GATAW Block Cipher

A New Block Cipher Algorithm

Steven Nataniel Kodyat - 13519002
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
13519002@std.stei.itb.ac.id

Christopher Justine William - 13519006
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
13519006@std.stei.itb.ac.id

Daffa Ananda Pratama Resyaly - 13519107
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
13519107@std.stei.itb.ac.id

***Abstraksi*—Makalah ini membahas tentang implementasi cipher blok baru yang dirancang untuk meningkatkan keamanan data pada pengiriman informasi melalui jaringan internet. Cipher blok ini dirancang dengan algoritma yang mangkus untuk memastikan keamanan data selama proses pengiriman. Pertama-tama, makalah ini menjelaskan tentang dasar-dasar cipher blok dan mengapa cipher blok penting dalam keamanan data. Di bagian selanjutnya, makalah ini membahas tentang dasar teori dari algoritma cipher blok. Penulis kemudian menjelaskan rancangan algoritma cipher blok yang dikembangkannya. Lalu, penulis melakukan eksperimen terhadap algoritma tersebut berikut dengan menganalisis keamanannya terhadap serangan. Terakhir, makalah ini memberikan kesimpulan tentang algoritma cipher blok yang dikembangkannya.**

Kata kunci—cipher blok, keamanan

I. Pendahuluan

Dalam era digital seperti saat ini, pengiriman informasi melalui jaringan internet menjadi semakin penting dalam kehidupan sehari-hari. Namun, keamanan data selama proses pengiriman masih menjadi masalah yang harus diatasi. Data yang dikirimkan melalui jaringan internet dapat dengan mudah diakses dan disalahgunakan oleh pihak yang tidak bertanggung jawab, seperti *hacker* atau pencuri data. Oleh karena itu, perlindungan data yang efektif dan aman selama proses pengiriman sangat diperlukan.

Cipher blok adalah teknik kriptografi yang digunakan untuk mengamankan data dalam pengiriman informasi melalui jaringan internet. Cipher blok mengenkripsi data dengan algoritma kriptografi yang kuat sehingga data menjadi tidak dapat dibaca atau dimengerti oleh pihak yang tidak berhak. Cipher blok bekerja dengan cara membagi data menjadi blok-blok kecil dan kemudian mengenkripsi setiap blok dengan algoritma kriptografi yang sama.

Meskipun cipher blok telah digunakan untuk meningkatkan keamanan data dalam pengiriman informasi melalui jaringan internet, namun semakin meningkatnya teknologi dan kecerdasan para penjahat dunia maya menuntut penggunaan algoritma cipher blok yang lebih kuat dan canggih. Oleh karena itu, diperlukan implementasi algoritma cipher blok baru yang dapat meningkatkan keamanan data pada pengiriman informasi melalui jaringan internet. Algoritma cipher blok baru ini dirancang dengan menggunakan teknologi terbaru dan metode kriptografi yang lebih kuat dan canggih dengan masih berbasiskan model algoritma TwoFish, sehingga dapat memberikan perlindungan data yang lebih aman dan efektif. Dalam makalah ini, akan dibahas tentang implementasi algoritma cipher blok baru dan manfaat yang diperoleh dengan penggunaan algoritma ini dalam keamanan data.

II. Dasar Teori

A. *Confusion*

Confusion merupakan prinsip yang diperkenalkan oleh Claude Shannon pada tahun 1949. Prinsip tersebut bertujuan untuk membuat sebuah *ciphertext* menjadi lebih sulit untuk dianalisis secara statistik dengan menyembunyikan hubungan statistik antara *plaintext*, *ciphertext*, dan kunci. Prinsip *confusion* dapat diimplementasikan dengan menggunakan teknik substitusi *non-linear*.

B. *Diffusion*

Diffusion merupakan prinsip yang diperkenalkan oleh Claude Shannon bersamaan dengan *Confusion*. Prinsip *diffusion* menyebabkan pengaruh satu bit pada *plaintext* dapat mempengaruhi nilai dari banyak huruf *ciphertext*. Prinsip tersebut bertujuan untuk menyebarkan pengaruh satu bit plaintext sebanyak mungkin pada ciphertext sehingga dengan adanya perubahan satu bit di dalam *plaintext* dapat mengakibatkan *ciphertext* tidak dapat diprediksi. Prinsip *diffusion* dapat diimplementasikan dengan menggunakan teknik permutasi atau transposisi secara berulang.

