4 merupakan perancangan berdasarkan pola Permainan Bentengan. Pada pola area permainan bentengan ditentukan bahwa ada tiga warna dimana warna merah mudah sebagai area dari tim 1 dan warna biru muda adalah area dari tim 2 yang kemudian ditentukan sebagai Pola A, pola area permainan bentengan kedua tim ditentukan ada 5 warna seperti halnya pola A ditambah warna merah tua sebagai area pengambilan tahanan dalam permainan bentengan dari tim 1 dan warna biru tua untuk tim 2 yang kemudian ditentukan sebagai Pola B, pola area penyerangan tim 1 di tentukan dengan adanya lebih banyak area merah untuk tim 1 yang kemudian ditentukan sebagai Pola C, pola area penyerangan tim 2 di tentukan dengan adanya lebih banyak area warna biru untuk tim 2 yang kemudian ditentukan sebagai Pola D dimana setiap pola dilakukan pengambilan dengan deret angka sesuai dengan warna yang ditentukan dari setiap pola agar didapatkan hasil yang lebih acak. selanjutnya dilakukan pengambilan kunci sesuai pola pengambilan kunci dapat dilihat pada gambar 5.



Gambar. 5. Pola Pergambilan Kunci

Gambar 5 merupakan pola yang dibuat untuk pengambilan kunci 1 dan pengambilan kunci 2 menggunakan pola atas, sedangkan untuk pengambilan kunci 3 dan pengambilan kunci 4 menggunakan pola bawah. Selanjutnya dilanjutkan dengan pengambilan bit dan kunci disetiap proses sebanyak 10 putaran enkripsi dan 10 putaran dekripsi sesuai dengan deret yang akan ditentukan untuk mendapatkan hasil yang lebih acak, kemudian dilakukan proses pencarian kombinasi terbaik dari keempat pola permainan bentengan yang telah dirancang untuk selanjutnya digunakan dalam proses enkripsi dan dekripsi.

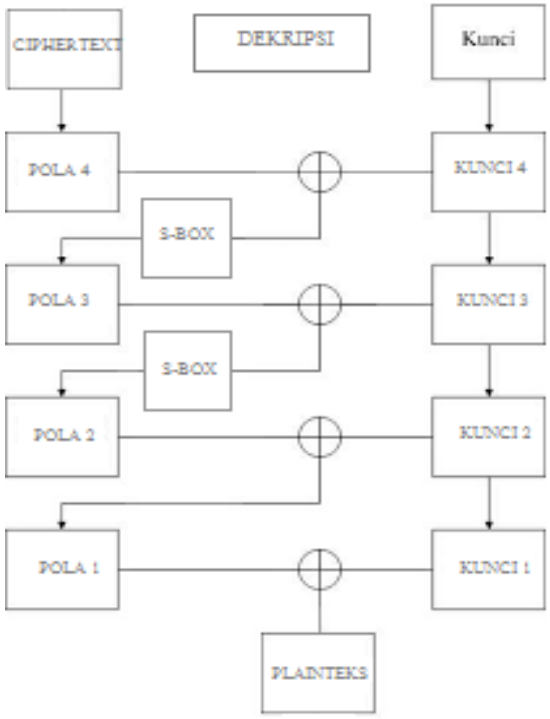
C. Tahap Perancangan Alur Proses Enkripsi dan Dekripsi



Gambar. 6. Diagram Proses Enkripsi

Gambar 6 merupakan alur proses enkripsi dengan ditambahakan *S-Box* agar mendapatkan hasil endkripsi yang lebih acak . Konsep dari proses enkripsi setiap putaran dapat dijabarkan sebagai berikut:

