Corona

W.J Hadiman[1], **J Tjandra**[1], **I Fadillah**[1]

[1] Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung, Coblong, Bandung 40132, Indonesia
E-mail: 13516026@std.stei.itb.ac.id,13516058@std.stei.itb.ac.id,13516128@std.stei.itb.ac.id

Abstract. Kriptografi adalah suatu hal yang penting untuk mengamankan informasi di jaman sekarang. Informasi sudah sangat cepat dan menjadikannya tidak terlalu aman. *Block cipher* adalah salah satu teknik pengaplikasian kriptografi modern dengan melakukan enkripsi terhadap blok yang terus bit-bit data. Sudah banyak algoritma yang cukup terkenal, tetapi kami mencoba mengusulkan algoritma baru bernama corona yang merupakan evolusi/perbaikan dari algoritma block cipher yang sudah ada sebelumnya. Pada awal, sama seperti DES kami mengacakan urutan bit input dengan permutasi. Lalu kemudian kami menggunakan feistel untuk melakukan pengacakan isi yang ada, terakhir kami kembalikan dengan menggunakan *invers* dari permutasi yang sudah dilakukan di awal.

Kata kunci. Block cipher, block cipher variation, conffusion, diffusion, corona algorithm

1. Pendahuluan

Kriptografi berasal dari bahasa Yunani *kryptós* yang berarti tersembunyi (*hidden* atau *secret*) dan *graphein* yang berarti menulis (*to write*). Menurut Kamus Merriam-Webster, kriptografi dapat diartikan sebagai *secret writing*/tulisan tersembunyi, atau juga *the enciphering and deciphering of messages in secret code or cipher also : the computerized encoding and decoding of information*.
Sesuai dengan arti tersebut, maka kriptografi adalah sebuah cara untuk mengirimkan pesan dari pengirim ke penerima pesan yang seharusnya tanpa diketahui orang lain. Pesan dienkripsi sebelum pengiriman dan penerima melakukan dekripsi agar isi pesan tersebut bisa terbaca.
Algoritma kriptografi dapat dibagi menjadi dua, klasik dan modern. Algoritma kriptografi klasik salah satu contoh adalah Caesar Cipher yang diciptakan oleh Julius Caesar yang digunakan pada jaman Romawi Kuno. Sedangkan algoritma modern yang umum digunakan sekarang adalah AES, RSA, 3DES, DES, dan algoritma lainnya. Algoritma tersebut dibangun dengan tujuan keamanan sehingga dari cipher yang dihasilkan, maka plainteks/pesan awal yang disematkan tidak mudah ditebak dan diketahui dengan menggunakan teknik-teknik umum seperti analisis frekuensi.
Hal ini dicapai dengan prinsip confusion dan diffusion dari Shannon. Algoritma ini menggunakan P-box dan S-box untuk operasi permutasi dan substitusi. Selain itu, algoritma ini memanfaatkan jaringan Feistel sehingga reversible baik untuk enkripsi serta dekripsi.

Kami memberikan nama algoritma ini adalah corona karena beberapa alasan. Pertama, corona sedang mewabah dan cukup banyak yang terjangkit ketika kami membuat algoritma ini. Kemudian, sampai seperti corona yang merupakan evolusi dari virus sebelumnya yaitu SARS, algoritma ini merupakan

evolusi dari algoritma *block cipher* yang sudah diciptakan sebelumnya dan kami lakukan modifikasi untuk menambah *diffusion dan confussion* saat melakukan enkripsi.

