ARDES : Sebuah Algortima Block Cipher Modifikasi Data Encryption Standard

Adhika Aryantio
13511061
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, ITB
Bandung, Indonesia

Muhammad Rian Fakhrusy
13511008
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, ITB
Bandung, Indonesia

Abstrak— **Pada makalah ini, akan diajukan sebuah algoritma block cipher yang dinamakan ARDES – Adhika-Rian Data Encrytion Standard. Algoritma ini akan menggunakan blok dengan panjang 64 bit dan 2 buah kunci, yaitu kunci A dan kunci B yang masing-masing panjangnya 64 bit. Kunci A dimasukkan oleh user dan kunci B merupakan permutasi dari kunci A. Seperti algoritma Data Encryption Standard, algortima ini juga yang menggunakan struktur jaringan Feitsel dan key generator. Namun, terdapat modifikasi pada loop, shifting dan cara pembagian bit pada algortima ini. Algoritma ARDES memiliki tingkat keamanan yang cukup baik seperti DES.**

Kata kunci : block cipher, skema feistel, key generator

I. PENDAHULUAN

Kriptografi merupakan salah satu bagian penting dari keilmuan komputer. Apalagi pada saat ini teknologi penyampaian pesan lewat internet berkembang dengan sangat pesat. Penyampaian pesan ini akan melalui saluran yang belum tentu aman. Oleh karena itu, kriptografi digunakan sebagai salah satu metode pengamanan pesan tersebut.

Block cipher adalah salah satu teknik dari kriptografi yang melakukan enkripsi pesan dalam ukuran panjang bit tertentu yang disebut blok. Blok-blok ini akan dioperasikan dengan berbagai cara tertentu. Cara yang banyak digunakan adalah substitusi, permutasi, feistel network dan operasi XOR. Key generator juga merupakan salah satu cara yang digunakan pada algortima block cipher. Gabungan dari beberapa cara inilah yang menghasilkan sebuah algortima block cipher.

II. TEORI SINGKAT

A. *Skema Feistel*

Skema feitsel menggunakan pembagian bit plain text atapun cipher text menjadi ruas kiri dan ruas kanan yang sama besar dalam melakukan enkripsi atau deskripsi. Setelah pembagian ruas dilakukan akan dilanjutkan dengan berbagai metode seperti permutasi, substitusi ataupun bit shifting ataupun berbagai metode lainnya untuk melakukan penyembunyian pesan asli. Kelebihan dari pemanfaatan skema ini adalah cara deskripsi dan enkripsi yang mirip sehingga lebih mudah dalam melakukan operasi enkripsi dan deskripsi pesan.

B. *Key Generator*

Key generator adalah proses untuk membentuk suatu kunci baru dari kunci yang dimasukkan dengan suatu bilangan acak yang dibangkitkan dengan pembangkit bilangan acak ataupun dengan pembangkit bilangan pseudo-random yang menggunakan umpan tertentu. Key generator ini digunakan pada kriptografi agar pesan dapat tersembunyi dengan baik dan dapat dilakukan deskripsi kembali dengan kunci yang sama.

III. RANCANGAN BLOCK CIPHER

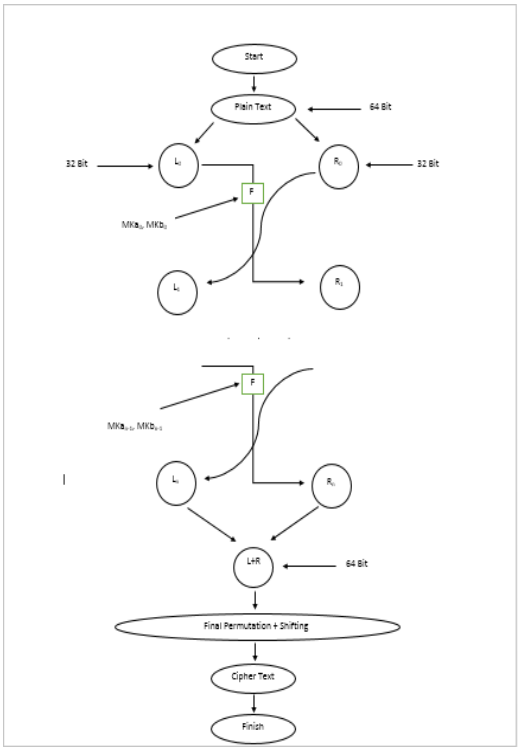
Algoritma ARDES memiliki arsitektur algoritma yang terdiri dari yaitu

