PERANCANGAN TEKNIK KRIPTOGRAFI *BLOCK CIPHER* BERBASIS POLA PETA ADMINISTRASI KALIMANTAN BARAT MENGGUNAKAN *KEY-DEPENDENT* S-BOX

Edo[1], Helfi Nasution[2], Muhammad Azhar Irwansyah[3]

[1,2,3] Jurusan Informatika, Fakultas Teknik, Universitas Tanjungpura
Jalan Prof. Dr. H. Hadari Nawawi, Pontianak, Indonesia
[1]eduarduse72@gmail.com, [2]helfi_nasution@yahoo.com, [3]irwansyah.azhar@gmail.com

Abstrak

Kriptografi adalah teknik pengamanan informasi dengan cara mengubah pesan menggunakan suatu metode enkripsi sehingga tidak dapat dibaca oleh pihak yang tidak berhak. *Block cipher* merupakan salah satu algoritma kriptografi yang menggunakan kumpulan bit dengan panjang tetap untuk mengenkripsi pesan, dengan cara pertukaran kode bit pesan sehingga membentuk suatu pesan baru yang tidak dapat dibaca (*ciphertext*). Penelitian dilakukan dengan tujuan merancang kriptografi *block cipher* baru yang merepresentasikan ciri khas pola peta administrasi Kalimantan Barat dalam pertukaran kode bitnya. Pola tersebut memiliki bentuk abstrak pada pembagian wilayah kabupaten/kota serta batas administrasinya, sehingga membuat rancangan algoritma kriptografi yang unik dan berbeda dengan algoritma kriptografi lainnya. Perancangan dilakukan dengan mengacu algoritma kriptografi *block cipher Advance Encryption Standard* (AES) yang ditetapkan oleh *National Institute of Standard and Technology* (NIST) sebagai standar pengamanan informasi didunia. Algoritma kriptografi yang dirancang juga menggunakan substitusi *box* (S-Box) dinamis yang dibangkitkan dengan kunci sehingga berbeda dengan S-box statis AES. Pengujian terhadap performa algoritma kriptografi menunjukkan hasil yang baik. Hasil pengujian *avalance effect* mendapatkan nilai rata-rata 50,524%. Simulasi waktu enkripsi per 500 blok data rata-rata membutuhkan waktu 3,514 detik. Analisis serangan *brute force* menunjukkan waktu yang diperlukan untuk melakukan *exhaustive search*, yaitu $1{,}341\ x\ 10^{152}$ detik atau setara $4{,}252\ x\ 10^{144}$ tahun. Algoritma kriptografi yang dihasilkan dapat bekerja dengan baik dalam 5 *mode* operasi *block cipher* yang direkomendasikan oleh NIST, yaitu *Electronic Code Book* (ECB), *Cipher Block Chaining* (CBC), *Cipher Feedback* (CFB), *Output Feedback* (OFB), dan *Counter* (CTR). Penelitian juga mengimplementasikan algoritma kriptografi ke dalam sebuah aplikasi surat elektronik berbasis *web*.

Kata kunci: *block cipher*, kalimantan barat, *advance encryption standard*, s-box dinamis, aplikasi surat elektronik

1. Pendahuluan

Perkembangan teknologi informasi yang begitu pesat saat ini memegang peranan penting dalam segala aspek kehidupan manusia. Teknologi informasi membuat masyarakat dapat membuat, mengubah, menyimpan, dan menyebarkan informasi dengan mudah. Kriptografi sebagai ilmu untuk menjaga kerahasiaan pesan dapat digunakan dalam mengamankan informasi dan data, yaitu dengan mengubah pesan menggunakan suatu metode enkripsi sehingga tidak dapat dibaca secara langsung oleh pihak yang tidak berhak (Dakhi et al., 2020; Silalahi & Sindar, 2020; Yusfrizal, 2019; Ziliwu et al., 2022).

Block cipher merupakan salah satu algoritma kriptografi yang menggunakan kumpulan bit dengan panjang tetap untuk mengenkripsi pesan, dengan kata lain membagi bit-bit *plainteks* menjadi blok dengan panjang yang sama (Murdowo, 2019). *Block cipher* dapat dilakukan dengan memodifikasi pola atau algoritma yang sudah ada, sehingga dapat menunjukkan ciri khas dari pola tertentu, yaitu dengan menggabungkan perhitungan operasi sederhana seperti, XOR atau substitusi yang dilakukan dalam beberapa putaran untuk meningkatkan keamanan pesan. Di dalam proses enkripsi maupun dekripsi, *block cipher* menggunakan operasi XOR dengan *output* yang dihasilkan dari proses enkripsi akan susah ditebak (Alam & Pratama, n.d.; Aziiz & Pakereng, 2020).

AES (*Advanced Encryption Standard*) merupakan algoritma *block cipher* yang telah ditetapkan sebagai standar pengamanan informasi dunia, yang menggunakan s-box yang bersifat statis, yang menggantikan pendahulunya, yaitu DES (*Data Encryption Standard*) (Aminudin & Hariyady, 2021; Azhari et al., 2022). Proses enkripsi AES menggunakan 4 transformasi dasar dengan urutan trasformasi *subbytes*, *shiftrows*, *mixcolumns*, dan *addroundkey* (Yudha & Laluma, 2019). S-box sendiri atau *substitution box* merupakan teknik dasar yang diperlukan dalam merancang *blok cipher* yang telah ditetapkan oleh *National Institute of Standard and*

Technology (NIST), dengan melakukan substitusi, baik substitusi bit maupun substitusi *byte*, dimana dapat menghasilkan hubungan nonlinier antara kunci dengan *ciphertext* dan memberikan efek *confusion* dari prinsip Shannon (Kumbara & Pakereng, 2019).

Dua prinsip dasar pada desain *block cipher* adalah *confusion* dan *diffusion*. Operasi-operasi sederhana, seperti substitusi dan permutasi, bila dilakukan berkali-kali pada suatu blok *plaintext* dapat menghasilkan *confusion* dan *diffusion* yang baik (Mulyadi, 2019; Ndruru & Zebua, 2022). Terdapat lima mode operasi yang direkomendasikan oleh *National Institute of Standard and Technology* (NIST) dalam *block cipher*, yaitu *Electronic Code Book* (ECB), *Cipher Block Chaining* (CBC), *Cipher Feedback* (CFB), *Output Feedback* (OFB), dan *Counter* (CTR) (Gulo, 2021).

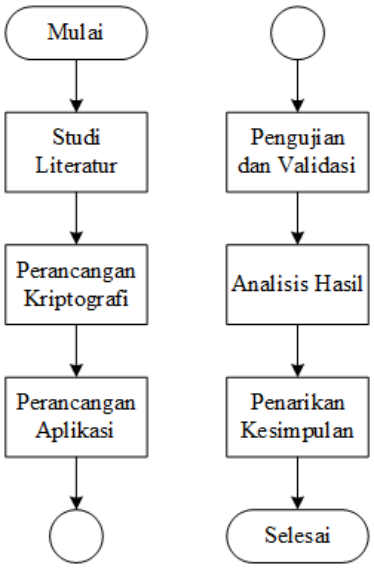
Peta administrasi Kalimantan Barat adalah peta yang menginformasikan batas-batas administratif terkecil sampai terbesar wilayah provinsi Kalimantan Barat, yang mana sampai saat ini terbagi atas 14 wilayah administratif kabupaten/kota, yang kemudian kabupaten/kota tersebut terbagi lagi dalam kecamatan dan desa yang jumlahnya mencapai ratusan. Pembagian wilayah kabupaten/kota serta batas administrasi provinsi Kalimantan Barat memiliki bentuk yang abstrak sehingga peta administrasi Kalimantan Barat menarik untuk dijadikan pola dalam perancangan teknik kriptografi *block cipher*, karena akan membuat rancangan algoritma kriptografi yang unik dan berbeda dengan algoritma kriptografi yang sudah ada.

