Doramei Block Cipher

A New Block Cipher Algorithm

Diky Restu Maulana (13520017)[1], Gede Sumerta Yoga (13520021)[2], Mahesa Lizardy (13520116)[3]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail): 13520017@std.stei.itb.ac.id, 13520021@std.stei.itb.ac.id, 13520116@std.stei.itb.ac.id

***Abstract*—Doramei Cipher merupakan salah satu jenis algoritma block cipher yang dikembangkan dengan tujuan untuk memberikan keamanan dan kecepatan dalam pengiriman pesan elektronik. Algoritma ini memiliki ukuran block sebesar 128 bit dan panjang kunci sebesar 128 bit. Doramei cipher menerapkan cipher berulang dengan jumlah 16 putaran. Doramei juga menerapkan prinsip Confusion dan Diffusion sehingga ciphertext yang dihasilkan akan sulit ditebak. teknik substitusi yang digunakan menggunakan dua S-Box berupa S-Box yang dibangkitkan dari key yang degenerate pada awal putaran dan S-box rijndael.**

Keywords: kriptografi, cipher, block cipher, Doramei Cipher

I. Pendahuluan

A. *Latar Belakang*

Kriptografi ilmu dan seni untuk menjaga keamanan pesan (Schneier, 1996). Dalam era digital seperti saat ini, keamanan informasi dan data adalah suatu hal yang sangat penting karena banyaknya penggunaan teknologi secara online. Kriptografi saat ini digunakan di dalam berbagai hal, seperti transaksi keuangan secara online, pengiriman email, hingga keamanan dalam jaringan komputer. Yang terbaru, kriptografi menjadi pondasi atau dasar dari teknologi yang sedang naik daun saat ini, yaitu blockchain, dan digunakan dalam cryptocurrency.

Pada dasarnya, terdapat empat layanan yang harus dipenuhi dalam kriptografi, yaitu kerahasiaan pesan (*Confidentiality*), keaslian pesan (*Data integrity*), keaslian pengirim dan penerima pesan (*Authentication*), dan anti penyangkalan (*Non-repudiation*). Confidentiality dan Authentication diperlukan agar hanya orang yang berhak yang dapat membaca data tersebut. Integritas data diperlukan agar data tidak dapat diubah atau dimanipulasi tanpa sepengetahuan pihak yang berwenang

Dengan pentingnya keamanan data dalam era saat ini dan sudah mulai sadarnya masyarakat terkait keamanan data tersebut, kriptografi menjadi semakin penting perkembangannya. Ini menjadi tantangan untuk selalu mengembangkan kriptografi memperhatikan serangan cyber yang juga berkembang semakin kompleks.

B. *Masalah*

Kriptografi banyak berurusan dengan keamanan data-data yang penting atau sifatnya rahasia. Tidak heran, banyak upaya-upaya yang dilakukan untuk menyerang sistem kriptografi yang ada. Serangan tersebut ada dua jenis, yaitu serangan pasif dan serangan aktif. Serangan pasif bertujuan hanya untuk memperoleh data sedangkan serangan aktif juga melakukan intervensi dan mempengaruhi sistem untuk keuntungan sebagian pihak.

Teknik-teknik yang digunakan untuk melakukan serangan tersebut ada dua, yaitu *brute force attack* dan *analytical attack*. Jika menggunakan teknologi sebelumnya, mungkin waktu yang dibutuhkan untuk melakukan *brute force attack* terhadap suatu sistem kriptografi membutuhkan waktu sampai 10^{18} tahun. Namun, dengan berkembangnya teknologi saat ini, waktu yang dibutuhkan pun berkurang dengan drastis. Terutama dengan adanya *kuantum computing* yang dapat menguraikan algoritma kriptografi saat ini dengan sangat cepat. Ini membuat data yang dienkripsi oleh algoritma kriptografi menjadi tidak aman. Oleh karena itu, perlu diadakan upaya untuk mengembangkan teknik kriptografi yang lebih kuat.

C. *Related Works*

Beberapa rancangan block cipher sudah dibuat sebelumnya. Salah satu rancangan block cipher dan menjadi pedoman bagi block cipher lainnya adalah Advanced Encryption Standard (AES). AES menggunakan ukuran blok 128 bit dan memiliki tiga varian kunci yaitu 128 bit, 256 bit, dan 512 bit. Selain AES terdapat beberapa rancangan block cipher lain seperti DES, Blowfish Twofish, CRAB, RC2, RC5 dan block cipher lainnya. Dalam merancang block cipher terdapat beberapa konsep yang harus diperhatikan seperti Prinsip Confusion dan Diffusion dari Shannon, Substitusi dan permutasi, Cipher berulang (iterated cipher), Pembangkitan kunci putaran, Jaringan Feistel (Feistel Network), dan Ukuran blok dan kunci

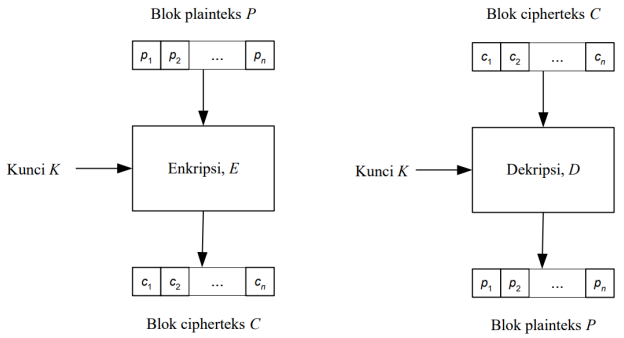
dalam penelitian ini, kami akan mengembangkan sebuah rancangan block cipher baru bernama Doramei cipher. block cipher yang dibuat akan menggunakan ukuran 128 bit. Doramei cipher juga menerapkan konsep mendesain sebuah block cipher seperti Prinsip Confusion dan Diffusion dari

Shannon, Substitusi dan permutasi, Cipher berulang (iterated cipher), dan Pembangkitan kunci putaran. Doramei Cipher juga menerapkan beberapa metode pada block cipher yang sudah ada dengan sedikit modifikasi sehingga menjadi lebih baik. perancangan ini dilakukan agar lebih memahami mengenai block cipher sebagai bahan pembelajaran serta dapat menjadi alternatif block cipher yang akan digunakan.

II. Teori Dasar

A. Block Cipher

Cipher blok adalah salah satu kategori cipher yang berbasis bit. Pada cipher blok, plainteks dibagi menjadi blok-blok bit dengan panjang yang sama. Beberapa ukuran yang umum, seperti 64 bit, 128 bit, 256 bit, dst. Setiap blok plainteks tersebut akan dilakukan enkripsi dengan suatu algoritma enkripsi E dan kunci k untuk membentuk blok-blok cipherteks. Selain itu, terdapat algoritma dekripsi D dengan menggunakan kunci k yang sama dengan proses enkripsi untuk mendapatkan kembali plainteks awal dengan menggunakan cipherteks hasil enkripsi sebelumnya.



Gambar 1. Diagram Umum Cipher Blok

B. Prinsip Confusion dan Diffusion

Pada tahun 1949, Claude shannon memperkenalkan prinsip confusion dan diffusion untuk membuat serangan terhadap sistem kriptografi berbasis statistik menjadi lebih sulit dilakukan. Ini karena sudah banyak cipher yang berhasil dipecahkan dengan memperhatikan data statistik antara cipherteks dan plainteks.

Prinsip confusion membuat hubungan statistik antara plainteks, cipherteks, dan kunci menjadi lebih tersembunyi. Ini membuat kriptanalis susah untuk mencari pola-pola statistik untuk memecahkan sistem kriptografi tersebut. Confusion ini biasanya dilakukan dengan teknik substitusi menggunakan S-Box.

Prinsip diffusion dilakukan dengan menyebarkan pengaruh bit pada plainteks atau kunci ke bit-bit lainnya untuk membentuk cipherteks. Ini membuat cipherteks menjadi semakin sulit untuk diprediksi. Diffusion sendiri dapat dilakukan dengan menggunakan teknik permutasi atau transposisi.

C. Substitusi dan Permutasi

Substitusi adalah menggantikan satu nilai dengan nilai lainnya. Proses substitusi dapat dilakukan dengan menggunakan sebuah tabel substitusi yang disebut dengan S-Box. S-Box merupakan tabel yang berisi nilai-nilai yang substitusi secara acak maupun menggunakan algoritma tertentu.

Permutasi adalah teknik untuk mengacak susunan bit di dalam sebuah blok bit sehingga akan menghasilkan blok dengan susunan yang baru. di dalam beberapa cipher block permutasi dilakukan dengan menggunakan tabel permutasi yang disebut dengan P-Box. P-Box menyatakan bit dari posisi sebelumnya

D. Cipher Berulang (Iterated Cipher)

cipher berulang merupakan proses melakukan proses mengubah blok plaintext menjadi ciphertext berulang-ulang kali sehingga dihasilkan cipher yang lebih kuat. setiap fungsi putaran nantinya akan dibangkitkan key yang merupakan *subkey* atau kunci putaran (*round key*)

E. Pembangkitan Kunci Putaran

setiap putaran di dalam iterated cipher akan dibangkitkan kunci putaran(*round key*) yang nantinya akan digunakan untuk proses enkripsi/dekripsi di iterasi tersebut. Kunci putaran dapat dibangkitkan dari kunci eksternal yang diberikan oleh user melalui proses yang dinamakan *key expansion* atau *key scheduling*. akan dilakukan komputasi yang kompleks sehingga menghasilkan sejumlah kunci putaran yang berbeda-beda

F. Jaringan Feistel

Jaringan Feistel bekerja dengan membagi pesan asli menjadi beberapa blok yang kemudian dioperasikan secara terpisah menggunakan fungsi enkripsi yang sama. Dalam jaringan Feistel, setiap blok data dibagi menjadi dua bagian yang sama besar. Bagian kiri digunakan sebagai masukan untuk operasi putaran, sementara bagian kanan digunakan sebagai masukan untuk fungsi enkripsi. Setelah diproses oleh fungsi enkripsi, bagian kanan di XOR dengan hasil operasi putaran pada bagian kiri. Selanjutnya, kedua bagian tersebut ditukar posisinya dan proses ini diulangi beberapa kali hingga mencapai jumlah putaran yang telah ditentukan.

G. Ukuran blok dan kunci

Ukuran blok dan kunci adalah dua parameter penting pada perancangan cipher blok. Ukuran blok pesan yang diproses selama enkripsi / dekripsi selalu tetap. semakin besar ukuran blok dapat memberikan efek *diffusion* yang lebih besar. Sedangkan semakin besar ukuran kunci mengarah ke efek confusion yang lebih besar dan lebih tahan terhadap serangan brute force. Namun, ukuran blok yang lebih besar dapat memperlambat kecepatan enkripsi / dekripsi

III. Rancangan Block Cipher DorameiCipher

A. Round Key Generation

Pembangkitan kunci pada tiap putaran memanfaatkan sebuah jaringan untuk *key scheduling*. Jaringan ini menyerupai

jaringan pada AES. Pembangkitan kunci dimulai dengan sebuah *external key* K sebagai kesepakatan antara pengirim dan penerima pesan. Kemudian, dilakukan *hash* dengan md5 untuk menghasilkan kunci dengan panjang 128 bit.

Beberapa konstanta dan fungsi yang terlibat dalam algoritma *key scheduling* yang juga dipakai dalam algoritma pembangkitan kunci ini adalah sebagai berikut.

$$\text{SubWord}(S) = \text{SubWord}(S_0S_1S_2S_3)$$
$$= S_{AES}(S_0)S_{AES}(S_1)S_{AES}(S_2)S_{AES}(S_3)$$

$$\text{RotWord}(S_0S_1S_2S_3) = S_1S_2S_3S_0$$

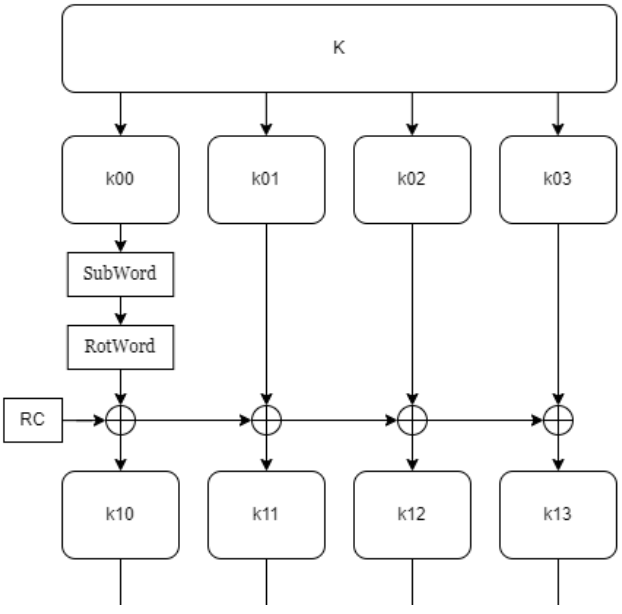
$$RC_1 = 1$$
$$RC_i = 2RC_{i-1}, \text{ jika } i > 1 \text{ dan } RC_{i-1} < 0x80$$
$$RC_i = 2RC_{i-1} \oplus 0x11B, \text{ jika } i > 1 \text{ dan } RC_{i-1} \geq 0x80$$

Kemudian, *external key* dipecah menjadi 4 bagian, yaitu k00, k01, k02, dan k03, yang masing-masing memiliki panjang 32 bit. Setiap pecahan ini disebut sebagai *subkey*.

Algoritma pembangkitan kunci untuk setiap *round* (K_i) adalah sebagai berikut.

$$k_{i,0} = \text{SubWord}(\text{RotWord}(k_{i-1,0})) \oplus RC_i$$
$$k_{i,1} = k_{i-1,1} \oplus k_0$$
$$k_{i,2} = k_{i-1,2} \oplus k_1$$
$$k_{i,3} = k_{i-1,3} \oplus k_2$$
$$K_i = k_{i,0}k_{i,1}k_{i,2}k_{i,3}$$

Berikut ini merupakan skema jaringan pembangkitan kunci:



Gambar 2. Skema Jaringan Pembangkitan Kunci

B. Konstruksi S-Box

Konstruksi S-Box adalah salah satu tahap awal dalam DorameiCipher. Terdapat dua S-Box yang digunakan, yaitu Rijndael S-Box dan S-Box yang dibuat berdasarkan key. S-Box kedua ini akan berukuran sama seperti Rijndael S-Box, yaitu 16 x 16. Jadi akan ada dua kali proses substitusi dalam satu putaran pada DorameiCipher.

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

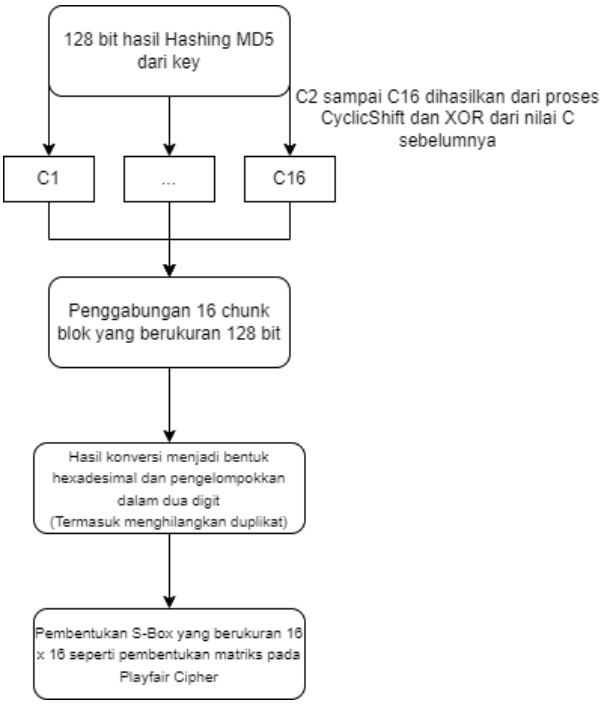
Gambar 3. Rijndael S-Box

Konstruksi S-Box berdasarkan key diawali dengan melakukan MD5 hash terhadap key sehingga dihasilkan blok sepanjang 128 bit hasil hashing. Setelah itu, akan dilakukan dua proses, yaitu CyclicShift dan XOR terhadap blok key yang dihasilkan sebelumnya.

- CyclicShift adalah proses pergeseran 4 bit ke kiri secara siklik. Jadi, misalkan kita memiliki blok sepanjang 16 bit berikut 1100011010111000. Setelah dilakukan CyclicShift, dihasilkan blok sebagai berikut 0110101110001100.
- Hasil dari CyclicShift terhadap blok tersebut akan dilakukan operasi XOR dengan blok tersebut sebelum dilakukan pergeseran

Hasil dari proses XOR tersebut akan disimpan dan digunakan untuk proses CyclicShift dan XOR selanjutnya. Runtutan proses ini dilakukan hingga diperoleh 16 blok sepanjang 128 bit termasuk blok awal hasil hashing.

Masing-masing blok tersebut selanjutnya digabungkan dan diubah ke dalam bentuk hexadesimal. Kemudian, kelompokkan dalam format dua digit dan hilangkan dua bentuk yang bernilai sama. Sekarang telah diperoleh beberapa nilai yang unik dalam hexadesimal. Karena kita perlu 256 nilai berbeda dan hasil dari proses sebelumnya pasti belum mencapai nilai tersebut, maka nilai - nilai dari 0x00 sampai 0xFF yang belum ada di dalam kumpulan nilai hexadesimal tersebut akan ditambahkan secara berurutan. Proses ini mirip seperti pembentukan matriks pada Playfair Cipher atau mungkin Extended Playfair Cipher yang berukuran sama. Setelah diperoleh 256 nilai dalam hexadesimal, nilai-nilai tersebut dimasukkan ke dalam matriks yang berukuran 16 x 16. S-Box ini dikonstruksi sekali saja di awal dan akan digunakan di setiap putaran pada proses enkripsi.



Gambar 4. Diagram pembentukan S-Box berdasarkan key

C. *P-Box*

P-Box yang digunakan memiliki ukuran 8. Artinya, setiap blok plaintext yang memiliki panjang 128 byte akan dibagi menjadi 16 blok 8 byte. Karena menggunakan jaringan feistel hanya bagian kanan dari blok tersebut yang akan diproses secara terpisah menggunakan P-Box. P-Box yang digunakan memiliki nilai tetap yang ditentukan sebelumnya, dan tidak berubah pada setiap tahap enkripsi atau dekripsi. Hal ini menjamin bahwa proses permutasi yang dilakukan selalu konsisten dan dapat diprediksi, sehingga memudahkan proses dekripsi. P-Box yang digunakan memiliki nilai sebagai berikut

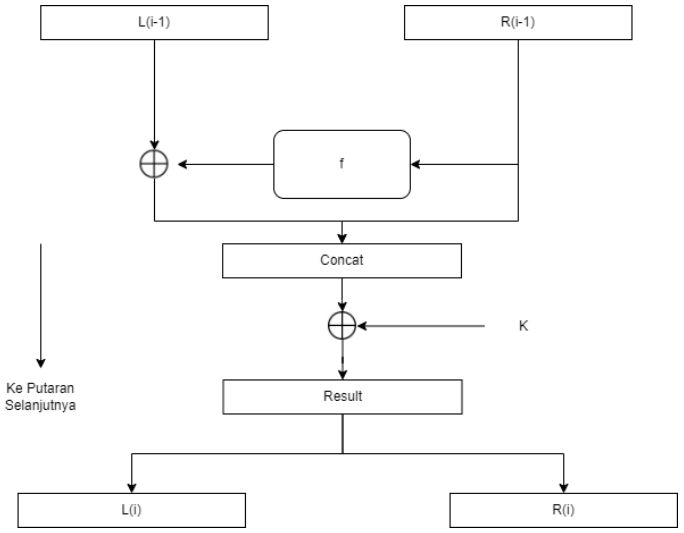
P-Box	6	3	0	4	2	7	5	1

Gambar 5. Tabel P-Box

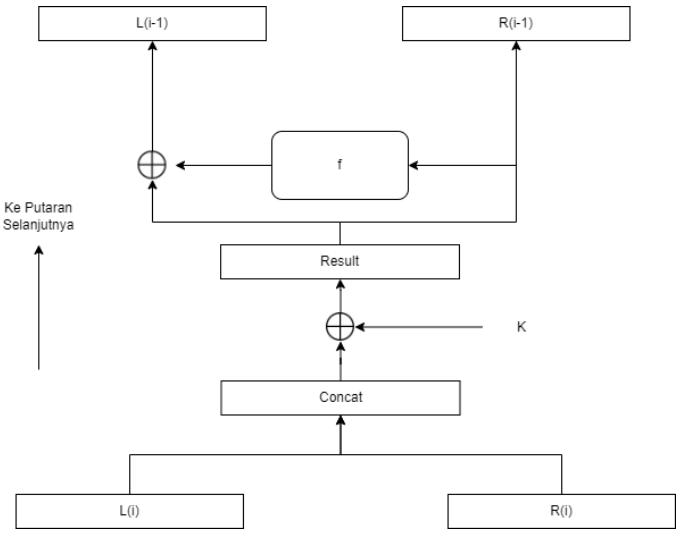
D. *Jaringan Feistel*

Dalam pengembangan algoritma Doramei Cipher, setiap blok pesan 128-bit akan dibagi menjadi dua bagian dengan masing-masing bagian berukuran 64-bit. Dalam proses enkripsi, bagian kanan pesan akan dioperasikan terlebih dahulu menggunakan sebuah fungsi putaran yang telah ditentukan.

Fungsi putaran ini akan memproses bagian kanan pesan dengan beberapa tahapan, seperti substitusi dan permutasi. Hasil dari tahapan-tahapan ini akan di XOR kan dengan bagian kanan pesan sebelumnya. Bagian kiri dan kanan pesan kemudian digabungkan dan di-XOR kan dengan kunci putaran. Kemudian hasil XOR tersebut dipisahkan menjadi bagian kanan dan kiri yang akan melakukan proses yang sama. Untuk proses dekripsi, langkah yang dilakukan hampir sama dan bisa dilihat langsung pada gambar 7 di bawah.



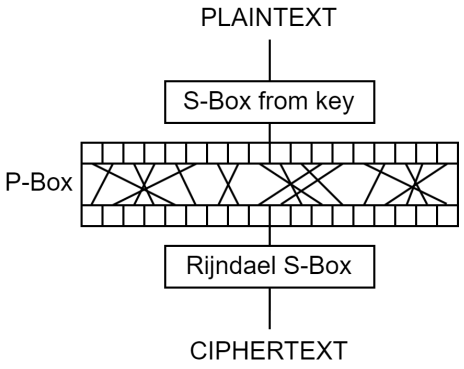
Gambar 6. Jaringan Feistel pada proses Enkripsi



Gambar 7. Jaringan Feistel pada Proses Dekripsi

E. *Round Function*

Dalam proses enkripsi Doramei Cipher, terdapat 16 putaran. Karena menggunakan jaringan Feistel, hanya byte bagian kanan yang dilakukan operasi. Bagian kanan yang dihasilkan dari jaringan Feistel akan disubstitusi dengan menggunakan S-Box. S-Box yang digunakan pada Doramei Cipher dibangkitkan berdasarkan kunci pada awal, sehingga setiap pesan yang dienkripsi akan menghasilkan S-Box yang berbeda-beda. Selanjutnya, dilakukan permutasi pada hasil substitusi S-Box untuk meningkatkan keamanan. Hasil permutasi tersebut akan disubstitusi lagi dengan menggunakan S-Box Rijndael. Fungsi putaran pada Doramei Cipher dapat dilihat pada gambar berikut ini.



Gambar 8. *Round Function* Doramei Cipher

IV. Eksperimen dan Pembahasan Hasil

A. Pengujian

Berikut akan dilakukan pengujian dengan menggunakan beberapa *plaintext* dan *key* yang berbeda

1. *Plaintext* berukuran *small* (30 kata)

Plaintext	
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Aenean commodo ligula eget dolor. Aenean massa. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Donec quam felis,	
Key	kriptografi
Ciphertext	
`úÑ¯âÜÀÖçÀ1=´lfÊ♦ëéÇ±KÔ#mWý>yÖü z;¬2ÊI¯¯ç↑÷°A¯ 1hgaÚ:r±cá5|¤l}ðQxìQÐ;M#¹Ù3:ââ◀Gèð¼û©Hù<j yîµßàc▬Ç_ îþ&g]LOdÖtªòÈ↨Q±&↑!ºÝÄÁ8ÊJÿß» Q¬ ß↔nHì<³fÇPÁ<N©G◀£WÏ♦Rw´Ö ¿²±↨!!E▼mNÃ↔&♠C_ævÕ↔;↨	
Waktu enkripsi	0.003025531768798828
Waktu dekripsi	0.0030040740966796875

2. *Plaintext* berukuran *medium* (100 kata)

Plaintext	
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Aenean commodo ligula eget dolor. Aenean massa. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Donec quam felis, ultricies nec, pellentesque eu, pretium quis, sem. Nulla consequat massa quis enim. Donec pede justo, fringilla vel, aliquet nec, vulputate eget, arcu. In enim justo, rhoncus ut, imperdiet a, venenatis vitae, justo. Nullam dictum felis eu pede mollis pretium. Integer tincidunt. Cras dapibus. Vivamus elementum semper nisi. Aenean vulputate eleifend tellus. Aenean leo ligula, porttitor eu, consequat vitae, eleifend ac, enim. Aliquam lorem ante, dapibus in, viverra quis, feugiat a,	
Key	kriptografi
Ciphertext	
`úÑ¯âÜÀÖçÀ1=´lfÊ♦ëéÇ±KÔ#mWý>yÖü z;¬2ÊI¯¯ç↑÷°A¯ 1hgaÚ:r±cá5|¤l}ðQxìQÐ;M#¹Ù3:ââ◀Gèð¼û©Hù<j yîµßàc▬Ç_ îþ&g]LOdÖtªòÈ↨Q±&↑!ºÝÄÁ8ÊJÿß» Q¬ ß↔nHì<³fÇPÁ<N©G◀£WÏ♦Rw´Ö ¿²±↨!!E▼▼4gyb¿R2→S>l→T↓P´NÖ2Ã S?>k¡ Ód↑,÷¸óï↑aR(îÁÚ¹0p Ä7◀ÀlY↨ÄZÁ»æÐ~Áh<YyJ¯☺o©Eµ2øF¢↓j¶ïxU@ÈÉ³Fì↨á÷b\áÐø Ðu)I↓ ÇÇÈµÞù³ø^►µÇÑ#õ→Q¹w/` ☻Ö▼ø(↔>¦zc)7¾ÃÄíÆý jÖêÀ~æ¬õÿz♠Ñ aý¥é6▬õp÷Û¢s¡b8Ê[Z▬h1◀ 1↨▲∟nþk-Y[ÿåñÂVí2á ¶ÉÔ ¸ÉQÓ£îÿ¿↑±~¡ª:ÅÍÚæ¶Á7/L>oÖW40FÑ|àl"íÏº$Ó2v©¸ØMô¸Ôaô?Èg Âº¶zÇ3§LýüÌUQþøNZ»ÓjmþÅHv<TÝ!g/B¹çrå²ÞNA·2☺:´?↔ºçz Õïüv9wãk Ô¼ø{ßLY↓¸Ä♦\hÉÊO¢ý ª}¨×y ³þQtTyfÀÄ ♦¨]%ö▬±▼n¯ TØ¥ÐLT8cì↓¤KJÂÄ♠ñø ñ\Ìê½W	
Waktu enkripsi	0.006004810333251953
Waktu dekripsi	0.0059893131256103516

3. *Plaintext* berukuran *large* (500 kata)

Plaintext
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Aenean commodo ligula eget dolor. Aenean massa. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Donec quam felis, ultricies nec, pellentesque eu, pretium quis, sem. Nulla consequat massa quis enim. Donec pede justo, fringilla vel, aliquet nec, vulputate eget, arcu. In enim justo, rhoncus ut, imperdiet a, venenatis vitae, justo. Nullam dictum felis eu pede mollis pretium. Integer tincidunt. Cras dapibus. Vivamus elementum semper nisi. Aenean vulputate eleifend tellus. Aenean leo ligula, porttitor eu, consequat vitae, eleifend ac, enim. Aliquam lorem ante, dapibus in, viverra quis, feugiat a, tellus. Phasellus viverra nulla ut metus varius laoreet. Quisque rutrum. Aenean imperdiet. Etiam ultricies nisi vel augue. Curabitur ullamcorper ultricies nisi. Nam eget dui. Etiam rhoncus. Maecenas tempus, tellus eget condimentum rhoncus, sem quam semper libero, sit amet adipiscing sem neque sed ipsum. Nam quam nunc, blandit vel, luctus pulvinar, hendrerit id, lorem. Maecenas nec odio et ante tincidunt tempus. Donec vitae sapien ut libero venenatis faucibus. Nullam quis ante. Etiam sit amet orci eget eros faucibus tincidunt. Duis leo. Sed fringilla mauris sit amet nibh. Donec sodales sagittis magna. Sed consequat, leo eget bibendum sodales, augue velit cursus nunc, quis gravida magna mi a libero. Fusce vulputate eleifend sapien. Vestibulum purus quam, scelerisque ut, mollis sed,

nonummy id, metus. Nullam accumsan lorem in dui. Cras ultricies mi eu turpis hendrerit fringilla. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; In ac dui quis mi consectetuer lacinia. Nam pretium turpis et arcu. Duis arcu tortor, suscipit eget, imperdiet nec, imperdiet iaculis, ipsum. Sed aliquam ultrices mauris. Integer ante arcu, accumsan a, consectetuer eget, posuere ut, mauris. Praesent adipiscing. Phasellus ullamcorper ipsum rutrum nunc. Nunc nonummy metus. Vestibulum volutpat pretium libero. Cras id dui. Aenean ut eros et nisl sagittis vestibulum. Nullam nulla eros, ultricies sit amet, nonummy id, imperdiet feugiat, pede. Sed lectus. Donec mollis hendrerit risus. Phasellus nec sem in justo pellentesque facilisis. Etiam imperdiet imperdiet orci. Nunc nec neque. Phasellus leo dolor, tempus non, auctor et, hendrerit quis, nisi. Curabitur ligula sapien, tincidunt non, euismod vitae, posuere imperdiet, leo. Maecenas malesuada. Praesent congue erat at massa. Sed cursus turpis vitae tortor. Donec posuere vulputate arcu. Phasellus accumsan cursus velit. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Sed aliquam, nisi quis porttitor congue, elit erat euismod orci, ac placerat dolor lectus quis orci. Phasellus consectetuer vestibulum elit. Aenean tellus metus, bibendum sed, posuere ac, mattis non, nunc. Vestibulum fringilla pede sit amet augue. In turpis. Pellentesque posuere. Praesent turpis. Aenean posuere, tortor sed cursus feugiat, nunc augue blandit nunc, eu sollicitudin urna dolor sagittis lacus. Donec elit libero, sodales nec, volutpat a, suscipit non, turpis. Nullam sagittis. Suspendisse pulvinar, augue ac venenatis condimentum, sem libero volutpat nibh, nec pellentesque velit pede quis nunc. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Fusce id purus. Ut varius tincidunt libero. Phasellus dolor. Maecenas vestibulum mollis

Key	kriptografi

Ciphertext

`úÑ¯âÜÀÖçÀ1=´lfÊ♦ëéÇ±KÔ#mWý>yÖü
z;¬2ÊI¯¯ç↑÷°A¯
1hgaÚ:r±cá5|¤l}ðQxìQÐ;M#'Ù3:ââ◀Gèð¼û©Hù<j
yîµßàc═Ç_
îþ&g]LOdÖtªòÈ↨Q±&↑!ºÝÄÁ8ÊJÿß» Q¬
ß↔nHì<³fÇPÁ<N©G◀£WÏ♦Rw´Ö
¿²±↨!!E▼▼4gyb¿R2→S>l→T↓P´NÖ2Ã
S?>k¡
Ód↑,÷¸óï↑aR(îÁÚ¹0p
Ä7◀ÀlY↨ÄZÁ»æÐ~Áh<YyJ¯☺o©Eµ2øF¢↓j¶ïxU@ÈÉ³Fì↨á÷b\áÐø
Ðu)I↓ ÇÇÈµÞù³ø^►µÇÑ#õ→Q¹w/` ☻Ö▼ø(↔>|zc)7¾ÄÃíÆý
jÔêÀ~æ¬õÿz♠Ñ aý¥é6═õp÷Û¢s¡b8Ê[Z═h1◀
1↨▲∟nþk-Y[ÿåñÂVí2á
¶ÊÔ
,ÉQÓ£îÿ¿↑±~¡ª:ÅÍÚæ¶Á7/L>oÖW40FÑ|àl"íÍº$Ó2v©¸ØMô,Ôaô?Èg
Â°¶zÇ3§LýüÍUQþøNZ»Ójmþ̊Hv<TÝ!g/B¹çrå²ÞNA·2☺:´?↔ºçz
Õïüv9wãk Ô¼ø{ßLY↓,Ä♦\hÉÊO¢ýª}¨×y
³þQtTyfÀÄ ♦¨]%ö═±▼n¯
TØ¥DLT8cì↓¤'á|ë:ÑþKJÕ3v0↑zª¯i³{z«pPäÝ═à▲Q∟àì#è],:iTü►~¢
ÿüÆ:ù
\«é0²!ø

↕:J~I4Õó,

§ÕðÂv(CB
☺A¸¢Ý8GôÀkdÂÇë8äË8ß3»7Øö
B(«X↨¶Ç½ð²ÙjËgH,¯¢.Ó,êlk³`±/
ºØÅl£7rXÚ
iÎ3Ýø87üSÄöjº`´ÛY{Þ[È-@oû;ºÔÐgW¶qeb?µ41↔#QÛ
fØZ)▼`ZõKhø ©PIJ»FRÌtòÝ

Ýeÿ%Áh÷
]Ã®y`♦QTbgí↓óòÌJÛtd ×↨QõØä÷àòýºWhXè§y xÑÇ♠`
ßfÐzã<BÞEÏ!j)iu:HÉ{Æ ñïÜÕ£▲Ç@69Á3â↑!í«
)v∟ñì▲tJ±û×═_↑zé¦;gH³#N:>jO~ôjõ!!►¶ÚJÉ►ßð4>V³♣☺ÌL$²¶}n
3q¶(º÷ö}(£íGFP3eeG:RÃÄ®ùFªjÍÍ»]═*ý¬RídFQ¢∟°¡D%ªEí'Øæ«>↨
3→☻!>÷]T♥=yÓûìqlvÛRTOv
]s3ºÏÃO¸
☺En¡²☺S↑4°|´¸ÿgË▲¬ôPØLM³lB}ÊG·ÉF8ºú«ÏÎ¦Qó\==±,ÎPDõ¶♣R[¨
ïÆ£f[Öí î↔♥ÉÖHèÓAyñ*↨ªª_$ûU³Ô%◀þâ¶¯ñç£YúX>
ÛÊ¿Ëc(◀$V▲Ú¸►↨JèWáÚµD¬×!ürIé@®s¡[↓è¡´J{¹ÌÉ^u♦☻«Ïæb☺
óÀ(4äªu.<E~¨ý^-W\¼ØâIReÆnKh═→÷S¼WÁí´»\═Ú↨ÍÈ(zWÔ→
d¦*¾c
QÙ♦(µÊ¨%▲v5ý<æc♥:/âJ}§)jÊ$►±õêÀþ#Ç9m"P◀À`UQÔ<Å►¶b
ñ~gø{Sä½═
KÎ²S¯æÆºfr\´ãØ1¥═Ü1_c¬]]&!VÑÓ
p/|é(þøº>+¤YÀýWUx«ZõØ¥
+ûqO}÷[☺M» 7@¤W¸éDÇzÌ►°V¼î£yåM↑$'¯9ý~~ôâõËë↑Ñ¶» Æ
RÖh.9♦ÃÔ▲Ï!"PBiÝ♠∟ä3ã/Ð]ÿ\q∟_ût+²═0jWvíîæè→¬«Ù3^º
Þ\S-FMéèüÁglA8uÄç8'WáË¤ÛÉJZ+åûµìäcaUS
×î\☻~oÂ½ã§@·ó,8►õ),'#ïdÁEyÚ.♣4jh\═õÅ▲¿3+Sïl¦¶¶yxÀ¶D9âË
hTö*z®â°Èù6_ü↨HÅN!aWdõöAJ!®_▼_î¤¼F²8═§ÔÆ¤G*[·¥¯5=À
♦¸QÃÁ¢×$!Ù§ gÕ3ÄtZÎíÏ►:¯ÛD¾∟¨═¥©
{M\«æjÞî◀P
#mU:i\═²øÊüá!!Ai'2òAeT,♠↑ä♣!!_i|Ræ÷Õ═b%L↔ëLñxà2(þÿ3↔↑Ñ
VéÒ^M:¶Ñ£©ñ{Xó` ²§ßò7"&tyïOS0÷ÁñQ8ð0½iXÆ
ññp!Wg9HÊY¥µ-}¾30µ↓ÍXZÌÚ2\]Ý¼x◀äöáá©ÄzR[mÚ¸¸mî♠H3]ý
ÞGË=MµÎ↑±ñû↨Ö═y¹¼¸¥¾AL¯r↔¹Ù¯¶¡A♣;By¦'"►↑-êJaãÐSø½ªß£
m³NrÙ
Å\IÄAyL¸pJ7(øV3dÃ¶#t;u:Ú<>↔ãµ▲éØÚ↑¿RòÈéB►·è©8¾4êâê♠
Q¾Ð
9èºããÍYíl¶ô
¤å+ã`ÀT¢%¤9Ã!¤rÛ?»Ì,qU¶Ïg0Ô#♥NÝ
R¥+☺ò×|Ý·3cí3b ¯¿Ô¿¶gi-6ÃÀ~Gº═
i"¥3¨.>¶YDìe&ùÂÅ~f81ãÒ©Ç♥^cí↓=ÌûÜ×"o_á0.öË ¿î×ý½>0¿8
[áUsô36%v×Ì»ø²À'Y¸á¾2ñxùÙÍk0t¸
é=*ÄáØg§♥v♣²►ëÓG´ÅGÒbn¤Ðïë/W:
MgV 7æ
ôÚhlQ_ÃÿÊ¾J´äÖ'Ç!ý¤/¿±¶])º+Ì6ù4|¡♦â
ÝsÂ«▲ÝãÄ%p×àþí·î+ÛÇJt?ãLèþ3×èÁQJÑ)ò@-\À|h®↔ÊþFÖÿÃY
døª|f◀°kÓû)¶Ê2ow*pñfk
vc{@Ð|LÍóÇa^4ã*ÔÔè.∟±»<∟è¡Ö═DcÓ=.ÞÁÎ8½ÛRù°ãßú,²ç¡gnf
kùó═ ªQnÔn¤
®tQwÃ▼Ô[qtæÅ8?§#1¡@¼☻Z0Õ♣úËt&'lË±XA♦=uâ?Ò&ÀÕ<
¡DÇ☻àÞ

Í═?MxºÏ¯↓D4u

Waktu enkripsi	0.022041797637939453
Waktu dekripsi	0.02052450180053711

4. *Plaintext* berukuran very *large* (800 kata)

Plaintext
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Aenean commodo ligula eget dolor. Aenean massa. Cum sociis natoque penatibus et magnis dis parturient montes,

nascetur ridiculus mus. Donec quam felis, ultricies nec, pellentesque eu, pretium quis, sem. Nulla consequat massa quis enim. Donec pede justo, fringilla vel, aliquet nec, vulputate eget, arcu. In enim justo, rhoncus ut, imperdiet a, venenatis vitae, justo. Nullam dictum felis eu pede mollis pretium. Integer tincidunt. Cras dapibus. Vivamus elementum semper nisi. Aenean vulputate eleifend tellus. Aenean leo ligula, porttitor eu, consequat vitae, eleifend ac, enim. Aliquam lorem ante, dapibus in, viverra quis, feugiat a, tellus. Phasellus viverra nulla ut metus varius laoreet. Quisque rutrum. Aenean imperdiet. Etiam ultricies nisi vel augue. Curabitur ullamcorper ultricies nisi. Nam eget dui. Etiam rhoncus. Maecenas tempus, tellus eget condimentum rhoncus, sem quam semper libero, sit amet adipiscing sem neque sed ipsum. Nam quam nunc, blandit vel, luctus pulvinar, hendrerit id, lorem. Maecenas nec odio et ante tincidunt tempus. Donec vitae sapien ut libero venenatis faucibus. Nullam quis ante. Etiam sit amet orci eget eros faucibus tincidunt. Duis leo. Sed fringilla mauris sit amet nibh. Donec sodales sagittis magna. Sed consequat, leo eget bibendum sodales, augue velit cursus nunc, quis gravida magna mi a libero. Fusce vulputate eleifend sapien. Vestibulum purus quam, scelerisque ut, mollis sed, nonummy id, metus. Nullam accumsan lorem in dui. Cras ultricies mi eu turpis hendrerit fringilla. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; In ac dui quis mi consectetuer lacinia. Nam pretium turpis et arcu. Duis arcu tortor, suscipit eget, imperdiet nec, imperdiet iaculis, ipsum. Sed aliquam ultrices mauris. Integer ante arcu, accumsan a, consectetuer eget, posuere ut, mauris. Praesent adipiscing. Phasellus ullamcorper ipsum rutrum nunc. Nunc nonummy metus. Vestibulum volutpat pretium libero. Cras id dui. Aenean ut eros et nisl sagittis vestibulum. Nullam nulla eros, ultricies sit amet, nonummy id, imperdiet feugiat, pede. Sed lectus. Donec mollis hendrerit risus. Phasellus nec sem in justo pellentesque facilisis. Etiam imperdiet imperdiet orci. Nunc nec neque. Phasellus leo dolor, tempus non, auctor et, hendrerit quis, nisi. Curabitur ligula sapien, tincidunt non, euismod vitae, posuere imperdiet, leo. Maecenas malesuada. Praesent congue erat at massa. Sed cursus turpis vitae tortor. Donec posuere vulputate arcu. Phasellus accumsan cursus velit. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Sed aliquam, nisi quis porttitor congue, elit erat euismod orci, ac placerat dolor lectus quis orci. Phasellus consectetuer vestibulum elit. Aenean tellus metus, bibendum sed, posuere ac, mattis non, nunc. Vestibulum fringilla pede sit amet augue. In turpis. Pellentesque posuere. Praesent turpis. Aenean posuere, tortor sed cursus feugiat, nunc augue blandit nunc, eu sollicitudin urna dolor sagittis lacus. Donec elit libero, sodales nec, volutpat a, suscipit non, turpis. Nullam sagittis. Suspendisse pulvinar, augue ac venenatis condimentum, sem libero volutpat nibh, nec pellentesque velit pede quis nunc. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Fusce id purus. Ut varius tincidunt libero. Phasellus dolor. Maecenas vestibulum mollis diam. Pellentesque ut neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. In dui magna, posuere eget, vestibulum et, tempor auctor, justo. In ac felis quis tortor malesuada pretium. Pellentesque auctor neque nec urna. Proin sapien ipsum, porta a, auctor quis, euismod ut, mi. Aenean viverra rhoncus pede. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Ut non enim eleifend felis pretium feugiat. Vivamus quis mi. Phasellus a est. Phasellus magna. In hac habitasse platea dictumst. Curabitur at lacus ac velit ornare lobortis. Curabitur a felis in nunc fringilla tristique. Morbi mattis ullamcorper velit. Phasellus gravida semper nisi. Nullam vel sem. Pellentesque libero tortor, tincidunt et, tincidunt eget, semper nec, quam. Sed hendrerit. Morbi ac felis. Nunc egestas, augue at pellentesque laoreet, felis eros vehicula leo, at malesuada velit leo quis pede. Donec interdum, metus et hendrerit aliquet, dolor diam sagittis ligula, eget egestas libero turpis vel mi. Nunc nulla. Fusce risus nisl, viverra et, tempor et, pretium in, sapien. Donec venenatis vulputate lorem. Morbi nec metus. Phasellus blandit leo ut odio. Maecenas ullamcorper, dui et placerat feugiat, eros pede varius nisi, condimentum viverra felis nunc et lorem. Sed magna purus, fermentum eu, tincidunt eu, varius ut, felis. In auctor lobortis lacus. Quisque libero metus, condimentum nec, tempor a, commodo mollis, magna. Vestibulum ullamcorper mauris at ligula. Fusce fermentum. Nullam cursus lacinia erat. Praesent blandit laoreet nibh. Fusce convallis metus id felis luctus adipiscing. Pellentesque egestas, neque sit amet convallis pulvinar, justo nulla eleifend augue, ac auctor orci leo non est. Quisque id mi. Ut tincidunt tincidunt erat. Etiam feugiat lorem non metus. Vestibulum dapibus nunc ac augue. Curabitur vestibulum aliquam leo. Praesent egestas neque eu enim. In hac habitasse platea dictumst. Fusce a quam. Etiam ut purus mattis mauris

Key	kriptografi

Ciphertext

`úÑ¯âÜÀÖçÀ1=´lfÊ♦ëéÇ±KÔ#mWý>yÖü
z;¬2ÊI¯¯ç↑÷°A¯
1hgaÚ:r±cá5|¤l}ðQxìQÐ;M#¹Ù3:ââ◀Gèð¼û©Hù<j
yîµßàc▬Ç_
îþ&g]LOdÖtªòÈ↨Q±&↑!ºÝÄÁ8ÊJÿß» Q¬
ß↔nHì<³fÇPÁ<N©G◀£WÏ♦Rw´Ö
¿²±↨!!E▼▼4gyb¿R2→S>l→T↓P´NÖ2Ã
S?>k¡
Ód↑,÷ óï↑aR(îÁÚ¹0p
Ä7◀ÅlY↨ÄZÁ»æÐ~Áh<YyJ¯☺o©Eµ2øF¢↓j¶ïxU@ÈÉ³Fì↨á÷b\áÐø
Ðu)I↓ ÇÇÈµÞù³ø^►µÇÑ#õ→Q¹w/` ☻Ö▼ø(↔>¦zc)7¾ÃÄíÆý
jÖêÅ~æ¬õÿz♠Ñ aý¥é6▬õp÷Û¢s¡b8Ê[Z▬h1◀
1↨▲∟nþk-Y[ÿåñÂVí2á
¶ÈÔ
,ÉQÓ£îÿ¿↑±~¡ª:ÅÍÚæ¶Á7/L>oÖW40FÑ|àl"íÏº$Ó2v©¸ØMô,Ôaô?Èg
Âº¶zÇ3§LýüÌUQþøNZ»Ójmþ̷ÅHv<TÝ!g/B¹çrå²ÞNA·2☺:´?↔ºçz
Õïüv9wãk Ô¼ø{ßLY↓,Ä♦\hÉÊOȼý ª}¨×y
³þQtTyFÀÄ ♦¨]%ö▬±▼n¯
TØ¥DLT8cì↓¤'á|ë:ÑþKJÕ3v0↑z ª¯i³{z«pPäÝ▬à▲Q∟ài#è],:iTü►~¢
ÿüÆ:ù
\«é0²!ø
↕:J~I4Õó,

§ÕðÂv(CB
☺A,¢Ý8GôÀkdÂÇë8äË8ß3»7Øö

B(«X↕¶Ç½ð²ÙjËgH,¯¢.Ó,êlk³`±/
ºØÅl£7rXÚ
iÎ3Ýø87üSÄöjº` ˆÛY{Þ[È-@oû;ºÔÐgW¶qeb?µ41↔#QÛ
fØZ)▼`ZõKhø ©PIJ»FRÌtòÝ

Ýeÿ%Áh÷
]Ã®y`♦QTbgí↓óòÌJÛtd ×↕QõØä÷àòýºWhXè§y xÑÇ♠`
ßfÐzã<BÞEÏ!j)iu:HÉ{Æ ñiÜÕ£▲Ç@69Á3â↑!í«
)v∟ñi▲tJ±û×▬_↑zé¦;gH³#N:>jO~ôjõ‼►¶ÚJÉ►ßð4>V³♣☺ÌL$²¶}n
3q¶(º÷ö}(£íGFP3eeG:RÃÄ®ùFªjÍ»]▬*ý¬RídFQ¢∟°¡D%ªEí'Øæ«<>↕
3→☻!>÷]T♥=yÓûìqlvÛRTOv
]s3ºÏÄO¸
☺En¡²☺S↑4°|´,ÿgË▲¬ôPØLM³lB}ÊG·ÉF8ºú«ÏÎ|Qó\==±,ÎPDõ¶♣R[¨
ïÆ£f[ÕíˆÎ↔♥ÉÒHèÓAyñ*↕ªIª_$ûU³Ô%◄þâ¶¯ñç£YúX>
ÛÊ¿Ëc(◄$V▲Ú¸►↕JèWáÚµD¬×!ürIé@®s¡[↓è¡´J{'ìÉ^u♦☻«Ïæb☺
óÀ(4äªu.<E~¨ý^-W\¼ØâIReÆnKh▬→÷S¼WÁí´»\▬Ú↕ÍÈ(zWÕ→
d¦*¾c
QÙ♦(µÊ¨%▲v5ý<æc♥:/âJ}§)jÊ$►±ôèÀþ#Ç9m"P◄À`UQÔ<Å►¶b
ñ~gø{Sä½▬
KÎ²S¯æÆºfr\´ãØ1¥▬Ü1_c¬]]&!VÑÓ
p/|é(þøº>+¤YÀýWUx«ZõØ¥
+ûqO}÷[☺M» 7@¤W¸éDÇzÌ►°V¼î£yâM↑$¹¯9ý~~ô♣õËë↑Ñ¶» Æ
RÖh.9♦ÃÔ▲Ï!"PBíÝ♠∟ã3ã/Ð]ÿ\q∟_ût+²▬0jWvíîæè→¬«Ù3^º
Þ\S-FMéèüÁglA8uÄç8'WáË¤ÛÈJZ+åûµiãcaUS
×î\☻~oÂ½ä§@·ó¸8►õ),'#ïdÁEyÚ.♠4jh\▬õÅ▲¿3+SïÌ¦¶¶yxÀ¶D9âË
hTö*z®â°Èù6_ü↕HÅN!aWdõöAJ!®_▼_î¤¼F²8▬§ÔÆ¤G*[·¥¯5=À
♦¸QÃÁ¢×$!Ù§ gÕ3ÄtZÎìÏ►:¯ÛD¾∟¨▬¥©
{M\«æjÞî◄P
#mU:i\▬²øÊüá!!Ai'2òAeT♠↑ä♣!!_i|Ræ÷Õ▬b%L↔ëLñxà2(þÿ3↔↑Ñ
VéÒ^M:¶Ñ£©ñ{Xó` ²§ßò7"&tyïOS0÷ÁñQ8ð0½ìXÆ
ññp!Wg9HÊY¥µ-}¾30µ↓ÍXZÌÚ2\]Ý¼x◄äöáá©ÄzR[mÚ,,mî♠H3]ý
ÞGË=MµÎ↑±ñû↕Ö▬y¹¼,¥¾AL¯r↔¹Ù¯¶¡A♣;By¦`"►↑-êJaãÐSø½ªß£
m³NrÙ
Å\IÄAyL,pJ7(øV3dÃ¶#t;u:Ú<>↔ãµ▲éØÚ↑¿RòÈéB►·è©8¾4êãê♠
Q¾Ð
9èºããÍYíl¶ô
¤å+å`ÀT¢%¤9Ã!¤rÛ?»Ì,qU¶Ïg0Ô#♥NÝ
R¥+☺ò×|Ý·3cí3b ¯¿Ô¿|¶gi-6ÅÀ~Gº▬
ì"¥3¨.>¶YDìe&ùÅÅ~f81ãÒ©Ç♥^cí↓=ÌûÜ×"o_á0.öË ¿î×ý½>0¿8
[áUsô36%v×Ì»ø²À'Y¸á¾2ñxùÙÍk0t¸
é=*ÄáØg§♥v♣²►ëÓG´ÄGÒbn¤Ðïë/W:
MgV 7æ
ôÚhlQ_ÃÿÊ¾4J´äÖ'Ç!ý¤/¿±¶])º+Ì6ù4|¡♦â
ÝsÅ«▲ÝãÄ%p×àþí·î+ÛÇJt?ãLèþ3«èÁQJÑ)ò@-\À¦h®↔ÊþFÖÿÃY
døª|f◄°kÓû)¶Ê2ow*pñfk
vc{@Ð¦LÎóÇa^4ã*ÔÔè.∟±»<∟è¡Ö▬DcÓ=.ÞÁÎ8½ÛRù°ãßú,²ç¡gnf
kùó▬ ªQnÔn¤
®tQwÃ▼Ô[qtæÅ8?§#1¡@¼☻Z0Õ♣úËt&'lË±XA♦=uâ?Ò&ÀÕ<
¡DÇ☻àÞk:CS«Ì?âUáJ▬|w]♥2▲◄‼5±*i¥\hÑüi{fCXf◄§'''½ÛÊ}lãN
ërðí§¹ù>R☻l;Ï|î/Áz\♣m1◄yÚ!!gÒÆÔM!ÊäÉG{½♦>ú\¦±í→§5àJW8è
b³¼1
Q↕ÙßMîú §1P§8o¹;BQ►U?Ë☻à¤é¾☺;;ÍW>Ä

ÀW!ª
ðÞ`☺X↓Ý£ó'µ(âÆèZdýFÌGKB(§ùßà@Â→6^îRÎrzLREµ↑G83ù±'ÿx¬
ç¶üa.QÀ|«&s@À½ëgÎ§£³¬ë
%¶À}¿§Pp
AKÔp(Ð↔Q¤¼\☺ÙMFhüÍ
oó|#&H¬♣&Y7QàWõê
♦d½çëBe6kç♦Å³÷bn´äÕ▬ä2R#`N}åí♠ò▼Äi«↓ù«`fÛ¥åiK♦ÊXÌx/kä
Ö®↓bõÏk¤♠\X♠Á*#m☻Ø½é→½O▼¨Õ±ó°ÊJd'×>ríîø↕SóÃOÒ%[©,»í
¤3▬☺i6¯`↕Ñ→9Ë`G16,%!!Ð×IRO»>ÕÉ∟~g♦ªÔxÓÒ☻ð(
©!Úèg5/.▲xN7æÿßbfÞ¤o|1☻ÝÜe@↕:àÎ¨è8»rP5Ot+Ä¼ÖZd[iÕyz8h
Qæ
þAHQ¼ôP1ù▼↓☺¦ò·↓¦ñþ▼(À¶å☺♦¡‼▼¼Ü|ÈM³1\¬/¯"³ÕýcZö23¸Ü
%.ÿÜiE▬Á♠ìREOj©ºcG↕LÅaác↕ÕTGzNÃ◄
_õô-{vù§ÐÁ#0↑WqüñD►◄#UÍî{C↕ó>eß kÝ Àï²2=
°↑SSw◄ýGÀìîø
«▲4N→s◄õîL)2/oÑÖÎÙ0·÷♥\«ÑFF¶Q<ÉiÉ@ëXÚÍÑ2ûGÁàËÏ]û▼I
D·U[♥.☻▼9¸×.à*♣È²!¼H2ÖÈªÔeåæì◄fî}¡ÐÞÆÞ×¼¡çê¤b8%äÜqïÚ
h\õ}æðÉ1,'t¾c¥2]µRø↓&%÷→ÃÚ>?EÎ¦mèegQ>eq§3¢

;âõ}Ü¶Q1hg+ô¶ðù¿xc¦iÐÒ¶Á¶*e2ÞkÖ♦àoÝwj ,¼½ß
)!÷k0¡Ù¨óËèKÊý(±²BÁÉ5ídÜd*AÁgz£KNvJÞ%av_¢±î»ÆÒ)ð→.OL
^Ý]ðfnûü< M4¿¿ûÒñW`Ä‼¯Jb{zÝËJófù▲b=Ì
yiJ!!'wPjzdwxZLé¶
[sÕÝLeûá¾¨áÂ▲↑que·
³®6ùÝmu
◄îßàecÌj→þî►6¿·ªÜ~v{t?,▬¶èÚr1þqÃ¦|>Â-d▲RäHcY¥ÚTU♦BG¬
2F♥PWnu
O¤G#p↕äzM£Ä¸©ÀS!¨$♠↓Áé♦1K½à~gÎ,]R§Gf©Å/0!Mù«▼¢
N¤æÒ<Ä÷0þßþôàëú▲0vaCt↓ä=ßhà!djí☺∟¤8~k'!CA÷)M]fV¡▬▼
∟éÎÃV¯D% yOi¢PcL▼éS¥ðÃ©j°gcâ»B^Ê
JH=Gj↕¡$b%ãÒÀ↔Í1gO&>Z2)Ëò°°∟K{t7%òqÚ0qÍuÓÚS©àóÅ«Zs
ïJ7!!▼Ë4AY▼OGÄà)`Æùóþ†dn©¤À²O]È¯àr\þYc¶¶÷Unæ¶<Yókuä
%5Åºn?b§/a}4fq!!`XÖ¨N¡z
îL
u§7OÊ~ähmüuHò]↓Ü+q{æ

«ÿ£GòÝc2}µkòM5►¬XÍw6◄|öj<m}Û`↕òòÙ6øYpn¿ó#xÕnOTJ©¾
Öí▼Cvò-óë,F[;Ö®♠Ð½Q.(8☺;GÂ'¶ò§Ó↑IK×¢▼¸!!=êP§¯µj,ø☺¹I&f
$ªc
↑Â↓µq6e4?@ÿª+¼¿ù0àÚUû.ñïÝdidp]+¹RKy37²þZý¤&":◄↕9S

Waktu enkripsi	0.03350329399108887
Waktu dekripsi	0.03099203109741211

Dari hasil pengujian menggunakan empat ukuran pesan, diperoleh waktu enkripsi dan dekripsi tergolong sangat cepat. Untuk ukuran pesan *very large* yang terdiri dari 800 kata dapat dilakukan dekripsi dan enkripsi kurang dari 0.05 ms. Selain itu, hal lain yang dapat disimpulkan adalah waktu enkripsi dan dekripsi berbanding lurus dengan panjang pesan. Hal tersebut masuk akal mengingat semakin panjang pesan maka semakin panjang blok *plaintext* yang akan diproses.

B. Analisis Efek Longsoran (Avalanche Effect)

Pengujian akan dilakukan dengan menggunakan plaintext “lorem ipsumdolor” kata dan key yaitu “kriptografi”

Perbedaan Plaintext	Persentase Perbedaan
lorem iqsumdolor	50%
loren iqsumdolor	50%
!orem ipsumdolor	50%
lorem ipsimdolor	50%
Rata-rata	50%

Perbedaan Key	Persentase Perbedaan
kriptograpi	99.90%
kriktografi	99.34%
kriptograf!	99.94%
criptografi	99.29%

Rata-rata	99.62%

Berdasarkan data tabel di atas, perubahan 1 byte pada *key* dan pada *plaintext* akan mempengaruhi *ciphertext* yang dihasilkan. Berdasarkan tabel tersebut persentase perubahan 1 byte yang dilakukan pada plain text memiliki persentase perbedaan rata-rata 50% sedangkan pada key memiliki persentase perbedaan rata-rata 99.62%

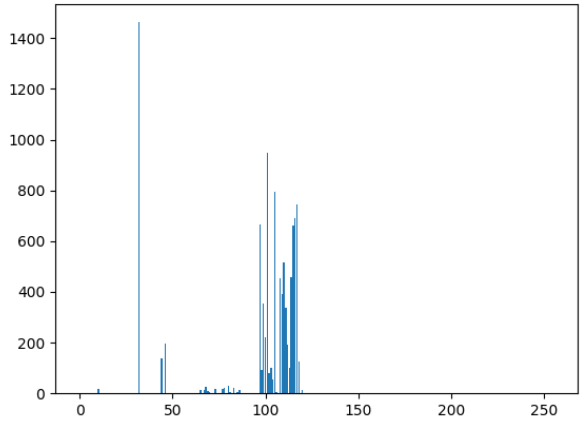
C. Analisis Ruang Kunci (Key Space)

Doramei Cipher memiliki kunci dengan ukuran 128 bit. Oleh karena itu, untuk melakukan serangan brute force dibutuhkan pengecekan sekitar $2^{128} = 3,4 \times 10^{38}$. Atas dasar tersebut, dapat disimpulkan bahwa Doramei cipher aman dari serangan *brute force*.

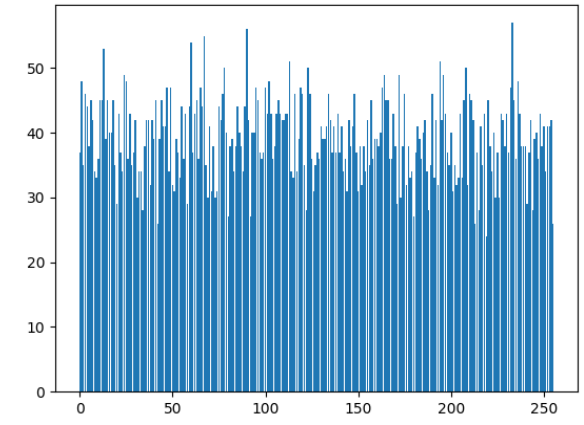
D. Analisis Statistik

Analisis statistik dilakukan dengan melihat frekuensi kemunculan tiap byte pada ciphertext. Untuk keperluan analisis prinsip *confusion*, digunakan teks lorem ipsum berukuran 10.000 bytes.

Berikut ini adalah histogram yang menunjukkan frekuensi kemunculan suatu nilai byte pada *plaintext* dan *ciphertext* hasil enkripsi menggunakan kunci “kriptografi”.



Gambar 9. Histogram Distribusi Kemunculan Nilai Byte pada *Plaintext*



Gambar 10. Histogram Distribusi Kemunculan Nilai Byte pada *Ciphertext*

Dapat dilihat pada histogram di atas, *cipherteks* memiliki distribusi yang merata dibandingkan dengan *plaintext*. Oleh karena itu, dapat disimpulkan bahwa algoritma Doramei cipher sudah memenuhi prinsip *confusion*.

ACKNOWLEDGMENT

Penulis ingin mengucapkan terima kasih kepada Dr. Ir. Rinaldi, M.T. yang telah memberikan bimbingan dan dukungan dalam penulisan artikel ini. Serta kami berterimakasih kepada Hokki Suwanda dan Michael Hans selaku asisten pada mata kuliah ini. Kami juga ingin mengucapkan terima kasih kepada tim penelitian yang terlibat dalam pengumpulan dan analisis data. Selain itu, penulis juga mengucapkan terima kasih kepada keluarga dan teman-teman yang memberikan dukungan moral selama proses penulisan artikel ini

V. KESIMPULAN DAN SARAN

Doramei cipher dapat digunakan sebagai block cipher untuk melakukan enkripsi dan dekripsi pada pesan. berdasarkan hasil tes analisis efek longsoran memiliki nilai yang baik. Kelebihan dari block cipher ini adalah key yang digunakan akan berpengaruh terhadap S-Box, serta setiap putaran key akan degenerate ulang. hal ini mengakibatkan ketika terjadi perubahan pada key maka hasil ciphertext akan berubah drastis. Selain itu, Doramei cipher juga sudah menerapkan prinsip *confusion* dengan baik dimana hasil *cipherteks* memiliki distribusi yang merata dibandingkan dengan *plaintext*. Namun, kelemahan yang masih terdapat pada Doramei cipher adalah kurangnya ketahanan terhadap perubahan pada plaintext yang hanya mengganti satu bit atau satu byte. hal ini dapat ditingkatkan kedepannya dengan penambahan fitur fitur baru yang dapat lebih menguatkan Doramei block cipher.

VI. DAFTAR REFERENSI

[1] Munir, Rinaldi. 2023. Slide Kuliah IF4020 Kriptografi: Serangan terhadap kriptografi.

[2] Munir, Rinaldi. 2023. Slide Kuliah IF4020 Kriptografi: Perancangan cipher blok (block cipher).

[3] Munir, Rinaldi. 2023. Slide Kuliah IF4020 Kriptografi: Cipher blok (block cipher) - Bagian 1.

[4] United States National Institute of Standards and Technology (NIST). 2001. *Federal Information Processing Standards Publication 197*: Announcing the Advanced Encryption Standard (AES).