LS Cipher Block

Hafizh Afkar Makmur
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Bandung, Indonesia
13514062@std.stei.itb.ac.id

***Abstract*—Ada beberapa prinsip dalam membuat sebuah cipher blok. Penulis pada kasus ini berusaha untuk membuat sebuah sistem unik menggunakan seluruh prinsip ini menggunakan fungsi urut (sort) sebagai fungsi enkripsi untuk jaringan Feistel. Ditunjukkan bahwa hasil enkripsi memenuhi seluruh prinsip dalam pembuatan cipher blok.**

Keywords—cipher blok; S-block; Feistel network; sort; confusion and diffusion (Shannon); LS cipher block

I. PENDAHULUAN

Kriptografi adalah sebuah ilmu yang sangat penting dalam beberapa dekade terakhir. Hal ini dikarenakan semakin seringnya pertukaran informasi oleh berbagai pihak di dunia, mulai dari informasi biasa antara teman sepena, ataupun infomasi penting militer yang bertanggung jawab terhadap jiwa jutaan orang. Karena itu, ilmu ini memiliki perkembangan yang sangat pesat untuk membuat sistem informasi yang bisa digunakan dengan sangat aman dan cukup mudah untuk dipakai oleh siapa saja atau dipakai sebanyak apapun.

Kriptografi intinya terdiri dari dua bagian, yaitu cara enkripsi dan dekripsi. Metode enkripsi yang digunakan diusahakan bisa sangat kuat sehingga enkripsi itu hanya bisa dipecahkan dengan metode dekripsi dan kunci tertentu. Begitu juga sebaliknya pihak sebaliknya berusaha untuk membuat metode dekripsi yang bisa membongkar sebuah enkripsi tanpa kunci yang diperlukan. Berbagai metode sudah ditemukan pada kedua sisi untuk membuat sistem yang lebih kuat dari sebelumnya.

Enkripsi terdiri dari dua bagian, cipher alir dan cipher blok. Cipher alir mengenkripsi pesan per bit atau byte sedangkan cipher blok mengenkripsi pesan per n-bit atau n-byte. Cipher alir bisa diimplementasikan dengan mudah dan mudah digunakan namun pada akhirnya cipher ini lemah terhadap bebagai serangan mulai dari serangan known-plaintext, ciphertext-only, ataupun flip-bit, yang masing-masing dapat digunakan tergantung tujuan serangan dan sumber daya yang dimiliki penyerang. Hal ini dapat diatasi dengan digunakannya cipher blok yang didesain untuk mengatasi serangan tersebut.

Ada beberapa prinsip dalam pembuatan cipher blok yaitu prinsip confusion dan diffusion [1], sistem cipher berulang, jaringan feistel [2], dan kotak-S. Prinsip ini diciptakan untuk memperkuat sebuah cipher namun juga meningkatkan fleksibilitas dari sebuah cipher. Prinsip ini mencakup hamper seluruh kemungkinan cipher yang bisa dibuat dan masih bisa didekripsi sehingga enkripsi dengan prinsip ini akan lebih kuat dari sistem cipher biasa yang sudah diciptakan sebelumnya.

Beberapa sistem cipher yang sudah dibuat dengan mematuhi prinsip ini adalah DES, AES, Blowfish, dan berbagai sistem lainnya. Selain itu, ada juga berbagai metode operasi untuk menggunakan cipher block di antaranya adalah ECB, CBC, PCBC, CFB, OFB, maupun CTR [3]. Berbagai sistem enkripsi itu di antaranya diciptakan untuk mengatasi berbagai masalah lain dalam sistem enkripsi yaitu perambatan error dalam ciphertext, panjang kunci, perbandingan panjang plaintext dan ciphertext, ataupun kemungkinan paralelisasi enkripsi dan dekripsi. Sistem enkripsi tersebut menyelesaikan masalah itu dengan berbagai cara di antaranya dengan membuat sistem pembangkitan bilangan acak khusus untuk kunci tertentu, sistem untuk menyambungkan setiap blok dengan blok lain agar pesan tidak sangatlah jelas sebagai substitusi satu-ke-satu. Sejauh ini sistem yang masih popular dipakai dalam berbagai sistem pemerintahan adalah AES atau Advanced Encryption System yang bisa memakai kunci 128, 192, ataupun 256 bit. AES menggunakan sistem ekstensif untuk pembangkitan kotak-S untuk substitusi yang digunakan beserta berbagai sistem enkripsi lain seperti jaringan Feistel dan lain-lain.