1. Memulai proses memasukkan data *plaintext* dan kunci berupa karakter yaitu 8 karakter atau 64 *bit.*
2. Data masukan *plaintext* ditransposisikan menggunakan pola 1 dan data masukan kunci ditransposisikan menggunakan kunci 1.
3. Deret dari pola 1 dan kunci 1 pada langkah ke-2 selanjutnya di-*Xor*-kan untuk ditransposisikan menggunakan pola 2.
4. Hasil pola 2 pada langkah ke-3 dan kunci 2 selanjutnya di-*Xor*-kan untuk ditransposisikan menggunakan pola 3.
5. Hasil pola 3 selanjutnya dilakukan substitusi menggunakan S-Box.
6. Hasil *S-Box* dan kunci 3 selanjutnya di-*Xor*-kan untuk ditransposisikan menggunakan pola 4.
7. Hasil pola 4 selanjutnya dilakukan substitusi menggunakan S-Box.
8. Hasil *S-Box* dan kunci 4 selanjutnya di-*Xor*-kan untuk menghasilkan *ciphertext*.
9. Hasil pada langkah ke-8 merupakan deret sebagai *ciphertext*.
10. Proses selesai dengan mendapatkan *chipertext* sesuai berapa banyak putaran yang dilakukan.



Gambar. 7. Diagram Proses Dekripsi

Gambar 7 merupakan alur proses dekripsi. Konsep dari proses dekripsi setiap putaran dapat dijabarkan sebagai berikut:

1. Memulai proses memasukkan data *ciphertext* dan kunci berupa karakter yaitu 8 karakter atau 64 *bit*

JUTEI Edisi Volume.3 No.1 April 2019
ISSN 2579-3675, e-ISSN 2579-5538
DOI 10.21460/jutei.2018.31.145

2. Hasil masukan *ciphertext* ditransposisikan menyesuaikan pola 4 selanjutnya dilakukan *Xor* dengan kunci 64 *bit* yang telah ditransposisikan menyesuaikan kunci 4.
3. Hasil *Xor* selanjutnya dilakukan substitusi menggunakan *S-Box*.
4. Hasil *S-Box* dari langkah ke-3 selanjutnya ditransposisi menyesuaikan pola 3.
5. Deret hasil langkah ke-4 dilakukan *Xor* dengan kunci 64 *bit* kunci 3.
6. Hasil *Xor* dari langkah ke-5 selanjutnya dilakukan substitusi menggunakan *S-Box*.
7. Hasil *S-Box* dari langkah ke-6 selanjutnya ditransposisi menyesuaikan pola 2.
8. Hasil dari pola 2 selanjutnya di-*Xor*-kan untuk ditransposisikan menyesuaikan pola 1.
9. Hasil pola 1 pada langkah ke-8 dan kunci 1 selanjutnya di-*Xor*-kan untuk ditransposisikan menghasilkan *plaintext*.
10. Proses selesai dengan mendapatkan *plaintext* sesuai berapa banyak putaran yang dilakukan.

D. Batasan Masalah

Untuk tidak memperluas ruang lingkup pembahasan maka diberikan batasan-batasan dalam penelitian ini,yaitu;

1. Proses enkripsi dan dekripsi dilakukan pada teks.
2. Pola yang digunakan adalah pola permainan pada permainan tradisional bentengan.
3. Panjang bloknya adalah 64-*bit*.