Berikut beberapa penelitian terkait perancangan teknik kriptografi yang menggunakan pola tertentu dalam melakukan perancangannya, diantaranya penelitian yang dilakukan oleh Aziiz & Pakereng (2020) yang menggunakan pola batik ceplok Yogyakarta dalam perancangan teknik kriptografi *block cipher*. Selain itu, terdapat penelitian Prihanto & Pakereng (2020) yang merancang teknik kriptografi *block cipher* dengan menggunakan pola tarian sajojo Papua. Kemudian terdapat penelitian yang dilakukan oleh Fauzi & Wellem (2021), yang merancang teknik kriptografi *block cipher* berbasis pola *dribbling practice*.

Penelitian ini merancang teknik kriptografi *block cipher* dengan pola dan algoritma yang memberikan ciri khas pola peta administrasi Kalimantan Barat didalam proses pertukaran kode bitnya. Kalimantan Barat merupakan cakupan wilayah yang sangat luas sehingga untuk dapat merepresentasikannya secara utuh pola dalam teknik kriptografi yang dirancang menggunakan pertukaran kode dengan panjang 256 bit. Dengan dilakukan penelitian ini diharapkan dapat menghasilkan teknik kriptografi baru yang memiliki ciri khas berbeda dengan teknik kriptografi yang sudah ada. Teknik kriptografi yang dirancang menggunakan S-box dinamis (*Key Dependent S-box*) yang diharapkan dapat menambah kompleksitas enkripsi yang dihasilkan. Penggunaan S-box dinamis diharapkan mampu menambah kekuatan dari teknik kriptografi yang dirancang sehingga sulit untuk dipecahkan oleh *cryptoanalysis*.

2. Metode

Adapun tahapan-tahapan yang dilakukan dalam penelitian ini digambarkan dalam diagram alir penelitian Gambar 1 berikut.



Gambar 1. Diagram Alir Penelitian

Berdasarkan gambar 1, penelitian dilakukan dimulai dengan tahapan studi literatur, kemudian dilanjutkan dengan perancangan kriptografi, perancangan aplikasi surat elektronik, pengujian dan validasi, analisis hasil, dan diakhiri dengan melakukan penarikan kesimpulan.

2.1 Studi Literatur

Tahap pertama yang dilakukan dalam penelitian ini adalah studi literatur mengenai kriptografi, serta *block cipher* secara umum. Studi literatur dilakukan untuk memeroleh informasi tentang proses enkripsi, dekripsi dalam kriptografi dan data-data berkaitan yang diperlukan dalam proses perancangan kriptografi sehingga mempermudah proses analisis dan perancangan dalam pengerjaan kriptografi. Selain itu, dilakukan studi literatur terhadap salah satu algoritma kriptografi *block cipher*, yaitu *Advanced Encryption Standard* (AES) yang ditetapkan sebagai standar pengamanan informasi dunia. Pemahaman mengenai alur kerja algoritma AES sebagai metode yang akan dijadikan acuan dalam perancangan algoritma kriptografi yang diusulkan.

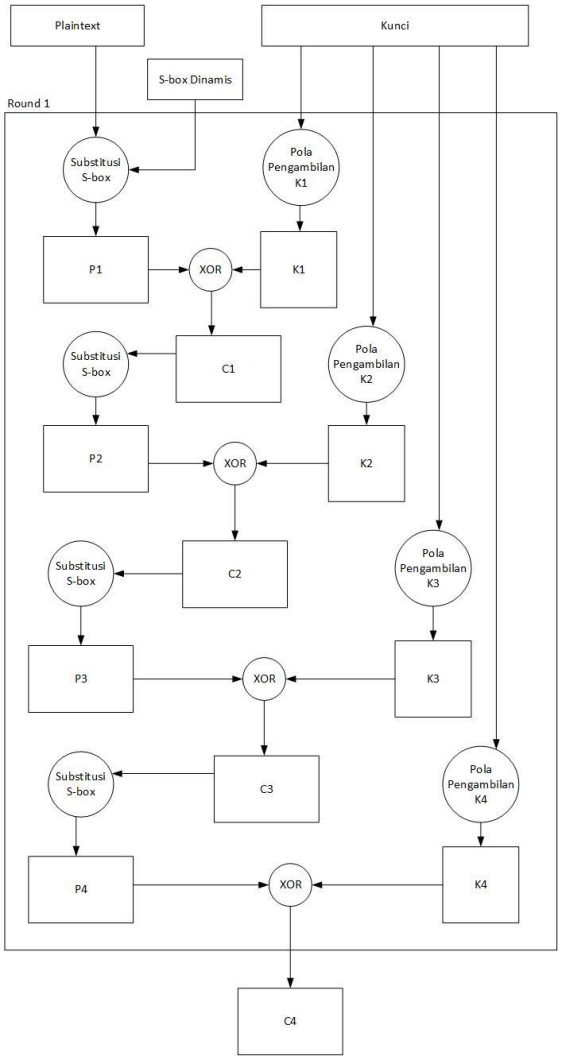
2.2 Perancangan Kriptografi

Pada tahap ini dilakukan perancangan kriptografi yang diusulkan, yaitu dengan menentukan pola kunci, proses transformasi dalam tiap putaran,

dan proses pembangkitan s-box dinamis yang akan digunakan.

2.2.1 Skema Enkripsi dan Dekripsi

Skema enkripsi menggambarkan bagaimana proses sebuah pesan diacak sehingga tidak dapat dikenali sebagaimana pesan aslinya. Sedangkan skema dekripsi menggambarkan bagaimana proses sebuah pesan yang telah diacak (enkrip) dikembalikan menjadi pesan aslinya. Skema enkripsi pada penelitian ini akan digambarkan menggunakan diagram alir (*flowchart*) dalam gambar 2 berikut.



Gambar 2. Skema Proses Enkripsi

Skema enkripsi dan dekripsi dalam algoritma kriptografi yang dirancang mengadaptasi *Advanced Encryption Standard* (AES), yaitu menggunakan proses substitusi dan transformasi dalam setiap putarannya. Berdasarkan diagram alir skema enkripsi pada Gambar 2, pada saat *plaintext* akan dienkripsi, maka akan dilakukan proses substitusi dengan tabel s-box dinamis yang telah dibangkitkan tiap awal proses enkripsi. Kunci yang digunakan dalam suatu proses enkripsi berupa 32 karakter ASCII. Dalam tiap-tiap penyandian *plaintext* memiliki ukuran blok 256 bit. Setelah proses substitusi, dilakukan transformasi terhadap hasil substitusi, yaitu operasi XOR dengan matrix kunci yang telah diacak menggunakan pola pengambilan kunci. Dalam satu putaran dilakukan proses substitusi dan transformasi berulang sebanyak 4 kali menggunakan pola pengambilan kunci yang berbeda. Pola pengambilan kunci yang dibedakan bermaksud untuk menambah nilai keacakan penyandian. Sebagaimana AES-256 perancangan kriptografi menerapkan fungsi putaran 14 kali.

