Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi)

journal homepage: http://journal.lembagakita.org/index.php/jtik

Perancangan Kriptografi Blok *Cipher* Berbasis Pola Gambar Rumah Adat Joglo

Samuel Dwi Bramantya [1*], Magdalena A. Ineke Pakereng [2]

[1*,2] *Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Kota Salatiga, Provinsi Jawa Tengah, Indonesia.*

a r t i c l e i n f o

Article history:
Received 4 April 2023
Received in revised form
29 July 2023
Accepted 20 August 2023
Available *online* October 2023

DOI:
https://doi.org/10.35870/jtik.v7i4.1085

Keywords:
Block Cipher; Cryptography; Joglo Traditional House; S-Box.

Kata Kunci:
Block Cipher; Kriptografi; Rumah Adat Joglo; S-Box.

a b s t r a c t

Cryptography is a scientific discipline used to maintain data security. To increase the level of security, cryptographic development is needed by implementing 64 bit Block Cipher Cryptography based on the Joglo traditional house image pattern. This approach produces random ciphertext, which is useful in changing data in the form of clear messages (plaintext) into messages that cannot be understood (ciphertext). The designed pattern is 64 bits long and then converted back into plaintext. This cryptographic design is based on the description of the Joglo traditional house, using encryption and decryption processes combined with XOR operations. The S-Box substitution table is used for byte transposition, which aims to obtain Ciphertext. The research results show that the 64 bit block cipher cryptographic system by applying the avalanche effect to the Joglo traditional house image pattern can be considered an effective cryptographic system. The correlation value achieved reached 53.125%, validating its ability to maintain data security.

a b s t r a k

Kriptografi merupakan disiplin ilmu yang digunakan untuk menjaga keamanan data. Untuk meningkatkan tingkat keamanan tersebut, pengembangan kriptografi diperlukan dengan menerapkan Kriptografi Block Cipher berukuran 64 bit yang berbasis pada pola gambar rumah adat Joglo. Pendekatan ini menghasilkan ciphertext yang bersifat acak, yang memberikan kegunaan dalam mengubah data berupa pesan yang jelas (plaintext) menjadi pesan yang tidak dapat dimengerti (ciphertext). Pola yang dirancang sepanjang 64 bit kemudian diubah kembali menjadi plaintext. Perancangan Kriptografi ini berbasis pada gambaran rumah adat Joglo, dengan menggunakan proses enkripsi dan dekripsi yang dikombinasikan dengan operasi XOR. Tabel substitusi S-Box digunakan untuk transposisi byte, yang bertujuan untuk mendapatkan Ciphertext. Hasil penelitian menunjukkan bahwa sistem kriptografi block cipher 64 bit dengan menerapkan efek avalanche pada pola gambar rumah adat Joglo dapat dianggap sebagai sistem kriptografi yang efektif. Nilai korelasi yang dicapai mencapai 53.125%, memvalidasi kemampuannya dalam menjaga keamanan data.

Corresponding Author. Email: 672017278@student.uksw.edu [1].

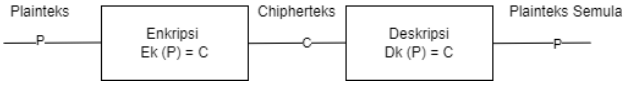
1. Latar Belakang

Perkembangan teknologi informasi yang semakin pesat dari waktu ke waktu telah memberikan dampak signifikan terhadap kebutuhan informasi. Kenaikan permintaan terhadap teknologi informasi menjadikan keamanan data informasi sebagai aspek kritis yang perlu diatasi. Keamanan data informasi menjadi esensial untuk memastikan bahwa sistem keamanan data dapat diandalkan oleh pihak berwenang. Oleh karena itu, perlu dilakukan upaya maksimal dalam menciptakan keamanan data dengan menerapkan persandian yang sulit dipecahkan. Salah satu metode yang sering digunakan untuk tujuan tersebut adalah kriptografi. Kriptografi memegang peran utama dalam menjaga keamanan informasi pada berbagai aspek, mulai dari percakapan melalui telepon genggam, transaksi di lembaga perbankan, hingga penggunaan kriptografi dalam aktivasi peluru kendali [1].

Dalam upaya mendesain kriptografi block cipher yang baru, baik, dan aman, diperlukan algoritma dan kunci yang bersifat acak. Perancangan kriptografi block cipher juga memerlukan adanya pola yang terintegrasi dengan baik bersama algoritma dan kunci. Lebih lanjut, keberadaan jenis kriptografi yang inovatif sangat diinginkan untuk melengkapi serta meningkatkan jenis-jenis kriptografi yang telah ada sebelumnya. Mengingat kebutuhan akan algoritma dengan pola yang unik, penelitian ini memfokuskan pada perancangan kriptografi berbasis pola gambar rumah adat Joglo. Setiap blok plaintext dikelompokkan ke dalam blok-blok berukuran 64 bit, menghasilkan 24 pola yang beragam. Dengan latar belakang masalah tersebut, penelitian ini ditujukan untuk menginvestigasi perancangan kriptografi block cipher 64 bit yang mengadopsi pola gambar rumah adat Joglo sebagai basisnya.