E. Pseudocode

TABEL II
PSEUDOCODE PROSES ENKRIPSI DAN DEKRIPSI

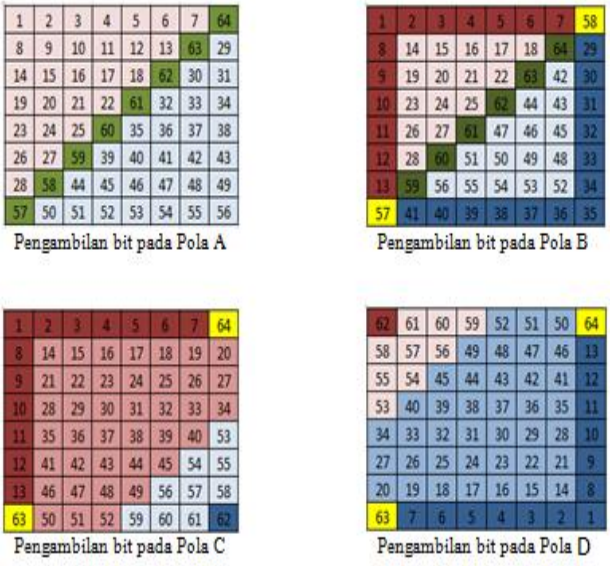
Proses Enkripsi {Program ini digunakan untuk melakukan proses enkripsi data 64 *bit*}	**Proses Dekripsi** {Program ini digunakan untuk melakukan proses dekripsi data 64 *bit*}
Kamus P,P1,K,P1,P2,P3,P4 = integer K1,K2,K3,K4,C1 = integer	
Start Input P Read P P to ASCII ASCII to BINER From BINER = blok matriks P, Input BINER P Transposisi menggunakan Pola Permainan Tradisional Bentengan Pola 1 (Pola B) Output P Input K Read K K to ASCII ASCII to BINER From BINER = blok matriks K, Input BINER	Start K <- Traposisi K4 Input K Read K K to ASCII ASCII to BINER From BINER = blok matriks K, masukan BINER K4 Transposisi menggunakan pola Kunci 4 Output K = K4 K3<- Transposisi K4 K3 Transposisi menggunakan pola Kunci 3 Output K2 = K3 K2<- Transposisi K3 K2 Transposisi menggunakan pola Kunci 2
K Transposisi menggunakan Pola Kunci 1 Output K Print P P=P1 K=K1 P1<- P1⊕ K1 From P1 = blok matriks Pola 1, Input P1 P1 Transposisi menggunakan Pola Permainan Tradisional Bentengan Pola 2 (Pola C) Output P1 From K1 = blok matriks Kunci 1, Input K1 K1 Transposisi menggunakan pola Kunci 2 Ouput K1 Print P1 P1=P2 K1=K2 P2<- P2⊕ K2 From P2 = blok matriks Pola 2, Input P2 P2 Transposisi menggunakan Pola Permainan Tradisional Bentengan Pola 2 (Pola A) Output P2 From K2 = blok matriks Kunci 2, Input K2 K2 Transposisi menggunakan pola Kunci 3 Ouput K2 Print P2 P2=P3 K2=K3 Print P3 Biner S-box<- Subtitution Hexa P3 P3 to HEXA From HEXA = Tabel S-box, Input HEXA HEXA Substitusi menggunakan S-box Print BINER S-box = P3 P3<- P3⊕ K3 From P3 = blok matriks Pola 3, Input P3 P3 Transposisi menggunakan Pola Permainan Tradisional Bentengan Pola 4 (Pola D) Output P3 From K3 = blok matriks Kunci 3, Input K3 K3 Transposisi menggunakan pola Kunci 4 Ouput K3 Print P3 P3=P4 K3=K4	Output K1 = K2 K1 Transposisi menggunakan pola Kunci 1 C = P4 P3<- Transposisi dari hasil P4⊕ K4 From BINER P4 = blok matriks Pola 4 (Pola D), Masukan BINER P4 P4⊕ K4 Transposisi terbalik menggunakan Pola Permainan Tradisional Bentengan Pola 4 (Pola D) Biner S-box Inverse <- Substitution Hexa P4 P4 to BINER BINER to HEXA From HEXA = Tabel S-box Inverse, Input HEXA HEXA Substitusi menggunakan S-box From BINER S-box = blok matriks Pola4 (Pola D), Masukan BINER S-box Print P3 K4 = K3 P3 = P2 P2<- Transposisi dari hasil P3⊕ K3 From BINER P3 = blok matriks Pola 3 (Pola A), Masukan BINER P3 P3⊕ K3 Transposisi terbalik menggunakan Pola Permainan Tradisional Bentengan Pola 3 (Pola A) Biner S-box Inverse <- Substitution Hexa P3 P3 to BINER BINER to HEXA From HEXA = Tabel S-box Inverse, Input HEXA HEXA Substitusi menggunakan S-box From BINER S-box = blok matriks Pola 3 (Pola A), Masukan BINER S-box Print P2 K3 = K2 P2 = P1 P1<- Transposisi dari hasil P2⊕ K2 From BINER P2 = blok matriks Pola 2 (Pola C), Masukan BINER P2 P2⊕ K2 Transposisi terbalik menggunakan Pola