C. *Teknik Substitusi*

Teknik substitusi bertujuan untuk memetakan sejumlah nilai bit masukan menjadi sejumlah bit keluaran. Hal tersebut dilakukan untuk meningkatkan efek *confusion*. Substitusi dapat diimplementasikan dengan menggunakan suatu kotak-S yang berisi matriks substitusi yang berperan dalam proses pemetaan nilai bit.

D. Teknik Permutasi

Teknik permutasi bertujuan untuk mengacak susunan bit di dalam sebuah blok bit sehingga menghasilkan susunan yang baru. Jika substitusi dapat menambah efek *confusion*, permutasi dapat menambah efek *diffusion*. Permutasi dapat diimplementasikan dengan menggunakan suatu matriks permutasi hingga pergeseran untuk mengubah susunan bit.

E. Cipher Berulang

Teknik cipher berulang bertujuan untuk menghasilkan cipher yang lebih kuat dengan melakukan *enciphering* sejumlah putaran. Jumlah putaran yang semakin banyak dapat meningkatkan efek *diffusion*. Cipher berulang dapat diimplementasikan dengan menggunakan suatu fungsi transformasi f yang dieksekusi berulang kali untuk yang mengubah *plaintext* menjadi *ciphertext*.

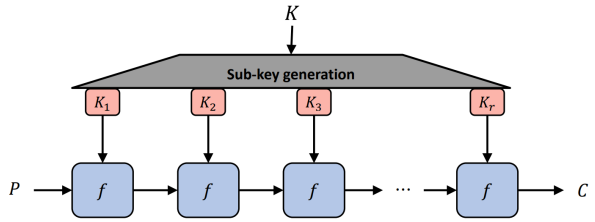

Fig. 1. Gambaran Umum Cipher Berulang. Sumber: Munir R. (2023). Block Cipher (Bagian 1)

F. Jaringan Feistel

Jaringan feistel merupakan sebuah struktur yang menerapkan *enciphering* pada setiap putarannya. Jaringan feistel pada umumnya dilakukan pada setiap blok *plaintext* dengan membagi blok tersebut menjadi dua bagian yang akan melalui proses transformasi menjadi masukkan untuk putaran selanjutnya seperti yang terlihat pada Fig.2. Struktur jaringan feistel bersifat *reversible* yang artinya untuk melakukan dekripsi, jaringan feistel dieksekusi secara berlawanan arah dengan proses enkripsi.

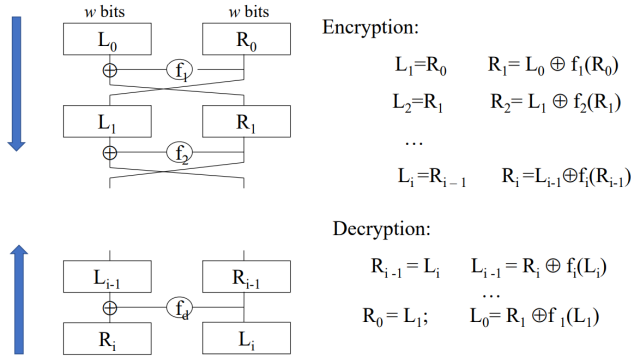

Fig. 2. Gambaran Umum Jaringan Feistel. Sumber: Munir R. (2023). Block Cipher (Bagian 1)

G. Cipher Block Chaining (CBC)

Cipher Block Chaining (CBC) merupakan sebuah mode yang dapat digunakan untuk membuat adanya ketergantungan antar blok pesan. Seperti yang terlihat pada Fig.3, setiap blok *ciphertext* tidak hanya bergantung pada blok *plaintext* tetapi juga pada seluruh blok *plaintext* sebelumnya.