Sedangkan pada proses dekripsi, substitusi dan transformasi yang dilakukan berupa kebalikan dari proses enkripsi. Substitusi yang dilakukan pada proses dekripsi menggunakan *invers* s-box dinamis. Transformasi dalam proses dekripsi dilakukan dengan operasi XOR, dimana pola pengambilan kunci yang digunakan urutannya dibalik. Proses dekripsi menerapkan fungsi putaran 14 kali sebagaimana proses enkripsi dilakukan.

2.2.2 Pola Pengambilan Kunci

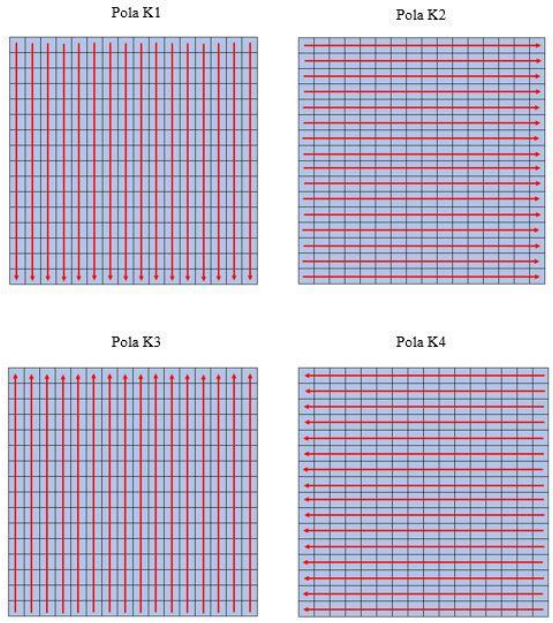
Proses enkripsi pada perancangan teknik kriptografi penelitian ini, bekerja dengan mengacak bit pesan. Pesan, maupun kunci akan dikonversi menjadi bit pembentuknya sebelum masuk ke dalam skema enkripsi. Berikut rancangan pola pengambilan kunci apabila menggunakan peta administrasi Kalimantan Barat yang ditunjukkan oleh Gambar 3.

68	69	1	70	71	72	73	74	75	76	77	78	79	80	81	82
83	2	3	84	85	86	87	88	89	90	91	4	5	92	93	94
6	7	8	46	95	96	97	98	99	100	9	10	11	12	13	14
231	47	48	49	201	101	202	203	204	15	16	17	18	19	20	102
50	51	21	22	205	206	23	207	208	24	25	26	27	28	29	103
209	210	30	31	211	212	32	213	214	33	34	35	36	37	104	105
106	232	52	215	216	217	38	218	219	220	221	222	223	224	107	108
109	53	54	55	225	39	40	226	56	57	227	228	229	110	111	112
113	58	59	233	234	235	236	60	61	62	63	230	114	115	116	117
118	119	64	41	42	237	238	65	66	120	121	122	123	124	125	126
127	128	43	44	45	239	240	67	129	130	131	132	133	134	135	136
137	138	139	140	241	242	243	141	142	143	144	145	146	147	148	149
150	151	152	244	245	246	247	153	154	155	156	157	158	159	160	161
162	163	164	165	248	249	250	166	167	168	169	170	171	172	173	174
175	176	177	178	251	252	253	179	180	181	182	183	184	185	186	187
188	189	190	191	254	255	256	192	193	194	195	196	197	198	199	200

Gambar 3. Pola Pengambilan Kunci

Gambar 3 tersebut merupakan pola pengambilan kunci yang dirancang menggunakan peta administrasi Kalimantan Barat, dimana pada saat awal kunci diterima adalah 32 karakter ASCII yang kemudian dikonversi dalam bit. Kunci yang telah dikonversi dalam bit kemudian diacak, yaitu dengan pengambilan bit sesuai nomor-nomor yang tertera pada Gambar 3 tersebut. Bit kunci yang diambil sesuai urutan pola, kemudian dimasukkan ke dalam matrix baru dan digunakan untuk operasi XOR.

Pada penelitian ini, bit kunci yang diambil berdasarkan pola pengambilan kunci tersebut dimasukkan ke dalam matrix baru yang diusulkan, yang dibedakan menjadi 4 pola masukan kunci, yaitu pola K1, pola K2, pola K3, dan pola K4. Gambar 4 berikut menerangkan pola masukan kunci yang terbentuk.



Gambar 4. Pola Masukan Kunci

Berdasarkan gambar 4, pola masukan kunci K1 merupakan pemasukan bit yang dilakukan dari atas ke bawah, dan kemudian dilanjutkan terhadap setiap kolomnya secara berurutan. Pola masukan kunci K2 merupakan pemasukan bit yang dilakukan dari kiri ke kanan, dan kemudian dilanjutkan terhadap setiap barisnya secara berurutan. Pola masukan kunci K3 merupakan proses pemasukan bit yang dilakukan dari bawah ke atas, dan kemudian dilanjutkan ke kolom selanjutnya secara berurutan. Pola masukan kunci K4 merupakan pemasukan bit yang dilakukan dari kanan ke kiri, dan kemudian dilanjutkan ke baris berikutnya secara berurutan.

Kombinasi yang dihasilkan melalui pola pengambilan kunci dengan 4 variasi pola masukan kunci ke dalam matrix baru yang dirancang adalah 24 kombinasi, yang kemudian akan dicari pola masukan yang paling baik untuk digunakan, yaitu dengan melakukan percobaan mencari nilai korelasi. Percobaan dilakukan menggunakan 18 kunci dengan indeks perubahan bit yang bervariasi untuk mengenkripsi *plaintext* yang sama. *Plaintext* yang digunakan dalam percobaan yang dilakukan, yaitu "MERDEKABELAJARBERSAMAUNTANPONTNK".

Tiap kombinasi pola dilakukan percobaan sebanyak 18 kali untuk kemudian dicari nilai korelasinya. Kombinasi pola terbaik didapatkan dengan menghitung nilai rata-rata korelasi dari 18 kali percobaan yang dibandingkan satu sama lain. Tabel 1 berikut merupakan rangkuman perbandingan hasil perhitungan untuk nilai korelasi tiap pola masukan kunci yang terbentuk.

Tabel 1. Perbandingan Nilai Korelasi Tiap Pola Masukan Kunci

No.	Pola	Rata-rata Korelasi
1	**1-2-3-4**	**-0.01215817**
2	1-2-4-3	0.03778419
3	1-3-2-4	0.09318935
4	1-3-4-2	-0.057410399
5	1-4-2-3	0.03371472
6	1-4-3-2	-0.157607857
7	2-1-3-4	0.055066719
8	2-1-4-3	0.280665558
9	2-3-1-4	0.117626814
10	2-3-4-1	0.039565665
11	2-4-1-3	-0.127602376
12	2-4-3-1	0.045373803
13	3-1-2-4	0.087689853
14	3-1-4-2	0.06382514
15	3-2-1-4	-0.070610111
16	3-2-4-1	0.166660338
17	3-4-1-2	0.146058031
18	3-4-2-1	-0.023981093
19	4-1-2-3	0.025799928
20	4-1-3-2	-0.064956963
21	4-2-1-3	0.181016424
22	4-2-3-1	0.071524156
23	4-3-1-2	-0.138101626
24	4-3-2-1	-0.026126281

Berdasarkan tabel 1 tersebut, diperoleh hasil perancangan pola kunci terbaik, yaitu dengan urutan pemasukan kunci 1-2-3-4, dengan nilai rata-rata korelasi yang dihasilkan adalah -0.01215817. Dengan demikian, maka akan digunakan pola tersebut dalam setiap tahapan perancangan teknik kriptografi ini.