Banyak penelitian telah dilakukan dalam bidang kriptografi block cipher. Salah satu penelitian yang relevan adalah Perancangan Kriptografi Block Cipher Berbasis pada Teknik Tanam Padi dan Bajak Sawah. Penelitian ini membahas implementasi block cipher dengan 8 putaran proses enkripsi dan dekripsi. Hasil penelitian menunjukkan bahwa penggunaan teknik tanam padi dan bajak sawah menghasilkan metodologi kriptografi yang efisien dan memenuhi lima tuple (*Five-tuple*). Kesimpulan akhir dari penelitian tersebut adalah kriptografi block cipher berbasis teknik tanam padi dan bajak sawah lebih efektif dengan menggunakan AES-128 [2]. Penelitian lain Perancangan Kriptografi Simetris Berbasis Pada Pola Gambar Rumah Adat Tongkonan, yang dilaksanakan oleh Adrian Sugiarto pada tahun 2014. Penelitian ini mencakup penerapan algoritma kriptografi block cipher dengan pola pengambilan plaintext yang menghasilkan ciphertext acak, sangat berbeda dengan plaintext. Algoritma block cipher 64 bit berbasis pola rumah adat Tongkonan menggabungkan 9 putaran pada setiap proses enkripsi, dimana setiap putaran melibatkan 4 proses. Pada setiap putaran, plaintext awal disubsitusi menggunakan tabel S-Box AES dengan pengujian avalanche effect [3].

Keamanan dalam sistem kriptografi simetris tergantung pada kerahasiaan kunci. Namun, kelemahan sistem ini terletak pada kebutuhan pengirim dan penerima pesan untuk memiliki kunci yang sama, sehingga diperlukan metode yang aman untuk berbagi kunci [1]. Gambar 1 memperlihatkan skema proses enkripsi dan dekripsi dalam kriptografi simetris.



Gambar 1. Alur kriptografi Simetris [3]

Notasi "P" pada Gambar 1 merujuk pada plaintext atau pesan asli yang berfungsi sebagai informasi. Simbol C mencerminkan hasil dari enkripsi terhadap plaintext, yang disebut ciphertext. "E" dan "D" adalah fungsi Enkripsi dan Dekripsi, sementara "k" merupakan bagian dari himpunan blok kunci. Sistem kriptografi terdiri dari Five Tuple, yaitu "P" (plaintext), "C" (ciphertext), "K" (ruang kunci/keyspace), E (himpunan fungsi enkripsi ek: P → C), dan D (himpunan fungsi dekripsi dk: C → P). Setiap kunci k ∈K memiliki aturan enkripsi ek ∈ E yang berkorespondensi dengan aturan dekripsi dk ∈ D. Ek dan dk merupakan fungsi sedemikian rupa sehingga dk(ek(x)) = x untuk setiap plaintext x ∈P [5]. Block Cipher adalah teknik dalam kriptografi modern yang membagi plaintext menjadi blok-blok bit, lalu dienkripsi menggunakan kunci menjadi blok-blok bit ciphertext. Ukuran blok yang umum digunakan adalah

128-bit atau 64-bit. Operasi XOR menjadi perantara dalam proses enkripsi dan dekripsi plaintext, ciphertext, dan kunci [4]. Dalam teknik block cipher yang baik, diharapkan adanya perubahan yang signifikan antara satu bit input yang dapat mengubah lebih dari satu bit pada setiap proses alur enkripsi plaintext. Perubahan ini dikenal sebagai avalanche effect (AE), yang dijelaskan oleh persamaan pada Gambar 2.

$$AE = \frac{Jumlah\ Perubahan\ Bit}{Total\ Keseluruhan\ Bit} x\ 100\%$$

Gambar 2. Rumus *Avalanche Effect*

S-Box (*Substitution Box*) merupakan prinsip penting dalam perancangan block cipher, dimana S-Box digunakan untuk mengubah nilai dan menyamarkan hubungan antara kunci dan ciphertext. Proses ini melibatkan substitusi bilangan hexadecimal dalam tabel S-Box, menghasilkan output yang baru [5]. Tabel S-Box yang digunakan dalam penelitian ini terlihat pada Gambar 3.

		Y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
X	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 3. Tabel S-BOX

Dalam pengujian, korelasi digunakan sebagai teknik statistik untuk mengukur intensitas hubungan antara dua variabel. Koefisien korelasi memberikan indikasi kekuatan hubungan tersebut, dengan klasifikasi tingkat hubungan tertentu diberikan pada Tabel 1.

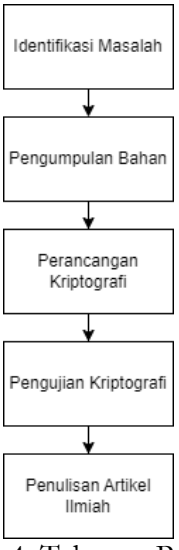
Tabel 1. Klasifikasi Koefisien Korelasi

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

Dengan memahami konsep-konsep dasar tersebut, penelitian ini bertujuan untuk merancang kriptografi block cipher 64 bit berbasis pola gambar rumah adat Joglo. Tujuan akhirnya adalah menghasilkan sistem kriptografi yang aman dan efektif, menjawab panggilan untuk terus meningkatkan tingkat keamanan data di era informasi yang semakin kompleks.