Adapun kelebihan dari CBC adalah setiap blok *plainteks* yang sama tidak selalu akan menghasilkan blok *ciphertext* yang sama juga. Namun, adanya satu kesalahan bit pada sebuah blok ciphertext dapat mengakibatkan kesalahan tersebut merambat ke semua blok ciphertext selanjutnya.

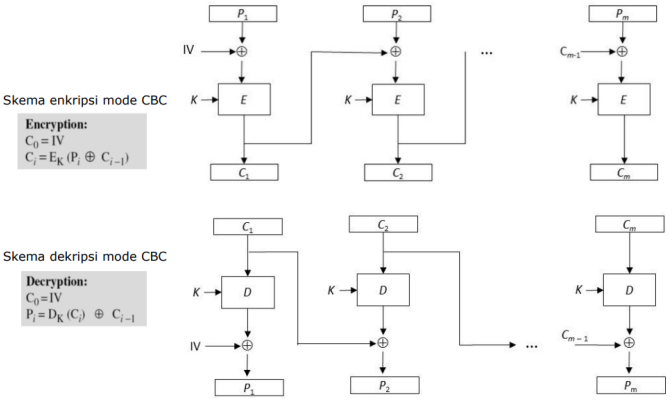

Fig. 3. Gambaran Umum Mode CBC. Sumber: Munir R. (2023). Block Cipher (Bagian 1)

III. Rancangan Block Cipher

Algoritma yang diajukan dalam makalah ini dapat mengenkripsi pesan dengan ukuran masing-masing blok nya panjang 128 bit dan ukuran kunci panjang 128 bit. Adapun jumlah putaran enciphering yang dilakukan adalah sebanyak 16 kali. Algoritma in menggunakan TwoFish sebagai dasar referensi dengan melakukan modifikasi pada jaringan feistel.

A. Jaringan Feistel

Algoritma ini menggunakan struktur jaringan *type-two* feistel yang dapat melakukan enkripsi pesan yang telah dikelompokkan menjadi sekumpulan blok dengan panjang 128 bit. Setiap blok pesan akan dibagi menjadi 4 sub-bagian dengan panjang 32 bit, yaitu X1, X2, X3, dan X4 seperti yang terlihat pada Fig.4. Blok pesan yang telah dibagi menjadi 4 bagian tersebut akan melalui 16 kali putaran *enciphering*. Untuk setiap putaran, X1 dan X2 akan melalui proses substitusi S-Box, hasil substitusi tersebut kemudian melalui proses pertukaran nilai yang melibatkan operasi XOR dengan dua buah kunci 32-bit dan operasi penjumlahan dalam modulus 2^32. Hasil pertukaran nilai tersebut akan melalui proses permutasi P-Box yang hasilnya kemudian akan melalui operasi XOR dengan X3 dan X4.

Selain menerapkan cipher berulang untuk setiap blok pesan, algoritma ini juga menerapkan mode CBC yang mengakibatkan adanya ketergantungan antar blok sehingga dapat meningkatkan efek *diffusion*.