1. ARDES mengenkripsi *plain text* per 64 bits
2. ARDES memiliki kunci A dan kunci B yang akan digunakan sebagai kunci enkripsi dan kunci dekripsi
3. ARDES melakukan *loop* sebanyak 10 kali
4. Sub kunci ARDES di *generate* berdasarkan subkunci sebelumnya
5. ARDES menggunakan 2 enkripsi dengan kunci A dan dan kunci B dengan melakukan perhitungan XOR

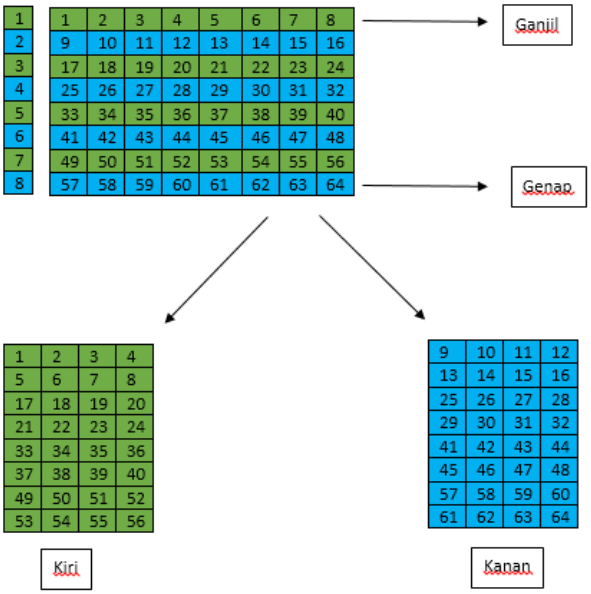
Arsitektur besar yang dimiliki oleh ARDES dapat dilihat pada Gambar III.1.

A. *Pembagian Plain Text*

Pada arsitektur ARDES yang dapat dilihat pada Gambar III.1, Plain text yang akan dienkripsi dibagi menjadi dua bagian yaitu bagian kiri dan bagian kanan. Pembagian plain text ke kiri dan ke kanan dilakukan dengan mengisikan baris ganjil memasuki bagian kiri arsitektur dan baris genap memasuki bagian kanan arsitektur. Cara pembagian plain text ini dapat dilihat pada Gambar III.2.



Gambar III.1. Arsitektur ARDES



Gambar III.2. Pembagian Plain Text

B. Pembangkitan Kunci B

Kunci B merupakah kunci tambahan yang didapatkan dari Kunci A. Kunci B didapatkan dengan menggunakan permutasi dari Kunci A. Panjang kunci A adalah 64 bit sehingga panjang kunci B yang dilakukan adalah 64 bit juga. Permutasi yang digunakan untuk menghasilkan kunci B dapat dilihat pada Gambar III.3

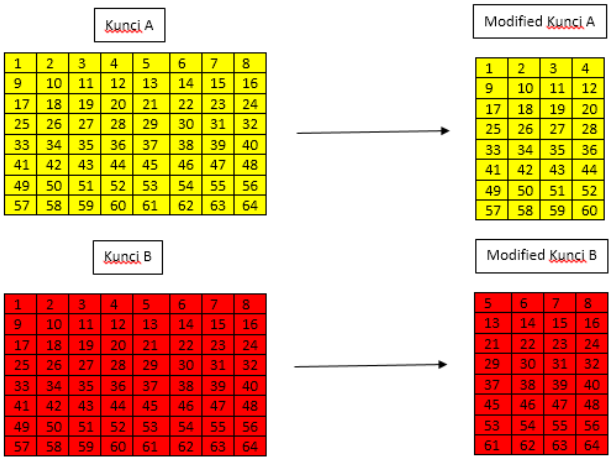
64	40	32	8	16	24	48	56
63	39	31	7	15	23	47	55
62	38	30	6	14	22	46	54
61	37	29	5	13	21	45	53
60	36	28	4	12	20	44	52
59	35	27	3	11	19	43	51
58	34	26	2	10	18	42	50
57	33	25	1	9	17	41	49