2. Metode Penelitian

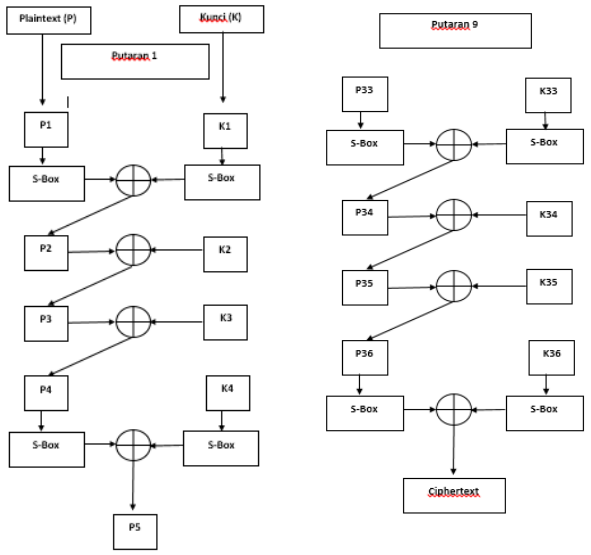
Tahapan penelitian dibagi menjadi 5 (lima) tahap yaitu: (1) identifikasi masalah, (2) pengumpulan data, (3) pengumpulan bahan, (4) pengujian kriptografi, (5) penulisan hasil artikel ilmiah. Berikut tahapan-tahapan yang dapat dilihat pada Gambar 4.



Gambar 4. Tahapan Penelitian

Pada Gambar 4 dijelaskan bahwa Tahapan Indentifikasi Masalah yaitu tahapan pertama dimana melakukan pembatasan masalah terhadap kriptografi block cipher menggunakan pola gambar rumah adat Joglo. Tahapan kedua yaitu Pengumpulan bahan-bahan yang akan digunakan sebagai perancangan pola tersebut. Mengumpulkan data penelitian terdahulu yang saling terkait dengan penelitian sehingga mendapatkan algoritma baru dalam kriptografi block cipher. Tahap ketiga yaitu Perancangan Kriptografi ini melakukan proses enkripsi dan dekripsi serta membuat kunci yang akan dikombinasikan XOR dengan tabel substitusi S-Box. Untuk Tahap Pengujian menggunakan alur simetris yaitu plaintext

yang akan diubah menjadi beberapa bit dan diporoses dengan enkripsi. Tahap yang terakhir yaitu penulisan artikel ilmiah. Tahap ini melakukan penulisan laporan dan hasil penelitian tentang perancangan kriptografi block cipher menggunakan pola gambar rumah adat Joglo. Perancangan kriptografi merupakan proses enkripsi disaat plaintext yang disubtitusikan menggukan tabel S-Box AES. Lalu di setiap proses enkripsinya terdepat 4 proses plaintext (P) dan 4 proses kunci (K) dan diulang-ulang hingga 9 putaran. Perancangan proses enkripsi dapat dilihat pada Gambar 5.



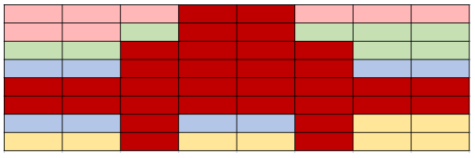
Gambar 5. Alur Proses Enkripsi

1) Membuat Plaintext (P): Tahapan pertama melibatkan pembuatan plaintext, yang selanjutnya diubah menjadi representasi biner sesuai dengan tabel ASCII. Ini membentuk dasar untuk proses enkripsi selanjutnya.
2) Rancangan Enkripsi dan Kunci: Proses ini melibatkan rancangan enkripsi dan kunci dengan total sembilan putaran. Setiap putaran terdiri dari empat proses. Plaintext dan kunci pada setiap putaran akan disubstitusi ke dalam tabel S-Box, sebuah langkah penting untuk menyamarkan hubungan antara kunci dan ciphertext.
3) Putaran Pertama (P1): Pada putaran pertama, plaintext (P1) diubah dengan menggunakan pola gambar rumah adat Joglo. Selanjutnya, hasil transformasi ini disubstitusikan ke dalam tabel S-Box untuk dilakukan operasi XOR terhadap K1. K1 sendiri sudah mengalami proses substitusi dengan tabel S-Box. Hasil operasi ini menghasilkan P2.
4) Proses Iteratif: Proses P2 selanjutnya mengalami transformasi dengan pola gambar rumah adat Joglo dan dioperasikan dengan K2 menggunakan XOR, menghasilkan P3. Proses ini berlanjut dengan iterasi yang sama, di mana P3 menghasilkan P4, dan seterusnya. Tahapan ini terus berputar hingga mencapai sembilan putaran, menghasilkan Ciphertext.

Melalui serangkaian langkah ini, proses enkripsi memanfaatkan pola gambar rumah adat Joglo sebagai elemen kunci yang unik. Kombinasi substitusi, XOR, dan transformasi pada setiap putaran menciptakan tingkat keamanan yang diharapkan dalam pengembangan kriptografi block cipher.

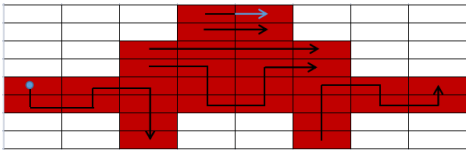
3. Hasil dan Pembahasan

Dengan algoritma pola gambar rumah adat Joglo ini digunakan sebagai suatu proses pengambilan bit dalam matriks Plaintext dan kunci. Berikut adalah pembuatan pola perubahan gambar rumah adat Joglo dapat dilihat pada Gambar 6.