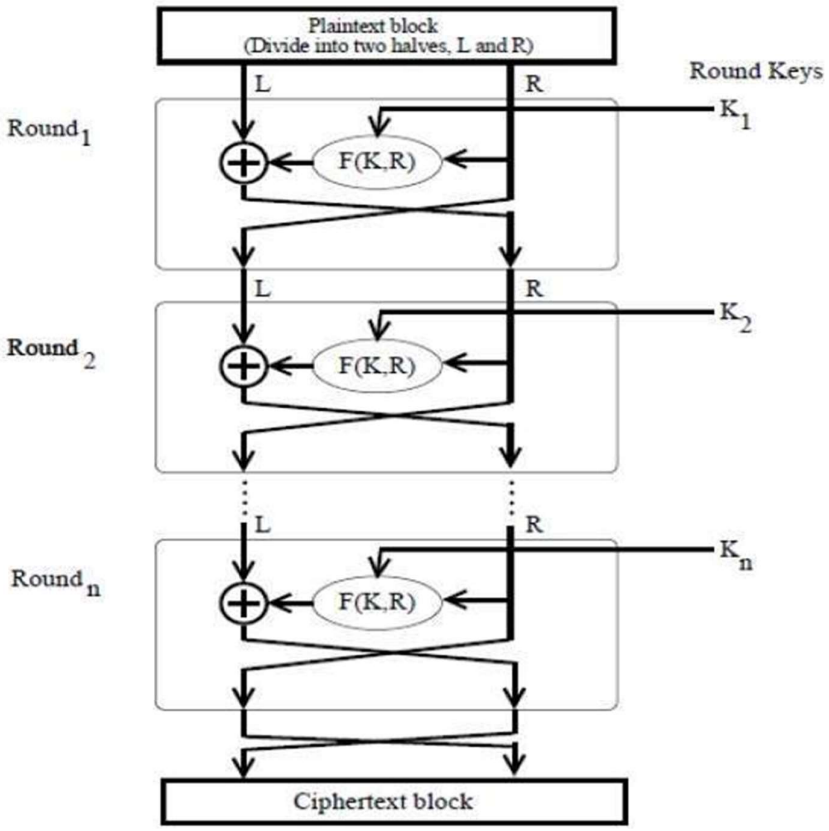
2. Dasar Teori

2.1. Diffusion dan Confusion

Claude E. Shannon pada 1949 mengatakan bahwa dalam analisis statistik akan sulit dilakukan jika dilakukan dua metode, yaitu confusion dan diffusion. [1]. Confusion sendiri berarti hubungan antara key dan ciphertext sulit untuk dilihat sehingga tidak mudah untuk mencari korelasi dan menganalisis hubungannya. Sementara diffusion berarti jika kita mengubah salah satu karakter pada plaintext, maka perubahan yang cukup besar akan terjadi juga pada ciphertext, begitu juga dengan sebaliknya, dengan demikian untuk melakukan analisis dibutuhkan jumlah plaintext yang sangat besar dan tidak feasible. untuk dilakukan.

2.2. Jaringan Feistel

Jaringan Feistel adalah sebuah jaringan tingkat tinggi yang membentuk sebuah struktur yang invertible (dapat dibalik) dari komponen-komponen yang non-invertible (tidak dapat dibalik). [3] Struktur dari Jaringan Feistel adalah sebagai berikut: [4]



Gambar 1. Jaringan Feistel

(Sumber: https://www.tutorialspoint.com/cryptography/images/feistel_structure.jpg)

1) Input (plaintext) dibagi menjadi dua bagian, kiri (L) dan kanan (R)
2) Pada setiap putaran, maka dilakukan operasi, yaitu untuk bagian kanan tidak akan diubah dan diteruskan lalu ditukar menjadi bagian kiri putaran berikutnya. (R_i menjadi L_{i+1}).
3) Sedangkan pada bagian kiri, dilakukan operasi XOR (□) dengan hasil dari fungsi $f_i(K,R_i)$ yang merupakan fungsi yang menerima input key, dan bagian kanan (R).
4) Hasil dari operasi □ berikut ditukar menjadi bagian kanan putaran berikutnya. (L_i menjadi R_{i+1}).