Gambar III.3. Tabel Permutasi Pembangkit Kunci B

Permutasi dilakukan dengan mengisikan bit 1 diisikan dengan bit 64, bit 2 diisikan dengan 40 dan seterusnya hingga bit 64 diisikan dengan bit 49. Dengan menukar nukar bit dengan menggunakan permutasi tersebut maka akan didapatkan kunci B.

C. Modifikasi Kunci A dan Kunci B

Kunci A dan Kunci B digunakan untuk mengenkripsi plain text. Kunci A dan Kunci B memiliki memiliki panjang 64 bit sedangkan plain text yang sudah dibagi memiliki panjang 32 bit oleh karena itu kunci A dan kunci B harus dilakukan modifikasi agar memiliki panjang 32 bit. Modifikasi kunci A dan kunci B dapat dilihat pada Gambar III.4.



Gambar III.4. Modifikasi Kunci A dan B

Kunci A dimodifikasi dengan menghapus 4 x 8 kolom terakhir sedangkan Kunci B dimodifikasi sebaliknya dengan menghapus 4 x 8 kolom pertama.

D. Pembangkit SubKunci A dan SubKunci B

Algoritma ARDES menggunakan *looping* sebanyak 10 kali untuk itu diperlukan subkunci A dan subkunci B untuk mengenkripsi *text* pada setiap *looping*nya. Kunci A dan kunci B membangkitkan subkunci masing-masing sehingga kunci A

dan kunci B bersifat *independent*. Pembangkitan kunci menggunakan perhitungan permutasi dimana tabel permutasi yang pertama yaitu sebagai berikut :

Tabel III.1. Initial Permutation SubKunci A

32	31	30	29
9	10	11	28
8	1	12	27
7	2	13	26
6	3	14	25
5	4	15	24
18	17	16	23
19	20	21	22

Tabel III.2. Initial Pemutation SubKunci B

32	13	14	15
31	12	1	16
30	11	2	17
29	10	3	18
28	9	4	19
27	8	5	20
26	7	6	21
25	24	23	22

Tabel initial permutation pada Tabel III.1 dan Tabel III.2 akan digunakan untuk membangkitkan tabel permutasi yang digunakan untuk subkunci berikutnya. Rumus yang digunakan untuk menampilkan table permutasi pada subkunci A berikutnya adalah pada 3 kunci pertama dengan menggeser angka – angka pada baris ganjil n ke kanan dan pada baris genap n ke kiri dan 7 kunci sisanya dengan menggeser kolom ganjil n ke atas dan kolom genap n ke bawah.

Sedangkan untuk pembangkitan tabel permutasi pada 3 subkunci B pertama adalah dengan menggeser angka – angka pada baris ganjil n ke kiri dan pada baris genap n ke kanan dan untuk 7 kunci sisanya dengan menggeser kolom ganjil n ke bawah dan menggeser kolom genap n ke atas. Bagaimana membangkitkan subkunci A dan B dapat dilihat pada Gambar III.5 dan Gambar III.6

E. S-Box

S-Box digunakan untuk melakukan subtitusi terhadap nilai yang ada. Dalam pengembangan algoritma ARDES S-Box yang digunakan berupa 8 buah S-Box dimana setiap S-Box mewakili baris dari suatu *plain text.* Contohnya, bila baris satu pada 4x8 array maka akan disubtitusi dengan S-Box pertama. S-Box yang digunakan yaitu sebagai berikut :