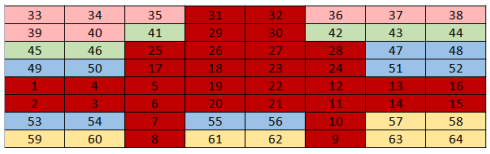
Gambar 6. Pola Rumah Adat Joglo

Gambar 6 dijelaskan bahwa pembuatan pola gambar rumah adat Joglo dengan cara menempatkan pola rumah adat Joglo menjadi 64-bit yang diberi dengan warna merah pada area.



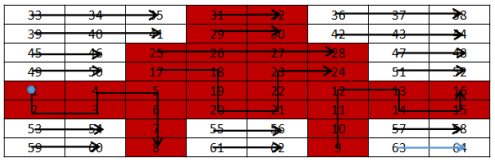
Gambar 7. Arah Pengambilan *Bit* pada Pola

Gambar 7 menjelaskan tentang pengambilan bit pada pola rumah adat Joglo di mana menunjukkan arah dari anak panah harus mengikuti pola rumah adat Joglo.

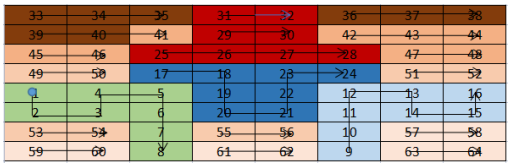


Gambar 8. Penomoran *Bit*

Gambar 8 menjelaskan bentuk pada penomoran bit. Gambar 9 menjelaskan dengan cara pengambilan bit yang dilakukan pada setiap 8-bit berurutan dengan mengikuti urutan penomoran angka 1 hingga 64. Di setiap alur diberikan anak panah berwarna hitam. Alur pengambilan bit mengikuti arah anak panah dengan dimulai dari lingkaran biru dan berakhir hingga arah anak panah berwarna biru.

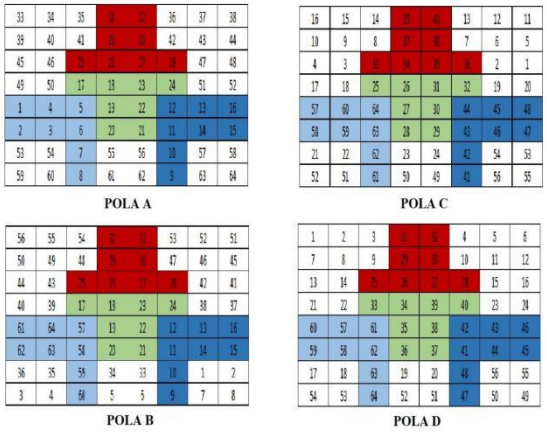


Gambar 9. Alur Pengambilan *Bit*



Gambar 10. Pemisahan Alur per 8 *Bit*

Gambar 10 menjelaskan bahwa untuk pengambilan per 8 bit di setiap blok dengan memberikan berbagai warna yang sudah dikelompokkan.



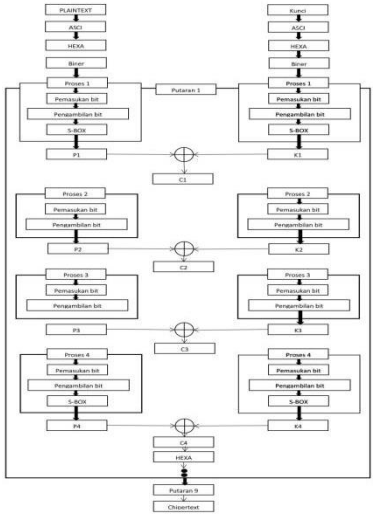
Gambar 11. Pola ABCD Rumah Adat Joglo

Pada Gambar 11 terdapat pola (A, B, C, D) pola rumah adat Joglo yang berbeda, pola-pola tersebut terlihat dengan cara pengambilan bit yang berbeda-beda berdasarkan yang sudah dirancang, lalu dilakukan proses pengujian kolerasi dengan mengkombinasikan urutan pola-pola untuk mendapatkan nilai korelasi yang terbaik. Pengujian menggunakan plaintext "FTI UKSW" dan menggunakan kunci "FAKULTAS". Masing-masing kombinasi terdiri dari 6 kombinasi berbeda, misalnya kombinasi A terdiri atas A-B-C-D, A-B-D-C, A-C-D-B, A-C-B-D, A-D-B-C, dan A-D-C-B, sedangkan kombinasi B terdiri atas B-C-D-A, B-C-A-D, B-D-A-C, B-D-C-A, B-A-C-D, B-A-D-C, dan seterusnya hingga kombinasi D. Berdasarkan hasil pengujian korelasi, maka hasil terbaiklah yang akan digunakan sebagai acuan perancangan dalam proses enkripsi dan dekripsi.

Tabel 2. Hasil Rata-rata Korelasi

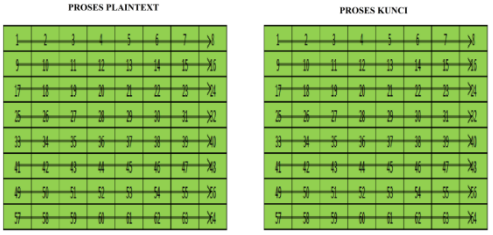
Pola	Nilai korelasi	Pola	Nilai korelasi
ABCD	0,168949496	CABD	0,309358148
ABDC	0,219586358	CADB	0,845416201
ACBD	0,501187285	CBAD	0,511904235
ACDB	0,367337664	CBDA	0,219602202
ADBC	0,303474444	CDAB	0,321355244
ADCB	0,303474444	CDBA	0,473637714
BACD	0,574438951	DABC	0,30868748
BADC	0,245297384	DACB	0,440948163
BCAD	0,869357416	DBAC	0,267644051
BCDA	0,753286508	DBCA	0,111710224
BDAC	0,252938333	DCAB	0,624993144
BDCA	0,396717292	DCBA	0,413557024

Tabel 2 menunjukkan bahwa urutan kombinasi pola dengan rata-rata korelasi terbaik terdapat pada urutan pola D-B-C-A dengan nilai korelasi adalah 0,111710224. Kombinasi tersebut menjadi acuan dalam perancangan kriptografi simetris berbasis pada pola gambar rumah adat Joglo, serta akan dilanjutkan proses enkripsinya hingga 9 putaran untuk menghasilkan ciphertext. Urutan kombinasi proses plaintext dan kunci ABCD dimasukkan ke dalam konsep kerja dasar enkripsi kriptografi block cipher dan digabungkan dengan tabel substitusi S-Box. Proses enkripsi dan dekripsi dapat dilihat pada Gambar 12.



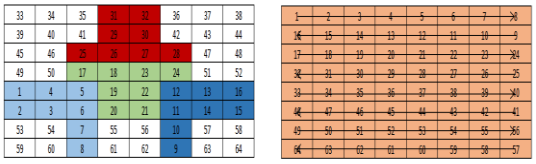
Gambar 12. Proses Kerja Enkripsi

Gambar 12 menjelaskan bagaimana proses enkripsi secara keseluruhan dengan gabungan antara konsep dasar enkripsi algoritma kriptografi block cipher menggunakan metode transposisi dibantu dengan tabel substitusi S-Box. Langkah-langkah proses tersebut dapat dijelaskan sebagai berikut: 1) Plaintext dan kunci; 2) Plaintext dan kunci sebelum input dalam Proses 1 diubah menjadi format ASCII dan kemudian diubah kembali dalam bentuk HEXA, dan berakhir menjadi bentuk HEXA bentuk biner; 3) Plaintext biner dan kunci dimasukkan dalam proses 1 untuk selanjutnya adalah input dan mengambil bit dalam pola untuk membuat P1 dan K1. P1 dan K1 diganti menggunakan tabel S-Box. Hasil substitusi P1 dan K1 diproses pada notasi XOR untuk menghasilkan C1. lalu C1 dan K1 adalah hasil untuk masuk ke proses 2; 4) File biner C1 dan K1 disertakan dalam proses 2 mengeksekusi input dan output bit sesuai dengan pola untuk menghasilkan P2 dan K2. P2 dan K2 di-XOR untuk membuat C2. C2 dan K2 adalah hasil untuk dimasukkan dalam proses 3; 5) Biner C2 dan K2 dimuat ke dalam proses 3 dengan memasukkan dan mengambil bit sesuai pola yang akan dihasilkan P3 dan K3. P3 dan K3 di XOR untuk membuat C3. C3 dan K3 adalah hasil untuk dimasukkan dalam proses 4; 6) Biner C3 dan K3 dimasukkan Proses 4 input dan transfer bit sesuai pola untuk nanti diganti dalam tabel substitusi S-box untuk menghasilkan P4 dan K4. P4 dan K4 diproses pada notasi XOR untuk menghasilkan C4. Biner C4 dikonversi ke HEXA. Lakukan hal yang sama untuk putaran berikutnya, yaitu ikuti langkah 1-6, dengan hasil substitusi C4 dan K4 menjadi acuan putaran berikutnya. S-Box itu sendiri berfungsi untuk transformasi SubBytes() agar cocok dengan masing-masing byte dari array state.



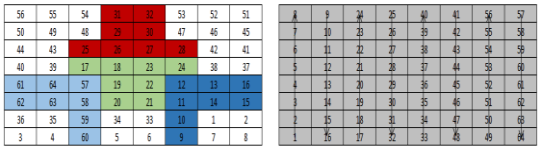
Gambar 13. Pola Pemasukan *Bit* dan *Plaintext* dan Kunci

Gambar 13 menjelaskan proses pemasukan bit plaintext dan kunci dari setiap karakter di mana setiap karakter mempunyai 8 bit. Setiap karakter dimasukkan berurutan dengan mengisi blok bagian kiri ke kanan sesuai arah panah.



