Blox: Algoritma Block Cipher

Fikri Aulia(13513050)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung,
Jl. Ganesha 10 Bandung 40132,
13513050@std.stei.itb.ac.id

Adin Baskoro Pratomo (13513058)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung,
Jl. Ganesha 10 Bandung 40132,
13513058@std.stei.itb.ac.id

***Abstract*—Makalah ini membahas mengenai rancangan algoritma blok cipher baru. Algoritma ini menggunakan blok dengan ukuran 128 bit. Blok ininantinya akan diubah dengan menggunakan jaringan feistel. Untuk setiap byte ganjil pada blok akan dipertukarkan dengan byte yang berada kanannya. Selanjutnya blok akan di XOR dengan kunci, dan kemudian hasil XOR akan digeser ke kanan sebesar satu blok. Setelah byte-byte pada blok digeser, blok akan disubtitusikan dengan menggunakan S-Box dan kemudian di XOR kan kembali dengan kunci. Pada algoritma ini, terdapat 3 mode operasi yang dapat digunakan. Yaitu mode Electronic Code Book, Chain Block Cipher, dan Cipher-Feedback 8bit.**

Kata kunci—block cipher, enkripsi, subtitusi, plaintext, ciphertext

I. PENDAHULUAN

Kriptografi (cryptography) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu kripto dan graphia. Kripto artinya menyembunyikan, sedangkan graphia artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data .Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi.

Seiring dengan semakin berkembangkan internet saat ini, keamanan informasi menjadi salah satu topik penting yang harus diperhatikan. informasi atau pesan yang ditransmisikan dari suatu tempat ke tempat lain melalui banyak jaringan sangat rentan terhadap penyadapan sehingga menimbulkan banyak masalah dan kerugian. cara yang umum dipakai untuk mengamankan informasi tersebut adalah dengan menggunakan teknik kriptografi. beberapa teknik yang dapat digunakan salah satunya adalah teknik Block Cipher.

Block Cipher merupakan cara kriptografi untuk melakukan enkripsi dan dekripsi kepada sebuah pesan dengan cara membagi pesan-pesan tersebut ke dalam beberapa blok. Tiap blok dapat mempengaruhi hasil enkripsi berikutnya sehingga jika blok yang dikirim sama, belum tentu hasil enkripsi blok tersebut sama juga. Makalah ini akan membahas mengenai algoritma cipher baru yang menggunakan prinsip Chain Block Cipher sehingga hasil enkripsi dari suatu block akan mempengaruhi block selanjutnya. selain itu, algoritma block cipher ini akan menggunakan prinsip jaringan feistel dan s-Box untuk memperkuat algoritma sehingga sulit untuk dipecahkan.

II. DASAR TEORI

A. Cipher Block

Algoritma cipher block merupakan salah satu cara kriptografi yang membagi pesan-pesan yang akan diubah menjadi blok-blok pesan dengan ukuran tertentu. sekalin itu, keluaran dari proses kriptografi blok ini akan berupa blok-blok pesan. sehingga akan memudahkan pengiriman pada suatu jaringan.

Cipher block pada umumbya terbagi menjadi tiga jenis yaitu, Electronic Code Block (ECB), Cipher Block Chaining (CBC), Cipher-Feedback (CFB), dan Output-Feedback(OFB).

pada ECB, setiap block dienkripsi dan dideskripsi secara independen dengan cara memasukkan blok ke dalam suatu fungsi, yang nantinya akan emnjadi blpk cipher. pada ECB, hasil suatu enkripsi blok tidak akan mempengaruhi proses enkripsi blok yang lain. penggunaan metode ini kurang aman karena setiap blok yang sama akan menghasilkan blok cipher text yang sama pula. sehingga dapat dipecahkan dengan analisa kriptanalis.

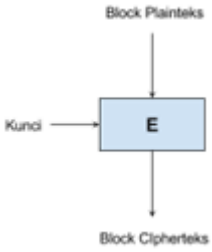


Figure 1. Electronic Code Block (ECB)[Algoritma Kripto Modern, oleh M, Rinaldi. 2015]

Pada metode CBC, tiap blok bergantung dengan blok yang lain dalam enkripsi dan dekripsinya. Enkripsi dan dekripsi pada metode ini membutuhkan sebuah blok baru yang disebut IV (*Initialization Vector*) yang akan digunakan pada XOR pertama tahap dekripsi maupun enkripsi. Selanjutnya nilai yang di XOR kan dengan blok berikutnya adalah blok sebelumnya.

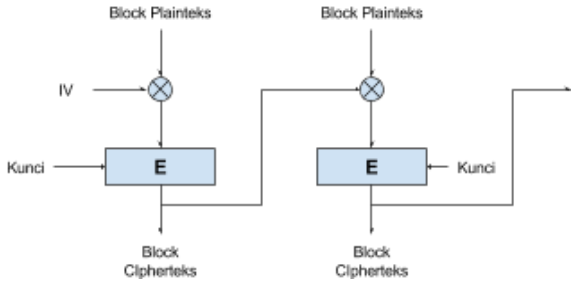


Figure 2. Cipher Block Chaining(CBC) [Algoritma Kripto Modern, oleh M, Rinaldi. 2015]

Pada CFB, metode ini memperbaiki kelemahan yang ada pada metode CBC, seperti jika terjadi blok yang belum lengkap dan mengurangi kesalahan dekripsi data jika data rusak selama perjalanan. Metode ini dapat bekerja pada unit-unit blok yang cukup kecil sehingga dapat menyerupai *stream-cipher*.

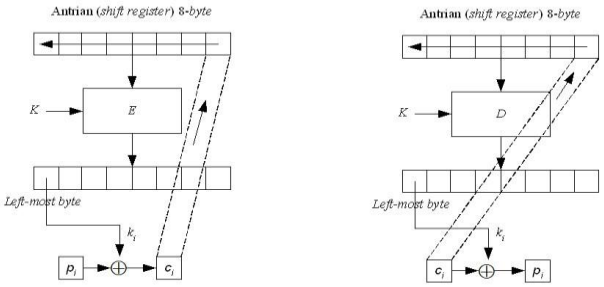


Figure 3. Cipher-Feedback (CFB) [Algoritma Kripto Modern, oleh M, Rinaldi. 2015]

Pada metode OFB, hanya sedikit berbeda dengan CFB, perbedaannya terdapat pada IV yang digunakan pada fungsi E kedua dan seterusnya berasal dari hasil fungsi E dengan masukan Kunci dan IV sebelumnya. Hal ini menyebabkan OFB bisa mengolah blok selanjutnya tanpa harus menunggu XOR selesai dilakukan pada blok sebelumnya.

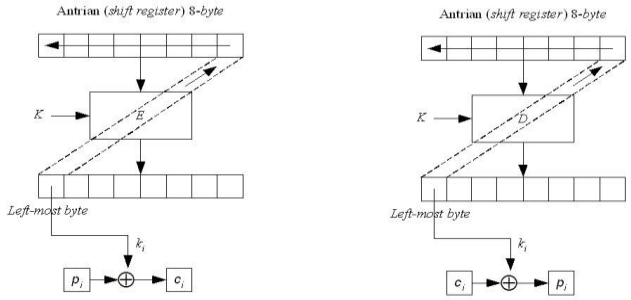


Figure 4. Cara kerja OFB [Algoritma Kripto Modern, oleh M, Rinaldi. 2015]

Semua metode diatas, jika dibalik akan menghasilkan metode dekripsi yang dapat digunakan untuk membaca pesan yang telah terenkripsi melalu salah satu metode tersebut.

B. Prinsip Konfusi dan Difusi

Konfusi dan difusi merupakan salah satu cara kriptografer untuk memperkuat kriptografi sehingga tidak dapat melakukan analisis frekuensi dan memberikan perbedaan besar pada *ciphertext* hanya dengan sedikit perubahan pada *plaintext*.

Konfusi adalah metode untuk menghilangkan bentuk statistik yang dapat muncul pada sebuah bahasa atau katakata yang beraturan, hal ini dapat dilakukan dengan cara melakukan subtitusi sehingga mengubah *input* secara drastis ketika menjadi *output*.

Difusi adalah metode untuk menyebarkan pengaruh perubahan dari suatu karakter atau bagian pada *input* dapat mengubah banyak atau seluruh bagian *output*. Metode yang dapat digunakan untuk melakukan hal ini adalah menggunakan permutasi. Dengan difusi ini, pola-pola yang ada seharusnya hilang atau tersebar.

C. Jaringan Feistel

Jaringan Feistel merupakan salah satu struktur yang digunakan didalam kriptografi. Sistem yang digunakan pada jaringan Feistel ini adalah dengan membagi *plaintext* menjadi dua bagian. Masing-masing bagian akan diperlakukan dengan berbeda.

Bagian kanan *plaintext* akan di masukan kedalam suatu fungsi F dengan menggunakan kunci K_x dimana x merupakan nomor putaran yang sedang dilakukan. Bagian kiri *plaintext* selanjutnya akan di XOR dengan bagian kanan *plaintext* hasil keluaran setelah melalui fungsi F dengan kunci K_x. Selanjutnya kedua bagian tersebut kembali digabungkan kembali, namun dipertukarkan antara bagian kiri dengan bagian yang kanan.

Proses tersebut dapat dilakukan berkali-kali untuk mendapatkan hasil yang lebih *random* dari sebelumnya. Cara untuk mendekripsi jaringan Feistel ini adalah dengna membalikkan proses diatas.

III. RANCANGAN ALGORITMA

Secara umum, algoritma ini menggunakan jaringan feistel yang diulang sebanyak 16 kali. Besar blok pesan yang digunakan adalah sebesar 128 bit yang kemudian dibagi menjadi dua bagian, 64 bit untuk pesan bagian kiri dan 64 bit untuk pesan bagian kanan. Kunci internal akan digenerate sebanyak 16 kali, satu kunci untuk setiap perulangan jaringan feistel. Panjang kunci yang dimasukkan pengguna minimal 64 bit. Apabila pengguna memasukkan kunci dengan panjang lebih dari 64 bit, yang terpakai hanya 64 bit. Hal ini karena pada algoritma ini ukuran blok tetap.

A. Jaringan Feistel

Jaringan Feistel yang digunakan pada algoritma ini membagi blok menjadi dua bagian sama besar yaitu 64 bit pada bagian kiri dan 64 bit pada bagian kanan. Pesan pada bagian kanan akan diubah dengan menggunakan round function. Kemudian, pesan pada bagian kanan akan diisi dengan hasil XOR antara bagian kiri dengan hasil round function. Dan pesan bagian kiri akan diisi dengan hasil round function.

Skema jaringan feistel dapat dilihat pada gambar berikut :

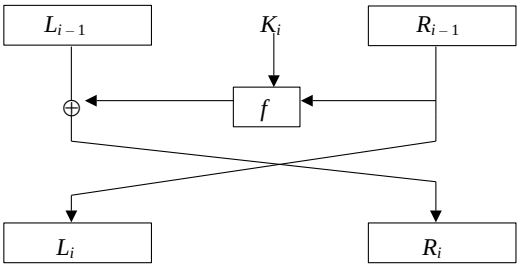


Figure 5. Jaringan Feistel [Algoritma Kripto Modern, oleh M, Rinaldi. 2015]

B. Round Function

Pada round function akan dilakukan beberapa proses diantaranya adalah pertukaran blok, rotasi, XOR, dan subtitusi dengan mengunakan S-Box. Alur yang digunakan pada round function adalah sebagai berikut :

1) Pertukaran byte
pertukaran byte dilakukan dengan menukarkan suatu byte dengan bit yang berada di sampingnya. Byte yang sudah ditukar tidak diproses lagi. Contohnya pada blok berukuran 8 byte berikut:

10	fa	6b	10	00	ff	5c	6b

Setelah dilakukan pertukaran bit, maka blok akan menjadi seperti berikut:

fa	10	10	6b	ff	00	6b	5c

2) Lakukan XOR antara blok dengan kunci

3) Rotasi blok
Rotasi blok akan dilakukan dengan menggeser blok ke kanan sebanyak satu kali secara siklik. Misalkan pada blok dengan 8 bit berikut :

10	fa	6b	10	00	ff	5c	6b

Setelah dilakukan pergeseran, maka blok akan menjadi seperti berikut:

6b	10	fa	6b	10	00	ff	5c

4) Substisusi dengan S-Box
Substitusi blok akan dilakukan dengan menggunakan S-Box sehingga menghasilkan blok yang lebih teracak. S-Box dibangun secara acak dengan bantuan kakas random.org. Berikut adalah S-Box yang penulis gunakan pada algoritma ini:

```
8a f6 a9 51 12 b7 0e 83 54 53 06 2e e7 9d 3f f1
3e a9 1e e0 de e2 b8 eb 1b 48 0c 17 63 b2 b5 c2
49 e3 c5 e2 25 f0 f9 50 26 e9 1d ad fb ed bb 7f
0b 78 96 8b e3 e7 7f eb 2a 1f 62 58 f1 e5 df 73
fd df 4e b7 8a aa c0 03 f2 6a ea 0f 17 19 20 b3
35 ef 73 fb 46 fe 31 33 5f 42 a0 92 ee 6e 22 e1
99 f7 42 e7 bf 71 e0 7e ed 17 1e 88 d7 04 4c 0e
3c 96 ac cc 69 a9 43 53 b6 b4 76 f3 35 81 84 9c
bd 78 49 f8 c4 33 83 23 d7 75 39 f3 bc 4f 2d 95
75 c0 bd 9c 00 ff 26 a7 7e 78 af 49 58 56 c3 a8
36 b0 54 ac 1f a3 f7 f0 bb 63 e7 6d 04 12 84 dc
2d 91 89 1a cb 39 ed 85 0a 76 53 61 8c 74 0c 4d
f3 ac 7f 74 32 2e 7a ad 48 eb b3 9c 8e a7 7c dd
c8 cf 5e 78 6f 12 f4 72 58 f1 ff b3 d7 d9 90 64
84 48 8a 81 23 c5 11 1c eb be 44 5a 07 70 88 99
2e 5f a7 65 85 1f a1 d1 9c 68 7f 36 43 aa c4 cc
```

5) Lakukan XOR kembali antara blok dengan kunci

C. Key Schedule

Pembangkitan kunci internal dilakukan dengan menggeserkan byte kunci ke kanan sebanyak perputaran jaringan feistel. Jika jaringan feistel berada pada perputaran pertama, maka kunci yang akan digunakan adalah kunci hasil pergeseran ke kanan sebanyak satu pergeseran, jika jaringan feistel berada pada putaran ke dua, maka kunci yang digunakan adalah kunci hasil pergeseran ke kanan sebanyak 2 pergeseran. Hal yang sama dilakukan juga pada putaran berikutnya.

D. Hasil Pengujian

Berikut merupakan hasil pengujian yang dilakukan plaintext dengan menggunakan Electronic Code Block (ECB) dan Cipher Block Chaining (CBC).

1) Menggunakan ECB

Kunci : kriptografi

Plaintext :

```
the quic brown fox jumps over the lazy dog
```

Plaintext (hex) :

```
74 68 65 20 71 75 69 72 20 62 72 6f 77 6e
20 66 6f 78 20 6a 75 6d 70 73 20 6f 76 65
72 20 74 68 65 20 6c 61 7a 79 20 64 6f 67
00 00 00 00 00 00
```

Ciphertext :

```
zÍöø‰Ÿ·üýQ9D¼ûå«ü0ê'"³~KÌ¥
```

Ciphertext(hex) :

```
c8a2 4d0d d355 24fe e28b 491a f2c7 0373
40c0 e85c 6c38 b106 5b25 224c 6460 c270
0008 ec0b 885f fe56 7a7b f30e a974 5d48
```

2) Menggunakan CBC

Kunci : kriptografi

Plaintext :

```
the quic brown fox jumps over the lazy dog
```

Plaintext (hex) :

```
74 68 65 20 71 75 69 72 20 62 72 6f 77 6e
20 66 6f 78 20 6a 75 6d 70 73 20 6f 76 65
72 20 74 68 65 20 6c 61 7a 79 20 64 6f 67
00 00 00 00 00 00
```

Ciphertext :

```
¹51<Š(j˜|ÌÀ"–îó`»CŒÆTŽÖŠõb—§
```

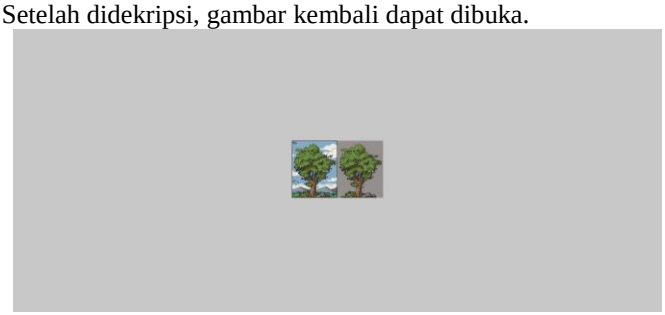
Ciphertext(hex) :

```
3193 75f0 92a5 d5f8 5b23 5bee 00e7 8b84
ccc9 63ea 8d61 af29 e316 21e6 0c3c 4d42
5fa4 0a3c fe92 a2bf c61d 9478 3f56 8bfb
```

Enkripsi gambar:

Gambar yang dienkripsi tidak dapat dibuka pada program *image viewer*.

Setelah didekripsi, gambar kembali dapat dibuka.



3) Menggunakan CFB

Kunci : 12345678

Plaintext :

```
the quic brown fox jumps over the lazy dog
```

Plaintext (hex) :

```
74 68 65 20 71 75 69 72 20 62 72 6f 77 6e
20 66 6f 78 20 6a 75 6d 70 73 20 6f 76 65
72 20 74 68 65 20 6c 61 7a 79 20 64 6f 67
00 00 00 00 00 00
```

Ciphertext :

```
����*�
Mm��')C������N7�-G�������kZ�)b�@�
��d�xi�
```

Ciphertext(hex) :

```
14 F8 84 A3 84 2A E1 20 4D 6D A7 93 27 29
43 9B F6 A7 BA 94 4E 37 E2 1E 1D 47 A3 BA
80 F5 9E A5 C1 6B 5A 9F 29 62 C8 40 F4 E6
FE 64 A4 78 69 AF
```

IV. ANALISIS

A. Analisis Frekuensi

Salah satu teknik kriptanalisis yang umum digunakan oleh kriptanalis adalah dengan melakukan analisis frekuensi. Proses analisis frekuensi ini dilakukan denan mencocokkan frekuensi kemunculan dari huruf-huruf yang dihasilkan dari proses kriptografi.

Dengan melakukan pemerataan kemunculan frekuensi huruf-huruf pada ciphertext, maka diharapkan dapat mempersulit proses kriptanalisis.

Histogram dari ciphertext dibuat dengan menggunakan kakas bytehist yang dapat diperoleh di

https://cert.at/downloads/software/bytehist_en.html

Dalam percobaan, digunakan pesan “the quick brown fox jumps over the lazy dog” dan menghasilkan histogram penyebaran huruf sebagai berikut :

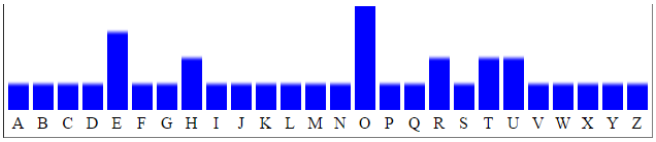


Figure 6. Penyebaran Huruf sebelum dienkripsi

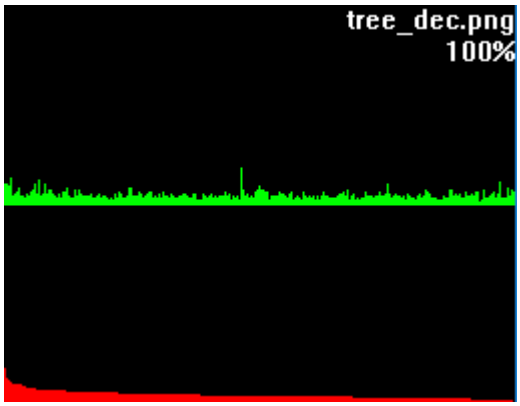


Figure 7 Histogram awal gambar uji

Setelah dilakukan proses enkripsi, diperoleh cipher text dengan histogram sebagai berikut :

Mode ECB:

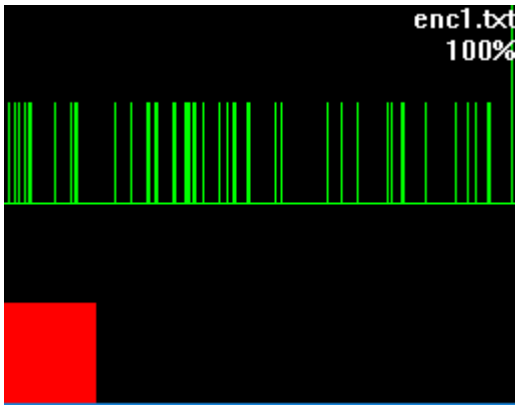


Figure 8 Histogram hasil enkripsi ECB

Mode CBC:

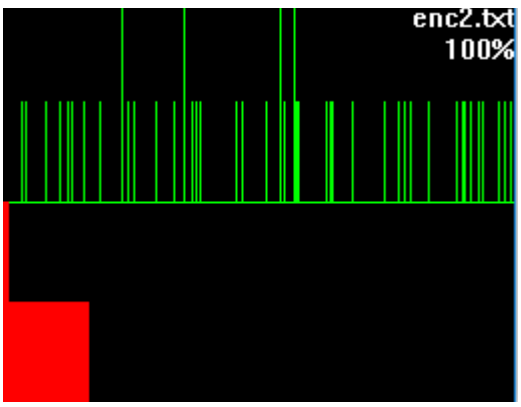


Figure 9 Histogram hasil enkripsi CBC

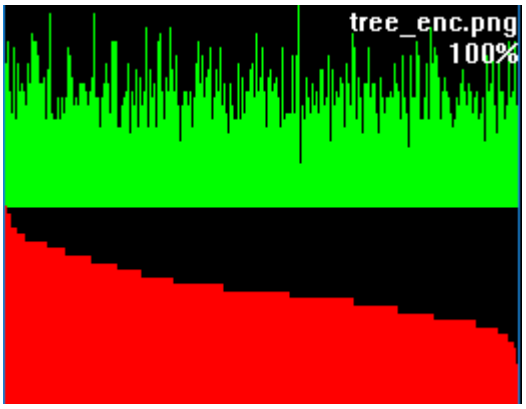


Figure 10 Histogram hasil enkripsi gambar dengan mode CBC

Mode CFB:

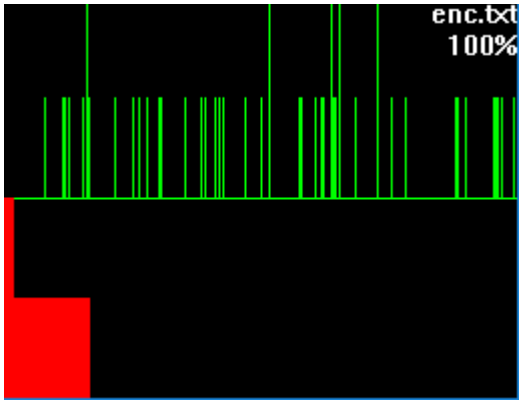


Figure 11 Histogram hasil enkripsi CFB

Dari histogram tersebut, dapat dilihat bahwa persebaran byte hasil enkripsi cukup merata.

B. Sedikit Perbedaan Plaintext

ECB :

the quic brown fox jumps over the lazy dog
c8 a2 4d 0d d3 55 24 **fe** e2 8b 49 1a f2 c7 03 **73** 40 c0 e8 5c 6c 38 b1 06 5b 25 22 4c 64 60 c2 70 00 08 ec 0b 88 5f fe 56 7a 7b f3 0e a9 74 5d 48

the quir brown fox jumps over the lazy dog
c8 a2 4d 0d d3 55 24 **89** e2 8b 49 1a f2 c7 03 **8f** 40 c0 e8 5c 6c 38 b1 06 5b 25 22 4c 64 60 c2 70 00 08 ec 0b 88 5f fe 56 7a 7b f3 0e a9 74 5d 48

CBC :

the quic brown fox jumps over the lazy dog
31 93 75 f0 92 a5 d5 **f8** 5b 23 5b ee 00 e7 8b **84** cc c9 63 ea 8d 61 af **29** e3 16 21 e6

0c 3c 4d **42** 5f a4 0a 3c fe 92 a2 **bf** c6 1d 94 78 3f 56 8b **fb**

the quir brown fox jumps over the lazy dog
31 93 75 f0 92 a5 d5 **03** 5b 23 5b ee 00 e7 8b **c8** cc c9 63 ea 8d 61 af **c7** e3 16 21 e6 0c 3c 4d **0f** 5f a4 0a 3c fe 92 a2 **c3** c6 1d 94 78 3f 56 8b **20**

CFB 8bit :

the quic brown fox jumps over the lazy dog
14 F8 84 A3 84 2A E1 20 4D 6D A7 93 27 29 43 9B F6 A7 BA 94 4E 37 E2 1E 1D 47 A3 BA 80 F5 9E A5 C1 6B 5A 9F 29 62 C8 40 F4 E6 FE 64 A4 78 69 AF

the quir brown fox jumps over the lazy dog
14 F8 84 A3 84 2A E1 **31** 4D **D3** A7 **F2** 27 **BA** 43 **61** F6 **71** BA **05** 4E **55** E2 **11** 1D **E0** A3 **2F** 80 **1C** 9E **C5** C1 **0E** 5A **C7** 29 **CA** C8 **AB** F4 **15** FE **FF** A4 **00** 69 **68**

Dari hasil percobaan tersebut, terlihat bahwa sedikit perubahan pada plaintext tidak memberikan perubahan yang signifikan pada ciphertext. Terutama pada penggunaan metode ECB. Sehingga penggunaan algoritma blockcipher ini tidak cocok untuk pengiriman pesan yang sama atau sebagian besar konten sama dan dikirim berulang-ulang. Perubahan paling banyak terlihat pada mode CFB 8 bit.

C. Sedikit Perbedaan Kunci

ECB :

kriptografi
C8 A2 4D 0D D3 55 24 FE E2 8B 49 1A F2 C7 03 73 40 C0 E8 5C 6C 38 B1 06 5B 25 22 4C 64 60 C2 70 00 08 EC 0B 88 5F FE 56 7A 7B F3 0E A9 74 5D 48

kroptografi
D5 A2 72 EC 5C 55 50 FE 45 8B 6B A2 5D C7 ED 73 43 C0 AF 35 AE 38 1B 06 B6 25 99 67 9A 60 73 70 A8 08 DE 50 0A 5F 4C 56 47 7B 56 0A 00 74 5A 48

CBC :

kriptografi
31 93 75 F0 92 A5 D5 F8 5B 23 5B EE 00 E7 8B 84 CC C9 63 EA 8D 61 AF 29 E3 16 21 E6 0C 3C 4D 42 5F A4 0A 3C FE 92 A2 BF C6 1D 94 78 3F 56 8B FB

kroptografi
AF 93 3B 38 F1 A4 07 F8 4F 23 19 C3 0F FA FC 84 B1 C9 E3 15 8D F3 8E 29 61 16 63 46

24 1C 4D 42 26 A4 D9 23 8E 5F A0 BF 86 1D 85 36 AA C9 F6 FB

CFB :

12345678
14 F8 84 A3 84 2A E1 20 4D 6D A7 93 27 29 43 9B F6 A7 BA 94 4E 37 E2 1E 1D 47 A3 BA 80 F5 9E A5 C1 6B 5A 9F 29 62 C8 40 F4 E6 FE 64 A4 78 69 AF

12345677
27 AA 70 3F A8 23 0A AB 10 03 75 21 B1 29 05 15 43 FD 60 55 D5 30 A5 D2 8A 7D 31 24 00 4F F3 3E 8B 3C 74 98 E7 89 8A 58 D0 BC FB 79 ED CA 10 36

D. Bruteforce Attack

Algoritma ini menggunakan kunci sebesar 64-bit didalam melakukan enkripsi dan dekripsi. Sehingga terdapat sekitar 2^64 kemungkinan kunci yang harus dicoba untuk memecahkan ciphertext. Dengan kemampuan komputasi pencobaan kunci sebanyak 10 juta kunci per detik, memerlukan waktu sekitar 1,4 x 10^6 tahun untuk memecahkan kunci tersebut.

Selain waktu yang cukup lama untuk memecahkan kunci secara bruteforce, algoritma ini melakukan proses penggantian dan pergeseran yang cukup banyak sehingga menghasilkan ciphertext yang lebih tidak teratur. Sehingga akan mempersulit penyerang untuk memecahkan pesan yang dikirimkan.

V. KESIMPULAN

Algoritma yang kami buat memiliki kekuatan dalam menangani analisis frekuensi. Hal ini terlihat dari bentuk histogram yang cukup merata untuk *file* teks biasa. Pada *file* gambar, histogram asal dan histogram hasil enkripsi memiliki perbedaan pola yang cukup signifikan. Algoritma ini memiliki kelemahan pada difusi. Sedikit perubahan pada plainteks hanya berpengaruh sedikit pada cipherteks. Meski demikian, perubahan tersebut tidak terlalu berpola, terutama pada mode CFB. Hasil paling buruk terlihat pada mode ECB. Hal ini diakibatkan sifat dasar ECB, yaitu setiap blok dienkripsi dengan cara yang sama.

REFERENSI

[1] http://www.informatika.stei.itb.ac.id/~rinaldi.munir/ diakses sebelum 28 oktober 2016

[2] http://www.tutorialspoint.com/cryptography. diakses sebelum 27 oktober 2016.

PERNYATAAN

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

Bandung, 28 Oktober 2016

Fikri Aulia (13513050)

Adin Baskoro (13513058)