S-Box 1

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	0

S-Box 2

0	15	2	3	1	6	7	8
9	13	10	11	12	14	4	5

S-Box 3

1	3	11	14	4	8	0	2
9	15	6	12	13	10	7	5

S-Box 4

0	3	15	9	8	2	1	14
4	6	13	5	10	7	11	12

S-Box 5

3	5	1	0	11	12	13	2
6	4	8	7	14	9	15	10

S-Box 6

15	0	10	1	3	8	7	5
9	12	11	14	2	4	13	6

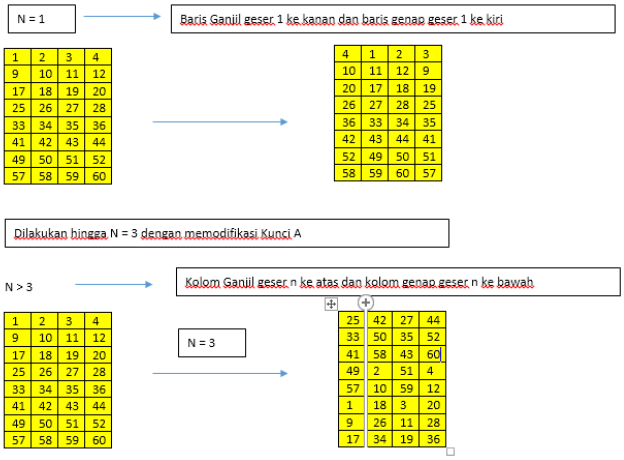
S-Box 7

14	1	0	12	11	2	15	4
9	13	5	6	10	3	7	8

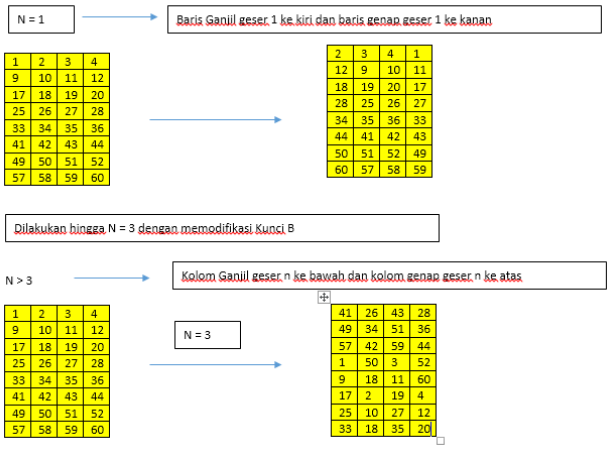
S-Box 8

13	2	5	12	10	14	0	7
11	1	3	8	15	9	4	6

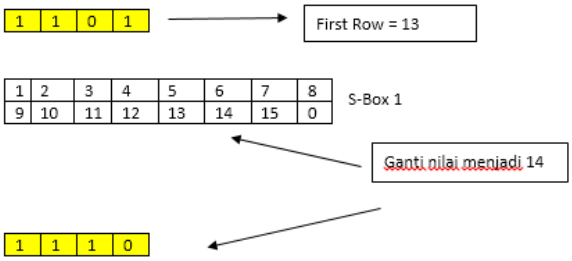
Pada baris pertama S-Box merupakan index 0-7 sedangkan baris kedua S-Box merupakan 8-15 .Cara menggunakan S-Box yaitu dengan menjumlahkan bit-bit pada baris ke n lalu dari hasilnya tersebut mengacu pada baris S-Box n yang mana, lalu ganti nilai baris n dengan dengan nilai pada kolom ke jumlah bit baris n pada S-Box. Gambaran pergantian dapat dilihat pada Gambar III.7.



Gambar III.5. Pembangkitan Subkunci A



Gambar III.6. Pembangkitan Subkunci B



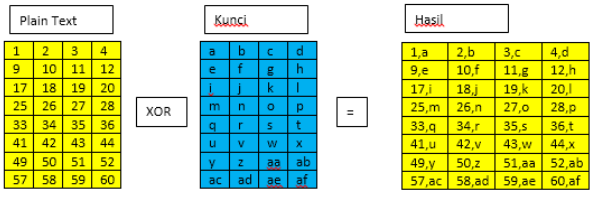
Gambar III.7. Pergantian dengan S-Box

F. Fungsi F

Fungsi F merupakan fungsi enkripsi yang terdapat pada algoritma ARDES , Fungsi F terdiri dari yaitu