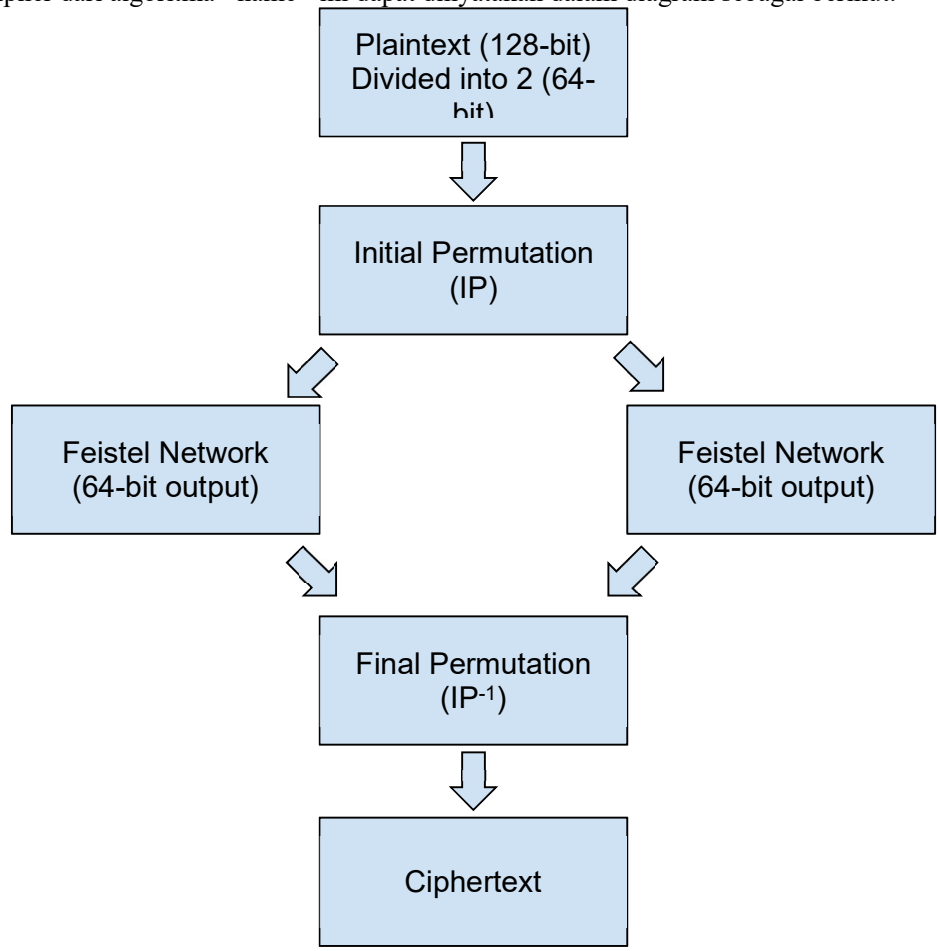
2.3. Deret Padovan

Deret Padovan digunakan sebagai parameter pergeseran pada saat pembuatan kunci. Barisan Padovan

adalah sebuah barisan yang memiliki relasi rekurens sebagai berikut: [5]
P(n) = P(n-2) + P(n-3) dengan syarat P(0) = P(1) = P(2) = 1.

3. Proposed Block Cipher

Block Cipher ini beroperasi dalam blok 128-bit, dan operasi dilakukan secara bit. Arsitektur Umum Block Cipher dari algoritma <name> ini dapat dinyatakan dalam diagram sebagai berikut:



Gambar 2 - Struktur Umum Algoritma <name>

Selain itu, algoritma dalam jaringan Feistel yang menerima input 64-bit ini dipecah menjadi 32-bit untuk bagian kiri dan bagian kanan, dan kemudian setiap bagian tersebut dipecah kembali menjadi dua bagian sepanjang 16-bit. dapat dinyatakan pada diagram sebagai berikut:

Gambar 3 - Operasi yang terjadi setiap Putaran

Putaran pada 2 buah jaringan Feistel pada algoritma ini masing-masing terjadi sebanyak 16 putaran, dengan menggunakan 32 buah kunci internal. Kunci 1 sampai kunci 16 digunakan untuk jaringan fiestel 1 dan kunci 17 sampai kunci 32 digunakan untuk jaringan Feistel 2. Awalnya dari hasil permutasi awal akan dipisah menjadi dua bagian yang masing-masing panjangnya 64 bit. Setiap bagian ini akan memasuki jaringan Feostel. Pada Jaringan Fiestel bagian tersebut dipisah lagi menjadi 2 bagian yang masing-masing panjangnya 32 bit. Proses putaran tersebut dapat dirumuskan sebagai berikut.
L(n) = R(n-1) >> 16
R(n) = L(n-1) xor F(R(n-1), K) >> 16

Fungsi pada setiap putaran F(R, K) adalah berupa fungsi substitusi menggunakan S-box. Terdapat 8 S-box yang digunakan untuk substitusi sehingga dari input 96-bit, setiap 8-bit disubstitusi menggunakan S-box yang berbeda sehingga menghasilkan output 32-bit. Ilustrasi fungsi adalah sebagai berikut:

Gambar 4 - Ilustrasi Fungsi

Untuk pembangkitan key pada setiap putaran, maka diperlukan input key berupa teks dengan panjang sembarang, kemudian dengan menggunakan MD5 untuk encoding sehingga diperoleh list sepanjang 128-bit untuk kunci awal. Dari 128-bit itu, 32-bit digunakan sebagai seed, dan 96-bit digunakan sebagai kunci (K). Pergeseran elemen saat pembangkitan kunci menggunakan barisan Padovan, f(n) = f(n-2) + f(n-3). Illustrasi pembangkitan kunci dapat dilihat sebagai berikut:

4. Simulasi dan Pembahasan Hasil

Implementasi dari block cipher yang dibuat menggunakan bahasa python. Data testing yang digunakan di simpan dalam file dengan *extension* txt. Data test tersebut berisi diambil dari sebuah puisi yang berjudul "Untukmu Ibu Untukmu Ayah" dengan kunci "bisa yok bisa".

Berikut ini adalah teks dari plainteks yang akan di enkripsi:

Untukmu Ibu Untukmu Ayah

sayangmu,.. Kasihmu,.. selalu kau berikan padaku,..
Kau banting tulangmu,..
kau peras keringatmu,..

Namun kau selalu berusaha tersenyum didepanku,..
Walau ku sering mengecewakanmu,..
kau tak pernah berhenti memberi semua itu,..
Kau pun juga tak pernah sedikitpun meminta balasan dariku,..

Karena ku tau,.. kau lakukan semua itu,..
Hanya untuk membuatku bahagia,.
Kau terangi hidupku,..
kau pelita dalam setiap langkahku,..

Plainteks ini di ubah kedalam bentuk bit - bit, kemudian di kelompokan masing-masing 128, untuk kelompok terakhir yang kurang dari 128 bit akan di expand dengan bit 0. Hasil enkripsi dari bit - bit tersebut kemudian dikonversi ke dalam hexadesimal. Berikut ini adalah cipherteks hasil dari enkripsi plainteks tersebut.

D3 3F 48 D8 AA 6F 26 21 42 9E AE 81 30 68 6A 5C FD C9 CA 39 D9 6B 51 92 94 B4 08 E6 D8
93 9B 81 FD 08 70 44 46 45 66 90 3F 3B E1 C2 45 56 28 6D 43 02 68 9E A8 7E A3 41 7B 16 F0
60 31 6E 53 0C 7B 4A 37 0C F4 25 E6 D9 69 51 91 97 18 98 BF A4 19 C4 30 39 B3 6F C6 CF
07 71 C0 76 18 8A 4E E6 95 00 70 B2 40 4C C6 E0 52 65 1C CF D0 E6 7E 29 79 2A F6 0E 68
20 FE 56 28 1A 1D D7 82 C9 DD DB 22 6C B0 B9 99 BE E6 16 F1 C9 4D 6B D8 2F 65 70 18 68
66 56 48 24 FE 8A 1C 31 56 5D 97 52 2F 04 FE 60 16 19 02 64 3C 14 93 3A 22 2F 8D 68 65 DC
44 3C A8 46 1D A5 F4 90 DE 93 06 65 D7 39 74 29 78 24 EB 02 07 09 BE 0E 7C 7E 0C FD E0
FE 0D B1 97 30 2D 1B 29 31 6E 44 40 33 60 CF AD 25 DF 25 45 0F BB 0A 6A 61 36 A6 28 F8
9E 51 94 94 73 F6 59 8E EF 00 23 36 2D 16 E4 20 BC D5 24 E8 CB 26 FA 00 63 9E 9E DC C6

2C 14 93 E6 3A 23 09 1E 1D C7 6A BD 26 7F 09 E8 99 44 6D D3 41 68 91 E5 F1 21 32 C9 AE 61 CC F4 85 61 11 C0 FB AA 06 F3 B0 24 BA 13 AB 22 48 A3 96 AA 76 AC DD 35 6E A2 F0 A9 BC DF 56 62 21 7C 15 29 11 F3 97 84 61 B6 B7 CD 8A F0 8A AE 76 76 C6 62 7D 8E B6 70 8E C1 45 DA 2C 3F 4F C7 74 28 7A FA 8F 65 AB 93 C7 EC 79 2E 26 67 04 FF A8 AA 8A 75 A0 E2 A4 93 90 72 79 A7 47 BF 9E DC 55 7C 5D 3A 29 E1 63 B2 97 F6 B2 6D 42 C7 1C 3A 10 AC 42 29 1A 53 A7 1A 05 97 93 46 0E 6D 05 BC 2E 68 DA 49 9B B2 0B 00 9E D2 3D 7F 44 5E 0C 3E 53 9A 98 0C A2 EF FB AF 50 35 F1 AB 13 6C 59 17 13 E9 62 C8 F3 D6 A5 13 4B BD 33

Proses eksekusi untuk melakukan enkripsi adalah 25.16 s dan waktu untuk mendekripsinya adalah 25.24 s.