2.2.3 S-Box Dinamis

S-box dinamis dirancang dengan tujuan untuk mengatur vektor s-box. S-box dinamis ini sendiri dirancang dengan menggunakan kunci rahasia yang berupa rangkaian permutasi acak nilai 16 hexadesimal. Berikut langkah yang dilakukan dalam proses pembangkitan s-box dinamis, yang ditunjukan dalam tabel 2.

Tabel 2. Langkah Pembangkitan S-Box Dinamis

Langkah – langkah	Rentetan Nilai (dalam hexadesimal)
Rangkaian Permutasi	B2EF119982954120CBBAB1DD812E8CF1
S1 sebelum di atur	B 2 E F 1 1 9 9 8 2 9 5 4 1 2 0
S1 sesudah di atur	B 2 E F 1 9 8 5 4 0 3 6 7 A C D
S2 sebelum di atur	C B B A B 1 D D 8 1 2 E 8 C F 1
S2 sesudah di atur	C B A 1 D 8 2 E F 0 3 4 5 6 7 9

Berdasarkan tabel 2, pada langkah pertama pembangkitan s-box dinamis, rangkaian permutasi dibangkitkan menggunakan fungsi php, dimana

panjang rangkaian permutasi yang digunakan adalah 32 karakter hexadesimal. Selanjutnya, rangkaian permutasi dibagi menjadi dua, dimana 16 karakter pertama digunakan untuk S1 dalam mengatur baris s-box dan 16 karakter berikutnya digunakan untuk S2 dalam mengatur kolom s-box. Rangkaian S1 dan S2 kemudian diatur, yaitu untuk penggunaan karakter yang sama tidak diperbolehkan dalam satu rangkaian, sehingga karakter tersebut akan diganti dengan karakter hexadesimal yang berbeda pada akhir rangkaian.

Setelah rangkaian kunci rahasia S1 dan S2 selesai diatur, s-box standar AES kemudian disusun ulang. Urutan baris dan kolom dari s-box standar AES disusun sesuai dengan nilai S1 dan S2. Hasil dari susunan ulang s-box ini disebut S-box berdasarkan kunci rahasia. S-box yang dibangkitkan juga dapat di *invers* untuk digunakan pada proses dekripsi.

Gambar 5 berikut merupakan s-box yang terbentuk berdasarkan kunci rahasia dalam rangkaian S1 dan S2.

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

Gambar 5. S-Box Berdasarkan Kunci Rahasia

Gambar 6 berikut merupakan *invers* s-box yang terbentuk berdasarkan kunci rahasia dalam rangkaian S1 dan S2.

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

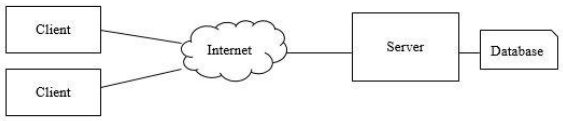
Gambar 6. *Invers* S-Box Berdasarkan Kunci Rahasia

2.3 Perancangan Aplikasi Surat Elektronik

Setelah teknik kriptografi selesai dirancang, penelitian dilanjutkan dengan merancang aplikasi surat elektronik atau email. Perancangan aplikasi email dilakukan untuk mengimplementasikan teknik kriptografi yang sudah dibangun. Perancangan aplikasi email dilakukan melalui beberapa tahapan, yaitu perancangan arsitektur aplikasi, perancangan *Data Flow Diagram* (DFD), perancangan *Entity Relationship Diagram* (ERD), dan perancangan struktur antarmuka aplikasi.

2.3.1 Arsitektur Aplikasi

Berikut arsitektur aplikasi email yang digambarkan dalam gambar 7.



Gambar 7. Arsitektur Aplikasi

Berdasarkan gambar 7 tersebut, aplikasi email dirancang berbasis *website* dengan menggunakan bahasa pemrograman php, sehingga setiap pengguna perlu terhubung ke internet agar dapat bertukar pesan menggunakan aplikasi tersebut. Teknik kriptografi yang telah dirancang sebelumnya, akan diimplementasikan pada proses penyimpanan data oleh server ke dalam *database*. Pesan yang tersimpan dalam *database* aplikasi merupakan pesan yang telah dienkripsi, sehingga apabila terjadi pencurian data terhadap aplikasi, pesan tetap aman karena tidak dapat dibaca oleh pencuri.

2.3.2 Data Flow Diagram (DFD)

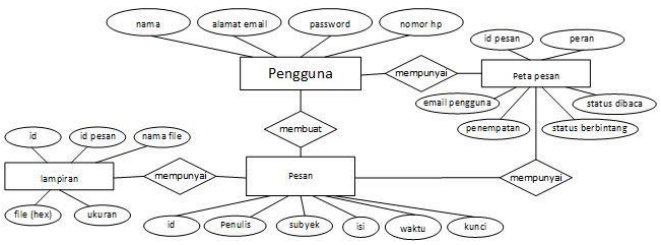
Berikut *Data Flow Diagram* (DFD) aplikasi email yang digambarkan dalam gambar 8.

Gambar 8. *Data Flow Diagram* (DFD)

Berdasarkan *Data Flow Diagram* (DFD) yang terdapat pada Gambar 8 tersebut, aplikasi email yang dirancang mendukung satu jenis pengguna yang memiliki peran yang sama dan dapat saling bertukar pesan, baik pesan yang berisi teks, maupun *file*, yang kemudian akan dienkripsi oleh aplikasi untuk menjaga keamanannya.

2.3.3 Entity Relationship Diagram (ERD)

Berikut *Entity Relationship Diagram* (ERD) aplikasi email yang digambarkan dalam gambar 9.

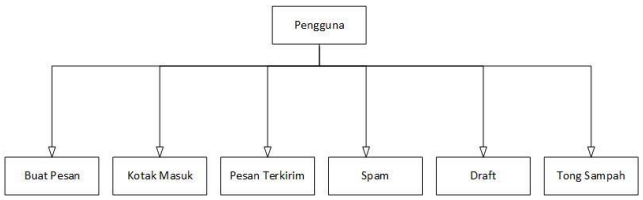


Gambar 9. *Entity Relationship Diagram* (ERD)

Gambar 9 menunjukkan bahwa aplikasi email yang dirancang terdiri atas empat entitas, yaitu pengguna, pesan, peta pesan, dan lampiran.

2.3.4 Struktur Antarmuka Aplikasi

Berikut rancangan struktur antarmuka aplikasi email yang digambarkan dalam gambar 10.