Print P4 Biner S-box<- Subtitution Hexa P4 P4 to HEXA From HEXA = Tabel S-box, Input HEXA HEXA Substitusi menggunakan S-box Print BINER S-box = P4 P4<- P4⊕ K4 From P4 = blok matriks Pola 4, Input P4 P4 = C1 Output C1 Print C1 Repeat End	Permainan Tradisional Bentengan Pola 2 (Pola C) Print P1 P1 = P P<- Transposisi dari hasil P1⊕ K1 From BINER P1 = blok matriks proses 1, Masukan BINER P1 P1⊕ K1 Transposisi terbalik menggunakan Pola Permainan Tradisional Bentengan Pola 1 (Pola B) Print P P to BINER BINER to ASCII ASCII to *CHAR* Print P Repeat End

IV. HASIL DAN PEMBAHASAN

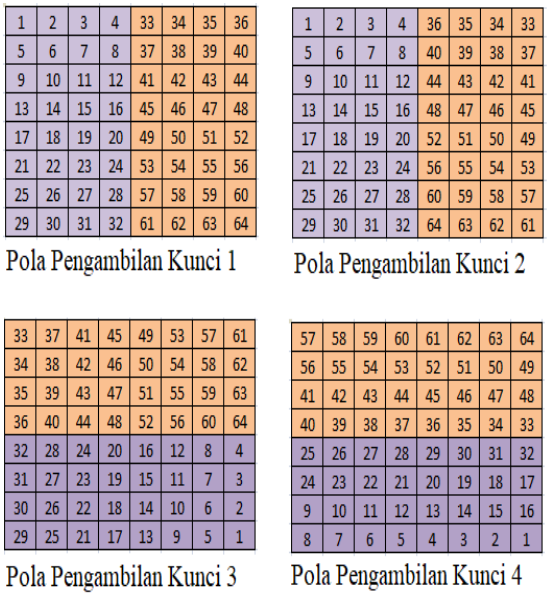
Dalam bagian ini akan membahas tentang algoritma Perancangan Kriptografi *Block Cipher* 64 *bit* Berbasis Pola Permainan Tradisional Bentengan Jawa Barat secara lebih rinci.

Dalam algoritma ini Pola Permainan Tradisional Bentengan Jawa Barat digunakan sebagai proses pemasukan dan pengambilan *bit*. Pola tersebut ditunjukkan pada Gambar 6.



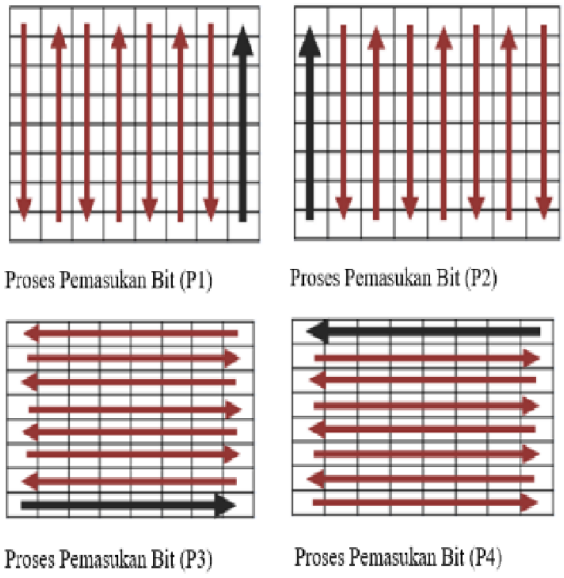
Gambar. 6. Pola Permainan Bentengan

Pada Gambar 6 menunjukan empat pola yang berbeda, dimana pola-pola tersebut menunjukan pola permainan pada permainan bentengan, dengan memperhatikan pola penyerangan, daerah permainan aman dan daerah permainan dari kedua pasukan. Berdasarkan pola-pola yang sudah dirancang, dilakukan pengujian korelasi dengan mengkombinasikan urutan pola untuk menemukan nilai korelasi terbaik.



Gambar. 7. Pola Pengambilan Kunci

Gambar 7 merupakan pola yang digunakan untuk memasukkan kunci kedalam tabel 8x8 dengan urutan sesuai angka pada pola Gambar 7. Dalam proses enkripsi dan deskripsi juga terdapat pola pemasukan *bit* kedalam blok-blok *plaintext* dan kunci. Ada 4 pola pemasukan bilangan yang digunakan sebagai alur pemasukan bilangan pada proses ini, dapat dilihat dalam Gambar 8.