5. Analisis Keamanan

5.1. Perubahan Kecil Pada Cipherteks

Misal pada saat dekripsi terjadi kerusakan pada salah satu bit di awal chiperteks contohnya “1” menjadi “0”. Perubahan yang terjadi tidak terlalu signifikan pada hasil dekripsi jika menggunakan kunci yang benar.

Untukmu Ibt(Untukmu Ayah

sayangmu,.. Kasihmu,.. selalu kau berikan padaku,..
Kau banting tulangmu,..
kau peras keringatmu,..

Namun kau selalu berusaha tersenyum didepanku,..
Walau ku sering mengecewakanmu,..
kau tak pernah berhenti memberi semua itu,..
Kau pun juga tak pernah sedikitpun meminta balasan dariku,..

Karena ku tau,.. kau lakukan semua itu,..
Hanya untuk membuatku bahagia,.
Kau terangi hidupku,..
kau pelita dalam setiap langkahku,..

5.2. Perubahan Kecil Pada Kunci

Misal pada saat proses dekripsi kunci yang digunakan salah “bisa yuk bisa”, maka perubahan hasil dekripsi yang terjadi cukup signifikan.

áØ«ïal¡bW«
ûæ~ïx´ÂñÂ-O¯aw½ªR!¤¤!å9-+Â¢Ü{Àh
ÖÂcëÂ0ÌVÚéÅ\ñR&ànoîY/J¦¼¶ý¼g.4qîåC LêDöë÷O½¾Ü¨¾>½ì÷!Üþ
!k0{¬Áîùmûð~gªn<
2°òf3
m\Yq8ôi«nX5yÌ'1m~°fÉPãd¨±$`NZSÌCÐßôÐÑ×?ó
´àç,·ÉÄngVØIx.k®æv£3"AíÂÈ-»[å¼KÈú;eïñ®ätéz±
7ÂTÛe÷_-oºUÖ
úhùä÷PrÇ+ñ Þ$P?v
ZÅÑÔÊ-ÂO%.»0fÿù=qÎLoî²Ù
pT¨'·¥éA®£÷àhÅ ¦Ó´ Â§Ü¤£ÐpOL Êd¦bÑ¡t³J Ü(¿

|ø³GcI¹únðé®G)ÔLÏê¹uU°µîã·{Ü³20»_FÄcÁÙýrï¬£xÀÞ

5.3. Perubahan Kecil pada Plainteks

Misal huruf 'U' terakhir pada kata pertama pada plainteks (Untukmu) berubah menjadi (Untukma) maka terdapat perbedaan 7 byte untuk cipherteks yang dihasilkan.

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

6. Daftar Referensi

[1] Claude E. Shannon, "Communication Theory of Secrecy Systems", *Bell System Technical Journal*, vol. 28-4, pages 656–715, 1949.

[2] Wade Trappe and Lawrence C. Washington, *Introduction to Cryptography with Coding Theory. Second edition.* Pearson Prentice Hall, 2006.

[3] Ninghui Li. Purdue University CS555 Cryptography. Topic 9: Block Cipher Construction and DES.https://www.cs.purdue.edu/homes/ninghui/courses/555_Spring12/handouts/555_Spring12_topic09.ppt

[4] Tutorialspoint.com, Feistel Block Cipher https://www.tutorialspoint.com/cryptography/feistel_block_cipher.htm

[5] Weisstein, Eric W. "Padovan Sequence." From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/PadovanSequence.html

[6] Kuhn T 1998 Density matrix theory of coherent ultrafast dynamics *Theory of Transport Properties of Semiconductor Nanostructures (Electronic Materials* vol 4*)* ed E Schöll (London: Chapman and Hall) chapter 6 pp 173–214

Acknowledgments

Terima kasih atas Tuhan YME, beserta seluruh anggota kelompok Tugas Besar ini sehingga Tugas Besar ini bisa diselesaikan dengan baik dan tepat waktu.