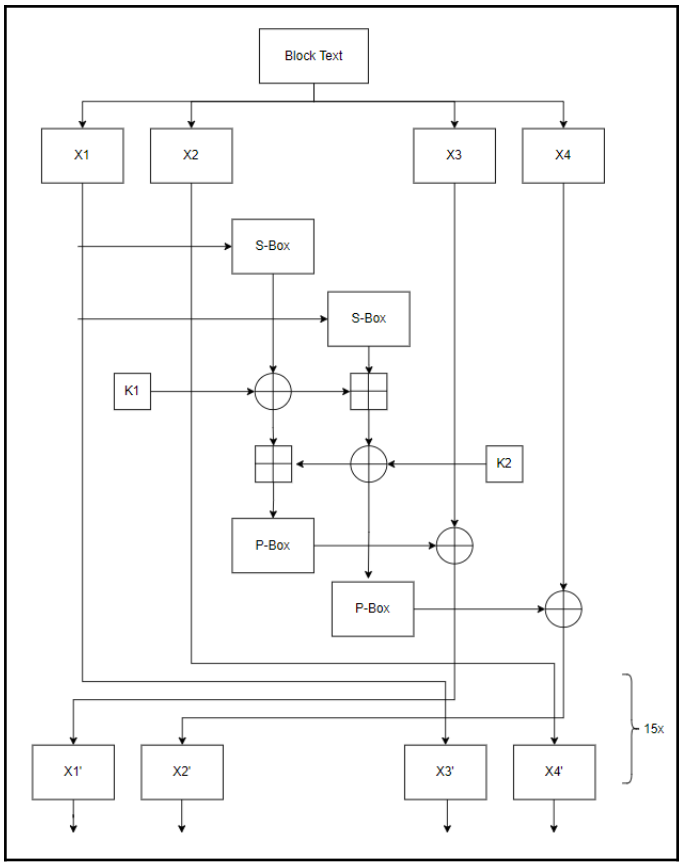

Fig. 4. Arsitektur Jaringan Feistel

B. *Pembangkitan Kunci Putaran*

Kunci putaran adalah kunci rahasia yang digunakan dalam algoritma cipher blok untuk menghasilkan kunci enkripsi yang berbeda pada setiap putaran enkripsi. Kunci putaran memainkan peran penting dalam menjaga keamanan data yang dienkripsi dengan cipher blok, karena setiap putaran enkripsi menggunakan kunci putaran yang berbeda sehingga sulit bagi pihak yang tidak berhak untuk memprediksi pola kunci enkripsi yang digunakan. Kunci putaran dihasilkan dari kunci utama yang dimasukkan ke dalam algoritma cipher blok, dan biasanya berbeda pada setiap putaran enkripsi. Dengan penggunaan kunci putaran yang berbeda pada setiap putaran enkripsi, algoritma cipher blok dapat memberikan keamanan data yang lebih tinggi dan mencegah serangan kriptografi seperti serangan Brute Force dan serangan Cipher text-only. Berikut merupakan prosedur pembangkitan kunci putaran dari algoritma yang dibangun.

1) *Key Whitening*

Key whitening adalah teknik kriptografi yang digunakan untuk meningkatkan keamanan data dalam algoritma cipher blok. Teknik ini melibatkan penggunaan dua kunci yang berbeda dalam proses enkripsi dan dekripsi data. Kunci pertama adalah kunci utama yang digunakan untuk menghasilkan kunci putaran dalam algoritma cipher blok, sedangkan kunci kedua disebut sebagai kunci whitening atau kunci putih yang digunakan untuk mengenkripsi atau mendekripsi blok data setelah proses enkripsi atau dekripsi dengan algoritma cipher blok.

Pada prosedur *key whitening* dari algoritma yang dibangun, pertama kunci eksternal yang berukuran 128 bit diubah menjadi *array of bytes* dua dimensi yang berukuran 4 x 4. Kemudian, akan dilakukan operasi XOR antara setiap *byte* dalam *array of bytes* tersebut dengan dua buah konstanta yang masing-masing berukuran 32 bit sehingga dihasilkan kunci perantara yang berukuran 128 bit.

2) *Key Schedule*

Key schedule adalah proses atau algoritma yang digunakan dalam kriptografi kunci simetris (symmetric-key cryptography) untuk menghasilkan kunci-kunci putaran (round keys) yang digunakan dalam proses enkripsi atau dekripsi. Kunci putaran adalah kunci rahasia yang dihasilkan dari kunci utama (master key) dan digunakan dalam setiap putaran enkripsi atau dekripsi dalam algoritma cipher blok.

Pada prosedur *key schedule* dari algoritma yang dibangun, dilakukan permutasi siklik dengan beberapa ketentuan dari kunci perantara yang telah dihasilkan dari fungsi *key whitening*. Hasil dari operasi permutasi ini adalah *key schedule* yang berupa *array of bytes* dua dimensi berukuran 4 x 4.

3) *S-Box Generation*

S-box adalah singkatan dari *substitution box* atau kotak substitusi. S-box merupakan sebuah tabel atau fungsi matematika yang digunakan dalam algoritma kriptografi untuk melakukan substitusi pada blok data yang dienkripsi. Setiap nilai input dalam blok data dienkripsi diganti atau digantikan dengan nilai output yang berbeda sesuai dengan tabel S-box yang telah ditentukan.