Gambar 10. Rancangan Struktur Antarmuka Aplikasi

Rancangan struktur antarmuka aplikasi yang ditunjukkan pada gambar 10, dirancang dengan sangat sederhana, yaitu aplikasi dapat menampilkan semua pesan milik pengguna yang dipisah berdasarkan jenis pesan yang ingin ditampilkan oleh pengguna. Jenis pesan dikategorikan sesuai dengan posisi pesan dan peran pengguna dalam pesan tersebut untuk memudahkan pengguna dalam mengelola pesan miliknya.

2.4 Pengujian dan Validasi

Pengujian akan dilakukan untuk mengetahui apakah kriptografi yang dihasilkan dapat berjalan dengan baik dan melakukan enkripsi, maupun dekripsi sesuai dengan yang diharapkan. Nilai korelasi dalam beberapa percobaan pola akan dihitung, kemudian dicari yang terbaik. Selain itu, pada tahap ini juga akan dilakukan identifikasi jika terdapat ketidakkonsistenan dalam kriptografi yang dihasilkan, maka kemudian akan digunakan sebagai dasar perbaikan.

2.5 Analisis Hasil

Analisis hasil dilakukan setelah tahap pengujian dan validasi untuk mengetahui karakteristik dari kriptografi yang dihasilkan, yaitu dengan mencoba beberapa mode operasi *block cipher*.

2.6 Penarikan Kesimpulan

Berdasarkan semua tahapan yang telah dilakukan, kemudian dirumuskan dalam kesimpulan untuk diketahui apakah kriptografi yang terbentuk layak untuk diimplementasikan.

3. Hasil dan Pembahasan

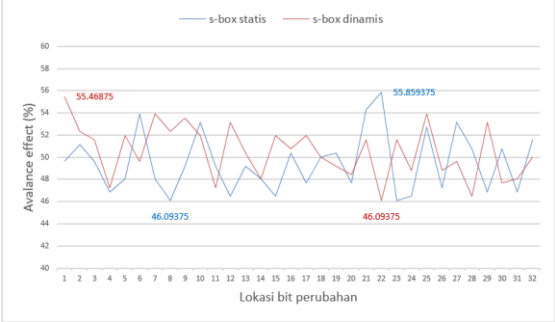
Berikut dipaparkan hasil dan pembahasan yang diperoleh melalui penelitian yang telah dilakukan, yaitu hasil perancangan kriptografi, hasil percobaan mode operasi *block cipher*, dan hasil perancangan aplikasi.

3.1 Hasil Perancangan Kriptografi

Berikut analisis keamanan terhadap teknik kriptografi yang telah dirancang untuk melihat seperti apa hasilnya dan mengetahui gambaran kekuatan keamanan yang terbentuk.

3.1.1 *Avalanche Effect*

Menurut Sermeno, Secugal, dan Mistio (2021) dalam Umam et al., 2022, *avalanche effect* merupakan salah satu ciri untuk menentukan baik tidaknya suatu algoritma kriptografi. *Avalanche effect* menggambarkan besarnya perubahan bit *chipertext* yang dihasilkan dengan merubah satu bit dari *plaintext*. Pada Gambar 11, terlihat hasil pengujian *avalanche effect* terhadap algoritma kriptografi yang telah dirancang pada penelitian ini.



Gambar 11. Hasil Pengujian *Avalanche Effect*

Berdasarkan Gambar 11 tersebut, hasil pengujian *avalanche effect* terlihat cukup baik, dengan nilai yang diperoleh berkisar 46% - 56%. Pada rancangan teknik kriptografi menggunakan s-box statis, *avalanche effect* yang diperoleh memiliki nilai rata-rata 49,499%, sedangkan penggunaan s-box dinamis memberikan hasil *avalanche effect* dengan nilai rata-rata 50,524%. Jadi, selisih nilai rata-rata *avalanche effect* yang dihasilkan, yaitu 1,025%, dimana menunjukkan bahwa penggunaan s-box dinamis tidak memberikan dampak perubahan yang signifikan terhadap nilai *avalanche effect*. Secara keseluruhan, nilai yang diperoleh melalui pengujian *avalanche effect* menunjukkan bahwa perubahan bit membuat sebuah perbedaan yang cukup besar sehingga menyulitkan *cryptanalyst* untuk melakukan serangan.

3.1.2 Simulasi Waktu dan Kompleksitas Algoritma

Simulasi waktu dilakukan untuk mengukur lama waktu yang dibutuhkan oleh algoritma untuk memroses sepenuhnya panjang data tertentu. Kompleksitas algoritma sangat memengaruhi simulasi waktu, namun hasil pengukuran tidak dapat memberikan nilai secara konstan. Hal ini disebabkan simulasi waktu juga bergantung pada alat penelitian yang digunakan, misalnya kecepatan prosesor yang selalu berubah. Pada penelitian ini, dilakukan simulasi waktu dengan mengukur lama waktu yang dibutuhkan untuk mengenkripsi 500 *block* data. Tabel 3 berikut dipaparkan rata-rata waktu yang dibutuhkan dalam proses enkripsi dengan menggunakan s-box statis dan s-box dinamis.

Tabel 3. Simulasi Waktu Enkripsi

	Simulasi Waktu
S-box Statis	3.502436988
S-box Dinamis	3.514756076

Berdasarkan tabel 3 tersebut, waktu rata-rata yang diperoleh untuk melakukan proses enkripsi memiliki perbedaan yang tidak jauh. Dengan selisih waktu yang begitu kecil, dapat digambarkan bahwa penambahan s-box dinamis tidak memengaruhi beban pemrosesan yang begitu besar kepada algoritma yang dirancang sehingga teknik kriptografi yang dirancang sangat layak untuk digunakan.

Pertumbuhan kompleksitas algoritma disajikan dengan menggunakan konsep notasi big-o agar dapat mengestimasi waktu efisiensi relatif. Algoritma akan mentransformasi objek masukan menjadi objek keluaran dengan waktu eksekusi yang merupakan fungsi dari objek masukan. Semakin besar objek masukan, maka semakin lama pula waktu yang dibutuhkan untuk menghasilkan objek keluaran. Gambar 12 berikut merupakan *pseudocode* algoritma kriptografi yang dirancang dalam penelitian ini.

```
Algoritma enkripsi(plaintext)
    generate kunci
    ambil bit kunci dengan pola kalbar
    bikin matrix dengan pola masukan k1
    bikin matrix dengan pola masukan k2
    bikin matrix dengan pola masukan k3
    bikin matrix dengan pola masukan k4                    } O(1)
    generate kunci (s-box dinamis)
    susun matrix s-box dinamis
    for 1 to plaintext.length do
      for 1 to 14 do
            substitusi s-box
            XOR k1
            substitusi s-box
            XOR k2
            substitusi s-box                  } O(1)       } O(n)
            XOR k3
            substitusi s-box
            XOR k4
      end for
    end for
```

Gambar 12. *Pseudocode* Algoritma Kriptografi

Dengan menggunakan aturan notasi big-o, pertumbuhan kompleksitas algoritma kriptografi *block cipher* berbasis pola peta administrasi Kalimantan Barat menggunakan *key-dependent* s-box membentuk fungsi *linear* atau O(n). Kompleksitas O(n) *linear* merupakan kompleksitas yang paling dominan yang ditemukan pada algoritma yang dirancang, sehingga dengan mengacu pada aturan notasi big-o kompleksitas lain dapat diabaikan. Fungsi *linear time* adalah ketika *runtime* dari fungsi kita berbanding lurus dengan jumlah input yang diberikan. Berdasarkan Gambar 12, dapat disimpulkan bahwa semakin banyak jumlah *input* yang diberikan, maka waktu proses/*runtime* dari fungsi tersebut akan semakin besar.