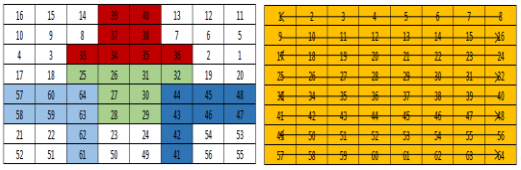
Gambar 14. Pola Pengambilan dan Pola Transpose Plaintext dan Kunci Proses 1

Gambar 14 menjelaskan bagaimana pola pengambilan serta transpose plaintext serta kunci. Bit diambil tiap 8-bit berurutan angka. Setelah itu dimasukkan kembali ke dalam kolom matriks baris awal dari kiri ke kanan, serta buat baris kedua dari kanan ke kiri, berikutnya ikuti arah panah serta urutan angka pada Gambar 14. Setelah diambil setiap 8 bit, P1 diproses dengan Tabel S-BOX kemudian dimasukkan ke dalam tabel matrix. Berdasarkan proses tersebut diciptakan P1 serta K1. P1 serta K1 diproses XOR menghasilkan C1.



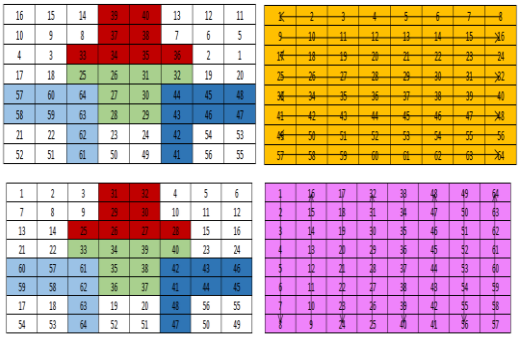
Gambar 15. Pola Pengambilan dan Pola Transpose Plaintext dan Kunci Proses 2

Gambar 15 menjelaskan tentang proses pengambilan plaintext 1 yang dihasilkan dari C1. Proses ke 2 dilakukan mengikuti arah panah mulai 1 hingga 64.



Gambar 16. Pola Pengambilan dan Pola Transpose Plaintext dan Kunci Proses 3

Gambar 16 menjelaskan tentang proses pengambilan *plaintext* 2 yang dihasilkan dari C2. Proses ke 3 dilakukan mengikuti arah panah mulai 1 hingga 64.



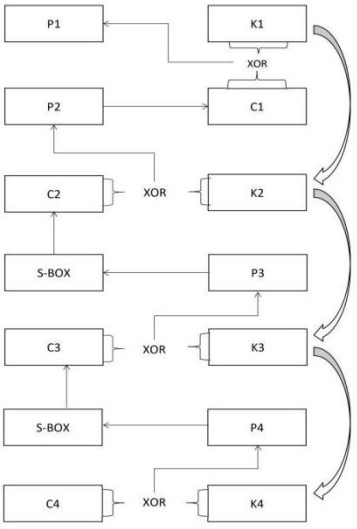
Gambar 17. Pola Pengambilan dan Pola Transpose Plaintext dan Kunci Proses 4.

Gambar 17 menjelaskan tentang proses pengambilan plaintext 3 yang dihasilkan dari C3. Kemudian P4 diproses menggunakan Tabel S-BOX, lalu dimasukan kembali ke dalam tabel matriks mengikuti arah panah. Untuk pengujian algoritma akan dicoba dengan mengambil plaintext adalah FTI UKSW dan kunci adalah FAKULTAS. Kemudian melewati proses enkripsi yang sudah dijabarkan sebelumnya hingga memperoleh ciphertext yang sudah dikonversi ke dalam nilai hexadecimal. Hasil ciphertext tersebut bisa dilihat pada Tabel 3.

Tabel 3. *Ciphertext* Setiap Putaran

Putaran	*Chipertext*
Putaran 1	6A92608484234FFD
Putaran 2	73B3E91FD5FDE8FB
Putaran 3	8D12938EB641356
Putaran 4	F651D589B729866
Putaran 5	D466AA5ADAA2936E
Putaran 6	42C078FAFDD2B7B7
Putaran 7	78B34827F346675
Putaran 8	51F78EC54814559
Putaran 9	8BBF018B7816455

Gambar 18 adalah alur proses pengembalian ciphertext ke plaintext. Pola yang digunakan sebagai pola pengambilan bit pada proses enkripsi hendak digunakan sebagai pola pengambilan pada proses dekripsi. Sebaliknya pola pemasukan yang digunakan pada proses enkripsi hendak digunakan selaku pola pengambilan proses dekripsi sehingga bisa dikatakan pola gambar rumah adat Joglo digunakan sebagai pola pemasukan bit pada proses dekripsi.



Gambar 18. Alur Proses Dekripsi

Proses dekripsi yaitu kebalikan dari proses enkripsi. Dekripsi dicoba dengan memproses kunci hingga putaran kelima setelah itu ciphertext dimasukkan serta dioperasikan dengan notasi XOR terhadap K4 pada proses keempat. Hasil tersebut setelah itu dimasukkan ke dalam matriks P4 menggunakan pola gambar rumah adat Joglo. Proses Algortima enkripsi dan dekripsi dapat dijabarkan pada Tabel 4.