Prosedur *s-box generation* dari algoritma yang dibangun adalah perlakuan operasi XOR dari *key schedule* yang didapat sebelumnya dengan sebuah konstanta tabel S-box lainnya yang dihasilkan dari pembagian desimal pi menjadi beberapa buah byte. Dari operasi XOR tersebut, didapatlah tabel S-box baru berupa *array of bytes* dua dimensi berukuran 4 x 4 yang selanjutnya digunakan pada proses *sub-keys generation*.

4) *Sub-Keys Generation*

Prosedur *sub-keys generation* dari algoritma yang dibangun adalah, pertama, perlakuan operasi penjumlahan dari setiap byte *key schedule* dengan *s-box* yang telah dihasilkan dari proses sebelumnya sehingga didapat *sub-keys* perantara. Kemudian, akan dilakukan operasi XOR antara *sub-keys* perantara dengan akar dari bilangan desimal dalam pi dalam representasi byte sehingga dihasilkanlah *sub-keys* final berupa *array of bytes* dua dimensi berukuran 32 x 4 yang merupakan kunci internal.

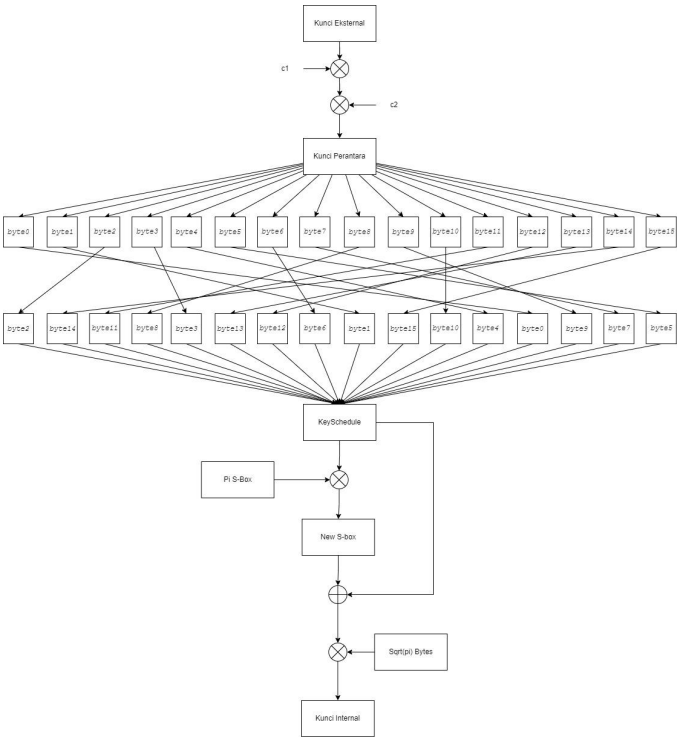

Fig. 5. Skema Pembangkitan Kunci

C. Substitusi

Substitusi (*substitution*) dalam block cipher adalah proses mengubah nilai input tertentu dalam blok *plaintext* menjadi nilai output dalam blok *ciphertext*. Hal ini dilakukan dengan mengganti nila input tersebut dengan nilai yang sudah dipetakan sebelumnya pada sebuah tabel substitusi (substitution table atau S-box).

Tabel substitusi tersebut biasanya berisi sejumlah nilai-nilai acak yang disusun dalam bentuk matriks. Proses ini dilakukan secara berulang-ulang sesuai dengan rancangan jaringan *feistel* yang telah dibuat. Substitusi ini penting untuk meningkatkan keamanan dalam block cipher karena memperumit pola dan struktur plaintext yang muncul pada *ciphertext* yang dihasilkan. Pada rancangan *block cipher* yang dibuat, tabel substitusi dibangkitkan secara acak. Fungsi substitusi yang telah dibuat menerima input *4 bytes* dan mengeluarkan output *4 bytes*. Input ini langsung dipetakan melalui Tabel S-box yang sudah dibangkitkan secara acak. Terdapat dua buah S-box dalam rancangan *block cipher* yang telah dibuat. Keduanya dibangkitkan secara acak.

D. Permutasi

Permutasi dalam block cipher adalah operasi yang mengacak posisi bit-bit dalam sebuah blok *plaintext* atau *ciphertext*. Permutasi digunakan untuk memperumit struktur dari plaintext atau ciphertext sehingga membuat pola yang terlihat sulit diidentifikasi atau diprediksi.

Pada rancangan yang telah dibuat, fungsi Permutasi yang telah dibuat menerima input berupa *4 bytes*, lalu dari *bytes* tersebut akan dipermutasikan secara *bit*, dan dikembalikan menjadi *4 bytes*. Dalam *block cipher* yang telah dibuat, terdapat dua buah p-box yang dibangkitkan secara acak.

IV. Eksperimen dan Pembahasan

A. Hasil Eksperimen

Berikut adalah hasil eksperimen *block cipher* yang telah dibuat.

```
Testcase 0 -> kriptografi
E       :  EgdFl9gskUd5gwAXvOn6BA==
E (HEX) :  [12 07 45 97 D8 2C 91 47 79 83 00 17 BC E9 FA 04]
D       :  kriptografi
E(T)    :  71.709µs
D(T)    :  54.083µs
Testcase 1 -> kr1ptografi
E       :  +DMg3yl2LmExawQ/ZDeGRw==
E (HEX) :  [F8 33 20 DF 29 76 2E 61 31 6B 04 3F 64 37 86 47]
D       :  kr1ptografi
E(T)    :  8.917µs
D(T)    :  6.209µs
Testcase 2 -> christo daffa abc
E       :  EPvrwSN0JfAZB5Ham2v0godKjJdzhAyyeV8ONM+dSvI=
E (HEX) :  [10 FB EB C1 23 74 25 F0 19 07 91 DA 9B 6B F4 82 87
4A 8C 97 73 84 0C B2 79 5F 0E 34 CF 9D 4A F2]
D       :  christo daffa abc
E(T)    :  16.333µs
D(T)    :  12.042µs
Testcase 3 -> christo daffa abd
E       :  EPvrwSN0JfAZB5Ham2v0guV8PBq1sDcXsJwz6+rzTnw=
E (HEX) :  [10 FB EB C1 23 74 25 F0 19 07 91 DA 9B 6B F4 82 E5
7C 3C 1A B5 B0 37 17 B0 9C 33 EB EA F3 4E 7C]
D       :  christo daffa abd
E(T)    :  13.708µs
D(T)    :  11.208µs
Testcase 4 -> christo viel daf
E       :  1QXk2Iu6cSXm2LXNDXqCTw==
E (HEX) :  [D5 05 E4 D8 8B BA 71 25 E6 D8 B5 CD 0D 7A 82 4F]
D       :  christo viel daf
E(T)    :  7.834µs
D(T)    :  5.459µs
```

Fig. 6. Hasil Eksperimen Pertama

```
Testcase 5 -> christo viel d4f
E       :  W9OZ/fiUigvc1UOlibJXjw==
E (HEX) :  [5B D3 99 FD F8 94 8A 0B DC D5 43 A5 89 B2 57 8F]
D       :  christo viel d4f
E(T)    :  7.833µs
D(T)    :  5.167µs
Testcase 6 -> christo vieldaff
E       :  G24UOWf8oNg6NJA/0IZiTg==
E (HEX) :  [1B 6E 14 39 67 FC A0 D8 3A 34 90 3F D0 86 62 4E]
D       :  christo vieldaff
E(T)    :  7.667µs
D(T)    :  5.792µs
Testcase 7 -> khristo vieldaff
E       :  0cTrdj/8L+TNoSon1IIfjA==
E (HEX) :  [D1 C4 EB 76 3F FC 2F E4 CD A1 2A 27 D4 82 1F 8C]
D       :  khristo vieldaff
E(T)    :  8.25µs
D(T)    :  5.25µs
Testcase 8 (1691 characters)
E(T)    :  794.791µs
D(T)    :  745.125µs
sTestcase 9 (196144444 characters)
E(T)    :  1m28.808320166s
D(T)    :  1m28.55861475s
```

Fig. 7. Hasil Eksperimen Kedua

Sebagai penjelas, E adalah hasil enkripsi dalam basis 64, sedangkan E (HEX) adalah hasil enkripsi dalam *hexadecimal*. D adalah hasil dekripsi, E(T) adalah waktu untuk enkripsi, dan D(T) adalah waktu untuk enkripsi. Untuk jumlah yang sangat besar, hasil dekripsi dan enkripsinya dihilangkan agar konten dalam makalah ini ringkas dan padat.

Hasil diatas dilakukan pada lingkungan sistem operasi **MacOS** dengan Spesifikasi 10 Core CPU dan 16 GB RAM dan dibuat menggunakan bahasa Golang.

B. Analisis Keamanan

1) Analisis Efek Longsoran

Cipher yang dirancang memakai mode *Cipher Block Chaining (CBC),* Seperti yang sudah dijelaskan pada bagian sebelumnya, perubahan sebuah karakter pada blok awal akan mengubah total blok-blok selanjutnya. Namun, apabila perubahan karakter hanya pada blok akhir, maka blok awal tidak akan tersentuh. Namun, hal ini sebenarnya sudah cukup aman karena sulit ditebak. Bisa dilihat pada hasil di bagian sebelumnya untuk memperjelas paragraf ini.

2) Analisis Ruang Kunci

Cipher ini memakai kunci 128-bit atau setara dengan 16 byte. Untuk melakukan serangan brute force, maka kombinasi kunci yang mungkin harus dicari sebanyak 2 pangkat 128. Jika kita memiliki komputer yang dapat mencoba satu juta kemungkinan dalam satu detik, maka dibutuhkan waktu sekitar $5{,}4 \times 10^{24}$ tahun untuk menemukan kunci yang tepat.

V. KESIMPULAN

Algoritma GATAW merupakan algoritma block cipher yang dirancang untuk meningkatkan keamanan data pada pengiriman informasi. Algoritma ini dapat mengenkripsi pesan dengan ukuran masing-masing blok nya panjang 128 bit dan ukuran kunci panjang 128 bit. Adapun jumlah putaran *enciphering* yang dilakukan adalah sebanyak 16 kali. Algoritma in menggunakan TwoFish sebagai dasar referensi dengan melakukan modifikasi pada jaringan feistel. Berdasarkan hasil pengujian, algoritma ini berhasil melakukan enkripsi dan dekripsi dengan sangat cepat. Secara analisis keamanan, algoritma ini sudah memiliki efek longsoran dan ruang kunci yang sulit. Namun, dari segi analisa keamanan lainnya, algoritma ini masih dapat diperbaiki lagi, karena tabel S-box dan P-box yang dibangkitkan secara acak dan hanya berjumlah masing-masing dua untuk setiap putaran.

REFERENCES

[1] Munir R. (2023). *Block Cipher (Bagian 1)*. Retrieved March 5, 2023, from https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2022-2023/13-Block-Cipher-Bagian1-2023.pdf

[2] Munir R. (2023). *Review Beberapa Block Cipher (Bagian 1: DES dan Triple DES)*. Retrieved March 5, 2023, from https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2022-2023/15-Beberapa-block-cipher-bagian1-2023.pdf

[3] Munir R. (2023). *Review Beberapa Block Cipher (Bagian 2: GOST, RC5, dll)*. Retrieved March 5, 2023, from https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2022-2023/16-Beberapa-block-cipher-bagian2-2023.pdf

[4] Hsiao, W. S. J., Gulliver, A. T. (2012). *MARC – A New Block Cipher Algorithm*. Retrieved March 5, 2023, from https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2014-2015/Paper%20Block%20Cipher%202.pdf

[5] Hsiao, W. S. J., Gulliver, A. T. (2012). *MARC – A New Block Cipher Algorithm*. Retrieved March 5, 2023, from https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2014-2015/Paper%20Block%20Cipher%202.pdf

[6] Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C., & Ferguson, N. (1998). *Twofish: A 128-Bit Block Cipher*. Retrieved March 5, 2023, from https://www.schneier.com/wp-content/uploads/2016/02/paper-twofish-paper.pdf