Gambar. 8. Proses Pemasukan Bit

Proses pemasukan *bit* untuk pola A (P1), pola B (P2), pola C (P3), dan pola D (P4). Proses pemasukan *bit* yang pertama yaitu *bit* diambil dan dimasukkan dari kanan ke atas dan pemasukkan *bit* ini berada di P1. Pada P2 *bit* yang masuk dari kiri ke atas, P3 menggunakan pemasukan bilangan dari

JUTEI Edisi Volume.3 No.1 April 2019
ISSN 2579-3675, e-ISSN 2579-5538
DOI 10.21460/jutei.2018.31.145

kiri ke kanan dan P4 pemasukan bilangannya dari kanan ke kiri seperti yang sudah ditunjukkan oleh Gambar 8.

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

Gambar. 9. Pola Pemasukan Semua Kunci dan Pola

Gambar 9 digunakan untuk mengambil kunci berupa bit-bit angka dari semua kunci dan semua pola. Berdasarkan pola-pola yang sudah dirancang, dilakukan pengujian korelasi dengan mengkombinasikan urutan pola untuk menemukan nilai korelasi terbaik. Pengujian dilakukan menggunakan contoh *plaintext* "DIESUKSW" menggunakan kunci "BUDAYAKU".

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

TABEL II

TABEL KORELASI

KOMBINASI	KORELASI	KOMBINASI	KORELASI
A-B-C-D	0,175554195	C-A-B-D	0,07094519
A-B-D-C	0,396589271	C-A-D-B	0,455755988
A-C-B-D	0,616470856	C-B-A-D	0,233775829
A-C-D-B	0,774782132	C-B-D-A	0,70605206
A-D-B-C	0,120677473	C-D-A-B	0,401713777
A-D-C-B	0,373648423	C-D-B-A	0,4528763
B-A-C-D	0,352940991	D-A-B-C	0,112224426
B-A-D-C	0,20768874	D-A-C-B	0,23701872
B-C-A-D	0,003342485	D-B-A-C	0,530353293
B-C-D-A	0,341655101	D-B-C-A	0,413038925
B-D-A-C	0,168779286	D-C-A-B	0,073302369
B-D-C-A	0,49097391	D-C-B-A	0,450597736

Tabel 2 menunjukan hasil kombinasi pola dan mendapatkan nilai korelasi terbaik pada kombinasi pola B-C-A-D dengan nilai korelasinya mendekati 0. Kombinasi ini lah 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 matrik 8x8 menggunakan pola permainan bentengan yang berbeda-beda pada setiap proses.

Selanjutnya dalam tahap pengujian algoritma dilakukan dengan mengambil *plaintext* "DIESUKSW" dan kunci "BUDAYAKU" dengan menggunakan pola kombinasi B-C-A-D. Setelah melewati proses enkripsi yang sudah dijelaskan sebelumnya maka mendapatkan *ciphertext* yang telah diubah dalam bilangan hexadecimal.

TABEL V
Hasil Perubahan P2 dan P4 Setiap Putaran Setelah Dilakukan Proses S-Box

Putaran	*Plaintext*	Hexa Sebelum Proses S-BOX	Hexa Sesudah Proses S-BOX
1	P3	24E7DC4482244DCF	A6B0938611A6655F
	P4	384D547A3028F975	7665FDBD08EE693F
2	P3	FC5D3BF859C26B21	558D49E115A8057B
	P4	6A5EC8195C3F8F1F	589DB18EA72573CB
3	P3	E5B522014992A76C	2AD29409A47489B8
	P4	5B650F98D3593907	57BCFBE2A9155B38
4	P3	4F9FDA6F270B165F	926E7A063D9EFF84
	P4	12AE5DD793A58CC9	39BE8D0D2229F012
5	P3	38DB46E0D0AEEE31	769F98A060BE992E
	P4	B2F8D9BA8C682834	3EE1E5C0F0F7EE28
6	P3	9A9278A63C96907B	3774C1C56D359603
	P4	34D388E47FBF0038	28A997AE6BF45276
7	P3	EA0678F2ED3339E4	BBA5C10453665BAE
	P4	B78ACC2DC14AEE8F	20CF27FADD5C9973
8	P3	769D64DC9C05C757	0F758C931C3631DA
	P4	313F9D8A2FF88368	2E2575CF4EE141F7
9	P3	2508E42ED00FDE28	C2BFAEC360FB9CEE
	P4	E195E5A7E2EFB145	E0AD2A893B615668
10	P3	B1D5B83EB832E32A	56B59AD19AA14D95
	P4	259F7E28B9DB814E	C26E8AEEDB9F91B6

Tabel 5 merupakan hasil dari proses S-BOX yang dilakukan pada setiap putaran untuk proses *Plaintext* 3 dan *Plaintext* 4. Proses S-BOX dilakukan agar *Ciphertext* yang dihasilkan pada setiap akhir putaran menjadi lebih acak.

