Algoritma Rainy

Algoritma Block Cipher

Hani'ah Wafa
Teknik Informatika / Sekolah Tinggi Elektro dan Informatika
ITB
Bandung, Indonesia
haniahwafa@gmail.com

Dinda Yora Islami
Teknik Informatika / Sekolah Tinggi Elektro dan Informatika
ITB
Bandung, Indonesia
dindayorai@gmail.com

***Abstrak*—Block cipher adalah algoritma kriptografi yang populer digunakan dalam menjaga kerahasiaan pesan. Hal ini dikarenakan block cipher lebih *powerfull* dibandingkan dengan stream cipher. Namun tetap saja algoritma block cipher ini lambat laun dapat terpecahkan. Sehingga banyak kalangan yang mengajukan algoritma-algoritma block cipher yang baru. Makalah ini juga mengajukan algoritma block cipher baru yaitu Rainy yang terinspirasi dari algoritma DES. Algoritma Rainy mengimplementasikan struktur feistel dan menerapkan prinsip *diffusion* dan *confusion*. Algoritma ini menggunakan ukuran block dengan tiga pilihan dan ukuran kunci sebesar 128 bit. Rainy juga dapat beroperasi pada berbagai mode operasi seperti ECB, CBC, CFB, OFB, dan CTR.**

Keywords—kriptografi, block cipher, jaringan feistel, enkripsi, dekripsi, s-box, confusion, diffusion

I. PENDAHULUAN

Setiap orang memiliki informasi yang ingin dirahasiakan dari orang lain. Mereka memiliki berbagai macam cara untuk merahasiakan informasi ini, salah satunya dengan memanfaatkan kriptografi. Kriptografi merupakan ilmu dan seni dalam menjaga keamanan pesan[1]. Kriptografi sudah dipakai dari zaman dahulu. Dalam sejarah tercatat bangsa mesir kuno sekitar 4000 tahun yang lalu telah menggunakan kriptografi untuk menulis pesan di dinding piramida.

Seiring perkembangan teknologi, algoritma yang dahulu dianggap aman sekarang telah bisa dipecahkan, Hal ini menyebabkan munculnya berbagai algoritma kriptografi yang memenuhi standar keamanan. Standar keamanan pada kriptografi meliputi terjaga kerahasiaannya, keasliannya, *authentication*, dan *non repudiation*.

Beberapa algoritma kriptografi yang terkenal yaitu algoritma DEA dan algoritma AES. Algoritma DEA atau yang biasa disebut DES merupakan algoritma cipher block kunci-simetri. Algortima DES ini memanfaatkan struktur feistel sehingga tidak diperlukan algoritma dekripsi yang berbeda dengan enkripsi.

Algoritma standar pengganti DES adalah algoritma AES. AES merupakan algoritma block cipher dengan menggunakan sistem permutasi dan subtitusi. Algoritma AES ini merupakan algoritma buatan pemenang lomba membuat standar algoritma kriptografi baru yang diadakan oleh *National Institute of Standards and Technology (NIST)*.

Pada makalah ini penulis akan membahas sebuah rancangan block cipher yang terinspirasi dari DES yaitu algoritma Rainy. Algoritma ini melakukan cipher berulang dengan round sebanyak 24 kali, memanfaatkan jaringan *Feistel*, dan menerapkan permutasi, serta subtitusi dengan box-S.

II. DASAR TEORI

A. Block Cipher

Block cipher merupakan sebuah fungsi yang memetakan n-bit blok plaintext menjadi n-bit blok ciphertext, dimana n merupakan panjang blok[2]. Panjang kunci yang digunakan untuk melakukan enkripsi sama dengan panjang blok. Algoritma enkripsi menghasilkan blok cipherteks dengan ukuran yang sama dengan blok plainteks.

Blok cipher dapat dijalankan dalam beberapa metode yaitu *Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB) dan Counter Mode*. Berikut penjelasan dari masing-masing cara pengoperasian cipher blok.

1. *Electronic Code Book (ECB)*

   Pada mode *Electronic Code Block* masing-masing blok plainteks di enkripsi dengan kunci yang sama secara independen. Keuntungan dari mode ini adalah tidak perlu mengenkripsi file secara linear dan jika terjadi kesalahan maka hanya mempengaruhi cipherteks yang bersangkutan. Kelemahan dari mode ini yaitu blok plainteks yang sama selalu di enkripsi menjadi blok cipher yang sama sehingga pihak lawan dapat memanipulasi cipherteks.

2. *Cipher Block Chaining (CBC)*

   Pada dasarnya, konsep enkripsi mode CBC sama ECB, namun ada perbedaan bahwa plainteks yang akan dienkripsi terlebih dahulu dilakukan XOR dengan ciphertext fase sebelumnya. Keuntungan menggunakan mode CBC adalah sulit dipecahkan oleh kripanalis. Kelemahan mode CBC adalah jika terjadi kesalahan pada blok ciphertext maka akan mempengaruhi blok ciphertext berikutnya.

3. *Cipher Feedback (CFB)*

   Mode ini mengatasi kelemahan pada mode CBC jika diterapkan pada komunikasi data. Tidak seperti metode sebelumnya mode CFB tidak menggunakan blok plaintext sebagai masukan dari fungsi enkripsi. Pada mode CFB, pada proses enkripsi dan dekripsi keduanya memakai fungsi enkripsi. CFB mengenkripsikan cipher blok seperti pada cipher aliran.

4. *Output Feedback (OFB)*

   Mode OFB mirip dengan mode CFB, kecuali n-bit dari hasil enkripsi terhadap antrian disalin menjadi elemen posisi paling kanan di antrian. Kesalahan 1-bit pada blok plainteks hanya mempengaruhi blok cipherteks yang berkoresponen saja.

5. *Counter Mode*.

   Mode counter tidak melakukan perantaian (chaining) seperti pada CBC. Counter merupakan sebuah nilai berupa blok bit yang ukurannya sama dengan ukuran blok plainteks. Nilai counter harus berbeda dari setiap blok yang di enkripsi.

B. *Jaringan Feistel*

Jaringan Feistel merupakan struktur simetris yang digunakkan dalam pembangunan block cipher. Jaringan Feistel memiliki sifat reversible sehingga tidak perlu membuat algoritma baru untuk mendeskripsikan chiperteks menjadi plaintext.

C. *Confusion dan Diffusion*

Claude Shannon memperkenalkan prinsip *confusion* dan *diffusion* pada makalah klasiknya tahun 1949. Prinsip ini untuk membuat serangan statistik menjadi rumit. Dua prinsip tersebut menjadi panduan dalam merancang algoritma kriptografi.

1. *Confusion*

   Merupakan prinsip yang menyembunyikan hubungan yang ada antara plainteks, cipherteks, dan kunci. Confusion dapat direalisasikan dengan menggunakan algoritma subtitusi yang kompleks.

2. *Diffusion*

   Merupakan prinsip yang menyebarkan pengaruh satu bit plainteks atau kunci ke sebanyak mungkin cipherteks. Salah satu cara diffusion yaitu melakukan operasi permutasi.

D. *S-Box*

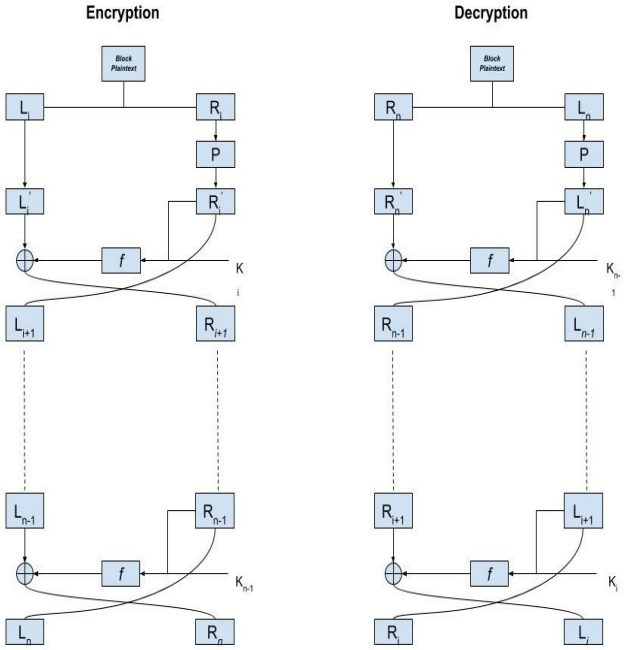
S-Box atau kotak-S adalah matriks yang berisi subtitusi sederhana yang memetakan satu atau lebih bit dengan satu atau lebih bit yang lain. Kotak-S merupakan satu-satunya langkah nirlanjar di dalam algoritma, karena operasinya adalah *look-up table*. Masukan dari operasi *look-up table* dijadikan sebagai indeks kotak-S, dan keluarannya adalah entry di dalam kotak-S.

III. ALGORITMA RAINY

A. Gambaran Umum Algoritma Rainy

Algoritma yang diajukan pada makalah ini menggunakan jaringan feistel dengan ukuran blok fleksibel : 64, 128, dan 256 bit dengan menggunakan kunci dengan ukuran 128 bit, jumlah putaran sebanyak 24 kali dan melakukan permutasi serta subtitusi dengan Box-S.

Alur dari algoritma Rainy adalah menerima inputan plainteks, dan inputan ukuran bloks yang diinginkan. Kemudian plainteks akan dibagi blok-blok dengan ukuran blok sesuai dengan inputan.



Gambar 1. Algoritma Rainy

Proses pada setiap blok di algoritma Rainy sebagai berikut

1. Setiap blok dibagi menjadi blok L_i dan blok R_i seperti pada gambar 1. i merupakan nilai iterasi pada algoritma rainy. Block masuk ke jaringan Feistel
2. Blok R_i mengalami permutasi,
3. Blok R_i hasil permutasi masuk ke fungsi-*f*
4. Dibangkitkan kunci internal sesuai dengan iterasi yang terjadi
5. Kunci internal masuk ke fungsi-*f*
6. Melakukan XOR antara blok L_i dan hasil fungsi-*f*
7. ganti nilai R_{i+1} dengan hasil proses 6 yaitu hasil XOR antara blok L_i dengan hasil fungsi-*f*
8. ganti nilai L_{i+1} dengan hasil fungsi-*f*
9. Ulangi proses 2 sampai 8 sebanyak 24 kali putaran

B. Permutasi

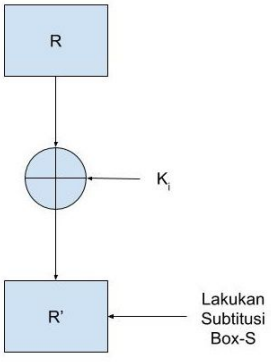
Pada algoritma Rainy memanfaatkan prinsip Diffusion dari Shannon yaitu berupa permutasi. Permutasi yang dilakukan pada algoritma ini berupa

1. Blok R_i disimpan disebuah matriks dengan ukuran nrows x ncols, disini nrow ditetapkan menjadi 4 baris
2. Baris ke i mod 4 dilakukan shift kiri sebanyak i mod column. Dimana column merupakan nilai dari panjang blok R dibagi 4, dan i disini merupakan putaran ke-i
3. Kemudian matriks di gabung lagi menjadi matriks 1 dimensi yang akan menghasilkan R_{i-1}

C. Fungsi F

Fungsi F pada algoritma Rainy terbagi menjadi dua bagian sebagai berikut.

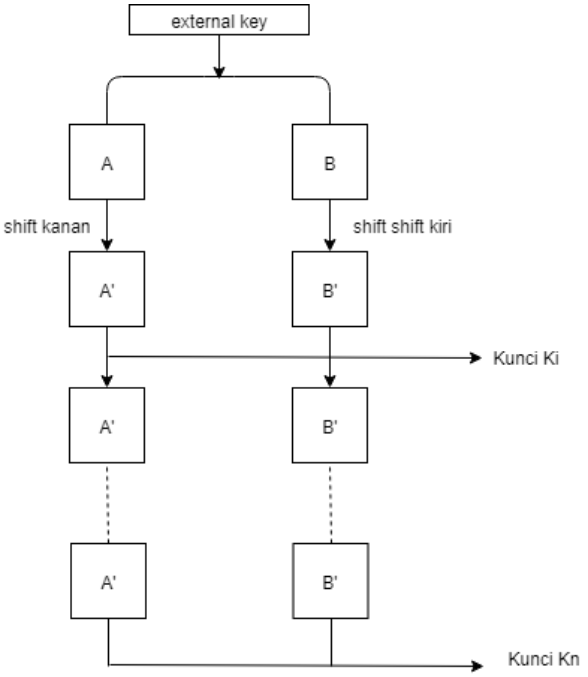
1. Block-R pada iterasi ke-i di xor dengan kunci internal ke-i. Dimana kunci internal ini akan dibangkitkan berdasarkan kunci eksternal dari masukkan pengguna.
2. Lakukan subtitusi block-R dengan menggunakan box-s. Subtitusi dilakukan per 8 bit. Box-s yang digunakan juga dibangkitkan berdasarkan kunci eksternal yang dimasukkan oleh user.



Gambar 2. Fungsi F

D. Pembangkitan Kunci Internal

Untuk menjalankan *fungsi-f* membutuhkan input kunci internal. Kunci internal dibangkitkan dari kunci external yang diinput oleh user. Setiap putaran yang terjadi di jaringan feistel memiliki kunci internal yang berbeda-beda, tergantung pada iterasi nya.



Gambar 3. Pembangkitan kunci internal

Proses pembangkitan kunci internal dilakukan dengan cara:

1. Kunci eksternal dibagi 2 menjadi A dan B seperti pada di gambar 3.
2. A dan B kemudian diubah menjadi matriks dengan ukuran nrows x ncols. nrows ditetapkan dengan nilai 8 baris
3. Lakukan shift kiri pada matriks B dan shift kanan pada matriks A. Jumlah shift yang dilakukan tiap matriks sejumlah fibonaci(i) mod column. Dimana column merupakan nilai dari panjang A atau B dibagi 8, dan i merupakan putaran ke-i
4. Matriks A dan B diubah menjadi matriks dengan ukuran baris sama dengan 1.
5. Gabung matriks A dan B menjadi Kunci K_i

Pembangkitan kunci internal bergantung pada nilai kunci internal putaran sebelumnya. Pada gambar 3 nilai n pada Kn merupakan nilai kunci pada putaran terakhir..

E. Pembangkitan Box-S

Di awal pengeksekusian program, box-s berisi 256 elemen yang berupa bilangan bulat berurutan mulai dari 0 hingga 255. Saat fungsi pembangkitan box-s dipanggil, fungsi akan menerima masukan berupa kata kunci yang dimasukkan oleh pengguna. Kemudian jumlah dari nilai karakter ASCII pada

kunci tersebut akan dijadikan sebagai umpan dalam pembangkitan box_s. Setelah penghitungan umpan selesai, box_s akan di-*shuffle* dengan menggunakan fungsi random.seed(). Box-s yang telah di-*shuffle* tersebut yang kemudian akan digunakan dalam proses subtitusi block pada algoritma Rainy.

IV. SIMULASI DAN PEMBAHASAN HASIL

Pada bagian ini, akan dijelaskan hasil implementasi block cipher yang telah penulis rancang. Eksperimen yang akan dilakukan pada algoritma Rainy menggunakan 5 teknik block cipher, yaitu *Electronic Code Book (ECB), Cipher Block Chaining (CBC), CIpher Feedback (CFB), Output Feedback (OFB), dan mode counter*.

Pada pengujian kali ini digunakan kunci dan plainteks sebagai berikut

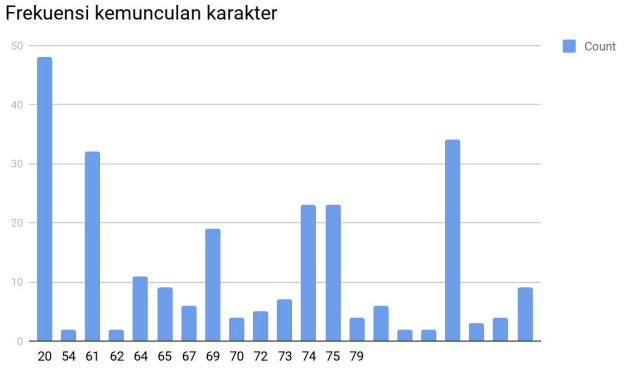
Kunci :

Lagu Naik Delman

Plainteks :

Pada Hari Minggu ku turut ayah ke kota. Naik delman istimewa kududuk di muka. Ku duduk samping pak kusir yang sedang bekerja. Mengendali kuda supaya baik jalannya.Tuk tik tak tik tuk tik tak tik tuk tik tak tik tuk. Tuk tik tak tik tuk tik tak suara sepatu kuda.

Frekuensi plainteks



Gambar 4. Grafik frekuensi kemunculan karakter plainteks

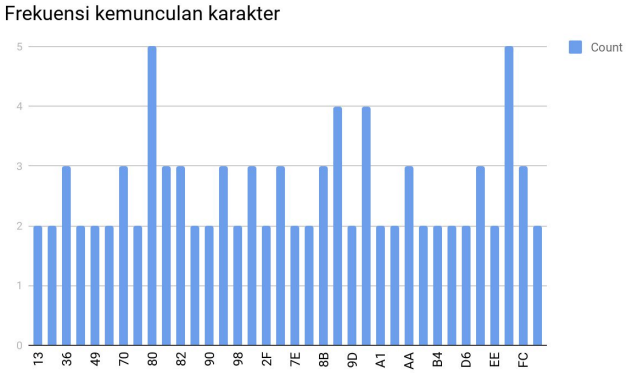
A. Pengujian dengan Mode ECB

Cipherteks dalam heksadesimal :

2F AC 3F 78 B3 B2 C4 84 73 8A A1 19 B5 04 97 69 BA 80 BC EB F4 92 02 84 EA B9 93 03 9B 90 2B 13 9A 56 F1 97 10 1F 6A 39 71 43 7F 2F 39 1D 8C F9 D6 EB 1F 5E 5B 5A 83 8A 6D 33 34 FC 9A 81 F9 94 A1 6B 3E 80 9F AA 36 98 70 B4 A4 FC 9A 81 F9 9D 6A 49 8B 80 9F AA 36 98 70 B4 A4 FC 9A 81 F9 9D 6A 49 8B 80 9F AA 36 C1 A8 21 72 90 CA 7B EE 27 AB 79 82 97 60 B9 FD 82 E5 0C 1B 5F 8B 80 EE B7 DD 44 CC 7E BD 13 FD 31 71 F9 D9 4D B1 EB 58 0E D6 12 61 57 61 34 9F 9C 25 66 42 89 E2 B3 F5 FB 7E 82 B8 70 2D 1F 2A 0D 0A

Waktu eksekusi enkripsi : 0.17453289031982422 detik Waktu eksekusi dekripsi : 0.15166020393371582 detik

Analisis Frekuensi



Gambar 5. Grafik frekuensi kemunculan karakter hasil enkripsi dengan metode ECB

B. Pengujian dengan Mode CBC

Cipherteks dalam heksadesimal :

03 25 9D 1D F1 EB 72 42 62 7E 95 49 7C 54 B7 F6 E0 C4 F7 50 4E E0 BF 6A 57 CD 7A 57 56 1A 2F B2 96 77 0F 8C 3D EE 27 90 49 98 0D 0A 16 BB EE DF D4 15 4A B9 96 0D 0A D2 72 E2 82 D1 86 2A 86 2B 7A C9 9B 35 45 BA 5A D3 87 C9 37 0F A7 04 9E 17 FB 6F D0 B4 03 80 D7 10 02 D5 86 48 34 5B DB F0 4F 43 94 F0 77 86 6E 88 F8 44 AD F3 A9 4E E8 79 12 8B 8C D3 CD 68 C7 DB B1 1F 9B 0D 0A B3 D7 4B BA F6 5D 3A 36 D2 C2 01 FB A2 DC 58 83 3B F0 A6 BC FC 3E 3A 7B 7E 6C 43 23 D3 24 96 BF D2 BD A9 98 78 55 1F FA 51 39 B5 E9 81 AF ED AD 6D B4 F1 71 E3 05 66 DC C7 50 D4 96 CC 4C E6 65 70 DD F8 0D 0A 20 7B 82 E6 76 81 8E 89 28 61 1C E0 3C 60 EE 8D B4 A7 77 0D 0A 6C E2 6E 10 17 59 FF DA 3A 46 0D 0A 4F 32 F4 14 F5 EB F8 BC 6B 23 B0 85 BF 12 22 56 0C 6A 27 85 32 E8 11 E9 44 3E 7A E9 95 A6 97 E0 15 BA 89 92 3F 04 03 30 A0 0D 0A 01 3A 9D

Waktu eksekusi enkripsi : 0.31986117362976074 detik Waktu eksekusi dekripsi : 0.1511368751525879 detik

Analisis Frekuensi

Gambar 6. Grafik frekuensi kemunculan karakter hasil enkripsi dengan metode CBC

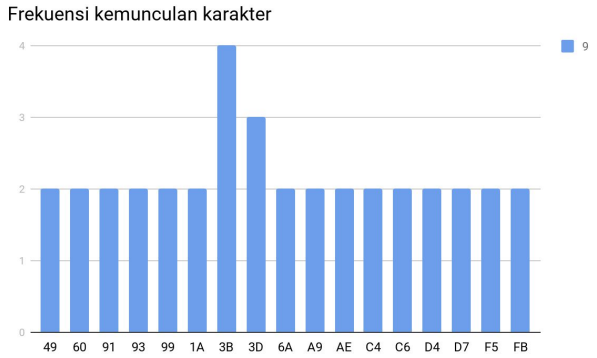
C. Pengujian dengan Mode CFB

Cipherteks dalam heksadesimal :

03 25 9D 1D F1 EB 72 42 62 7E 95 49 7C 54 B7 F6 E0 C4 F7 50 4E E0 BF 6A 57 CD 7A 57 56 1A 2F B2 96 77 0F 8C 3D EE 27 90 49 98 0D 0A 16 BB EE DF D4 15 4A B9 96 0D 0A D2 72 E2 82 D1 86 2A 86 2B 7A C9 9B 35 45 BA 5A D3 87 C9 37 0F A7 04 9E 17 FB 6F D0 B4 03 80 D7 10 02 D5 86 48 34 5B DB F0 4F 43 94 F0 77 86 6E 88 F8 44 AD F3 A9 4E E8 79 12 8B 8C D3 CD 68 C7 DB B1 1F 9B 0D 0A B3 D7 4B BA F6 5D 3A 36 D2 C2 01 FB A2 DC 58 83 3B F0 A6 BC FC 3E 3A 7B 7E 6C 43 23 D3 24 96 BF D2 BD A9 98 78 55 1F FA 51 39 B5 E9 81 AF ED AD 6D B4 F1 71 E3 05 66 DC C7 50 D4 96 CC 4C E6 65 70 DD F8 0D 0A 20 7B 82 E6 76 81 8E 89 28 61 1C E0 3C 60 EE 8D B4 A7 77 0D 0A 6C E2 6E 10 17 59 FF DA 3A 46 0D 0A 4F 32 F4 14 F5 EB F8 BC 6B 23 B0 85 BF 12 22 56 0C 6A 27 85 32 E8 11 E9 44 3E 7A E9 95 A6 97 E0 15 BA 89 92 3F 04 03 30 A0 0D 0A 01 3A 9D

Waktu eksekusi enkripsi : 0.1830599308013916 detik
Waktu eksekusi dekripsi : 0.19382166862487793 detik

Analisis Frekuensi



Gambar 7. Grafik frekuensi kemunculan karakter hasil enkripsi dengan metode CFB

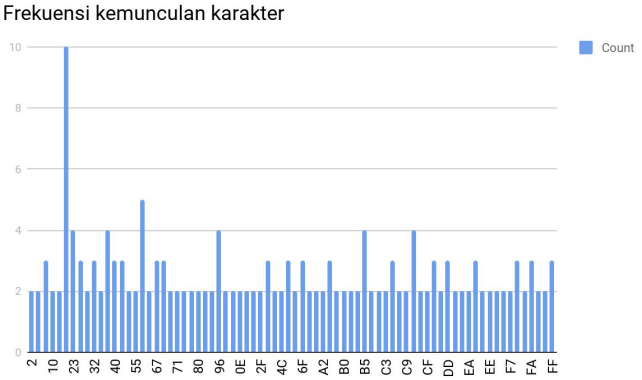
D. Pengujian dengan Mode OFB

Cipherteks dalam heksadesimal :

89 10 02 67 0F 58 FE 71 F6 4F CD 30 4C 33 F6 58 AC FA F0 2B D3 32 51 38 C0 86 25 4B A6 B5 BF B6 A1 16 61 F9 35 6F B5 73 9B B3 3F 7A 97 67 44 B4 02 CE 8E E3 FA C9 B0 3C FF 1B 0E 0D 0A 2E CD 79 EB FF 2C 1A 52 14 23 8C 68 88 C6 16 27 A4 6A 44 88 D6 DA DD F4 ED FE 6F 5E E3 A7 E9 F7 99 CC 33 96 1C DD 72 3F A7 60 5B 55 01 30 0F 67 58 FF C4 C4 F7 90 64 CD B5 EE EC A4 46 5A B7 9C 39 C8 EA 50 FA BF F0 55 92 85 3A 2F D8 D1 F8 E0 AD 96 06 40 C3 EA 2F 20 D8 43 96 90 74 CF 3D 72 ED 0E AE 10 31 06 71 E2 6A 30 40 DD 78 42 1B F9 20 40 20 20 20 20 20 20 CD 6C 64 C9 A5 06 E9 E5 C4 5D 68 04 68 0D 0A 58 23 23 B3 65 D9 20 20 17 04 96 93 3E 80 BA 5C 37 4B 35 D0 0B 7C 77 69 6E CE CF FB B7 80 23 9C 48 B0 E1 D3 C7 B5 35 EC 84 4C A2 31 F8 69 7E D3 9A C7 EE DB 26 32 EC 58 C1 AB FB F8 A4 45 C3 A2 9A 74 4F 4F 35 19 66 6F 22 32 59 3F 7B B1 52 44 B1

Waktu eksekusi enkripsi : 0.18407583236694336 detik
Waktu eksekusi dekripsi : 0.20818471908569336 detik

Analisis Frekuensi



Gambar 8. Grafik frekuensi kemunculan karakter hasil enkripsi dengan metode OFB

E. Pengujian dengan Mode Counter

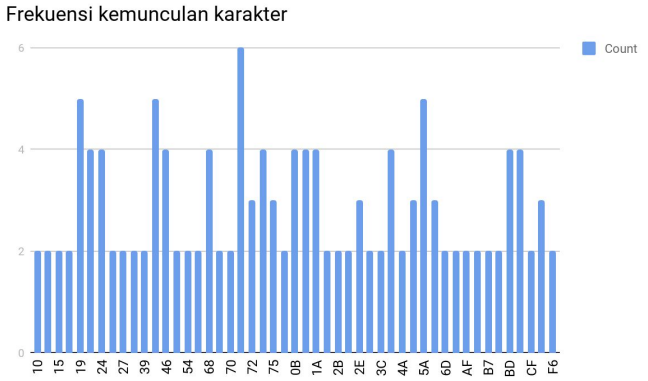
Cipherteks dalam heksadesimal :

69 5B 2E 17 C9 56 B7 6B CF 7E 4F 31 17 B4 26 46 3C 4D 6C 75 B3 75 C5 7E 40 21 5C AC 15 13 6D 0F 2B 50 AF 75 A3 69 C5 70 0B 1F A8 F9 15 13 62 5A 24 19 BA 79 BB 72 CD 30 4C 74 54 B8 1A 46 6D 5A 3C 50 71 38 AF 63 CA 39 0B 27 01 61 0F 2D 5C 40 7D A4 68 C5 70 0B 19 0F B7 16 03 68 4B 2E 55 37 38 BD 77 C0 3F 0B 27 33 A9 10 1F 67 0F 2D 58 9D 73 F6 68 C5 32 4A 3A 68 A0 10 48 52 5A 24 19 42 71 BD 22 D0 3F 40 74 E5 B0 1A 46 72 5A 24 19 E8 71 BD 22 D0 3F 40 74 BA B0 1A 46 72 5A 24 19 1A 71

BD 22 D0 3F 40 74 54 26 5C 3A 58 80 79 F6 71 C1 2E 4A 20 11 D9 71 66 06 2F 4F 39 D4 18 D6 22 CF 2B 4F 35 E9

Waktu eksekusi enkripsi : 0.19124937057495117 detik
Waktu eksekusi dekripsi : 0.17771673202514648 detik

Analisis Frekuensi.



Gambar 9. Grafik frekuensi kemunculan karakter hasil enkripsi dengan metode Counter

Berdasarkan hasil eksperimen dengan menggunakan metode *Electronic Code Book (ECB), Cipher Block Chaining (CBC), CIpher Feedback (CFB), Output Feedback (OFB), dan mode counter* bahwa metode yang waktu eksekusi nya paling efisien adalah dengan metode *Electronic Code Block (ECB)*.

Frekuensi kemunculan karakter cipherteks dapat kita lihat pada gambar 5 yang memanfaatkan metode ECB, gambar 6 memanfaatkan CBC, gambar 7 memanfaatkan CFB, dan gambar 8 memanfaatkan OFB serta gambar 9 yang memanfaatkan metode Counter. Dari grafik dapat kita lihat bahwa frekuensi kemunculan karakter hampir merata sehingga akan menyulitkan kriptanalis dalam menganalisis cipherteks dengan teknik analisis frekuensi.

V. ANALISIS KEAMANAN

A. Analisis Difusi dan Konfusi

1) Perubahan Satu Bit Kunci

Plainteks :

Pada Hari Minggu ku turut ayah ke kota. Naik delman istimewa kududuk di muka. Ku duduk samping pak kusir yang sedang bekerja. Mengendali kuda supaya baik jalannya.Tuk tik tak tik tuk tik tak tik tuk tik tak tik tuk. Tuk tik tak tik tuk tik tak suara sepatu kuda.

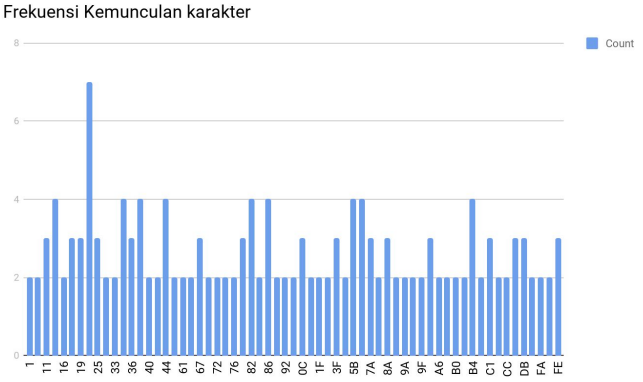
Kunci Pertama :

Lagu Naik Delman

Hasil Cipherteks Pertama :

8C 71 85 45 05 4D E2 58 46 D6 60 B0 6B 37 9F BA 69 B5 72 CB D3 7A E8 8C 0F 94 7D 1C A9 7F F0 BE 80 FA DB EC 94 89 DC 8C 01 64 74 2E B7 20 20 20 20 36 FE 62 0E D3 48 46 E8 90 BE 67 7F 99 82 2C B7 E7 ED F8 2F AC 3F 78 B3 B2 C4 84 73 8A A1 19 B5 04 97 69 BA 80 BC EB F4 92 02 84 EA B9 93 03 9B 90 2B 13 9A 56 F1 97 10 1F 6A 39 71 43 7F 2F 39 1D 8C F9 D6 EB 1F 5E 5B 5A 83 8A 6D 33 34 FC 9A 81 F9 94 A1 6B 3E 80 9F AA 36 98 70 B4 A4 FC 9A 81 F9 9D 6A 49 8B 80 9F AA 36 98 70 B4 A4 FC 9A 81 F9 9D 6A 49 8B 80 9F AA 36 C1 A8 21 72 90 CA 7B EE 27 AB 79 82 97 60 B9 FD 82 E5 0C 1B 5F 8B 80 EE B7 DD 44 CC 7E BD 13 FD 31 71 F9 D9 4D B1 EB 58 0E D6 12 61 57 61 34 9F 9C 25 66 42 89 E2 B3 F5 FB 7E 82 B8 70 2D 1F 2A

Analisis Frekuensi



Gambar 10. Grafik frekuensi kemunculan karakter

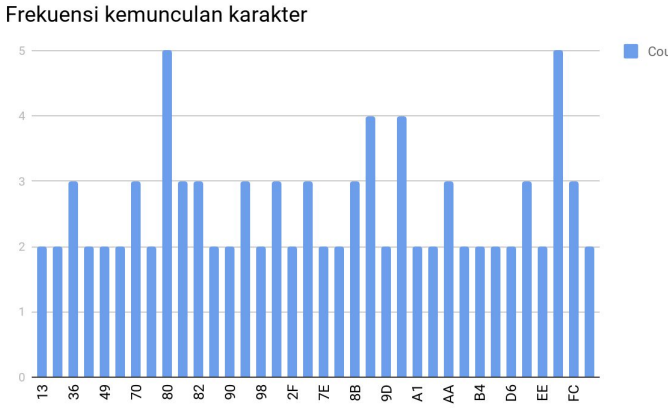
Kunci Kedua :

Lagu Naik Delmas

Hasil Cipherteks Kedua :

2F AC 3F 78 B3 B2 C4 84 73 8A A1 19 B5 04 97 69 BA 80 BC EB F4 92 02 84 EA B9 93 03 9B 90 2B 13 9A 56 F1 97 10 1F 6A 39 71 43 7F 2F 39 1D 8C F9 D6 EB 1F 5E 5B 5A 83 8A 6D 33 34 FC 9A 81 F9 94 A1 6B 3E 80 9F AA 36 98 70 B4 A4 FC 9A 81 F9 9D 6A 49 8B 80 9F AA 36 98 70 B4 A4 FC 9A 81 F9 9D 6A 49 8B 80 9F AA 36 C1 A8 21 72 90 CA 7B EE 27 AB 79 82 97 60 B9 FD 82 E5 0C 1B 5F 8B 80 EE B7 DD 44 CC 7E BD 13 FD 31 71 F9 D9 4D B1 EB 58 0E D6 12 61 57 61 34 9F 9C 25 66 42 89 E2 B3 F5 FB 7E 82 B8 70 2D 1F 2A

Analisis Frekuensi



Gambar 11. Grafik frekuensi kemunculan karakter

2) Perubahan Satu Bit Plainteks
Kunci :

Lagu Naik Delman

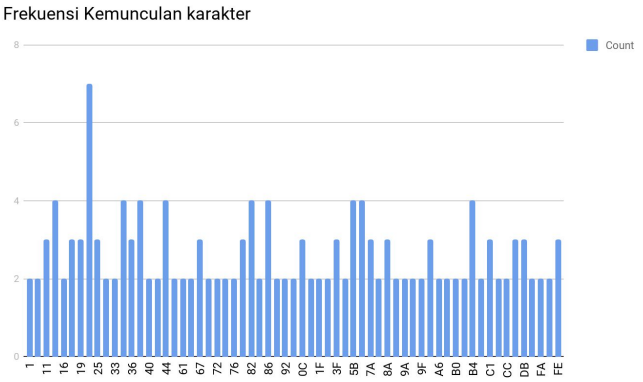
Plainteks Pertama :

Pada Hari Minggu ku turut ayah ke kota. Naik delman istimewa kududuk di muka. Ku duduk samping pak kusir yang sedang bekerja. Mengendali kuda supaya baik jalannya.Tuk tik tak tik tuk tik tak tik tuk tik tak tik tuk. Tuk tik tak tik tuk tik tak suara sepatu kuda.

Hasil Cipherteks Pertama :

8C 71 85 45 05 4D E2 58 46 D6 60 B0 6B 37 9F BA 69 B5 72 CB D3 7A E8 8C 0F 94 7D 1C A9 7F F0 BE 80 FA DB EC 94 89 DC 8C 01 64 74 2E B7 20 20 20 20 36 FE 62 0E D3 48 46 E8 90 BE 67 7F 99 82 2C B7 E7 ED F8 2F AC 3F 78 B3 B2 C4 84 73 8A A1 19 B5 04 97 69 BA 80 BC EB F4 92 02 84 EA B9 93 03 9B 90 2B 13 9A 56 F1 97 10 1F 6A 39 71 43 7F 2F 39 1D 8C F9 D6 EB 1F 5E 5B 5A 83 8A 6D 33 34 FC 9A 81 F9 94 A1 6B 3E 80 9F AA 36 98 70 B4 A4 FC 9A 81 F9 9D 6A 49 8B 80 9F AA 36 98 70 B4 A4 FC 9A 81 F9 9D 6A 49 8B 80 9F AA 36 C1 A8 21 72 90 CA 7B EE 27 AB 79 82 97 60 B9 FD 82 E5 0C 1B 5F 8B 80 EE B7 DD 44 CC 7E BD 13 FD 31 71 F9 D9 4D B1 EB 58 0E D6 12 61 57 61 34 9F 9C 25 66 42 89 E2 B3 F5 FB 7E 82 B8 70 2D 1F 2A

Analisis Frekuensi



Gambar 12. Grafik frekuensi kemunculan karakter

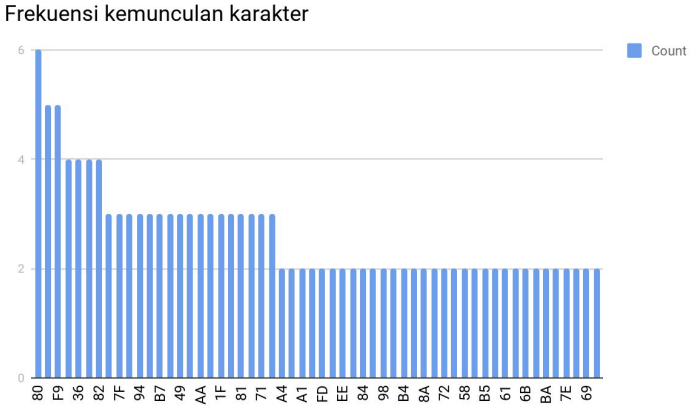
Plainteks Kedua :

Qada Hari Minggu ku turut ayah ke kota. Naik delman istimewa kududuk di muka. Ku duduk samping pak kusir yang sedang bekerja. Mengendali kuda supaya baik jalannya.Tuk tik tak tik tuk tik tak tik tuk tik tak tik tuk. Tuk tik tak tik tuk tik tak suara sepatu kuda.

Hasil Cipherteks Kedua :

49 71 85 45 05 4D E2 58 C1 D6 60 B0 6B 37 9F BA 69 B5 72 CB D3 7A E8 8C 0F 94 7D 1C A9 7F F0 BE 80 FA DB EC 94 89 DC 8C 01 64 74 2E B7 20 20 20 20 36 FE 62 0E D3 48 46 E8 90 BE 67 7F 99 82 2C B7 E7 ED F8 2F AC 3F 78 B3 B2 C4 84 73 8A A1 19 B5 04 97 69 BA 80 BC EB F4 92 02 84 EA B9 93 03 9B 90 2B 13 9A 56 F1 97 10 1F 6A 39 71 43 7F 2F 39 1D 8C F9 D6 EB 1F 5E 5B 5A 83 8A 6D 33 34 FC 9A 81 F9 94 A1 6B 3E 80 9F AA 36 98 70 B4 A4 FC 9A 81 F9 9D 6A 49 8B 80 9F AA 36 98 70 B4 A4 FC 9A 81 F9 9D 6A 49 8B 80 9F AA 36 C1 A8 21 72 90 CA 7B EE 27 AB 79 82 97 60 B9 FD 82 E5 0C 1B 5F 8B 80 EE B7 DD 44 CC 7E BD 13 FD 31 71 F9 D9 4D B1 EB 58 0E D6 12 61 57 61 34 9F 9C 25 66 42 89 E2 B3 F5 FB 7E 82 B8 70 2D 1F 2A

Analisis Frekuensi



Gambar 13. Grafik frekuensi kemunculan karakter

3) Perubahan Panjang Block yang Digunakan

Plainteks :

Pada Hari Minggu ku turut ayah ke kota. Naik delman istimewa kududuk di muka. Ku duduk samping pak kusir yang sedang bekerja. Mengendali kuda supaya baik jalannya.Tuk tik tak tik tuk tik tak tik tuk tik tak tik tuk. Tuk tik tak tik tuk tik tak suara sepatu kuda.

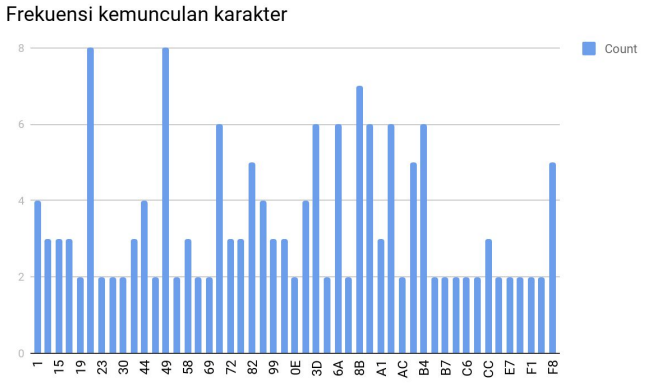
Kunci :

Lagu Naik Delman

Cipherteks dengan Panjang Block 64 Bits:

E2 95 45 74 B0 72 0D 0A A1 75 15 20 20 20 20 20 BA 42 32 97 16 BA A8 E6 20 8C AB F8 DC 31 B1 30 B0 0E 6F A9 AF 3D 80 9E A1 F6 01 F2 BB AE 90 20 3F F3 8A 69 7A 19 44 43 E1 F8 93 D8 30 42 81 CE 3A 1B EF A5 EA B4 62 18 AD 11 F1 9A 24 17 71 A2 06 12 E7 B5 22 6C 57 11 61 9A 98 C6 5A A7 F2 58 57 BC 2A AC B0 54 37 14 CB 94 9A B6 99 6E 3D CB 15 17 66 C3 8E 3D A6 72 E3 8B 99 6F 88 01 CF 29 B2 E9 F4 50 69 D1 E2 EB 0F 17 3B 19 99 ED 45 29 15 61 B0 A4 80 D2 4E 8B 01 9A ED F7 6D 33 34 F1 A1 6B 3E F8 70 B4 A4 49 6A 49 8B 94 70 B4 A4 3D 6A 49 8B F8 70 B4 A4 49 6A 49 8B 94 70 B4 A4 3D 6A 49 8B F8 70 B4 A4 49 6A 49 8B 94 70 E7 72 3D 6A 83 82 65 9A 0C 1B 11 82 44 CC 82 B0 0C 1B B7 23 44 CC 82 9A 0C 1B B7 82 44 CC F5 E5 23 0E 42 DD 20 D0 C6 80 BF A0 4E 01 2E DF 1E 58 4A 58 26 B6 AC EC

Analisis Frekuensi

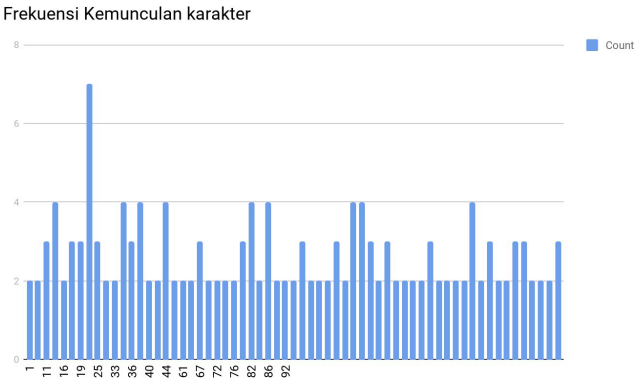


Gambar 14. Grafik frekuensi kemunculan karakter

Cipherteks dengan Panjang Block 128 Bits:

8C 71 85 45 05 4D E2 58 46 D6 60 B0 6B 37 9F BA 69 B5 72 CB D3 7A E8 8C 0F 94 7D 1C A9 7F F0 BE 80 FA DB EC 94 89 DC 8C 01 64 74 2E B7 20 20 20 20 36 FE 62 0E D3 48 46 E8 90 BE 67 7F 99 82 2C B7 E7 ED F8 2F AC 3F 78 B3 B2 C4 84 73 8A A1 19 B5 04 97 69 BA 80 BC EB F4 92 02 84 EA B9 93 03 9B 90 2B 13 9A 56 F1 97 10 1F 6A 39 71 43 7F 2F 39 1D 8C F9 D6 EB 1F 5E 5B 5A 83 8A 6D 33 34 FC 9A 81 F9 94 A1 6B 3E 80 9F AA 36 98 70 B4 A4 FC 9A 81 F9 9D 6A 49 8B 80 9F AA 36 98 70 B4 A4 FC 9A 81 F9 9D 6A 49 8B 80 9F AA 36 C1 A8 21 72 90 CA 7B EE 27 AB 79 82 97 60 B9 FD 82 E5 0C 1B 5F 8B 80 EE B7 DD 44 CC 7E BD 13 FD 31 71 F9 D9 4D B1 EB 58 0E D6 12 61 57 61 34 9F 9C 25 66 42 89 E2 B3 F5 FB 7E 82 B8 70 2D 1F 2A

Analisis Frekuensi

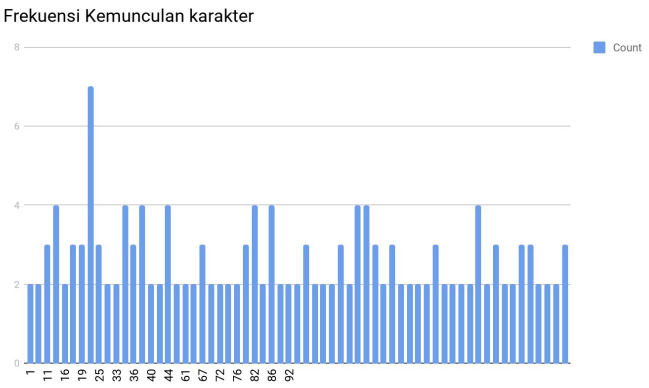


Gambar 15. Grafik frekuensi kemunculan karakter

Cipherteks dengan Panjang Block 256 Bits:

E2 6D B4 0C 9C BF 7A 58 34 3A 9E 36 B9 16 55 0E B0 A1 B4 F5 2E 11 28 9F 41 FE D0 1F 97 18 43 A0 37 80 33 A1 03 68 18 90 48 81 75 40 E7 20 14 DB 8A 01 96 BB 61 95 DC AB 92 E5 81 64 8F 97 78 9B B4 62 0C 91 38 85 66 6D 11 20 36 25 3D D2 A3 82 11 F1 12 34 A6 5E 06 34 DB B3 87 49 9A 7B 99 12 74 71 3F 01 FE 5B 61 A8 47 E8 18 25 98 A2 C8 8C 75 77 AB 3F 7C 8A FF 40 D3 DA 8E 76 EE 67 4E 44 FA 88 6D D7 A6 C1 4F 04 12 69 C6 FA 19 37 06 FB 54 B2 FE 2D 19 62 B2 C8 E4 DB A7 B4 2C C1 3F 76 8A 6D 33 34 D1 9A 81 F9 6A 5B 68 82 7A 37 3E 16 94 A1 6B 3E 83 9F AA 36 4E 7A 20 5B C1 EF B5 0D 0A 9C 25 12 26 CC 37 67 44 F7 1F 86 82 91 8C 30 28 FB 7E F0 86 53 65 F1 67 29 35 CF 52 86 DD 72 D9 82 7B 0C 1B 83 55 B0 D2 19 43 5B 72 20 20 20 20 B9 2F 92 B7 4A 44 CC C9 B1 0E D2 F3 4C 44 50 C3 86 73

Analisis Frekuensi



Gambar 16. Grafik frekuensi kemunculan karakter

Dari ketiga jenis perubahan di atas dapat dilihat bahwa hanya dengan pengubahan satu bit pada kunci atau pengubahan satu bit pada plainteks yang digunakan dalam melakukan enkripsi ternyata dapat memberikan perubahan yang cukup signifikan pada cipherteks yang dihasilkan. Begitu pula dengan pengubahan panjang block yang digunakan dalam melakukan enkripsi. Ciphertext yang dihasilkan akan berbeda secara cukup signifikan antara enkripsi dengan penggunaan block sepanjang 64 bit, 128 bit, maupun 256 bit.

B. Analisis *Brute Force Attack*

Brute force attack adalah jenis serangan yang menggunakan metode trial-and-error untuk mendapatkan informasi yang diinginkan. Pada brute force attack, software digunakan untuk menghasilkan semua kemungkinan tebakan kunci untuk dapat melakukan deskripsi terhadap ciphertext. Dengan menggunakan jenis serangan ini, kunci dapat ditemukan oleh penyerang, tapi dengan waktu yang sangat lama.

Algoritma Rainy menggunakan kunci dengan panjang 64 bit, sehingga akan ada 2^{64} atau 1,8446744 x 10^{19} kemungkinan kunci yang perlu dicoba oleh penyerang. Selain itu, algoritma rainy juga memiliki tiga pilihan ukuran panjang block untuk melakukan enkripsi. Sehingga kemungkinan yang harus dicoba oleh penyerang ada sebanyak 3 x 1,8446744 x 10^{19} atau 55.340.232 x 10^{7}. Dengan asumsi bahwa mesin yang digunakan membutuhkan waktu 0,1 detik untuk melakukan dekripsi, maka untuk mencoba seluruh kemungkinan tersebut penyerang akan membutuhkan waktu sebanyak 55.340.232 x 10^{6} detik atau 640.511.944 hari atau 1.779.200 tahun.

Waktu yang dibutuhkan penyerang dalam melakukan serangan ini sangatlah lama, sehingga dapat dikatakan bahwa algoritma rainy hampir tidak mungkin dapat dipecahkan dengan melakukan *brute force attack*.

VI. KESIMPULAN DAN SARAN PENGEMBANGAN

Penggunaan algoritma block cipher dalam kriptografi dapat membuat keamanan pesan lebih terjaga. Hal ini dikarenakan algoritma block cipher akan membuat relasi antara plaintext dan ciphertext semakin samar, sehingga akan menyulitkan kriptanalis dalam memecahkan ciphertext.

Berdasarkan hasil simulasi dan analisa yang telah dilakukan, penggunaan prinsip konfusi dan difusi membuat frekuensi kemunculan karakter di cipherteks menjadi tidak terlalu berbeda signifikan antara karakter yang satu dengan yang lain. Namun perlu lebih diperhatikan lagi desain yang digunakan dalam mengimplementasikan prinsip konfusi dan difusi tersebut agar, perbedaan frekuensi kemunculan karakter pada plaintext menjadi serata mungkin. Pilihan penggunaan ukuran block yang beragam juga membuat ciphertext yang dihasilkan menjadi lebih tidak dapat terprediksi.

Selain hal di atas penggunaan s-box yang bersifat dinamis juga disarankan untuk membuat relasi antara plaintext dengan ciphertext menjadi semakin samar dan algoritma cipher block yang dibuat menjadi lebih sulit untuk dipecahkan oleh kriptanalis.

VII. UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Allah SWT, karena berkat rahmat dan karunianya makalah ini dapat selesai pada waktunya. Tak lupa juga, penulis ingin menyampaikan terima kasih kepada Bapak Dr. Ir. Rinaldi Munir, MT selaku dosen mata kuliah IF4020 Kriptografi yang telah membagikan ilmunya kepada penulis. Selain itu, penulis juga ingin menyampaikan terima kasih kepada kedua orang tua yang selalu mendukung penulis.

REFERENCES

[1] A. Menezes, P. van Oorschot, dan S. Vanstone. 1996. Handbook of Applied Cryptography. CRC Press

[2] Munir, Rinaldi. 2019. Slide Kuliah IF4020 Kriptografi: Algoritma Kriptografi Modern.

[3] Munir, Rinaldi. 2019. Slide Kuliah IF4020 Kriptografi: Pengantar Kriptografi.

[4] Nurezkapahlevi (2012, 25 April). *Kriptografi Simetrik :Dasar Block Cipher*. Dikutip 12 Maret 2019 dari Kriptografi dan Keamanan Informasi : https://ilmukriptografi.wordpress.com/2012/04/25/kriptografi-simetrik-dasar-block-cipher/

[5] Michael Hamburg (2014, 27 Desember). Dikutip 12 Maret 2019 dari https://www.quora.com/Cryptography-What-are-the-advantages-and-disadvantages-of-block-ciphers-over-stream-ciphers

[6] *Brute Force Attack*. Dikutip 13 Maret 2019 dari https://www.techopedia.com/definition/18091/brute-force-attack

PERNYATAAN

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

Bandung, 13 Maret 2019

Hani'ah Wafa
13516053

Dinda Yora Islami
13516067