4S5S: 4 Sehat 5 Sempurna

Eka Sunandika[1], **Muhammad Fariz Luthfan Wakan**[2].

[1,2] Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika (STEI), Institut Teknologi Bandung (ITB), Jalan Ganesha 10, Lb. Siliwangi, Kecamatan Coblong, Kota Bandung, Jawa Barat 40132
E-mail: 13517130@std.stei.itb.ac.id, 13517034@std.stei.itb.ac.id

Abstract. Kriptografi adalah teknik yang digunakan untuk menyembunyikan pesan agar tidak diketahui oleh pihak ketiga. Kriptografi modern dikembangkan untuk menggantikan kriptografi klasik yang sudah diketahui banyak orang. Salah satu algoritma kriptografi modern yang populer adalah menggunakan kunci simetris. *Block cipher* adalah salah satu implementasi kunci simetris yang melakukan enkripsi pada blok-blok pesan. Algoritma DES merupakan algoritma populer dalam *block cipher*. 4 Sehat 5 Sempurna merupakan algoritma yang melakukan modifikasi terhadap DES dengan mengubah pola jaring Feistel yang digunakan..
Keywords: 4 Sehat 5 Sempurna, Block Cipher, Cipher, DES, Feistel, Kriptografi.

1. Pendahuluan

Teknologi berkembang dengan sangat pesat selama beberapa dekade terakhir, khususnya di dunia maya. Pertukaran data terjadi di dunia maya setiap detiknya. Pertukaran tersebut melibatkan Internet sebagai media pengiriman dan penerimaannya. Permasalahan keamanan dalam pengiriman data atau pesan sudah ada sejak zaman dahulu. Semakin beragamnya media dan cara pengiriman pesan menyebabkan masalah tersebut semakin besar. Solusi untuk menyelesaikan permasalahan tersebut adalah memanfaatkan kriptografi dalam pengiriman pesan. Kriptografi merupakan ilmu mengenai teknik dalam melakukan enkripsi agar pesan yang dikirim tidak dapat dipahami orang yang menemukan pesan, dan dekripsi agar pesan yang telah terenkripsi tersebut dapat dipahami oleh penerima. Terdapat beberapa algoritma kriptografi yang sudah digunakan sejak zaman dahulu, tetapi bentuknya yang sederhana dan sudah banyak orang yang tau cara memecahkan pesan yang sudah di enkripsi tersebut, membuat algoritma tersebut tidak aman lagi. Maka dari itu, algoritma kriptografi selalu dikembangkan seiring dengan perkembangan teknologi untuk menjamin keamanannya.

1.1. DES

DES merupakan algoritma yang digunakan sebagai acuan pada *block cipher* yang akan diajukan. Algoritma ini dikembangkan oleh IBM pada tahun 1970an dan didesain oleh Horst Feistel. Dengan *block cipher,* algoritma ini akan mengoperasikan blok berukuran 64 bit plainteks yang ditransformasikan menjadi ciphertext dengan ukuran yang sama. Kunci yang digunakan berukuran 64 bit, tetapi hanya 56 bit yang terpakai. Blok yang dienkripsi diputar sebanyak 16 kali dengan menggunakan kunci internal 48 bit yang berbeda.

2. Dasar Teori

Berikut merupakan beberapa dasar teori yang terkait dengan masalah yang diangkat.

2.1. Kriptografi

Berasal dari bahasa Yunani yaitu *kryptós* yang memiliki arti tersembunyi dan *graphein* yang memiliki arti menulis. Merupakan teknik yang digunakan untuk berkomunikasi atau mengirim pesan dengan aman pada kehadiran pihak ketiga. Proses yang dilakukan adalah melakukan enkripsi dan dekripsi pada pesan. Pada perkembangannya dibagi menjadi kriptografi klasik dan modern. Kriptografi modern didasari oleh teori matematika dan memanfaatkan komputasi dari komputer. Tujuan dari kriptografi adalah untuk memastikan kerahasiaan pesan.

2.2. Cipher

Cipher merupakan algoritma yang digunakan dalam melakukan enkripsi dan dekripsi. Proses yang dilakukan pada enkripsi adalah mengubah *plaintext* menjadi *ciphertext* sehingga pesan tidak bisa dipahami pihak ketiga. Pada dekripsi, proses yang dilakukan adalah mengubah *ciphertext* menjadi *plaintext* agar bisa dipahami penerima. Terdapat 2 tipe kunci yang digunakan *cipher*. Pertama, algoritma kunci simetris yang menggunakan satu kunci untuk melakukan enkripsi dan dekripsi. Kedua, algoritma kunci asimetris yang menggunakan dua bentuk kunci yang berbeda, kunci publik untuk enkripsi dan kunci privat untuk dekripsi.

2.3. Block Cipher

Block Cipher merupakan algoritma yang melakukan operasi pada blok yang terdiri dari kumpulan bit pada ukuran tertentu. Algoritma ini menggunakan kunci simetris. Enkripsi dilakukan dengan bit-bit kunci dan dilakukan berulang-ulang terhadap blok-blok *ciphertext*. Dekripsi yang dilakukan memiliki cara yang mirip dengan proses enkripsinya.

2.4. *Confusion* dan *Diffusion*

Confusion dan *Diffusion* merupakan prinsip untuk merancang cipher yang aman. *Confusion* memiliki arti bahwa prinsip ini harus memastikan hubungan antara plainteks, cipherteks, dan kunci tersembunyi dan tiap bit *ciphertext* bergantung pada beberapa bagian kunci. Sehingga kunci sulit didapat dari satu blok dan meningkatkan ambiguitas. *Diffusion* memiliki arti bahwa satu bit yang kita ubah pada plainteks akan mengubah dengan drastis cipherteksnya. Sehingga dapat menyembunyikan hubungan antara cipherteks dengan plainteks dan menyulitkan penyerang untuk bisa memahami cipherteks yang berulang.

2.5. *Cipher* Berulang

Cipher berulang merupakan fungsi transformasi sederhana yang melakukan perulangan pada proses enkripsi. Setiap perulangan menggunakan *round key* sebagai input kedua yang dikombinasikan dengan plainteks. Perlu didesain dengan baik agar bisa menghindari serangan yang menyebabkan data bocor.

2.6. Jaringan Feistel

Jaringan Feistel merupakan teknik yang digunakan dalam konstruksi *block cipher*. Memiliki sifat reversibel dalam proses enkripsi dan dekripsi. Sehingga proses dekripsi yang dilakukan tidak perlu menggunakan algoritma baru. Menggunakan *round function* yang menerima dua input, blok pesan dan subkeynya. Proses substitusi dan permutasi pada jaringan yang dilakukan memastikan bahwa pesan bisa dienkripsi dan didekripsi. Blok pesan dibagi menjadi dua untuk bagian kiri dan kanan. Pada gambar dibawah diberikan ilustrasi mengenai jaringan feistel.

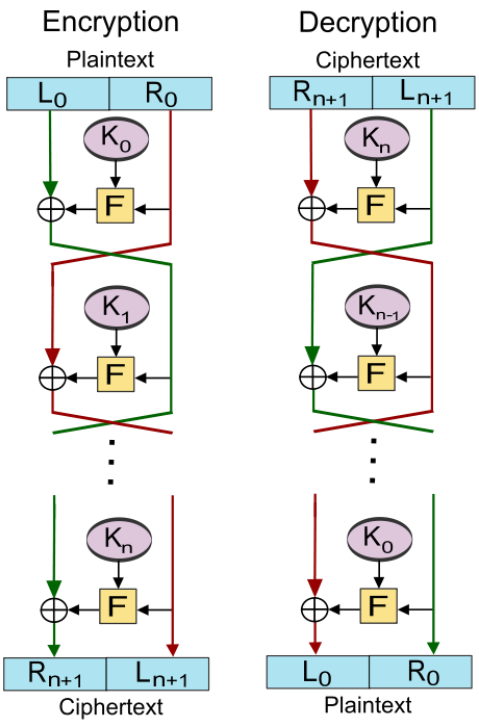

Figure 1. Ilustrasi Enkripsi dan Dekripsi pada Jaringan Feistel. Sumber https://id.wikipedia.org/wiki/Sandi_Feistel

2.7. Kotak-S

Merupakan matriks yang digunakan untuk melakukan substitusi bit-bit pesan. *Input* bit akan ditransformasikan menjadi output bit yang memiliki panjang berbeda (output bit lebih panjang). Operasi yang dilakukan adalah *look-up* table. Gambar dibawah merupakan contoh Kotak-S pada algoritma AES.

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure 2. AES S-Box (Rijndael S-Box). Sumber: https://www.researchgate.net/profile/Edwin_Arboleda/publication/318906543/figure/fig4/AS:790611112251395@1565507786848/AES-S-Box-Rijndael-S-Box-16.jpg

3. 4S5S: 4 Sehat 5 Sempurna

Block Cipher menerima input blok plainteks berukuran 64 bit dan akan dipecah menjadi 32 bit ketika memasuki jaringan Feistel. Terdapat 4 jaringan Feistel dengan jumlah putarannya masing-masing. Kunci yang digunakan bisa berukuran 64 bit. Struktur algoritma diilustrasikan pada diagram dibawah ini.

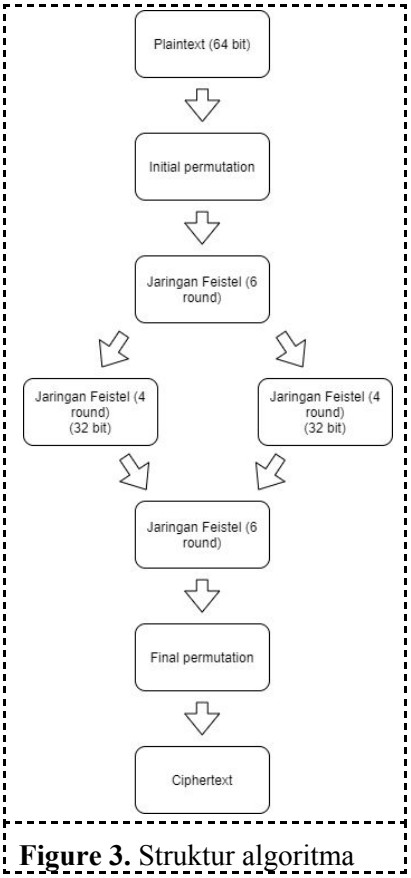

Figure 3. Struktur algoritma

Output dari jaringan Feistel pertama akan dipecah untuk masuk ke jaringan Feistel kedua dan ketiga. Setelah itu akan digabungkan lagi untuk masuk ke jaringan Feistel kempat. Total dari putaran yang dilakukan adalah 16 putaran dan key yang diperlukan sebanyak 32. Key tersebut dibangkitkan dari key awal. Proses pada bagian lainnya sama dengan cara kerja DES. *Round function* menggunakan S-box sebanyak 8 buah.

4. Eksperimen dan Analisis Hasil

Eksperimen dilakukan dengan menggunakan plainteks berikut.

> 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.

Dan dengan menggunakan kunci "*Crypting*".

Berikut hasil yang didapat setelah menggunakan plainteks dan kunci tersebut pada algoritma (mode EBC) yang dibentuk.

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

4.1. Analisis Hasil dengan Pengubahan Satu Bit Kunci

Jika satu bit kunci diubah pada saat melakukan dekripsi, dari "*Crypting*" menjadi "*CryptiNg*",

```
ÉÙëk…L?˜}Œäo©úê@9û∑xÒzÙF?`ÿ8ß˙¸†        gSK˜ë'∞~ı‡NÚ[∫4æ%b‹Y˜e'MR'ï
 :+ÒmBKuîk3·8:ìV¸FÙ,Œ¸ã∫≥Ô7à∏ÂÑ
K⁄ÙI¡%ÄqfSå√„$'ú,=NGëŸåÑ~û"ÿ≥¢Dq˜òΩ+Y0e5Õ«◊ò,ögk8÷¥>åÛ:˙á}fi3wÇ3|pπ(Ó"ò\¯–‹©£Ô1
Å#∞″Ôò–£¿F)Sé"Àñ≈Æ úì¥]«Ä)ê"$Cë≤bß≈∫dD/(˜∏|Àh'¸„dP†G«˙—ëAKΩKı"À˘`à`°Ç'+¢
auÎèÚ§LÚw'Ω5
äD@_∫ıŸ£æÙ‹åS«¯áı

"âΩ®m‰˘4¿êa$Øs¶Ç´∞ÄG6@8Åõπã¨8;:Ö€PBÉA+∞fPC?~»a;ß1˚◊àn¯Äá¿
‡Mðï¸µ¸†§¶ΩÊùÒ
Jœ0âÂRõ≈'Ä.ô¬Ç∞â^≤ªë'/À7üO 1Ï™ÚÕπØrA
>″æfi´T…ü°i˘µZ}rØl&ÒÛÅå
```

Plainteks yang terbentuk sudah tidak dapat dipahami lagi dan jauh dari plainteks semula.

4.2. Analisis Hasil dengan Pengubahan Satu Bit Plainteks

Jika mengganti 1 bit plainteks,

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.

cipherteks yang terbentuk,

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

Terjadi perubahan pada cipherteks yang terbentuk, tetapi tidak terlalu signifikan (perubahan pada blok yang bit-nya berubah saja).

4.3. Analisis Hasil dengan Pengubahan Satu Bit Kunci

Jika pada cipherteks terdapat perubahan 1 bit (`D0` -> `D1`),

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

```
BB 66 B5 06 B7 C6 3D 9D
```

Plainteks yang terbentuk setelah dilakukan dekripsi,

```
Lorem ipsum doloçÓÎå#'àet, 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.
```

Berdasarkan hal tersebut, keamanan masih perlu diperhatikan, karena plainteks yang terbentuk setelah dilakukan dekripsi dengan algoritma 4S5S tidak terjadi perubahan yang signifikan.

5. Kesimpulan dan Saran Pengembangan

Algoritma 4S5S (4 Sehat 5 Sempurna) merupakan algoritma DES yang membentuk tiga fase yang berisi 6 *round*, 4 *round* dan 6 *round*, yang mana 4 *round* akan dilakukan partisi terlebih dahulu. Ini dikembangkan untuk menyajikan teknik baru DES. Diperlukan penindaklanjutan lebih dalam pada algoritma ini untuk meningkatkan kerahasiaan pesan.

Saran pengembangan yang bisa dilakukan adalah dengan membuat blok pesan yang bisa di enkripsi berukuran lebih besar.

6. Referensi

[1] Rivest, Ronald L. 1990. "Cryptology". Dalam J. Van Leeuwen. Handbook of Theoretical Computer Science. 1. Elsevier.

[2] Menezes, Alfred J.; Oorschot, Paul C. van; Vanstone, Scott A. 2001. Handbook of Applied Cryptography

[3] National Institute of Standards and Technology, Data Encryption Standard (DES) . (U.S.: U.S. Department of Commerce)

Acknowledgments

Terima kasih kepada Allah SWT yang telah membantu kami dalam melancarkan pengerjaan *paper* ini hingga selesai. Kami juga bersyukur dan berterima kasih kepada dosen mata kuliah ini, yaitu bapak Dr. Ir. Rinaldi Munir, MT. yang telah mengajarkan kami materi kriptografi dengan baik dan menyenangkan. Terakhir, kami ucapkan terima kasih kepada keluarga kami yang telah mendukung kami dalam menjalankan segala kegiatan.