TABEL VI
HASIL SETIAP PUTARAN PADA PROSES ENKRIPSI

PUTARAN	HASIL HEXADESIMAL	HASIL *CHARACTER*
1	F828933F15A6A3FF	ø(“?¦£ÿ
2	472F8E9BFE267A56	G/Ž›þ&zV
3	6DB6D1AA9496D278	m¶Ñª”–Òx
4	96773901D63294A4	–w9Ö2”¤
5	78E3A871F17478F7	xã¨qñtx÷
6	D52232679BBD101C	Õ"2g›½
7	EF0FC9C83B1BBE64	ïÉÈ;¾d
8	7713FB0CB76AB16F	wû·j±o
9	706E789499A97A50	pnx”™©zP
10	5AC15DC04CCC2A9D	ZÁ]ÀLÌ* •

Hasil dari proses enkripsi di setiap putaran (dengan urutan 1-10) adalah *ciphertext* (C) yang berupa *character*. Hasil enkripsi di putaran ke 10 adalah *ciphertext* akhir, seperti ditunjukkan pada Tabel 6.

TABEL VII
HASIL *CIPHERTEXT* SETIAP PUTARAN PADA PROSES DEKRIPSI

Putaran	Hasil Hexadesimal	Hasil *Char*
1	44494553554B5357	DIESUKSW
2	CCF3B5BEA877BA94	Ìóµ¾¨wº”
3	720753A1E785C021	rS¡ç…À!
4	EB7FE7B6300146DD	ë • ç¶0FÝ
5	E4616B04A503E48	äa°JP>H
6	D9A9EC64A1195124	Ù©ìd¡Q$
7	547ED0A7AA9584D0	T~Ð§ª•„Ð
8	82298B10DB2018CA	‚)‹Û Ê
9	6B4D8AE2896B81E	kMŠâ–‚-
10	6DF1E42922D2B6B8	mñä)"Ò¶¸

Hasil dari proses dekripsi di setiap putaran (dengan urutan 10-1) adalah *plaintext* (P) yang berupa *character*.

Hasil dekripsi di putaran ke 1 adalah *plaintext* akhir yaitu “DIESUKSW” seperti ditunjukkan pada Tabel 7.

Pengujian korelasi digunakan untuk mengukur perbandingan antara plaintext dan ciphertext. Nilai korelasi berkisar antara 1 sampai -1, jika nilai korelasi mendekati angka 1 maka *plaintext* dan *ciphertext* memiliki hubungan yang kuat, sebaliknya jika mendekati angka 0 maka *plaintext* dan *ciphertext* memiliki hubungan yang lemah.

TABEL VIII
NILAI KORELASI SETIAP PUTARAN

PUTARAN	NILAI KORELASI
1	-0.167941956
2	0.46097939
3	-0.077297284
4	0.288528491
5	0.331359831
6	-0.312930533
7	-0.206316963
8	-0.120150745
9	0.007179597
10	-0.020620576

Tabel 8 menunjukan nilai korelasi setiap putaran, terdapat nilai korelasi yang paling tinggi pada putaran ke 2, sedangkan korelasi terendah terdapat pada putaran ke 9 dan dapat disimpulkan bahwa algoritma Kriptografi *Block Cipher* 64 *bit* Berbasis Pola Permainan Bentengan Jawa Barat ini menghasilkan hasil enkripsi yang baik antara nilai korelasi pada setiap putaran serta acak.

Pengujian *Avalanche Effect* dilakukan untuk mengetahui perubahan *bit* yang ada ketika *plaintext* diubah. Pengujian dilakukan dengan merubah karakter yang terdapat pada *plaintext* awal, sehingga akan menghasilkan perbedaan pada setiap putarannya.

