Cross-Box Block Cipher

Rizki Alif Salman Alfarisy
Teknik Informatika / Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Bandung, Indonesia
13516005@std.stei.itb.ac.id

Intan Nurjanah
Teknik Informatika / Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Bandung, Indonesia
13516131@std.stei.itb.ac.id

***Abstrak* — Algoritma block cipher merupakan algoritma dengan kunci simetri yang cukup sering digunakan saat ini. Algoritma block cipher cukup mudah untuk dirancang sehingga pengembangnya cukuplah banyak. Namun, agar algoritma block cipher aman digunakan, maka algoritma tersebut harus menerapkan prinsip confusion dan diffusion untuk mempersulit penyerang dan kriptanalis. Algoritma *Cross-Box* Cipher terfokus kepada pembagian blok plain teks menjadi 4 matriks untuk dioperasikan melalui jaringan feistel.Di dalam jaringan tersebut, algoritma menggunakan dua operasi penting yang digunakan untuk melakukan enkripsi. Operasi yang pertama adalah set operasi-operasi sederhana matriks. Sedangkan operasi kedua adalah operasi XOR yang dilakukan kepada antar matriks untuk menambah kekompleksan matriks.**

Kata Kunci* — Kriptografi, *block cipher*, matriks, operasi matriks, jaringan feistel, *confussion, diffusion

I. PENDAHULUAN

Kriptografi adalah ilmu mengenai teknik enkripsi dimana “naskah asli” (plaintext) diacak menggunakan suatu kunci enkripsi menjadi “naskah acak yang sulit dibaca” (ciphertext) oleh seseorang yang tidak memiliki kunci dekripsi. Kriptografi digunakan untuk menjaga keamanan informasi, kerahasiaan data, keabsahan data dan integritas serta otentikasi data dalam komunikasi yang aman dengan cara mengonversi pesan menjadi bentuk yang tidak bermakna bagi orang yang tidak berwenang. Kriptografi pada umumnya digunakan di bidang militer untuk melakukan pertukaran pesan, karena itu setiap orang berusaha untuk mengembangkan teknik kriptografi yang lebih baik dibandingkan yang lainnya.

Teknik kriptografi teruslah berkembang seiring dengan berjalannya waktu. Kriptografi yang awalnya dilakukan dengan melakukan substitusi ataupun transposisi, sekarang sudah mulai digantikan dengan teknik lainnya yang lebih kompleks. Salah satu dari teknik kriptografi yang populer saat ini adalah *block cipher,* yaitu algoritma untuk mengenkripsi dan mendekripsi informasi berupa kumpulan bit dengan panjang sama (*block*).

Algoritma *block cipher* biasanya menggunakan kombinasi transposisi dan substitusi dalam beberapa putaran untuk membuat enkripsi pesan lebih sulit ditebak. Namun, agar suatu *block cipher* dikatakan baik maka *block cipher* tersebut harus menerapkan konsep *confusion* dan *diffusion.* Kedua prinsip tersebut memastikan bahwa *block cipher* tersebut cenderung aman terhadap serangan kriptanalisis. Pada makalah ini, penulis merancang suatu algoritma *block cipher* bernama *Cross-Box cipher* yang memenuhi kedia konsep tersebut. *Cross Box Cipher* memecah blok pesan berukuran 64-bit menjadi 4 matriks dan melakukan operasi-operasi matriks di dalamnya untuk mendapatkan proses enkripsi yang cukup baik.

II. DASAR TEORI

A. *Block Cipher*

Block Cipher adalah teknik kriptografi dimana enkripsi dan dekripsi tidak dilakukan per bit, akan tetapi dilakukan tiap sekeumpulan bit yang disebut *block*. Enkripsi dilakukan dengan suatu kunci yang panjangnya minimal sepanjang panjang blok. Ada beberapa mode yang dapat digunakan dalam enkripsi menggunakan block cipher, diantaranya adalah :

1. Electronic code book (ECB)

   Electronic code book adalah mode enkripsi yang paling simpel dari *block chain.* Pada ECB, semua blok *plaintext* dienkripsi secara terpisah barulah digabungkan di akhir proses enkripsi. Hal yang sama juga dilakukan untuk dekripsi menggunakan ECB. Enkripsi dan dekripsi yang dilakukan secara terpisah ini memungkinkan proses enkripsi dan dekripsi untuk dilakukan di banyak thread sehingga prosesnya dapat dilakukan dengan lebih cepat. Akan tetapi, mode ini sudah jarang digunakan karena tidak efektif untuk mengenkripsi bitmap dan juga rentan terhadap *replay attack*.

