Jurnal Teknik Informatika (JUTIF)
Vol. 5, No. 4, August 2024, pp. 157-161

DOI: https://doi.org/10.52436/1.jutif.2024.5.4.2137
p-ISSN: 2723-3863
e-ISSN: 2723-3871

DESIGNING 64-BIT BLOCK CIPHER CRYPTOGRAPHY BASED ON THE PATTERN OF ONE OF KARO'S TRADITIONAL CLOTHS

Dandy Duggari Manik*[1], Ramos Somya[2]

[1,2]Department of Informatics Engineering, Faculty of Information Technology, Universitas Kristen Satya Wacana, Indonesia
Email: [1]672018233@student.uksw.edu, [2]ramos.somya@uksw.edu

(Article received: May 27, 2024; Revision: June 13, 2024; published: July 29, 2024)

Abstract

The ease of access to information technology in the modern era can be felt in various aspects of human life needs, one of which is exchanging information or exchanging data is an activity that has been carried out very often every day. With this convenience, the security and confidentiality of the data is also very important to consider because the information or data exchanged can contain important or confidential matters. In the exchange of data or information, of course, a security system is needed that ensures the data remains safe. One of the techniques to secure this data is to use cryptographic techniques. There have been many cryptographic techniques used or implemented to secure information, but many cryptographic techniques have been solved so that the ability to secure data is doubtful. One way to overcome this is to create a new cryptography or make changes to existing cryptography. Through this research, a cryptography will be created that uses the pattern of Karo traditional cloth and uses a 64-bit Block Cipher to produce a better encryption process.

Keywords: *Block Cipher, Cryptography, Encryption, Karo.*

PERANCANGAN KRIPTOGRAFI BLOCK CIPHER 64 BIT BERBASIS POLA SALAH SATU KAIN ADAT KARO

Abstrak

Kemudahan akses teknologi informasi di era modern dapat dirasakan dalam berbagai aspek kebutuhan hidup manusia, Salah satunya adalah bertukar informasi atau bertukar data merupakan sebuah kegiatan yang sudah sangat sering dilakukan setiap hari. Dengan adanya kemudahan ini, keamanan dan kerahasiaan dari data tersebut juga sangat penting untuk diperhatikan karena informasi atau data yang dipertukarkan dapat berisi hal yang penting atau bersifat rahasia. Didalam pertukaran data atau informasi tersebut tentunya dibutuhkan sistem keamanan yang menjamin data tersebut tetap aman. Salah satu teknik untuk mengamankan data tersebut ialah dengan menggunakan teknik kriptografi. Sudah sangat banyak teknik kriptografi yang digunakan atau diimplementasikan untuk mengamankan informasi, namun banyak teknik kriptografi yang sudah bisa dipecahkan sehingga kemampuan untuk mengamankan data menjadi diragukan. Salah satu cara untuk mengatasi hal tersebut adalah membuat kriptografi yang baru atau melakukan perubahan pada kriptografi yang sudah ada. Melalui penelitian ini maka akan dibuat sebuah kriptografi yang menggunakan pola kain adat Karo dan menggunakan Block Cipher 64 bit untuk menghasilkan proses enkripsi yang lebih baik.

Kata kunci: *Block Cipher, Enkripsi, Karo, Kriptografi.*

1. PENDAHULUAN

Perkembangan di dunia teknologi informasi di era modern saat ini memberikan kemudahan akses bagi para penggunanya. Salah satu benefit yang ditawarkan adalah pertukaran informasi atau data yang cepat [1]. Pertukaran data ini sangat bermanfaat bagi para pengguna karena pengguna dapat mengirim serta menerima informasi kepada pengguna lain [2]. Namun, pertukaran data tersebut tidak menjamin keamanan data tersebut sampai ke tujuan, karena banyak terjadi pencurian data yang notabene data tersebut ialah data rahasia atau penting, sehingga data tersebut bocor ke publik [3]. Isu keamanan data ini tentunya menjadi keraguan bagi para pengguna teknologi informasi karena para pengguna membutuhkan sistem yang membuat data tersebut menjadi aman [4].

Saat ini, di era yang dengan perkembangan teknologi digital yang sangat pesat, keamanan akan data dan informasi pribadi menjadi salah satu aspek

yang penting untuk tetap diperhatikan. Berbagai macam ancaman akan isu keamanan data pribadi yang dengan mudahnya tersebar menjadi sangatlah meningkat [5]. Permasalahan akan kejahatan siber, seperti halnya pencurian data, penyadapan data, dan eksploitasi akan kerentanan dari suatu sistem menjadi sebuah ancaman yang tidak dapat disepelekan untuk dapat melindungi informasi yang bersifat sensitif [6]. Selain itu, berdasarkan akan hasil statistik yang diperoleh dari Breach Level Indeks (BLI), mengungkapkan bahwa pada tahun 2016 silam banyak terjadi kasus akan kehilangan dan pencurian data di dunia yang telah mencapai angka 1.378.509.261, atau dalam hal tersebut dapat dijabarkan bahwa dalam sehari terjadi 3.776.738 kasus akan pencurian dan kehilangan data, serta dalam hitungan jam terjadi sebanyak 157,364 kasus [7]. Dari hasil tersebut pada tahun 2016 hanya terdapat 4% pembobolan data yang dianggap tidak berhasil, yang dikarenakan data yang akan dibobol terlah di enkripsi terlebih dahulu perusahaan [8].

Dari permasalahan tersebut peneliti tertarik untuk meneliti keamanan data. Dimana Salah satu solusi untuk memenuhi kebutuhan keamanan data para pengguna ialah dengan menggunakan teknik kriptografi [9]. Teknik tersebut bertujuan untuk memecah maupun menyamarkan data atau sering disebut enkripsi, sehingga ketika data dikirim, maka data tersebut akan disamarkan agar tidak diketahui oleh pihak lain yang tidak berhak mengetahui informasi tersebut sehingga data tersebut aman sampai ke tujuan [10].

Kriptografi sendiri merupakan sebuah ilmu dan seni yang digunakan untuk dapat menjaga akan keamanan dari suatu pesan agar dapat dikirim dari satu tempat ke tempat yang lainnya [11]. Dalam hal tersebut, kriptografi ini berguna memiliki hubungan yang erat dengan pengamanan dari suatu informasi [12]. Selain itu, kriptografi menjadi salah satu aspek penting yang memegang sebagai peran urama dalam menjaga keamanan dari informasi, mulai dari seperti halnya percakapan melalui telepon, transaksi yang dilakukan di lingkup perbankan, bahkan sampai dalam melakukan aktivitas peluru kendali pada pengunaan kriptografi itu sendiri [13].

Dalam algoritmanya, Block Cipher merupaka salah satu bentuk algoritma yang paling banyak digunakan [14]. Namun, algoritma Block Cipher sendiri yang ada pada saat ini, seperti halnya DES (Data Encryption Standard) dan AES (Advanced Encryption Standard) memiliki berbagai kelemahan jika diterapkan pada saat ini pula [15]. Kelemahan yang dimaksud, yaitu kelemahan akan keamanan akan panjang dari kuncinya yang begitu pendek dan sumber daya komputasi yang dibutuhkan begitu tinggi [16]. Oleh karena itu, melalui penelitian ini akan dibuat sebuah inovasi yang unik dimana pada perancangan kriptografi kali ini akan menggunakan pola kain adat Karo dan menggunakan Block Cipher 64 bit sehingga menghasilkan proses enkripsi yang lebih baik dan aman. Alasan penggunaan kain adat Karo sendiri, dikarenakan kain adat Karo ini sendiri memiliki struktur yang begitu kompleks dan teratur. Maka dari itu, karakteritik dari kain adat Karo inilah akan dimanfaatkan untuk melakukan perancangan dari algoritma kriptografi Block Cipher yang unik, lebih aman, dan efisien.

2. METODE PENELITIAN

Metode penelitian ini melalui 5 tahapan penelitian, yaitu pengamatan masalah, tinjauan pustaka, perancangan kriptografi, pengujian hasil kriptografi, penulisan laporan penelitian.

Gambar. 2 Tahapan Penelitian

1) Pengamatan masalah: Peneliti mengamati masalah yang terjadi mengenai keamanan data dan kriptografi. Peneliti menemukan kekurangan tingkat keamanan data dengan teknik kriptografi standar, sehingga peneliti menemukan pola baru.
2) Tinjauan pustaka: Peneliti mengumpulkan referensi yang akan digunakan dalam pembuatan kriptografi yang baru. Mengumpulkan beragam acuan sehingga menemukan pola yang unik dan aman.
3) Perancangan kriptografi: Setelah peneliti mendapatkan beragam referensi, langkah selanjutnya peneliti merancang algoritma kriptografi baru yaitu dengan menggunakan block chiper 64 bit dengan pola kain adat Karo.
4) Hasil Pengujian kriptografi: Setelah pengerjaan kriptografi selesai maka akan dilakukan pengujian dengan cara manual seperti enkripsi dan dekripsi pada teknik kriptografi dengan pola kain adat Karo.
5) Penulisan laporan: Setelah penelitian dan pengujian selesai maka peneliti akan menulis hasil dari penelitian yang sudah dilakukan dalam bentuk laporan.

3. HASIL DAN PEMBAHASAN

A. Pola Enkripsi dan Dekripsi

Pola 1

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

Gambar. 3 Pola 1 pengambilan *plaintext*

Pola 2

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

Gambar. 4 Pola 2 pemasukan *plaintext*

Pola 3

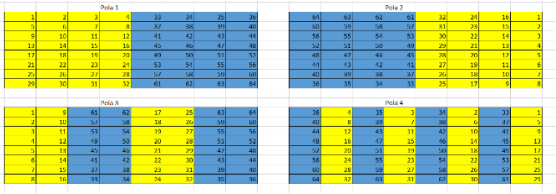
33	34	35	36	37	38	39	40
1	8	15	22	29	30	31	32
2	41	14	21	28	52	58	64
3	42	13	20	27	51	57	63
4	43	12	19	26	50	56	62
5	44	11	18	25	49	55	61
6	45	10	17	24	48	54	60
7	46	9	16	23	47	53	59

Gambar. 5 Pola 3 pengambilan *plaintext*

Pola 4

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

Gambar. 6 Pola 4 pengambilan *plaintext*



Gambar. 7 Pola untuk pengambilan *key*

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

Gambar. 8 Pemasukan bit

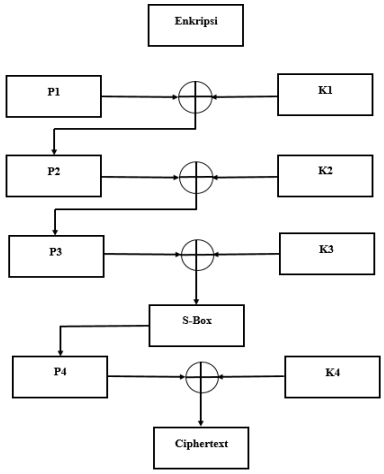
Pada Perancangan Kriptografi *Block Cipher* 64 bit Berbasis Pola Salah Satu Kain Adat Karo ini menggunakan pola seperti pada gambar 3, 4, 5, dan 6 sebagai pengambilan *plaintext*. Untuk pengambilan bit *key* menggunakan pola yang terdapat pada gambar 7. Gambar 8 merupakan pola atau urutan untuk untuk pemasukan setiap bit dari *plaintext* dan *key*.