Suatu teknik kriptografi dapat dikatakan sebagai sebuah teknik kriptografi jika memenuhi 5-*tuple* yaitu P, C, K, E, dan D. Akan ditunjukan bahwa perancangan ini memenuhi kelima (5-*tuple*). P adalah himpunan berhingga dari *plaintext*. Dalam penelitian perancangan ini menggunakan 256 karakter ASCII yang di ambil dari *table* ASCII, himpunan *plaintext* pada pola permainan bentengan merupakan himpunan berhingga. C adalah himpunan berhingga dari *ciphertext*. *Ciphertext* dihasilkan dalam 256 karakter ASCII. K, *keyspace* adalah himpunan berhingga dari kunci. Jumlah ruang kunci yang dipakai dalam perancangan ini adalah 256 karakter yang diambil dari ASCII. Sehingga ruang kunci merupakan himpunan berhingga . E, enkripsi, dan D, dekripsi, setiap ek : P→C dan dk : C → P adalah fungsi sedemikian hingga dk(ek(x)) = x, untuk setiap *plaintext* x∈P. Pembahasan sebelumnya telah membahas proses enkripsi dan dekripsi sehingga telah memenuhi tuple E dan D. karena telah memenuhi kelima kondisi maka pola permainan bentengan merupakan sebuah sistem kriptografi.

Tabel 9 adalah hasil dari pengujian *Avalanche Effect*, pada kasus ini *plaintext* awal adalah “DIESUKSW” yang kemudian diubah menjadi 20 pengujian. Terjadi perubahan bit pada setiap putarannya, pada putaran ke-3 dan putaran ke-7 perubahan *bit* nya terjadi cukup besar yaitu 57,813% dengan arti pada putaran ini terjadi perubahan *bit* yang baik, tetapi juga terjadi perubahan bit yang kecil pada putaran ke-4 yaitu sebesar 42,188% ini berarti perubahan *bit* nya kurang baik. Berdasarkan hasil putaran ke-1 sampai dengan putaran ke-10 dapat disimpulkan bahwa rata-rata hasil pengujian *Avalanche Effect* ini yaitu sebesar 51,563%.

JUTEI Edisi Volume.3 No.1 April 2019
ISSN 2579-3675, e-ISSN 2579-5538
DOI 10.21460/jutei.2018.31.145

TABEL IX
NILAI KORELASI SETIAP PUTARAN

pengujian ke	chiperteks	kunci	plainteks	hexa plainteks	Rata-rata perubahan bit	Rata-rata AE
1	Œ`¢³Å@Å	BUDAYAKU	NANDA123	8C600CA2B3C540C5	33	52%
2	ð€&Wñ'g	BUDAYAKU	UKSWFTI2	F08026571DF12767	31.2	49%
3	gKç7ÉVz	BUDAYAKU	KRIPTOGR	674BE737C9567A12	30	47%
4	Ÿëò<Z6Þ	BUDAYAKU	INFORMAS	9FEB05F23C5A36DE	33.3	52%
5	=4…Â‹ • bÙ	BUDAYAKU	ANAM6732	3D3485C28B9D62D9	31.6	49%
6	œ=Œuäèã •	BUDAYAKU	E2MAILKU	9C3D8C75E4E8E38F	33.4	52%
7	Ñß9ÏðUj”	BUDAYAKU	1KUDA82K	D1DF39CFF0556A94	32.2	50%
8	ê,W¥é	BUDAYAKU	INDO1945	02EA2C1B57A5E906	32.1	50%
9	b/ï]a÷	BUDAYAKU	NEGARAKU	13622FEF5D61F710	33	52%
10	²P‡d‰ì	BUDAYAKU	ASSASIN9	B2508764890619EC	31.6	49%
11	Î□X@}›Û	BUDAYAMU	BUDAYAMU	CE7F58407D9B12DB	32.6	51%
12	¡"H*§Iè	BUDAYAMU	SASUKEHH	A122482AA71149E8	32.1	50%
13	W÷Q–V[[	BUDAYAMU	37483HAK	57F751960E565B5B	33.3	52%
14	^ • • ¿Îë	BUDAYAMU	H2678JLP	5E8F7FBFCE081CEB	29.3	46%
15	7Ã$°ÑO¬©	BUDAYAMU	DENGARYA	37C324B0D14FACA9	31.4	49%
16	□ê%ç,	BUDAYAMU	WAKILKUK	8DEA1B25E7821709	33.9	53%
17	»:C6Fh@	BUDAYAMU	SELAMATT	BB3A430736466840	33.8	53%
18	„hNºÀÃâ¢	BUDAYAMU	92JA24JA	84684EBAC0C3E2A2	31	48%
19	¬Ä®n¸c	BUDAYAMU	N4ND4CH0	09ACC401AE6E8263	33.7	53%
20	ñqÏt¼Þ¢Š	BUDAYAMU	CHO1RUL4	F171CF74BCDEA28A	29.8	47%