2. Cipher Block Chaining (CBC)

   CBC adalah teknik enkripsi blok yang dicetuskan oleh IBM pada tahun 1976. Pada mode ini, semua blok plaintext di-XOR-kan dengan ciphertext yang sebelumnya dibuat. Untuk plaintext pertama, XOR akan dilakukan ke suatu blok random yang disebut *Initialization Vector (IV)* dengan ukuran yang sama dengan blok. Dengan ini, *cipher text* akan bergantung dengan *cipher text* sebelumnya.

   Mode ini cukup populer karena bisa menjawab permasalahan mengenai *replay attack* yang dimiliki oleh ECB. Akan tetapi, sebagai konsekuensi dari ketergantungan *cipher text* dengan teks sebelumnya maka proses enkripsi tidak dapat dilakukan secara

paralel. Sedangkan proses dekripsi masih dapat dilakukan secara paralel karena seluruh *cipher text* telah diketahui sebelumnya. Kelemahan terbesar dari mode ini adalah apabila terdapat satu kesalahan atau error di *plain text* maka kesalahan tersebut akan merambat ke seluruh teks dan merusak pesan yang akan dikirimkan.

3. Cipher Feedback (CFB)

   CFB memiliki konsep yang sama dengan CBC mengenai ketergantungan antar *cipher text.* Akan tetapi, perbedaan utama antara CFB dengan CBC adalah berbeda dengan CBC adalah input enkripsi di tuap bloknya. Pada CFB, input yang dienkripsi adalah *ciphertext* dari blok sebelumnya. Setelah *ciphertext* tersebut dienkripsi, barulah hasilnya di XOR kan dengan *plaintext* blok tersebut untuk mendapatkan hasil *ciphertext* untuk blok tersebut.

   Mode ini tidak menambah keamanan enkripsi dibandingkan dengan CBC. Akan tetapi, mode inimemungkinkan proses dekripsi dilakukan dengan algoritma yang sama dengan proses enkripsi. Sama dengan CBC, algoritma ini tidak memungkinkan enkripsi dilakukan secara paralel walaupun dekripsinya masih bisa dilakukan secara paralel. Masalah utama dari CBC mengenai kesalahan pada *plaintext* yang dapat terpropagasi ke seluruh *ciphertext* juga belum dapat dipecahkan.

4. Output Feedback (OFB)

   Mode operasi OFB mirip dengan mode CFB. Jika pada CFB n-bit antrian paling kanan dimasukkan dengan cipherteks, pada OFB, n-bit yang dimasukkan adalah n -bit hasil enkripsi terhadap antrian. Dengan metode ini, hasil *ciphertext* tidak bergantung kepada *plain text* sebelumnya sehingga dapat memecahkan permasalahan error pada *plaintext* yang dimiliki oleh CBC. Namun cara kerjanya yang mirip dengan *keystream cipher* memungkinkan (walau sangat jarang) dibuatnya pola enkripsi yang sama sehingga proses enkripsi menjadi berulang dan menurunkan keeamanan dari algoritma

5. Counter (CTR)

   Pada mode counter, *plaintext* pertama dienkripsi dengan menggunakan NONCE (*number used once)* yang fungsinya mirip dengan *Initialization Vector* pada mode-mode sebelumnya. Kemudian, blok-blok setelahnya akan dienkripsi dengan menggunakan NONCE + Counter dimana Counter adalah nilai yanh terus di-*increment* di setiap blok. Mode ini merupakan salah satu mode yang paling populer selain CBC dikarenakan proses enkripsi dan dekripsinya yang bisa dilakukan secara paralel serta error pada *plaintext* tidak akan berpengaruh ke seluruh *ciphertex.* Untuk menjamin keamanan dari mode ini, maka nilai dari NONCE harus terus diganti untuk setiap pengiriman pesan..

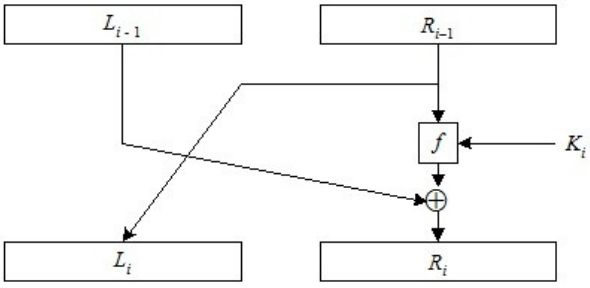
B. *Jaringan Feistel*

Struktur Feistel adalah suatu struktur simetris yang digunakan untuk mengkonstruksi block cipher. Block cipher yang menggunakan struktur Feistel akan memiliki fungsi enkripsi dan dekripsinya identik atau bahkan sama. Cara kerja struktur Feistel terbagi-bagi menjadi beberapa round. Pada setiap round, block input dibagi menjadi 2. Kemudian, setengah block pertama dijadikan masukan ke round function F bersama dengan kunci K. Hasil dari round function tersebut kemudian di-XOR dengan setengah block kedua. Setelahnya, hasilnya dijadikan input round function berikutnya, dan begitu seterusnya.

Jaringan Feistel memiliki sifat reversible. Hal ini ditunjukkan dengan persamaan berikut ini.

$$L_{i-1} \oplus \mathrm{f}(R_{i-1}, K_i) \oplus \mathrm{f}(R_{i-1}, K_i) = L_{i-1}$$

Berdasarkan persamaan di atas, fungsi XOR membuat jarigan feistel ini bersifat reversible. Agar dapat memperoleh Li-1 dari hasil XOR Li-1 dengan f(Ri-1, Ki), cukup dengan melakukan XOR pada hasil XOR sebelumnya dengan f(Ri-1, Ki). Hal ini juga yang menyebabkan fungsi f bisa dibuat serumit mungkin.



Gambar 1 Jaringan Feistel
Sumber : https://jrsricky.files.wordpress.com/2010/05/rickykkkk.jpg

C. *Shannon's Principle of Confusion and Diffusion*

Claude Shannon, seorang matematikawan asal Amerika memperkenalkan suatu prinsip dalam makalah klasiknya yang terbit pada tahun 1949, *Communication Theory of Secrecy System.* Prinsip yang dikeluarkan oleh Shannon ini terinspirasi oleh banyaknya algoritma kriptografi klasik yang dapat dipecahkan dengan menggunakan serangan statistik. Oleh karena itu, Shannon memperkenalkan prinsipnya, yakni prinsip *confusion* dan *diffusion* untuk menangani serangan statistik pada kriptografi. Berikut penjelasan dari kedua prinsip tersebut:

1. *Confusion*

   Prinsip ini menyatakan bahwa hubungan antara suatu kunci dengan *ciphertext-nya* harus dibuat sekompleks mungkin. Tujuan prinsip ini adalah untuk membuat para kriptanalis kesulitan mencari pola-pola statistik pada *ciphertext.* Prinsip ini

dapat dicapai dengan menggunakan substitusi yang kompleks pada algoritma kriptografi. Contoh dari algoritma yang memiliki *confusion* yang sangat baik adalah *One-Time Pad*.

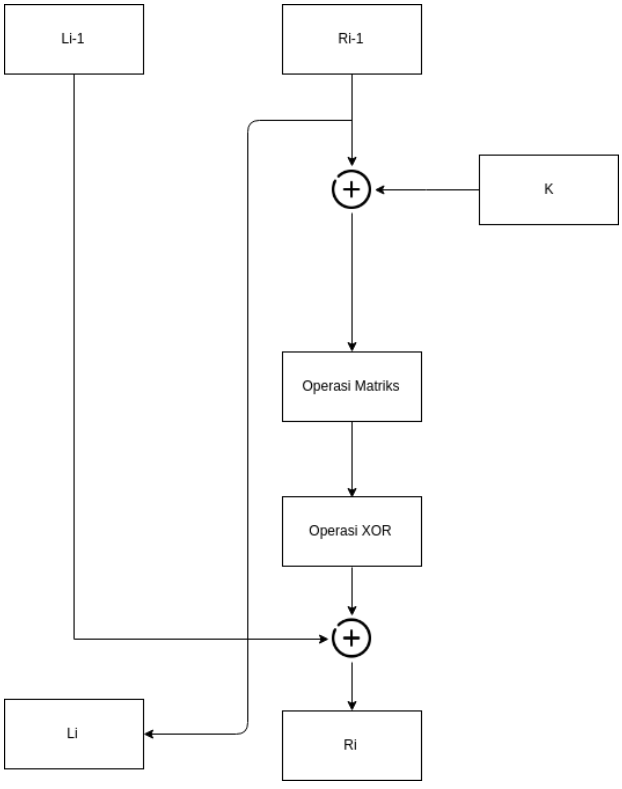
2. *Diffusion*

   Seperti namanya, prinsip ini menyatakan bahwa satu perubahan pada plaintext harus dapat menyebabkan perubahan yang tidak dapat diprediksi pada *ciphertext*. Prinsip ini pada umumnya dicapai dengan mnggunakan oeprasi permutasi yang sangat kompleks. Pengaplikasian prinsip ini biasanya dilakukan dengan menggunakan metode CBC dan CFB pada *block cipher.*

III. RANCANGAN ALGORITMA

A. *Algoritma secara keseluruhan*

Algoritma Cross-Box adalah algoritma yang memanfaatkan operasi-operasi matriks dalam proses enkripsinya. Ukuran blok dan kunci pada algoritma ini adalah 64-bit. Pada awalnya, plaintext akan diXOR kan dengan kunci. Kemudian hasilnya akan dipecah menjadi matriks berukuran 4x4 sehingga akan dihasilkan 4 matriks. Kemudian keempat matriks tersebut barulah akan dioperasikan menggunakan jaringan feistel sebanyak 8 putaran untuk menghasilkan cipher text dari Blok tersebut. Sedangkan untuk kunci dan pesan akan diberikan padding jika kurang dari 64 bit atau bukan merupakan kelipatan dari 64 bit.



Gambar 2 Jaringan Feistel *Cross-Box* Cipher

B. *Operasi Matriks*

Pada algoritma Cross-Box, keempat matriks yang telah dipecah pada awal enkripsi akan melakukan operasi-operasi berikut :

1. Operasi Shift Row
   Penggeseran seluruh baris pada matriks. Baris ke-1 akan menjadi baris ke-2, baris ke-2 akan menjadi baris ke-3 dan seterusnya.

1	0	0	1
1	0	0	1
1	0	1	0
0	1	1	0

↓

0	1	1	0
1	0	0	1
1	0	0	1
1	0	1	0

Gambar 3 Operasi Shift Row

2. Operasi Transpose
   Operasi ini sama dengan operasi transpose matriks pada umumnya. Pada operasi ini, kolom pada matriks akan ditukur menjadi baris pada matriks dan sebaliknya.

1	0	0	1
1	0	0	1
1	0	1	0
0	1	1	0

↓

1	1	1	0
0	0	0	1
0	0	1	1
1	1	0	0

Gambar 4 Operasi Transpose

3. Operasi Shift Column
   Penggeseran seluruh kolom pada matriks. Kolom ke-1 akan menjadi kolom ke-2, kolom ke-2 akan menjadi kolom ke-3 dan seterusnya.

1	0	0	1
1	0	0	1
1	0	1	0
0	1	1	0

↓

1	1	0	0
1	1	0	0
0	1	0	1
0	0	1	1

Gambar 5 Operasi Shift Column

4. Operasi Invers

1	0	0	1
1	0	0	1
1	0	1	0
0	1	1	0

↓

0	1	1	0
0	1	1	0
0	1	0	1
1	0	0	1

Gambar 6 Operasi Invers

Keempat matriks tersebut melakukan operasi tersebut pada setiap putaran secara bergantian. Misalkan jika pada putaran pertama matriks kedua melakukan operasi transpose, maka pada putaran kedua matriks tersebut akan melakukan operasi shift column, pada putaran ketiga akan melakukan operasi invers, dan seterusnya.

C. *Operasi XOR*

Operasi ini hanyalah operasi sederhana di mana matriks yang telah dioperasikan saling di-XOR kan satu sama lain. Urutan dari proses XOR ini dimulai dari Matriks 1 di XOR dengan Matriks 2, Kemudian Matriks 2 di XOR dengan matriks 3 dan seterusnya hingga matriks 4 di XOR dengan matriks 1. Alasan penggunaan operasi XOR ini adalah agar semua matriks saling mempengaruhi sehingga dapat mendukung proses *diffusion*

IV. PENGUJIAN

Bab ini menjelaskan mengenai hasil pengujian dari algoritma yang telah kami buat

A. Pengujian dengan menggunakan mode CBC

Pengujian dilakukan dengan menggunakan mode CBC sebagai mode yang paling sering digunakan pada kriptografi modern saat ini.

Plain Text

Teks

Musyawarah kerja HMIF dibubarkan karena tidak kuorum dengan keterangan yang hadir sebanyak 110/132. Untuk itu, akan diadakan musyawarah kerja pengganti yang rencananya akan diadakan minggu depan hehe.

Hex Code

4d 75 73 79 61 77 61 72 61 68 20 6b 65 72 6a 61 20 48 4d 49 46 20 64 69 62 75 62 61 72 6b 61 6e 20 6b 61 72 65 6e 61 20 74 69 64 61 6b 20 6b 75 6f 72 75 6d 20 64 65 6e 67 61 6e 20 6b 65 74 65 72 61 6e 67 61 6e 20 79 61 6e 67 20 68 61 64 69 72 20 73 65 62 61 6e 79 61 6b 20 31 31 30 2f 31 33 32 2e 20 55 6e 74 75 6b 20 69 74 75 2c 20 61 6b 61 6e 20 64 69 61 64 61 6b 61 6e 20 6d 75 73 79 61 77 61 72 61 68 20 6b 65 72 6a 61 20 70 65 6e 67 67 61 6e 74 69 20 79 61 6e 67 20 72 65 6e 63 61 6e 61 6e 79 61 20 61 6b 61 6e 20 64 69 61 64 61 6b 61 6e 20 6d 69 6e 67 67 75 20 64 65 70 61 6e 20 68 65 68 65 2e

Kunci

ayamgoreng

Cipher Text

Teks

dj?Ý□Ø□¤?##¹âõègË¶ù8ÿ$d□□5,a#
#çíª¥Ñ#Å□hz99__ê¾«9Ã
¢ï+¡5~ïFjf1#N#¾«ºêÛP□□~an&Äìøü#Kðô'©%iD¬/:fIR
2□ôï□Ìß□/ry*°ò²ÿ□a·ªnqn|%x8□C##Nµ¯ðñÚÄ□□□Ûrk±îò¾<□ ïj□
kn□□so###!□üº□□□□:29uøãõ½
#÷±<iqb□□*.#CHA&□ñ¸□□□□

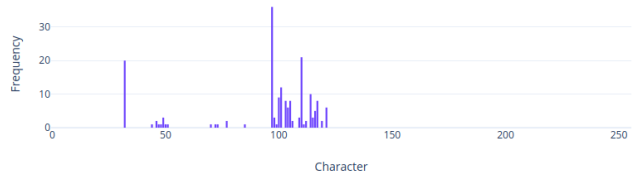
Hex Code

96 46 a3 fd d9 4d 89 4a 43 f1 60 7b 9e 2f 5e 86 7c bb 6f 93 8f f2 46 48 89 93 52 c6 11 a0 a1 5e 7e da aa 5d 10 1c 59 e6 87 a3 93 98 4e ab ea b3 9c 3a 2e f2 ba 13 57 ee f4 66 a6 63 11 04 e1 4b ea bb ae ad b5 09 79 b7 e6 16 e2 6c 4e cf 8f c0 64 bf 0f 42 7a 92 56 94 4a c2 f3 a6 64 95 20 a3 28 bf 4e f8 dc cd f8 92 f7 27 92 ab 0f 2b 2f f9 c6 1b 7a a6 e7 16 e7 c2 57 83 87 f4 31 b0 f4 eb 5a ff 0f 1d ac 49 b9 d9 ad b7 26 bb 1e ef 2b e3 c8 ea 0e f6 a7 f6 b6 e9 19 e7 36 f0 71 a0 00 b2 18 3f cb a9 c9 68 e9 43 a3 23 97 5f 8e 3f 5b d0 90 ef 7b 13 c9 71 62 95 91 2a 2e 07 43 48 41 26 87 f1 b8 8e 98 9f 87

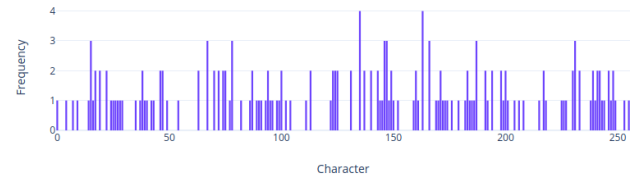
Waktu yang diperlukan	
Enkripsi	11240 microseconds
Dekripsi	12286 microseconds

B. Frequency Analysis

Plain Text



Cipher Text



Dapat dilihat pada perbandingan frequency analysis di atas terdapat perbedaan antara plain text dengan cipher text. Plain text memiliki range nilai hingga jumlah frekuensi maksimum 36, sedangkan pada cipher text jumlah frekuensi maksimum adalah 4. Selain itu dari grafik dapat dilihat bahwa pada ciphertext, karakter yang terbentuk merata untuk seluruh ASCII. Maka dari grafik tersebut dapat terbukti bahwa cipher ini memenuhi prinsip *Confusion* karena huruf yang sama dapat dienkripsi menjadi ciphertext yang berbeda.

C. Analisis pengubahan bit

Plain Text Awal

Deborah tidak boleh mengatakan kata-kata kotor dikarenakan dia adalah kadiv cultureHMIF.

Plain Text yang diubah

Deboroh tidak boleh mengatakan kata-kata kotor dikarenakan dia adalah kadiv cultureHMIF.

Cipher Text

Ib-p□Ø□□!
HI#òÿ÷¸ØH'8jo□fèhFS###_#sco□□ËÜMÆZB·ðâ¾Uy+pkxu,`
F##F##Uqò`x-□ÁÓKÀRIû´§jã3÷é&¾

Cipher Text dari Plain Text yang diubah

No-p□Ø□□!HI#òñ÷¸□E'8ao□fè/FS##_
~co□□ËÜM□ZB·þâ¾Nt+x`xu,`###F##Ujÿcp□□ÁÓK□P#û°-

§□Y'#ü2&¾

Berdasarkan hasil enkripsi dari dua teks di atas, dapat dilihat perubahan 1 karakter pada plain teks menyebabkan perubahan yang cukup banyak pada hasil *cipher text*. Hal ini membuktikan bahwa algoritma Cross-Box memenuhi prinsip diffusion karena satu perubahan dapat terpropagasi ke seluruh cipher text.

D. Analisis keamanan terhadap *brute force attack*

Panjang kunci dari algoritma *Cross-Box* sebesar 64 bit. Maka untuk melancarkan *brute force attack*, kripatanalis perlu mencoba 2^{64} kemungkinax`n yaitu sekitar $1.8 * 10^{19}$. Jika diasumsikan satu mesin membutuhkan 0.01 detik untuk melakukan satu kali dekripsi. Maka dibutuhkan sekitar $5.7 * 10^{10}$ tahun untuk mecoba seluruh kemungkinan tersebut. Oleh karena itu, menurut kami aman diasumsikan bahwa untuk mendapatkan kunci dengan menggunakan *brute force attack* hampir tidak mungkin.

V. Kesimpulan dan Saran

Berdasarkan hasil dari pengujian yang telah dilakukan, dapat disimpulkan bahwa algoritma *Cross-Box Cipher* merupakan algoritma yang sudah cukup aman. Hal ini dapat dilihat dari analisis pengubahan bit dan frekuensi yang membuktikan bahwa algoritma ini memenuhi prinsip *confusion* dan *diffusion*.

Akan tetapi, kelemahan dari algoritma ini adalah banyaknya operasi matriks yang kompleks. Operasi-operasi tersebut sangat mungkin memperlambat kecepatan enkripsi dan dekripsi jika panjang plain text bertambah. Saran dari penulis adalah menggunakan algoritma yang lebih mangkus dalam melakukan operasi-operasi matriks. Selain itu, algoritma ini juga dapat dikembangkan untuk melakukan operasi di ukuran blok yang lebih besar.

VI. Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada Tuhan Yang Maha Esa, karena atas bantuan, rahmat, dan berkat-Nya, makalah ini dapat selesai pada waktunya. Tak lupa juga, penulis ingin menyampaikan terima kasih kepada Bapak Dr. Ir. Rinaldi Munir 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. Penulis juga turut berterima kasih kepada semua orang-orang yang turut memberikan inspirasi kepada penulis dalam proses perancangan algoritma ini.

REFERENSI

[1] http://www.crypto-it.net/eng/theory/modes-of-block-ciphers.html diakses pada 11 Maret 2019, 19.22

[2] http://informatika.stei.itb.ac.id/~rinaldi.munir/ diakses pada 11 Maret 2019, 19.09

[3] https://www.researchgate.net/publication/303375974 diakses pada 12 Maret 2019, 23.23

PERNYATAAN

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

Bandung, 13 Maret 2019

Rizki Alif Salman Alfarisy	Intan Nurjanah
13516005	13516131