Salah satu hal paling menarik dalam salah satu prinsip ini adalah jaringan Feistel. Jaringan ini memungkinkan pembuatan sebuah sistem enkripsi yang sama persis dengan sistem dekripsi. Hal ini memungkinkan pembuatan sistem enkripsi yang sangat rumit tanpa perlu memikirkan sistem dekripsi, karena sistem enkripsi sama dengan sistem dekripsi. Hal ini dimungkinkan dengan pembagian pesan menjadi 2 dan penggunaan XOR untuk mencampurkan kedua pesan itu sedemikian rupa sehingga jika proses diulang maka proses akan menghasilkan 2 pesan semula. Hal ini membuka beberapa peluang sistem enkripsi yang menarik seperti yang akan digunakan penulis dalam cipher blok ini yang akan dijelaskan pada bagian berikut.

II. CIPHER BLOK LS

Tujuan penulis dalam pembuatan cipher blok ini dalam pembuatan sistem enkripsi yang bisa digunakan secara fleksibel sehingga sistem ini bisa digunakan dengan metode lain yang bisa digunakan untuk memperkuat sistem ini seperti CBC, OFB, counter, ataupun sistem cipher blok lain. Karena itu, cipher blok ini hanya bersifat merubah sebuah blok dan bisa digunakan berulang kali dengan kunci berbeda. Metode ini

tidak mempengaruhi hubungan antar satu blok dengan blok lain.

Cipher blok LS memanfaatkan kekuatan dari jaringan Feistel yaitu fungsi enkripsi bisa digunakan sebagai fungsi dekripsi. Berarti, fungsi enkripsi bisa merupakan sebuah fungsi yang sangat kompleks dan tidak bisa dibayangkan dekripsinya namun dengan jarigan Feistel fungsi dekripsi akan terbuat dengan sendirinya. Dengan logika ini, fungsi enkripsi yang digunakan bahkan tidaklah harus sebuah fungsi yang memiliki hubungan satu-ke-satu namun bisa satu-ke-n namun tetap bisa didekripsi. Hal ini bisa menjadi senjata untuk mematuhi prinsip confusion karena ciphertext yang sama bisa dihasilkan dari plaintext yang berbeda sehingga hubungan antara ciphertext dan plaintext sudah dihancurkan dengan hal ini. Beberapa fungsi yang bisa digunakan untuk ini adalah fungsi urut dengan mengurutkan seluruh byte baik menaik atau menurun, atau bahkan hanya fungsi uniform yang hanya mengembalikan satu nilai. Untuk cipher blok LS, digunakan fungsi urut karena fungsi ini juga mematuhi prinsip diffusion sehingga perubahan satu byte bisa mempengaruhi seluruh nilai dalam ciphertext.

Kemudian untuk memperbanyak kompleksitas dalam sistem dalam metode enkripsi dan untuk mengobfuskasi fungsi urut, digunakan kotak-S untuk mengobusfkasi pesan sebelum diurutkan. Kotak-S menggunakan tabel 16x16 yang dibangkitkan secara acak dengan menggunakan kunci seperti pada AES dan digunakan untuk mensubstitusi per byte. Tabel dibangkitkan dengan cara pertama tabel untuk (0x00, 0x00) diinisiasi dengan byte pertama pada key. Kemudian byte itu ditambah dengan 4 bit pertama byte kedua dan dikali 4 bit kedua kemudian di mod dengan 256 (1 byte). Jika isi tabel itu sudah diisi pada isi sebelumnya, maka isi tabel akan ditambah satu sampai isi tabel unik. Hal ini memerlukan kunci minimal sepanjang 256 byte. Namun, jika kunci kurang dari sepanjang itu, kunci bisa digunakan berulang secara periodik sampai seluruh tabel terisi.

Prinsip dari cipher berulang bisa diterapkan dalam jaringan Feistel yaitu dengan memanipulasi jumlah perulangan dalam jaringan Feistel. Dengan jumlah perulangan yang cukup, maka jaringan Feistel tidak mempunyai kelemahan untuk dimanfaatkan untuk membongkar sistem enkripsi ini.

Penulis menamakan sistem ini LS Cipher Block dengan LS merupakan singkatan dari “Lebak Siliwangi” yang merupakan lokasi dari kampus tempat penulis mempelajari ilmu ini.