Tabel 4. Enkripsi dan Dekripsi

Proses Enkripsi	Proses Dekripsi
1. Masukkan *Plaintext*	1. Masukkan *Ciphertext*
2. *Plaintext* diubah ke ASCII	2. Nilai *Ciphertext* diubah ke Biner
3. ASCII diubah ke HEXA	3. Biner C4 di-XOR-kan dengan K4
4. Nilai HEXA diubah ke BINER	4. Hasil XOR *Ciphertext* dan K4 di substitusikan dengan S-Box kemudian dimasukkan ke kolom matriks P4 menggunakan pola pengambilan *bit* proses A pada *Plaintext*
5. *Bit* Biner dimasukkan ke kolom matriks P1 menggunakan pola pemasukan *bit* proses B pada *Plaintext*	5. P4 ditransposisikan dari kolom matriks P4 dengan pola pemasukan *bit* proses A pada *Plaintext*
6. *Bit* P1 ditransposisikan dari kolom matriks P1 dengan pola pengambilan bit poroses D pada *Plaintext*	6. P4 = C3
7. Nilai pengambilan *bit* P1 disubstitusikan dengan tabel S-Box	7. C3 di-XOR dengan K3
8. Hasil substitusi S-Box P1 di-XOR dengan hasil substitusi S-Box K1 menghasilkan C1	8. *Bit* Biner hasil XOR antara C3 dan K3 dimasukkan ke kolom matriks P3 menggunakan pola pengambilan *bit* proses C pada *Plaintext*
9. C1 = P2	9. P3 ditransposisikan dari kolom matriks P3 dengan pola pemasukan *bit* proses C pada *Plaintext*
10. *Bit* Biner dimasukkan ke kolom matriks P2 menggunakan pola pemasukan bit proses B pada Plaintext	10. P3 = C2
11. Bit P2 ditransposisikan dari kolom matriks P2 dengan pola pengambilan *bit* proses B pada *Plaintext*	11. C2 di-XOR dengan K2
12. P2 di-XOR dengan K2 menghasilkan C	12. *Bit* Biner hasil XOR C2 dan K2 dimasukkan ke kolom matriks P2 menggunakan pola pengambilan *bit* proses B pada *Plaintext*
13. C2 = P3 menggunakan pola pemasukan *bit* proses C pada *Plaintext*	13. P2 ditransposisikan dari kolom matriks P2 dengan pola pemasukan *bit* proses B pada *Plaintext*
14. *Bit* Biner dimasukkan ke kolom matriks P3	14. P2 = C1
15. *Bit* P3 ditransposisikan dari kolom matriks P3 dengan pola pengambilan *bit* proses C pada *Plaintext*	15. C1 di-XOR dengan K1
16. P3 di-XOR dengan K3 menghasilkan C3	16. Nilai XOR C1 dan K1 disubstitusikan dengan tabel S-Box
17. C3 = P4	17. Hasil substitusi diubah ke Biner dimasukkan ke kolom matriks P1 menggunakan pola pengambilan *bit* proses D pada *Plaintext*
18. *Bit* Biner dimasukkan ke kolom matriks P4 menggunakan pola *bit* pemasukan proses A pada *Plaintext*	18. P1 ditransposisikan dari kolom matriks P1 dengan pola pemasukan *bit* proses D pada *Plaintext*
19. *Bit* P4 ditransposisikan dari kolom matriks P4 dengan pola pengambilan *bit* proses A pada *Plaintext*	19. P1 = *Plaintext*
20. Nilai pengambilan *bit* P4 disubstitusikan dengan tabel S-Box	20. Hasil *Plaintext* dalam bentuk biner
21. Hasil substitusi S-Box P4 di-XOR dengan hasil subtitusi S-Box K4 menghasilkan C4, hasil C4 merupakan nilai Biner	21. Biner *Plaintext* diubah ke dalam ASCII
22. Biner C4 diubah ke HEXA	22. 22. Nilai ASCII diubah ke dalam karakter

Tabel 4 merupakan algoritma proses enkripsi dan dekripsi. Proses enkripsi menghasilkan C4 dan proses dekripsi menghasilkan P1 awal. Algoritma proses Kunci (key), dijelaskan sebagai berkut:

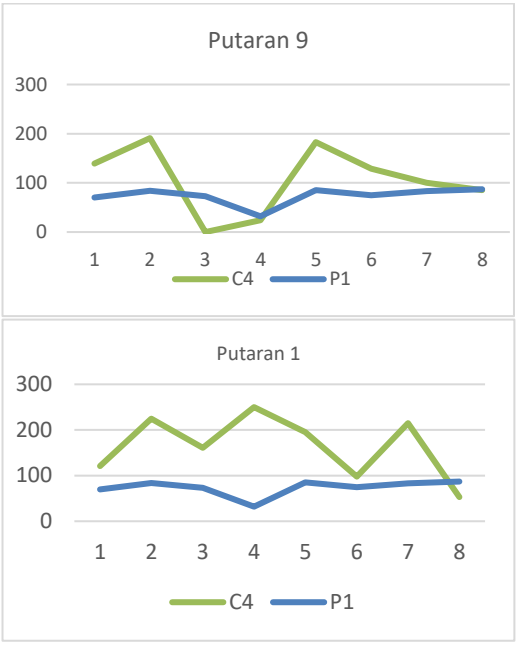
1) Masukkan Kunci
2) Kunci diubah ke ASCII
3) ASCII diubah ke BINER
4) Bit BINER dimasukkan ke kolom K1 menggunakan pola masuk Kunci
5) Bit Kunci ditransposisikan dengan pola Kunci D
6) Transposisi K1 = K2
7) K2 ditransposisikan menggunakan pola Kunci B
8) Transposisi K2 = K3
9) K3 ditransposisikan menggunakan pola Kunci C
10) Transposisi K3 = K4
11) K4 ditransposisikan menggunakan pola Kunci A.