3.1.3 *Brute Force*

Brute force attack merupakan salah satu cara yang paling sederhana untuk mencoba mendapatkan kunci dengan cara mencari semua kemungkinan kunci atau biasa disebut dengan *exhaustive search*. Biasanya serangan dengan teknik ini membutuhkan waktu yang sangat lama dikarenakan kemungkinan kunci sangatlah banyak. Pada algoritma kriptografi yang dirancang ini, panjang kunci yang dimiliki adalah 256-bit, dimana penggunaan s-box dinamis menambah panjang kunci menjadi 512-bit. Hal ini dikarenakan terdapat 2^{512} kemungkinan kunci yang dipergunakan, yang mana merupakan angka yang sangat besar. Pada penelitian ini, akan dilakukan perhitungan waktu menggunakan fungsi php *microtime* dan didapatkan bahwa waktu yang dibutuhkan untuk melakukan dekripsi satu blok data kurang lebih 0.01 detik. Secara matematis, waktu yang diperlukan untuk melakukan *exhaustive search* dapat dihitung $2^{512}\ x\ 0.01$ yaitu $1.341\ x\ 10^{152}$ detik atau setara $4.252\ x\ 10^{144}$ tahun. Melihat angka yang begitu besar, maka dapat dikatakan sangatlah tidak mungkin untuk melakukan serangan *brute force* pada algoritma kriptografi yang dihasilkan penelitian ini.

3.2 Hasil Percobaan Mode Operasi *Block Cipher*

Percobaan mode operasi *block cipher* dalam penelitian ini mengacu pada rekomendasi NIST, yaitu *Electronic Code Book* (ECB), *Cipher Block Chaining* (CBC), *Cipher Feedback* (CFB), *Output Feedback* (OFB), dan *Counter* (CTR). Kelima mode operasi *block cipher* tersebut akan diimplementasikan dalam teknik kriptografi yang dihasilkan penelitian ini.

Percobaan dengan mode operasi tersebut akan dilakukan dengan menggunakan kunci, yaitu "INFORMATIKAUNTANPONTIANAKBELAJAR". Selain itu, juga akan digunakan rangkaian S1 dengan susunan "CB7815092EA4F63D" dan digunakan rangkaian S2 dengan susunan "7053AB8D24F9C61E". *Plaintext* yang akan digunakan dalam melakukan percobaan adalah "*Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum*".

3.2.1 *Electronic Code Book* (ECB)

Berikut hasil percobaan terhadap algoritma kriptografi yang diperoleh dengan menggunakan mode *Electronic Code Book* (ECB), dimana dalam percobaan tersebut tidak terdapat *initialization vector*, yang ditunjukkan dalam Tabel 4.

Tabel 4. Hasil Percobaan Mode ECB

Initialization Vector (hex)	Tidak ada
Ciphertext (hex)	1991fe5c0e2009dcbcc070917ce290042 01064f5cc63222bbec60a67145f6f5995 ec9225f6fb0918aa0c144c50c6643717e 465b2a81214d6b894e9f1192b32ffe12ff

	e2577ccf6dc37d314844be2647d79e865 b288b468b311893dd651cd33ffef39fae1 49d5a8003e4537d0a7b1c44914b42285 bbc48a3fb16ca57670d86f9fb891a5dd7 747a82d7e45edf207c6fd6c3c0b30630b 151f726389f6f7519f1742b81f9ff272d5 6f00ab7eb8840241067d81e84a72a5c41 01153edf6b2cfdab6a63b91dc6ad814a8 623e45d8cb24351837d5e8862dccca717 243260ac35dcf17ff232fdc6b6e04302d3 ed614087cc69d6caaa66a32ccb49343ad 2a02945d4617731942dc8e49d5785919 67cb9c5065c43778e865b2cca67ed693a df8b2142b6f46166c45ec72d5f60d1945 9bf2a7a6188114156472d4921472a289 02d2849b63aeb891dc34859bdaf9d2614 5f202411867cbe89f2d88ca472ba28962 f119e98f65192fd86160d5192d3e459b7 21dc647c978ec6ae8bbfb78724d01fc2e 8d2b8f651791923405fba83bef459b72a 7be236c21a665e8d4d2ddb3436cbdf18d 2b4e7a2baedcec7247d7f891c03cf702e1 06811435ece85f63bc72b1c6575160cdf de3

3.2.2 *Cipher Block Chaining* (CBC)

Berikut hasil percobaan terhadap algoritma kriptografi yang diperoleh dengan menggunakan mode *Cipher Block Chaining* (CBC), dimana dalam percobaan tersebut terdapat *initialization vector*, yang ditunjukkan dalam tabel 5.

Tabel 5. Hasil Percobaan Mode CBC

Initialization Vector (hex)	fd0b27267477a3e26549326ac28b2d928 30057f9505f73e2906cb0afad3df399
Ciphertext (hex)	db1c7c257162d4bf704557b80dc433a89 b106d2712b25c8f70be21bc8e01b7d4fb cc90daf3d72cbe33495628cf853cdf0c22 5759d3af0b4eaedcdfa789d6574b02e2a a51fb25cdeaca86c51f82c395b84fec457 7013044cba1bd1db7da26e98e6928099 dc5bbfd525bf7644358959d9c86eaea67 667ca89c2377dc8fa08ad9c9a3429186e 1b6674bbecced478c39b2b8bd9bed633c 1932c6ea0c67f9fa8a3800bd27bc15bb9f 165aeb204aa79b22e5f0cc0cf633b4f14c 85a94d57bbade190ad9daee6c79e315c4 9b17e57eddf6576a83d51f832d6f0e0b3 9a9693ae34c52ce47864fa8fe31ce815bc 9a1844b20c64d71ae1c5916235b154a3 8fcd6fa9966ea5753639e553d1eda0657 3cd9c9ae979b0b1552826143ad0f28487 23678cbebd6282603f48a00363981910e 0aa3161182a75277a6b784baed28f1c23 c1286fca122ef4218d4e7403e5085dac2 86ab86e7332e4ab094e58b6fee16ca5d5 edddf9e30f9a532244a10a6708f04c0f4c 2dbf52ade0b6ffc8b10854a90c9a240ce4 6a54be6ba8b4381b41ed681ff3cc7b2f4 db14691ab1cff46a8b36c4a7ac3cc0210c b3d6e5fdfaa2d11c619562a86630ef0a74 f54db9c2ee70f26439f7dc0da92f08d

3.2.3 *Cipher Feedback* (CFB)

Berikut hasil percobaan terhadap algoritma kriptografi yang diperoleh dengan menggunakan mode *Cipher Feedback* (CFB), dimana dalam percobaan tersebut terdapat *initialization vector*, yang ditunjukkan dalam tabel 6.