III. Simulasi dan Pembahasan Hasil

Program ditulis menggunakan Bahasa Python karena kemudahannya untuk menulis program secara cepat sebagai proof-of-concept.. Dengan bahasa ini, fungsi enkripsi bisa ditulis dengan sederhana dengan

```
def f_encrypt(s, key):
    s_table = generate_s_table(key)
    return sorted(bytearray(s_table[a >> 4][a & ((1 << 4) - 1)] for a in s))
```

dan fungsi untuk membangkitkan kotak-S ditunjukkan dengan

```
index_string = 0
for i in range(16):
 for j in range(16):
  if i == 0 and j == 0:
    s_previous = s[index_string]
  else:
    s_left = s[index_string] >> 4
    s_right = s[index_string] & ((1 << 4) - 1)

    s_previous = ((s_previous + s_left) * s_right) % 0x100

    while s_previous in byte_list:
     s_previous += 1
     s_previous %= 0x100

    byte_list[s_previous] = 1

    s_table[i][j] = s_previous
    index_string += 1
    index_string %= len(s)
```

Fungsi ini akan digunakan sebagai fungsi enkripsi dalam jaringan feistel. Dalam jaringan feistel kunci bisa diambil dari potongan kunci yang panjang dan bisa diulang sebanyak n yang diinginkan.

Kita gunakan contoh pesan “LSCipher” (8 huruf, 64 bit, 1 blok) sebagai pesan standar untuk cipher ini. Informasi pesan dalam ASCII byte adalah `[76 83 67 105 112 104 101 114]`. Jaringan Feistel diatur dengan n = 51.

Pada contoh pertama digunakan kunci “KUNCIXXX”. Kunci ini memiliki informasi byte dalam ASCII `[75 85 78 67 73 88 88 88]`. Hasil enkripsi dari pesan ini adalah dalam tabel byte `[249 119 116 43 46 120 199 98]`.

Untuk contoh kedua, diubah kunci menjadi “KUNCIXXY”. Kunci ini memiliki informasi byte dalam ASCII `[75 85 78 67 73 88 88 89]`. Hasil enkripsi dari pesan ini adalah dalam tabel byte `[85 180 116 98 141 39 168 203]`. Terlihat bahwa perubahan satu huruf dalam kunci merubah seluruh isi dari ciphertext.

Untuk contoh ketiga, diubah menjadi “LSDipher” dengan kunci yang sama yaitu “KUNCIXXX”. Informasi pesan dalam ASCII byte adalah `[76 83 68 105 112 104 101 114]`. Hasil dari enkrripsi tersebut adalah `[200 121 227 28 165 237 134 185]`. Terlihat pula bahwa perubahan satu byte dalam pesan merubah keseluruhan ciphertext.

Terlihat bahwa sistem enkripsi ini sudah memenuhi seluruh prinsip cipher blok mulai dari confusion and diffusion, jaringan Feistel, cipher berulang, serta kotak-S. Sejauh ini penulis belum menemukan cara untuk membongkar ciphertext tanpa memerlukan kunci dari enkripsi ini. Cipher ini bisa digunakan bersamaan dengan berbagai metode operasi untuk cipher block mulai dari ECB, CBC, PCBC, CFB, OFB, maupun CTR.

Namun, kode ini belum secara eksplisit hanya menerima pesan sepanjan 8 byte/1 block. Implementasi lebih lanjut bisa memotong pesan menjadi pesan dalam blok-blok 8 byte dan menambahkan padding untuk pesan yang tersisa.

IV. Kesimpulan dan Saran Pengembangan

. Metode sederhana ini bisa digunakan sebagai langkah awal untuk eksplorasi penggunaaan fungsi 1-ke-n sebagai fungsi enkripsi untuk jaringan Feistel. Sistem enkripsi ini masih bisa dikembangkan untuk menutupi dan mendeteksi kelemahan yang mungkin ada dalam sistem ini serta meningkatkan kompleksitas dalam sistem ini tanpa mengurangi fleksibiltas dalam sistem ini.

Ucapan Terima Kasih

Terima kasih pada Tuhan Yang Maha Kuasa dengan rahmat dan kuasa-Nya sehingga penulis mampu menyelesaikan tugas ini. Ucapan terima kasih juga diucapkan pada Dr. Rinaldi Munir atas ilmunya mampu menunjukkan keindahan ilmu kriptografi kepada penulis.

References

[1] Shannon, Claude (1949). "Communication Theory of Secrecy Systems" (PDF). Bell System Technical Journal. 28 (4): 656–715.

[2] Katz & Lindell 2008, pp. 170–172.

[3] NIST Computer Security Division's (CSD) Security Technology Group (STG) (2013). "Block cipher modes". Cryptographic Toolkit. NIST. Retrieved April 12, 2013.