Pengujian korelasi dilakukan untuk mengukur seberapa acak perbandingan antara hasil enkripsi (ciphertext) serta plaintext. Nilai korelasi berkisar 1 hingga- 1, dimana jika nilai kolerasi mendekati 1 maka plaintext serta ciphertext mempunyai ikatan yang sangat kuat, namun bila mendekati 0 maka plaintext serta ciphertext mempunyai ikatan yang tidak kuat. Hasil pengujian korelasi bisa dilihat pada Tabel 5.

Tabel 5. Nilai Korelasi Setiap Putaran

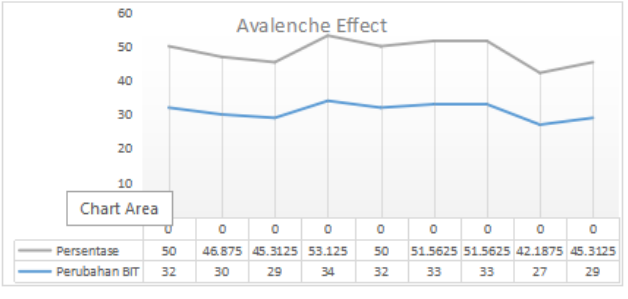
Putaran	Korelasi
Putaran 1	0,15663777
Putaran 2	0,84579409
Putaran 3	-0,634460517
Putaran 4	0,44354745
Putaran 5	0,326225604
Putaran 6	-0,176607737
Putaran 7	0,378709195
Putaran 8	-0,438908438
Putaran 9	0,556473154

Tabel 5 memperlihatkan jika tiap putaran mempunyai nilai kolerasi tidak kuat sehingga dapat disimpulkan kalau kriptografi simetris berbasis pada pola gambar Rumah Adat Joglo bisa menciptakan nilai korelasi enkripsi yang acak. Bentuk grafik yang dibuat dari hasil nilai korelasi ditunjukan pada Gambar 19.



Gambar 19 Grafik Perbandingan *Plaintext* dan *Ciphertext*

Gambar 19 memperlihatkan bahwa putaran satu dengan putaran yang lainya terdapat perbedaan yang mencolok atara plaintext dan ciphertext. Pengujian Avalanche Effect dilakukan untuk mengetahui seberapa banyak perubahan bit saat plaintext diubah. Pengujian dilakukan dengan merubah karakter yang terdapat pada plaintext awal, sehingga akan menghasilkan perbedaan pada setiap putaran.



Gambar 20 Grafik *Avalanche Effect*

Gambar 20 adalah hasil pengujian *Avalanche Effect*. Pada penelitian yang dibuat *plaintext* awal yaitu FTI UKSW lalu diubah menjadi SALATIGA. Menurut data pada grafik *Avalanche Effect* ditunjukkan bahwa hasil dari *Avalanche Effect* tertinggi adalah 53.125%.

4. Kesimpulan

Penelitian ini menunjukkan bahwa kriptografi block cipher 64-bit dengan basis pola Rumah Adat Joglo efektif dalam mengamankan data. Proses enkripsi menghasilkan ciphertext yang acak dan memiliki tingkat keamanan yang baik. Pengujian avalanche effect menunjukkan sensitivitas sistem terhadap perubahan pada plaintext, dengan perubahan mencapai 53.125%. Hal ini menegaskan bahwa sistem ini dapat diandalkan untuk melindungi data. Korelasi antara plaintext dan ciphertext menunjukkan nilai yang acak, menunjukkan ketidakmungkinan pola terprediksi. Sebagai alternatif kreatif, kriptografi ini dapat diimplementasikan untuk keamanan informasi yang handal, tetapi perlu pemeliharaan dan evaluasi terus-menerus seiring perkembangan teknologi demi menjaga responsibilitas keamanan yang berkelanjutan.

5. Daftar Pustaka

[1] Munir, R. 2006. Kriptografi. bandung. Informatika, 1(7).

[2] Widodo, A. 2018. *Perancangan Kriptografi Block Cipher Berbasis pada Teknik Bajak Sawah, Tanam Padi dan Panen Padi* (Doctoral dissertation, Program Studi Teknik Informatika FTI-UKSW). Available at: https://repository.uksw.edu/handle/123456789/15200.

[3] Sugiarto, A. and Sugiarto, A., 2017. *Perancangan Kriptografi Simetris Berbasis Pada Pola Gambar Rumah Adat Tongkonan* (Doctoral dissertation, Program Studi Teknik Informatika FTI-UKSW).

[4] Fauzi, R.R. and Wellem, T., 2021. Perancangan Kriptografi Block Cipher berbasis Pola Dribbling Practice. *AITI*, *18*(2), pp.158-172. DOI: https://doi.org/10.24246/aiti.v18i2.158-172.

[5] Choirul, N. and Pakereng, M.A.I., 2019. 64 BIT BLOCK CIPHER CRYPTOGRAPHY DESIGN BASED ON TRADITIONAL GAME PATTERNS WITH WEST JAVA. *Jurnal Terapan Teknologi Informasi*, *3*(1), pp.65-73. DOI: https://doi.org/10.21460/jutei.2019.31.145.

[6] Hendrian Ivan D., & PAKERENG, M. A. I., 2017. Perancangan Kriptografi Block Cipher Menggunakan Pola Tari Purisari Pati, Universitas Kristen Satya Wacana.