B. *Rancangan Alur Enkripsi dan Dekripsi*

Penjelasan alur perubahan dari *plaintext* menjadi *ciphertext* dideskripsikan melalui Gambar 9 dan alur perubahan *ciphertext* menjadi *plaintext* Kembali dideskripsikan melalui Gambar 10.

1) *Enkripsi:*

Proses enkripsi dari *plaintext* menjadi *ciphertext* pada Gambar 9 melalui beberapa tahap yaitu:

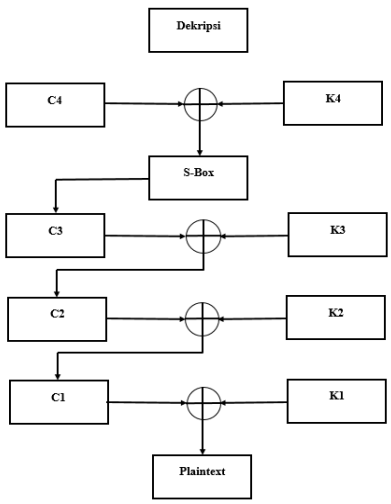


Gambar. 9 Rancangan alur enkripsi

1. Memasukkan plaintext yang berjumlah 8 karakter atau 64 bit.
2. *Plaintext* 1 melakukan transfromasi dengan pola kain adat Karo dan di-XOR dengan kunci 1 dan menghasilkan *plaintext* 2.
3. *Plaintext* 2 melakukan transformasi dengan pola kain adat Karo yang lain dan di-XOR lagi dengan kunci 2 untuk menghasilkan *plaintext* 3.
4. *Plaintext* 3 akan melakukan transformasi dengan pola kain adat Karo berikutnya dan di-XOR dengan kunci 3.
5. Setelah *plaintext* di-XOR dengan kunci 3, hasilnya akan ditransformasikan dengan S-Box sehingga menghasilkan *plaintext* 4.
6. *Plaintext* 4 melakukan transformasi dengan pola kain adat Karo berikutnya dan di-XOR dengan kunci 4 untuk menghasilkan *ciphertext*.

2) *Dekripsi:*

Proses dekripsi dari *ciphertext* menjadi *plaintext* pada Gambar 10 melalui beberapa tahap yaitu:



Gambar. 10 Rancangan alur dekripsi

1. Memasukkan *ciphertext* yang berjumlah 8 karakter atau 64 bit.
2. *Ciphertext* 4 melakukan transformasi dengan pola kain adat Karo dari enkripsi sebelumnya dengan urutan yang terbalik, kemudian di-XOR dengan kunci 4.
3. Hasil dari *ciphertext* 4 dan kunci 4 akan melakukan transformasi dengan S-Box untuk menghasilkan *ciphertext* 3.
4. *Ciphertext* 3 melakukan transformasi dengan pola kain adat Karo dan di-XOR dengan kunci 3, menghasilkan *ciphertext* 2.
5. *Ciphertext* 2 melakukan transformasi dengan pola kain adat Karo dan di-XOR dengan kunci 2, menghasilkan *ciphertext* 1.
6. *Ciphertext* 1 melakukan transformasi dengan pola kain adat Karo dan di-XOR dengan kunci 1, menghasilkan kembali *plaintext* yang sudah ditentukan sebelumnya.

3) *Korelasi:*

Untuk menentukan kombinasi pola yang akan digunakan dalam proses enkripsi dan dekripsi, perlu dicari nilai korelasi terhadap semua kombinasi pola. Dengan menggunakan contoh plaintext "BUDAYAJU" dan key "SALATIGA" akan mencari nilai korelasi yang paling tepat.

Tabel 1. Penghitungan Nilai Korelasi

Pola	Nilai	Pola	Nilai
1-2-3-4	-0.2318	3-2-1-4	0.583
1-2-4-3	0.2711	3-4-1-2	0.3306
1-4-2-3	0.106	3-2-4-1	0.4209
1-4-3-2	0.1391	3-4-2-1	0.1819
1-3-4-2	-0.0668	3-1-2-4	0.1321
1-3-2-4	0.1067	3-1-4-2	-0.5076
2-1-3-4	-0.595	4-1-2-3	-0.8378
2-1-4-3	-0.1278	4-1-3-2	-0.23
2-4-1-3	0.1278	4-3-1-2	-0.35
2-3-1-4	-0.2671	4-2-1-3	-0.384
2-4-3-1	0.3195	4-3-2-1	0.0155
2-3-4-1	-0.0962	4-2-3-1	-0.0935

Pada Tabel I telah dilakukan penghitungan nilai korelasi pada setiap kombinasi pola, diambil kombinasi yang memiliki nilai yang paling mendekati 0. Kombinasi pola 4-3-2-1 adalah pola yang paling mendekati nilai 0. Kemudian akan dilakukan proses enkripsi dan dekripsi menggunakan pola tersebut hingga 10 kali putaran. Untuk proses pada setiap putarannya masih menggunakan cara yang sama seperti sebelumnya.

Tabel 2. Hasil Pengujian

Putaran	Chiperteks	Hexa Plainteks	Nilai Korela-Si
1	fþÀ›Q("	66FEC09B512 89427	0.0155
2	›gtC1NAKí-SHY	9B6774433115 EDAD	0.0921
3	ª±ÂœÜtSYN HT	AAB1C29CDC 741609	-0.052
4	¸‹W‹-1" ³	B88B578B2D3 194B3	-0.0307
5	OòFS-US™KSYN	4FF21C2D1F3 34B16	0.0668
6	iéIÂ—WÔ7	69E949C29757 D437	0.1916
7	DC2úÜ;r'üDEL	12FADC3B729 1FC7F	0.2933
8	/èÁDLE~óÎÝ	2FE8C1107EF 3CEDD	0.3534
9	Š•ÅÊ0CR¾ë	8A95C5CA300 DBEEB	-0.0017
10	SYN—SP·Tü(|	169720B754FC 287C	-0.0949

Pada Tabel II menunjukkan hasil dari pengujian plainteks "BUDAYAJU" dan *key* "SALATIGA" menghasilkan cipherteks, hexa plainteks, dan nilai korelasi pada setiap putarannya. Pada bagian nilai korelasi, hubungannya menunjukkan hasil yang cukup rendah.

4. KESIMPULAN

Berda Pada penelitian Perancangan Kriptografi Block Cipher 64 bit Berbasis Pola Salah Satu Kain Adat Karo ini sudah memenuhi persyaratan 5-tuple untuk sebuah kriptografi. Dalam proses enkripsi, Perancangan Kriptografi Block Cipher 64 bit Berbasis Pola Salah Satu Kain Adat Karo menghasilkan hasil enkripsi yang acak. Sehingga keamanan data atau informasi terjamin, terutama dalam bentuk teks.

DAFTAR PUSTAKA

[1] N. C. Anam, "Perancangan Kriptografi Block Cipher 64 Bit Berbasis Pola Permainan Tradisional Bentengan Jawa Barat," *JUTEI*, vol. 3, no. 1, pp. 65–73, 2019, doi: 10.21460/jutei.2018.31.145.

[2] A. H. Alwan and A. H. Kashmar, "Block Ciphers Analysis Based on a Fully Connected Neural Network," *IHJPAS: Ibn Al-Haitham Journal For Pure and Applied Sciences*, vol. 36, no. 1, pp. 415–427, Jan. 2023, doi: 10.30526/36.1.3058.

[3] P. B. T. Kumbara and M. A. I. Pakereng, "Perancangan Teknik Kriptografi Block Cipher Berbasis Pola Permainan Tradisional Rangku Alu," *JuTISI: Jurnal Teknik Informatika dan Sistem Informasi*, vol. 5, no. 2, pp. 189–200, Sep. 2019, doi: 10.28932/jutisi.v5i2.1714.

[4] C. De Cannière, A. Biryukov, and B. Preneel, "An Introduction to Block Cipher Cryptanalysis," in *Proceedings of the IEEE*, Institute of Electrical and Electronics Engineers Inc., 2006, pp. 346–355. doi: 10.1109/JPROC.2005.862300.

[5] R. R. Fauzi and W. Theophilus, "Perancangan Kriptografi Block Cipher berbasis Pola Dribbling Practice," *AITI: Jurnal Teknologi Informasi*, vol. 18, no. 1, pp. 158–172, 2021.

[6] D. J. E. Prihanto and M. A. I. Pakereng,

"Perancangan Teknik Kriptografi Block Cipher Berbasis Pola Tarian Sajojo Papua," *ULTIMA Computing*, vol. 11, no. 2, pp. 71–80, 2019.

[7] A. K. Aziiz and M. A. I. Pakereng, "Perancangan Teknik Kriptografi Block Cipher Berbasis Pola Batik Ceplok Yogyakarta," *Justin: Jurnal Sistem dan Teknologi Informas*, vol. 8, no. 1, pp. 68–77, 2020.

[8] K. D. Cahyono and E. Mailoa, "Perancangan Kriptografi Block Cipher dengan Langkah Permainan Engklek," Salatiga , 2016.

[9] T. Thiranadya, M. Bulamey, and Hendry, "Perancangan Kriptografi Block Cipher Menggunakan Pola Logo Media Sosial," *JSON: Jurnal Sistem Komputer dan Informatika* , vol. 2, no. 2, pp. 115–122, 2021, doi: 10.30865/json.v2i2.2535.

[10] A. Gupta and N. K. Walia, "Cryptography Algorithms: A Review," *IJEDR: International Journal of Engineering Development and Research*, vol. 2, no. 2, pp. 1667–1673, 2014, [Online]. Available: www.ijedr.org

[11] D. D. Bili, M. A. I. Pakereng, and A. D. Wowor, "Perancangan Kriptografi Block Cipher dengan Langkah Kuda," Salatiga, 2015.

[12] Warkim, I. Lewenusa, and P. K. Karo, "Kriptografi Algoritma Advanced Encryption Standard dan Pengecekan Error Detection Cyclic Redundacy Check," *Jurnal FTI UNTAR*, 2015, [Online]. Available: http://fti.tarumanagara.ac.id/jurnal/index.php/jki

[13] S. D. Bramantya and M. A. I. Pakereng, "Perancangan Kriptografi Blok Cipher Berbasis Pola Gambar RUmah Adat Joglo," *JTIK: Jurnal Teknologi Teknologi Informasi dan Komunikasi*, vol. 7, no. 4, pp. 629–638, 2023.

[14] Edo, H. Nasution, and M. A. Irwansyah, "Perancangan Teknik Kriptografi Block Cipher Berbasis Pola Peta Administrasi Kalimantan Barat Menggunakan Key-Dependent S-Box," *JIP: Jurnal Informatika Polinema*, vol. 10, no. 3, pp. 323–332, 2024.

[15] M. Afsari, D. I. Mulyana, A. Damaiyanti, and N. Sa'adah, "Implementasi Mode Operasi Kombinasi Cipher Block Chaining dan Metode LSB-1 Pada Pengamanan Data text," *Jurnal Pendidikan Sains dan Komputer*, vol. 2, no. 1, pp. 70–82, 2022, doi: 10.47709/jpsk.v2i1.1381.

[16] H. Khair, J. D. M Saragih, and A. M. H. Pardede, "Pengamanan Data Teks Menggunakan Algoritma Modular Multiplication Based Block Chiper," *Information System Development*, vol. 6, no. 1, pp. 10–16, 2021.