Tabel 6. Hasil Percobaan Mode CFB

Initialization Vector (hex)	fd0b27267477a3e26549326ac28b2d928 30057f9505f73e2906cb0afad3df399
Ciphertext (hex)	618484d3073948d34a99993e787e8f28 5ee507e3520a0896ad6531e88e1c9b882 58713a51a36584d2dbcae5d7da20bea77 5266147a3d140bb2a8f50f47475680d2b 7a9d7dbf1f05159170a15c924142b9362 744efcac5cce24c08f0928ff9afee32a5c5 e7cb8fb867cd6a2f9204d53050792e85f 2b3206bf48aac94c332fff57795cb0970c c2c31dce1ba1dfe0dde166df6f1850e2b0 ef2edf73be6a86f05590f5858eb412c181 6ef2f6a2adec51278ca15289cdd8e2453 00fa16116cda1b4add8d4811af209051d 241dad167bec80435162f8d30a51ee6bf a4044672631478890217477530 54e6a7 170bd2b6edf36ade28a7a8df6f1aab488b 6243d0330bad2bd845e48cfb8498b78c2 854c04fd87acdffaa2645c1329947c1b1c 73e2acdc32cb85807b33ca523f848c48a ca2ac2944ef4f89526c57b465e925b015 af250a5851d44747c4a2819b4c4af95de 1a2ff20d08bd839bc958fe211182e43dcf 23ff973214ba165ff46a9a8be9a14bb20a 9fb1ee54fbaf199d1c2f3b3bbb3aa940bc d35cd205300827089145a7a72e02b599 d3744c7258b59d2574a69011f041ad7e7 d557b1e485af2d00c5bbd906ec2f2642a ac1ba63bddbf33d252b63407560a6eb

3.2.4 *Output Feedback* (OFB)

Berikut hasil percobaan terhadap algoritma kriptografi yang diperoleh dengan menggunakan mode *Output Feedback* (OFB), dimana dalam percobaan tersebut terdapat *initialization vector*, yang ditunjukkan dalam tabel 7.

Tabel 7. Hasil Percobaan Mode OFB

Initialization Vector (hex)	fd0b27267477a3e26549326ac28b2d928 30057f9505f73e2906cb0afad3df399
Ciphertext (hex)	618484d3073948d34a99993e787e8f28 5ee507e3520a0896ad6531e88e1c9b88b 3eddbe12ec18da41f1b9b6dd72dc3f02c 4463e5c190948ef933876d28acbeb78f1 078fada6a00f805d23fd3a91f1968253e6 50410ea208be91c058fdd783e475d38d1 ebffb52b161ea56883d0497ea5ee0c145 d489d1983fc23ca2eaafd336b4d7350f1c f2b4da40e6682a9b6b28afa8e3039ce30 ab8fc2fce109f9f626ff06deedd3e0a7f47 782182e2f351f0cb0d30c1b1dfb2ccc1e8 1fff82fbf9e5ba23b13a72ef6014c6bf41e bb702ee01d270e2f1b6f806ca900c2ee2 ea1bfadeeeee813b7fef7a7cb6fc71e844c 313bd056f8364e7889a6b58397e24c72f d8f0290d64ee975bf974f96b00f7f39ba3

	47ae7ccba1b1c6d41002b8ef82ec34f76 bf1aea197f60f09e6f4c4e0fd6678ac79c 8afed85f386c58b05cc2f5d6c15a577d31 6b0d6f1eea0bec26e31a5c2d1adb0eb8b 24c1b2db47ff7d396e8367b188a7c3e96 a1db19e7d757e7391e343142923cf6bb2 b5a7e5bb5431dc2e0d445ac9491a348dc 1c83ea7e7a9358045a7eaddc194c9c264 e65b44b84078beee7d6ebb8cf77d7a1a2 86f04af49c800602b46ae2b6c60aee521 1a66e4785c2fced8351bc6cc508

3.2.5 *Counter* (CTR)

Berikut hasil percobaan terhadap algoritma kriptografi yang diperoleh dengan menggunakan mode C*ounter* (CTR), dimana dalam percobaan tersebut terdapat *initialization vector*, yang ditunjukkan dalam Tabel 8.

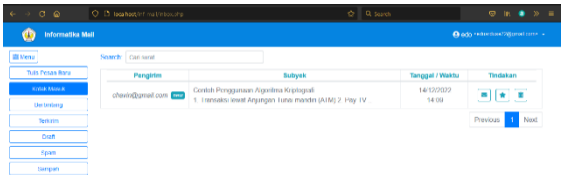
Tabel 8. Hasil Percobaan Mode CTR

Initialization Vector (hex)	fd0b27267477a3e26549326ac28b2d928 30057f9505f73e2906cb0afad3df399
Ciphertext (hex)	618484d3073948d34a99993e787e8f28 5ee507e3520a0896ad6531e88e1c9ba72 ecad7fa0b3f48ca1f82c92c697adf2542e a01ff1559048ee47070ad8955dfdc25cb 84fa013e5ed30594c939687edf2343a90 1ff1110058be97132f9da45cf5d2dc5c6f 01a2e0ddb1ed08d22617cdd2911e409f6 1c184183e16d2df89b1e9b3f3584c1f10 1260ddf0ed08424637ac26c47ec06f813 144dc2fc7135feda5ed46535d6d1fb482 e55db189380396c67c6235fa91dfd1e18 0c81e22430ec985fc9cd3284caf61b220 dcb1ed088216462da2541a90de9521c0 0c2ee6b31e09554d4d722cbcaec0d3a58 df1edec909787adc6c50fc1cf452101397 ff617ce9955cd41561cdcabf1a2e5dcc0f 988c236976dd2545a901ff520f0e8ef874 28ec8e559b2724c8cdeb482e5ecd0fd08 a24617fda2111ed07fd1d0b04c2e8717c eb8f57d28a3584caea04274c9e1a919b2 46c67da3e1fa92de9111c1196e8712ead 8959d5e061cbc7fc092e4edf1ed08a387 d7acb2d45e81cb11c160fc2fd7633e49e 55d5bd6d84d7ea063f0dd704d08a3861 63ce6c40fc01b11d1f078bee6d3dad9e5 5c88933d1caeb482642d206999d6d6c7 dc62111e00cb1170a15c2e1653ee28845 d6a4

3.3 Hasil Perancangan Aplikasi

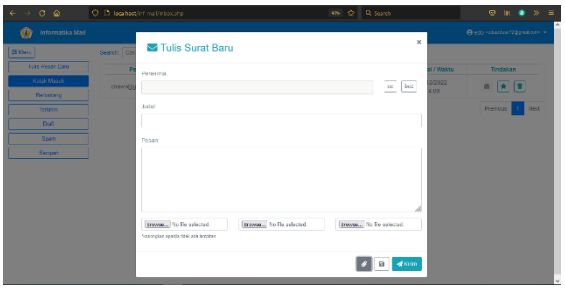
Aplikasi surat elektronik jurusan Informatika merupakan aplikasi yang dirancang dengan tujuan penggunanya dapat bertukar surat satu sama lain. Surat yang dikirim dapat berisi teks, gambar, video, dan dokumen dengan format yang telah ditentukan. Aplikasi surat elektronik ini juga memiliki tujuan khusus, yaitu sebagai media mengimplementasikan algoritma kriptografi yang telah dirancang.

Gambar 13 berikut merupakan halaman utama dari aplikasi surat elektronik yang dirancang.