V. KESIMPULAN

Berdasarkan penelitian yang dilakukan, dapat disimpulkan bahwa Perancangan Kriptografi *Block Cipher* 64 *bit* Berbasis Pola Permainan Tradisional Bentengan Jawa Barat dapat dikatakan sebagai sistem kriptografi yang baik. Dalam proses enkripsi, rancangan Kriptografi *Block Cipher* Berbasis Pola Permainan Tradisional Bentengan Jawa Barat ini menghasilkan *output* yang acak sehingga dapat digunakan sebagai alternatif dalam pengamanan data. rancangan Kriptografi *Block Cipher* Berbasis Pola Permainan Tradisional Bentengan Jawa Barat ini juga telah memnuhi 5-*tuple* yaitu P, C, K, E, dan D. karena telah memnuhi kelima kondisi maka pola permainan bentengan merupakan sebuah system kriptografi. Dalam pengujian *Avalanche Effect* yang dilakukan, menunjukan bahwa proses enkripsi di setiap putaran memiliki rata-rata hasil perubahan sebesar 51,563% yang berarti masuk kedalam kategori yang baik.

DAFTAR PUSTAKA

[1] Sabriyanto, & Virgono, A, 2008. *Analisis Perbandingan Performasi Algoritma Camellia dan AES (Advanced Encryption Standard) pada Block Cipher*. Institut Teknologi Bandung.

[2] Bili, D. D., Magdalena, A. I. P., Wowor, A. D., 2015. Perancangan Kriptografi *Block Cipher* dengan Langkah Kuda. Salatiga: Skripsi-S1 Sarjana Universitas Kristen Satya Wacana.

[3] Ledewara, Norman Dunga. 2016. Perancangan Kriptografi *Block Cipher* Menggunakan Pola Melempar Batu Ke Dalam Air. Universitas Kristen Satya Wacana: Salatiga.

[4] Setiawan, A. N., Wowor, A. D., 2015. Perancangan Algoritma pada Kriptografi *Block Cipher* dengan Teknik Langkah Kuda dalam Permainan Catur. Salatiga: Jurnal Setisi Universitas Kristen Satya Wacana.

[5] Mauliku, W. M., Magdalena, A. I. P., Wowor, A. D., 2015. Perancangan dan Implementasi Algoritma Kriptografi *Cipher Block* Berbasis pada Bentuk *Piramida dan Linear Congruential Generator*. Salatiga: Skripsi-S1 Sarjana Universitasi Kristen Satya Wacana.

[6] Dipanegara, A., 2011, “*New Concept Hacking*”. Jakarta: Agogos Publishig.

[7] Widodo, A, dkk., 2015 “Perancangan Kriptografi *Block Cipher* Berbasis pada Teknik Tanam Padi dan Bajak Sawah”.Teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana.

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

[9] Latuperissa, D, Pakereng, M. A. I., 2016 “Perancangan Algoritma Kriptografi *Block Cipher* 256 *Bit* Berbasis Pola Huruf B, M, E, W”. teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana.

[10] Tomasosa, E. L., Pakereng, M. A. I., 2016 “Pengaruh S-BOX *Advandce Encryption Standard (AES)* Terhadap *Avalanche Effect* Pada Perancangan Kriptografi *Block Cipher* 256 *Bit* Berbasis Pola Teknik Dansa Tali Dari Maluku”. Teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana.