Algoritma Block Cipher 2-LA-XOR

Luthfi Fadillah
Sekolah Teknik Elektro dan Informatika (STEI)
Institut Teknologi Bandung (ITB)
Bandung, Indonesia
13515072@std.stei.itb.ac.id

Azis Adi Kuncoro
Sekolah Teknik Elektro dan Informatika (STEI)
Institut Teknologi Bandung (ITB)
Bandung, Indonesia
13515120@std.stei.itb.ac.id

***Abstract*—Block Cipher adalah algoritma dalam kriptografi yang beroperasi pada sekumpulan bit dengan panjang tertentu yang biasa disebut dengan block. Pada makalah ini akan dijelaskan mengenai algoritma 2-La-XoR yang merupakan jenis ARX (Add, Rotate XoR). 2-La-XoR memiliki beberapa proses utama yaitu *Avalanche, Unavalanche, XORing, Key Expansion*. 2-La-XoR akan dioperasikan pada beberapa mode block cipher seperti ECB, CBC, CFB, OFB, dan CTR.**

Keywords—block cipher; feistel; confusion; diffusion; ARX; encryption; decryption;

I. Pendahuluan

Kriptografi adalah ilmu dan seni untuk menyembunyikan pesan (Schneier, 1996). Berdasarkan garis waktu, terdapat 2 jenis teknik kriptografi, yaitu kriptografi lama (*Old Cryptography*), yaitu teknik kriptografi yang muncul sebelum adanya komputer, dan kriptografi modern (*Modern Cryptography*), yaitu teknik kriptografi yang muncul setelah adanya komputer. Untuk saat ini, teknik kriptografi modern banyak digunakan, dikarenakan teknik kriptografi lama sudah dapat dipecahkan dengan komputer dalam waktu singkat, sedangkan beberapa teknik kriptografi modern masih sulit dipecahkan meski menggunakan komputer yang umum digunakan.

Salah satu algoritma kriptografi modern yang menjadi standar bagi algoritma-algoritma kriptografi terbaru adalah *Advanced Encryption Standard* (AES). AES merupakan algoritma kriptografi dengan jenis *block cipher*, yaitu algoritma yang melakukan enkripsi dan dekripsi pada setiap blok-blok pesan. Teknik kriptografi yang digunakan pada AES berfokus pada substitusi dan permutasi, dan teknik tersebut dilakukan sebanyak 10, 12, dan 14 putaran, tergantung dari panjang kunci yang digunakan (128-bit, 192-bit, dan 256-bit).

Algoritma baru yang diajukan memanfaatkan putaran yang minimal, yaitu hanya 3 putaran. Selain itu, teknik yang digunakan pada algoritma ini akan berfokus pada teknik *Add*, *Rotate*, dan *XOR* (*ARX*). Ketiga teknik tersebut akan difokuskan karena ketiga teknik tersebut menggunakan sumber daya yang lebih sedikit dibandingkan substitusi dan permutasi, seperti yang digunakan pada AES. Meskipun tidak berfokus pada substitusi dan permutasi, namun algoritma ini tetap akan menggunakan substitusi dan permutasi.

II. Dasar Teori

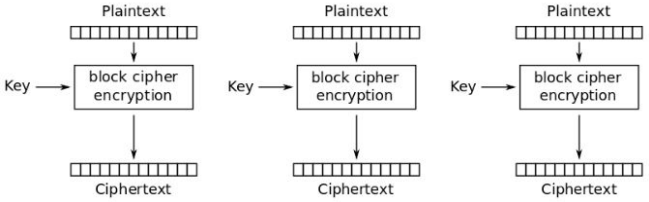
A. Block Cipher

Dalam kriptografi, *block cipher* adalah algoritma deterministik yang beroperasi pada kelompok bit dengan panjang tetap, yang disebut *block*, dengan transformasi yang tidak bervariasi yang ditentukan oleh kunci simetris. Cipher blok beroperasi sebagai komponen dasar penting dalam desain banyak protokol kriptografi dan banyak digunakan untuk mengimplementasikan enkripsi data massal.

Terdapat mode operasi dalam *block cipher*, yaitu *Electronic Code Book* (ECB), *Cipher Block Chaining* (CBC), *Cipher Feedback* (CFB), *Output Feedback* (OFB), dan *Counter* (CTR). Berikut merupakan penjelasan mengenai lima mode operasi yang telah disebutkan.

1. *Electronic Code Book* (ECB)

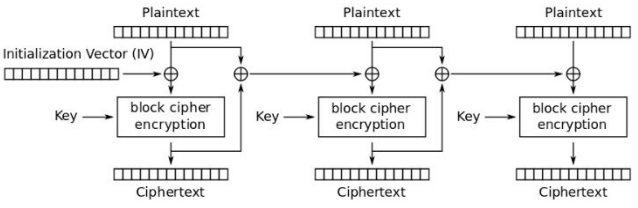
Mode ini merupakan mode yang paling sederhana. Pesan dibagi menjadi blok - blok, kemudian setiap blok di enkripsi secara independen. Kekurangan dari metode ini adalah kurangnya prinsip *diffusion*, hal ini dikarenakan ECB melakukan enkripsi blok plainteks menjadi blok cipher yang identik, tidak ada pola dari pesan yang disembunyikan.



Gambar 1. Operasi *block cipher* dengan ECB

2. *Cipher Block Chaining* (CBC)

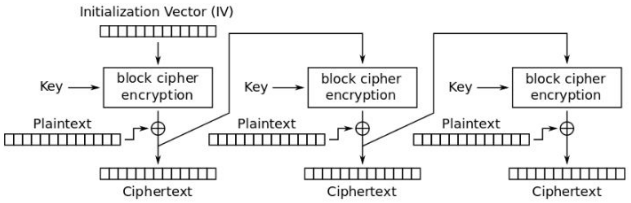
Pada mode CBC, setiap blok di enkripsi dengan memanfaatkan hasil enkripsi dari *block cipher* sebelumnya, sedangkan *block cipher* paling awal di enkripsi dengan *Initialization Vector*. Untuk setiap *block cipher* hasil enkripsi di operasikan XOR dengan *block cipher* selanjutnya. Kekurangan utama pada mode ini adalah enkripsi yang berurutan (tidak dapat diparalelkan) dan juga pesan harus di *padding* sesuai dengan ukuran *block cipher*.



Gambar 2. Operasi *block cipher* dengan CBC

3. *Cipher Feedback* (CFB)

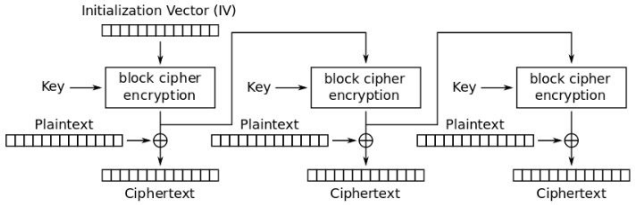
Berbeda dari mode CBC yang menggunakan blok *plaintext* sebagai masukan dari fungsi enkripsi. Enkripsi dilakukan dengan menggunakan *ciphertext* dari blok sebelumnya, kemudian dilakukan operasi XOR dengan *plainteks* untuk menghasilkan *cipherteks*.



Gambar 3. Operasi *block cipher* dengan CFB

4. *Output Feedback* (OFB)

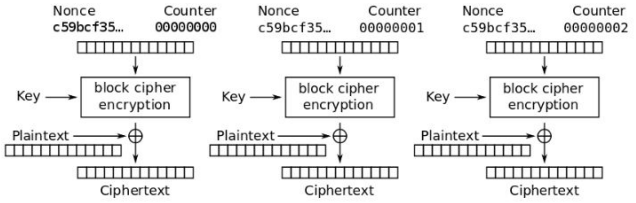
Mirip dengan metode CFB, namun yang menjadi masukan untuk operasi enkripsi blok adalah hasil output dari enkripsi blok sebelumnya.



Gambar 4. Operasi *block cipher* dengan OFB

5. *Counter* (CTR)

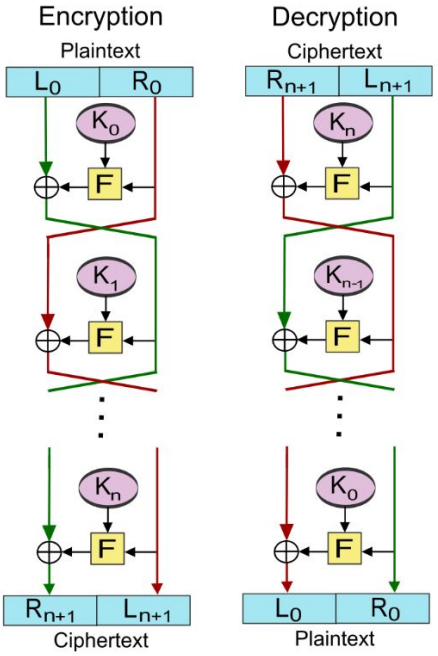
Mode counter menggunakan blok yang merupakan kombinasi dari *nonce* dan *counter* sebagai masukan untuk enkripsi. Nonce merupakan satu *Initialization Vector* yang acak dan dipakai untuk setiap blok selanjutnya. Pada tahap selanjutnya nilai *counter* bertambah.



Gambar 5. Operasi *block cipher* dengan CTR

B. Jaringan Feistel

Jaringan Feistel merupakan struktur simetris yang digunakan dalam pembangunan *block cipher*. Pada awalnya konsep ini diperkenalkan oleh karyawan IBM Horst Feistel dan Don Coppersmith, penggunaan pertama jaringan Feistel adalah pada *Lucifer block cipher*.



Gambar 6. Ilustrasi Jaringan Feistel

C. Confusion dan *Diffusion*

Kedua prinsip ini diperkenalkan pertama kali oleh Claude Shannon pada tahun 1949 melalui karyanya yang berjudul "*Communication Theory of Secrecy System*". Tujuan utama diperkenalkan prinsip ini adalah mempersulit kriptanalis dalam memecahkan *cipherteks* melalui metode analisis statistik.

1. *Confusion*

Confusion dalam konteks ini berarti proses perancangan plainteks, kunci, dan cipherteks yang memiliki hubungan yang dibuat serumit mungkin. Prinsip ini ditujukan agar kriptanalis kesulitan untuk menemukan pola - pola statistik yang mungkin muncul.

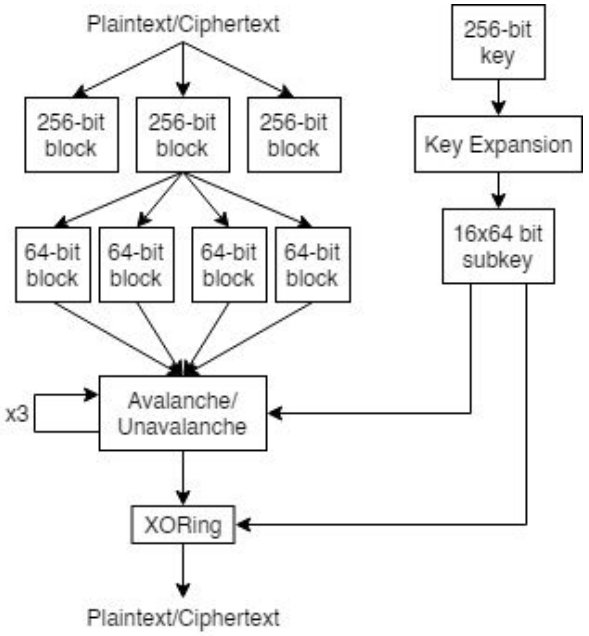
2. *Diffusion*

Diffusion merupakan prinsip yang digunakan untuk menyebarkan pengaruh dari bit plainteks atau kunci pada cipherteks. Pada *block cipher* yang memiliki prinsip ini, perubahan beberapa bit pada *plainteks* akan membuat perubahan yang tidak dapat diduga pada *cipherteks*.

III. Rancangan Block Cipher

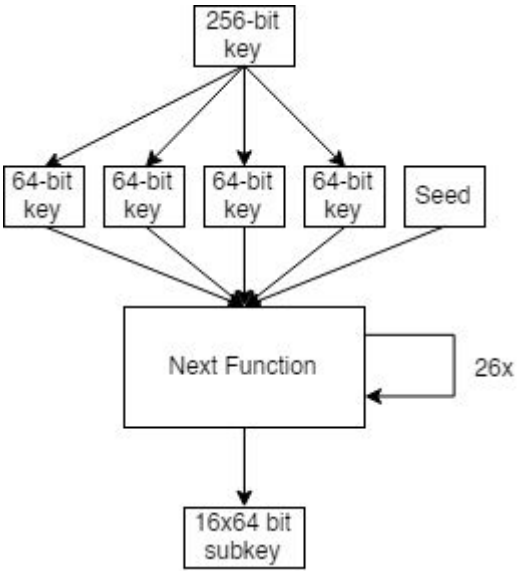
2-LA-XOR adalah algoritma *block cipher* yang menggunakan 256 bit kunci yang dipecah menjadi 4 bagian, masing-masing bagian berukuran 64 bit. Pesan (*plaintext*) yang menjadi input dipecah menjadi beberapa blok besar dengan ukuran blok sebesar 256 bit. 2-LA-XOR memiliki beberapa proses, yaitu *Avalanche*, *Unavalanche*, *XORing*, dan *Key Expansion*. Kunci yang sudah dipecah, diekspansi menjadi beberapa sub kunci dengan proses *Key Expansion*. Untuk proses enkripsi, blok pesan yang sudah dipecah menjadi 256 bit dipecah kembali menjadi blok-blok kecil berukuran 64 bit. Sub kunci tersebut, bersama dengan blok pesan, memasuki proses *Avalanche* sebanyak 3 putaran (*round*). Di dalam proses *Avalanche*, terdapat proses *Compress*, yang digunakan untuk melakukan kompresi acak dengan memanfaatkan operasi *right shift*, AND, dan XOR. Setelah 3 putaran proses *Avalanche* dilewati, dilanjutkan

dengan proses *XOR* antara blok pesan yang sudah teracak dengan sub kunci. Proses tersebut diulang jika masih ada blok-blok besar pesan yang belum diproses. Untuk proses dekripsi, karena menerapkan jaringan feistel, maka hanya dibalik prosesnya, dengan mengganti proses *Avalanche* menjadi *Unavalanche*.



A. Key Expansion

Proses *Key Expansion* memperluas masukan kunci menjadi 16 sub kunci. Sub kunci tersebut digunakan bersama dengan blok kecil pesan untuk proses pengacakan pesan (*Avalanche* dan *XOR*)



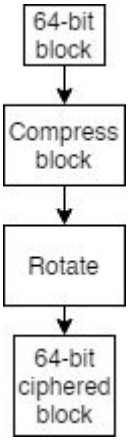
Next Function

```
Function Next(S):
  S = (S1, S2, S3, S4, S5)
  T = S2
  S2 = S3
  S3 = S4
  S4 = S5
  S5 = S1
  Y = S1 = Avalanche(S1, S1+T)
  return S
```

B. Avalanche / Unavalanche

Proses *avalanche* merupakan salah satu proses utama dalam melakukan enkripsi, selain proses *XOR*. Proses ini melakukan pengacakan pada pesan dengan menerapkan teknik *add* dan *rotate*. Didalam proses *avalanche*, terdapat proses *compress* yang melakukan kompresi acak pada pesan dan menerapkan teknik *add*. Pada 2-LA-XOR, proses avalanche dilakukan sebanyak 3 putaran.

Proses *unavalanche* adalah proses avalanche yang dibalik. *Unavalanche* digunakan untuk melakukan dekripsi pesan.



Avalanche Function

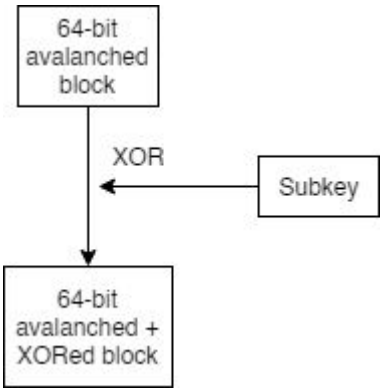
```
Function Avalanche(X, A):
  return  Rotate((X + A) <<< Compress(A))
```

Compress Function

```
Function Compress(X):
  X = (X >>  32) + X
  X = (X >> 11) ⊕ X
  X = (X >>  9) + X
  X = (X >>  6) + X
  Y = X ∧ 0x3f
  return Y
```

C. XORing

Proses *XORing* melakukan operasi XOR antara blok kecil pesan yang sudah melalui proses *avalanche* dengan subkey. Proses ini sama seperti operasi XOR pada umumnya.



IV. Simulasi Dan Percobaan Hasil

Pada bagian ini, akan dijelaskan hasil simulasi dan percobaan dari cipher ini pada 5 mode block cipher, yaitu ECB, CBC, CFB, OFB, dan CTR. Dalam percobaan ini digunakan kunci eksternal yaitu *bluemountain*.

Kunci	bluemountain
Plainteks	Lorem ipsum dolor sit amet consectetur adipisicing elit sed do eiusmod tempor incididunt ut labore et dolore magna aliqua
Hex dari plainteks	4c 6f 72 65 6d 20 69 70 73 75 6d 20 64 6f 6c 6f 72 20 73 69 74 20 61 6d 65 74 20 63 6f 6e 73 65 63 74 65 74 75 72 20 61 64 69 70 69 73 69 63 69 6e 67 20 65 6c 69 74 20 73 65 64 20 64 6f 20 65 69 75 73 6d 6f 64 20 74 65 6d 70 6f 72 20 69 6e 63 69 64 69 64 75 6e 74 20 75 74 20 6c 61 62 6f 72 65 20 65 74 20 64 6f 6c 6f 72 65 20 6d 61 67 6e 61 20 61 6c 69 71 75 61

A. Percobaan dengan ECB

Cipherteks	5f 29 93 66 ed 44 55 df d9 7c 8c 28 51 05 b9 72 2c 43 e6 8d 1e 83 22 2d 11 c5 42 8e 98 a4 5d b0 99 53 8d a4 d5 1b e1 ed b5 f6 83 27 23 79 5f 32 38 ae 5c 9f ab 39 ea d9 4f 9d ce 0b 58 a6 10 12 72 7e f3 e2 ba ed 88 90 1e cb db 71 e4 46 31 4e 7d d5 23 bb e6 57 9b e8 ee e2 73 4b 20 26 ee 91 08 e0 eb 34 e9 1f 23 5e 4c 53 a0 80 46 03 a2 ec 96 53 cb 96 df ad 94 89 00
Plainteks	4c 6f 72 65 6d 20 69 70 73 75 6d 20 64 6f 6c 6f 72 20 73 69 74 20 61 6d 65 74 20 63 6f 6e 73 65 63 74 65 74 75 72 20 61 64 69 70 69 73 69 63 69 6e 67 20 65 6c 69 74 20 73 65 64 20 64 6f 20 65 69
	75 73 6d 6f 64 20 74 65 6d 70 6f 72 20 69 6e 63 69 64 69 64 75 6e 74 20 75 74 20 6c 61 62 6f 72 65 20 65 74 20 64 6f 6c 6f 72 65 20 6d 61 67 6e 61 20 61 6c 69 71 75 61

B. Percobaan dengan CBC

Cipherteks	7a 31 4b 5b b8 6e 2a 45 8b 6d d7 ca 07 cd 32 c7 0d 01 0a 32 7a c3 32 55 02 b2 11 f3 4a a9 7f a5 9d e6 e6 bc 98 8c f9 a4 df e3 1f 80 d3 02 15 b1 5a c0 29 91 0a 65 84 d3 94 0a 86 c3 30 5d 3e 2e 59 55 3f 60 a9 b3 5a 0d 61 c0 9d 64 88 b6 b8 b1 31 dd 2b 90 06 b7 1a 95 c3 72 bc 3e 78 6b b6 ee 82 23 db e0 1b 16 94 5f fc 5f 55 93 a3 55 70 5d c6 a1 3f 9a 98 b1 14 d4 3c
Plainteks	4c 6f 72 65 6d 20 69 70 73 75 6d 20 64 6f 6c 6f 72 20 73 69 74 20 61 6d 65 74 20 63 6f 6e 73 65 63 74 65 74 75 72 20 61 64 69 70 69 73 69 63 69 6e 67 20 65 6c 69 74 20 73 65 64 20 64 6f 20 65 69 75 73 6d 6f 64 20 74 65 6d 70 6f 72 20 69 6e 63 69 64 69 64 75 6e 74 20 75 74 20 6c 61 62 6f 72 65 20 65 74 20 64 6f 6c 6f 72 65 20 6d 61 67 6e 61 20 61 6c 69 71 75 61

C. Percobaan dengan CFB

Cipherteks	a7 1c 5c 64 b6 20 d6 b0 8c 53 38 96 ca e9 95 3f 4a 54 fc 36 ba e9 cc df 45 34 56 cb 4f 3e 01 9f f8 81 1e 53 f1 a7 0c 83 3b 15 cf 4c 03 93 34 2f e0 f6 05 4c 87 57 33 41 2b 3e 9e d7 86 25 a6 6a 81 28 97 e6 ca c7 53 d0 b2 e9 49 98 14 d2 d7 13 79 8f b9 99 e1 2e 33 2f da 06 bd cc 21 0f f9 7f cc 11 55 17 e1 f8 7d 7b de 3f cb d2 74 3f 17 04 62 5c 48 b8 b4 77 7f 35 7a
Plainteks	4c 6f 72 65 6d 20 69 70 73 75 6d 20 64 6f 6c 6f 72 20 73 69 74 20 61 6d 65 74 20 63 6f 6e 73 65 63 74 65 74 75 72 20 61 64 69 70 69 73 69 63 69 6e 67 20 65 6c 69 74 20 73 65 64 20 64 6f 20 65 69 75 73 6d 6f 64 20 74 65 6d 70 6f 72 20 69 6e 63 69 64 69 64 75 6e 74 20 75 74 20 6c 61 62 6f 72 65 20 65 74 20 64 6f 6c 6f 72 65 20 6d 61 67 6e 61 20 61 6c 69 71 75 61

D. Percobaan dengan OFB

Cipherteks	eb 9f 93 ec 32 68 9b 5f 8b bb 1c 19 1a d1 ec 6e 51 4a 4c a1 f4 ac 6b 66 ba d9 ee a8 f7 c0 8f 28 9a cf fb 04 98 d6 3b 22 73 34 3b a8 5c 7d 95 80 49 da d2 b4 40 13 7f d4 ee 86 53 1a 63 72 39 1d 3c 1e 69 3b 9b cb 52 bd d9 21 29 a4 ee 16 6c c9 cc 48 9e 64 8f 45 dc 51 6b 21 df 5f ef 9c 49 8f 6f f6 45 35 d9 07 aa 4b d5 b8 6e 09 b4 11 15 ae 27 bb 0c 11 65 ba fb 74 97
Plainteks	4c 6f 72 65 6d 20 69 70 73 75 6d 20 64 6f 6c 6f 72 20 73 69 74 20 61 6d 65 74 20 63 6f 6e 73 65 63 74 65 74 75 72 20 61 64 69 70 69 73 69 63 69 6e 67 20 65 6c 69 74 20 73 65 64 20 64 6f 20 65 69 75 73 6d 6f 64 20 74 65 6d 70 6f 72 20 69 6e 63 69 64 69 64 75 6e 74 20 75 74 20 6c 61 62 6f 72 65 20 65 74 20 64 6f 6c 6f 72 65 20 6d 61 67 6e 61 20 61 6c 69 71 75 61

E. Percobaan dengan CTR

Cipherteks	eb ee e4 4a a1 a1 9b 86 e6 87 ee 75 01 c2 8a 0d d7 a5 5d 9b bf a0 5f 38 a7 3d a8 ae e4 39 e3 47 d6 20 90 6b 89 13 58 b7 9e ec 9f 9b 9b 4b 07 71 02 75 a2 38 18 25 80 dc 23 65 f7 72 95 0d 20 60 3b 35 c6 62 33 bf 5d 20 db ee 7b c6 d6 ef 67 fb 63 e5 f6 f3 5d 84 dc 63 87 77 44 9e 27 6c 72 61 28 bc 12 7e f5 e9 9a f7 6d 22 ea 8f 4b 15 d2 45 25 9e bc 6f b8 1f 79 1f 74
Plainteks	4c 6f 72 65 6d 20 69 70 73 75 6d 20 64 6f 6c 6f 72 20 73 69 74 20 61 6d 65 74 20 63 6f 6e 73 65 63 74 65 74 75 72 20 61 64 69 70 69 73 69 63 69 6e 67 20 65 6c 69 74 20 73 65 64 20 64 6f 20 65 69 75 73 6d 6f 64 20 74 65 6d 70 6f 72 20 69 6e 63 69 64 69 64 75 6e 74 20 75 74 20 6c 61 62 6f 72 65 20 65 74 20 64 6f 6c 6f 72 65 20 6d 61 67 6e 61 20 61 6c 69 71 75 61

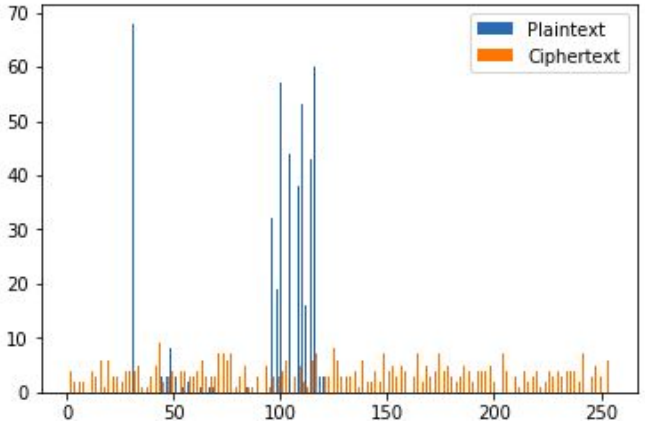
V. Analisis Keamanan

A. Brute force attack

Brute force attack merupakan salah satu cara yang paling sederhana untuk mencoba mendapatkan kunci dengan cara mencari semua kemungkinan kunci atau biasa disebut dengan *exhaustive search*. Biasanya serangan dengan teknik ini membutuhkan waktu yang sangat lama dikarenakan kemungkinan kunci sangatlah banyak.

2-La-XoR memiliki panjang kunci 256-bit. Hal ini mengimplikasikan bahwa terdapat 2^{256} kemungkinan kunci, yang mana merupakan angka yang sangat besar. Pada percobaan ini mesin yang digunakan dalam pengujian mampu menghabiskan waktu 0.02 detik untuk melakukan proses dekripsi. Dibutuhkan $2^{256} * 0.02 = 2.3158418 \times 10^{75}$ detik atau **7.3425549e+67 tahun**. Sehingga sangatlah tidak mungkin untuk melakukan serangan brute force pada cipher ini.

B. Analisis Statistik Plainteks dan Cipherteks



Gambar 7. Diagram frekuensi dari mode CTR

Berdasarkan gambar 7. dapat dilihat bahwa persebaran frekuensi pada cipherteks hampir menyerupai distribusi *uniform*. Dikarenakan distribusi yang merata inilah yang dapat membuat kriptanalis kesulitan dalam melakukan serangan dengan analisis frekuensi.

C. Confusion

Dalam percobaan ini, kami mendapatkan bahwa dengan mengganti sedikit bagian dari **key** yaitu karakter pertamanya. Didapatkan perbedaan sekitar 48.4 % dari ciphertext sebelum diubah. Dapat dikatakan bahwa confusion pada cipher ini sudah baik.

D. Diffusion

Dalam percobaan ini, kami mendapatkan bahwa dengan mengganti sedikit bagian dari **plainteks** yaitu karakter pertamanya. Didapatkan perbedaan sekitar 50.07 % dari ciphertext sebelum diubah. Dapat dikatakan bahwa confusion pada cipher ini sudah baik.

VI. Kesimpulan Dan Saran

Algoritma block cipher 2-La-XoR sudah dapat menerapkan struktur feistel yang memiliki fungsi dekripsi sama dengan fungsi enkripsinya. Algoritma ini juga sudah dapat bertahan dengan baik dari serangan - serangan seperti *brute force attack*, dan *analisis frekuensi*. Dari segi confusion dan diffusion juga sudah cukup baik sehingga menyulitkan kriptanalis dalam melakukan serangan.

Saran kedepannya adalah dikembangkannya varian ARX (Add, Rotate XoR) yang mampu lebih cepat dan *robust*.

Ucapan Terimakasih

Kami selaku penulis mengucapkan terimakasih kepada Tuhan Y.M.E., karena atas berkat, rahmat, dan karunia-Nya makalah ini dapat diselesaikan pada waktunya. Tak lupa terimakasih kepada dosen pengampu matakuliah ini yaitu beliau bapak Dr. Ir. Rinaldi Munir yang memberikan tugas ini sehingga kami mendapatkan pengalaman baik dalam membuat makalah ini. Terakhir kami juga mengucapkan terimakasih kepada teman - teman yang secara langsung maupun tidak membantu dalam penyelesaian makalah ini.

Daftar Pustaka

[1] Saulpaugh, Evan. 2015. XCRUSH A Familiyof ARX Block Ciphers. arXiv:1509.02584 [cs.CR]

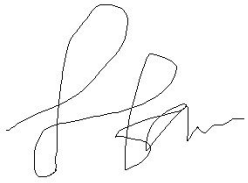
[2] Munir, Rinaldi. 2015. Slide Kuliah IF4020 Kriptografi: Algoritma Kriptografi Modern

[3] Munir, Rinaldi. 2015. Slide Kuliah IF4020 Kriptografi: Serangan terhadap Kriptografi

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, 2 April 2018



Luthfi Fadillah (13515072)

Azis Adi Kuncoro (13515120)