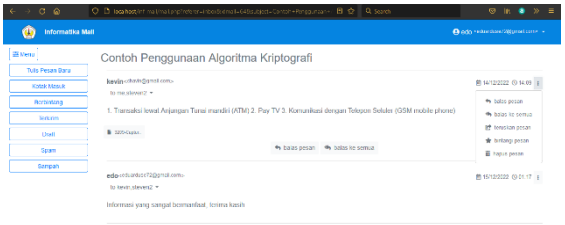
Gambar 13. Halaman Utama Aplikasi

Gambar 14 berikut merupakan form untuk membuat surat baru pada aplikasi surat elektronik yang dirancang.



Gambar 14. Form Pembuatan Surat Baru

Gambar 15 berikut merupakan tampilan surat yang terdapat pada aplikasi surat elektronik yang dirancang.



Gambar 15. Tampilan Surat

4. Kesimpulan

Berdasarkan paparan uraian mengenai penelitian yang telah dilakukan, maka dapat ditarik kesimpulan bahwa penelitian yang dilakukan menghasilkan algoritma kriptografi *block cipher* berbasis pola peta administrasi Kalimantan Barat menggunakan *key-dependent* s-box dengan nilai ketahanan yang cukup baik dan mampu bersaing dengan penelitian serupa yang sudah pernah dilakukan, serta mampu mengenkripsi berbagai jenis data komputer. Hal ini ditunjukkan dengan nilai *avalanche effect* yang dihasilkan memiliki rata-rata 50,524%, yang sangat dekat dengan nilai terbaik.

Adapun saran yang diberikan untuk pengembangan dalam penelitian selanjutnya, yaitu mengimplementasikan algoritma kriptografi dengan menggunakan *platform* lain, dimana perancangan algoritma kriptografi yang telah dilakukan pada penelitian ini menggunakan bahasa pemrograman php yang kemudian diimplementasikan ke dalam

sebuah aplikasi berbasis *web*. Selain itu, pola pengambilan kunci saat ini masih dilakukan secara manual dan berdasarkan perspektif penulis. Oleh sebab itu, untuk pengembangan dalam penelitian selanjutnya dapat dilakukan pola pengambilan kunci berdasarkan nomor letak peta (nlp) sesuai standar nasional.

Daftar Pustaka:

Alam, Y., & Pratama, H. N. R. (n.d.). HAD: Algoritma Block Cipher dengan Struktur Feistel dan Prinsip Confusion dan Diffusion dari Shannon. *Informatika.Stei.Itb.Ac.Id*. https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2019-2020/Makalah1/Makalah1-2020-04.pdf

Aminudin, A., & Hariyady, H. (2021). Analisa Kombinasi Algoritma AES Dengan Blum-Blum Shub Dan Chaotic Function. *Prosiding SENTRA (Seminar …*, 365–373. http://research-report.umm.ac.id/index.php/sentra/article/view/3927%0Ahttp://research-report.umm.ac.id/index.php/sentra/article/download/3927/3906

Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). *Jurnal Pendidikan Sains Dan Komputer*, *2*(01), 163–171. https://doi.org/10.47709/jpsk.v2i01.1390

Aziiz, A. K., & Pakereng, M. A. I. (2020). Perancangan Teknik Kriptografi Block Cipher Berbasis Pola Batik Ceplok Yogyakarta. *Jurnal Sistem Dan Teknologi Informasi (JUSTIN)*, *8*(1), 68. https://doi.org/10.26418/justin.v8i1.37135

Dakhi, O., Masril, M., Novalinda, R., Jufrinaldi, J., & Ambiyar, A. (2020). Analisis Sistem Kriptografi dalam Mengamankan Data Pesan Dengan Metode One Time Pad Cipher. *INVOTEK: Jurnal Inovasi Vokasional Dan Teknologi*, *20*(1), 27–36. https://doi.org/10.24036/invotek.v20i1.647

Fauzi, R. R., & Wellem, T. (2021). Perancangan Kriptografi Block Cipher berbasis Pola Dribbling Practice. *Aiti*, *18*(2), 158–172. https://doi.org/10.24246/aiti.v18i2.158-172

Gulo, N. (2021). RESOLUSI : Rekayasa Teknik Informatika dan Informasi Pengamanan Short Message Service (SMS) Menggunakan Algoritma Vibranium Cipher. *Media Online)*, *1*(5), 291–301. https://djournals.com/resolusi

Kumbara, P. B. T., & Pakereng, M. A. I. (2019). Perancangan Teknik Kriptografi Block Cipher Berbasis Pola Permainan Tradisional Rangku Alu. *Jurnal Teknik Informatika Dan Sistem Informasi*, *5*(2), 189–200. https://doi.org/10.28932/jutisi.v5i2.1714

Mulyadi, M. (2019). Aplikasi Kriptografi Pesan Teks Menggunakan Algoritma Advanced Encryption Standard 256 Bit (Aes-256) Dan Diffie Hellman. *Sisfo: Jurnal Ilmiah Sistem Informasi*, *3*(2), 23–38. https://doi.org/10.29103/sisfo.v3i2.6330

Murdowo, S. (2019). Mengenal Kriptografi Modern Sederhana Menggunakan Electronik Code Book (Ecb). *Infokam*, *2006*, 29–37. http://amikjtc.com/jurnal/index.php/jurnal/article/view/166

Ndruru, E., & Zebua, T. (2022). Pembangkitan Kunci Beaufort Cipher Dengan Teknik Blum-blum Shub pada Pengamanan Citra Digital. *Bulletin of Information Technology (BIT)*, *3*(2), 149–154. https://doi.org/10.47065/bit.v3i2.302

Prihanto, D. J. E., & Pakereng, M. I. (2020). Perancangan Teknik Kriptografi Block Cipher Berbasis Pola Tarian Sajojo Papua. *Ultima Computing : Jurnal Sistem Komputer*, *11*(2), 71–80. https://doi.org/10.31937/sk.v11i2.1454

Silalahi, L., & Sindar, A. (2020). Penerapan Kriptografi Keamanan Data Administrasi Kependudukan Desa Pagar Jati Menggunakan SHA-1. *Jurnal Nasional Komputasi Dan Teknologi Informasi (JNKTI)*, *3*(2), 182–186. https://doi.org/10.32672/jnkti.v3i2.2413

Umam, C., Handoko, L. B., Sari, C. A., Rachmawanto, E. H., & Hakim, L. A. R. (2022). Kombinasi Vigenere dan Autokey Cipher dalam Proses Proteksi SMS Berbasis Android. *Prosiding Sains Nasional Dan Teknologi*, *12*(1), 492. https://doi.org/10.36499/psnst.v12i1.7108

Yudha, G. S., & Laluma, R. H. (2019). Sistem Keamanan Jaringan Dalam Ujian Online Sma/Smk Menggunakan Metode Algoritma Advanced Encryption Standard (Aes). *Infotronik : Jurnal Teknologi Informasi Dan Elektronika*, *4*(2), 71. https://doi.org/10.32897/infotronik.2019.4.2.261

Yusfrizal. (2019). Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android. *JTIK (Jurnal Teknik Informatika Kaputama)*, *3*(2), 29–37. http://jurnal.kaputama.ac.id/index.php/JTIK/article/view/173

Ziliwu, K. B., Maslan, A., & Kremer, H. (2022). Implementasi Caesar Cipher pada Algoritma Kriptografi dalam Penyandian Pesan Whatsapp. *Jurnal Comasie*, *7*(2), 117–125.