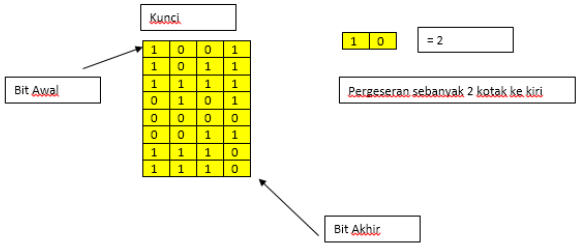
1. Fungsi XOR dengan menggunakan Kunci A
2. Fungsi pergeseran sesuai dengan bit akhir dan bit awal kunci A
3. Pergantian menggunakan S-Box
4. Fungsi pergeseran sesuai bit akhir dan bit awal kunci B
5. Fungsi XOR menggunakan Kunci B

Fungsi XOR yang diterapkan dapat dilihat pada Gambar III.8



Gambar III.8. Fungsi XOR

Pergeseran bit sesuai dengan bit akhir dan bit awal dari kunci, bit akhir dan bit awal tersebut kemudian dijumlahkan yang hasilnya merupakan jumlah kolom yang harus digeser ke kiri. Pergeseran dapat dilihat pada Gambar III.9.



Gambar III.9. Pergeseran pada Fungsi F

Pergantian S-Box sepertin yang dilakukan pada Subbab E.

G. Penggabungan Kembali

Penggabungan Kembali cipher text menjadi satu dilakukan setelah pengulangan selesai, diterapkan kembali fungsi permutasi menggunakan fungsi permutasi tabel A dan dilakukan shifting sebanyak 2 kali ke kiri.

Bagian kanan kemudian disusun menjadi baris genap lagi dan bagian kiri disusun menjadi baris ganjil lagi. Terbentuklah cipher text dengan panjang pesan 64 bit.

IV. ANALISIS KEAMANAN ARDES

ARDES memiliki tingkat keamanan yang cukup baik dibandingkan algoritma DES. Tingkat keamanan ARDES yaitu :

1. Brute Force diperlukan mem brute force 64 x 64 panjang kunci, karena kunci yang digunakan merupakan kunci ganda.
2. Semua fungsi saling tergantung dengan kuncinya, bila salah memasukkan kunci 1 bit saja maka semua hasil yang dikeluarkan akan berbeda.
3. Serangan ditengah tidak bisa dilakukan karena dilakukan pergantian menggunakan S-Box pada pertegahan proses enkripsi.

V. KESIMPULAN

ARDES merupakan algoritma baru yang ditawarkan dengan tingkat keamanan lebih baik dibandingkan DES dengan pengulangan yang dilakukan lebih cepat daripada DES dan algoritma enkripsi yang kompleks. ARDES mengandung asspek berikut :

1. Jaringan Feitsel sehingga mudah melakukan dekripsi yaitu dengan membalikkan alur enkripsi.

2. Berisifat Confusion dan Difusion sehingga bila 1 bit saja diubah maka akan menjalar ke proses lainnya serta memiliki loop sebanyak 10 kali.
3. Lama komputasi cukup lama karena kompleksnya algoritma

REFERENCES

[1] Microsoft, "Generating Keys for Encryption and Decryption", diakses dari https://msdn.microsoft.com/en-us/library/5e9ft273(v=vs.110).aspx pada 17 Maret 2015.

[2] RSA Laboratories, "Why is Cryptography important?", diakses dari http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/why-is-cryptography-important.htm pada 17 Maret 2015.

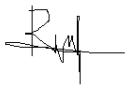
[3] J. Orlin Grabbea, "The DES Algorithm Illustrated", diakses dari http://page.math.tu-berlin.de/~kant/teaching/hess/krypto-ws2006/des.htm pada 16 Maret 2015.

[4] H.H Salih, A.T. Sadiq, dan A. K. Frhan, "Proposal of New Block Cipher Algorithm," Departement of Computer Science, University of Technology, Iraq.

PERNYATAAN

Dengan ini kami menyatakan bahwa makalah yang kami tulis ini adalah tulisan kami sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 18 Maret 2015



Adhika Aryantio
13511061

M. Rian Fakhrusy
13511008