Pengamanan Data Teks Pada Aplikasi *Chatting* Menggunakan Metode *Modular Multiplication Based Block Chiper* (MMB) Berbasis Android

Naria Sukma Dewi[1], Amri[2], Safriadi[3]

[1,3] *Jurusan Teknologi Informasi dan Komputer Politeknik Negeri Lhokseumawe*
Jln. B.Aceh Medan Km.280 Buketrata 24301 INDONESIA

[1]nariasukmadewi@gmail.com
[2]amri@pnl.ac.id
[3]safriadi@pnl.ac.id

***Abstrak*— Aplikasi *chatting* telah menjadi media komunikasi digital yang digunakan oleh setiap kalangan, mempermudah manusia dalam mengirim pesan maupun menerima pesan. Pesan-pesan yang disampaikan ada kalanya berupa pesan yang bersifat rahasia sehingga tidak semua pihak dapat melihat pesan tersebut. Namun sering terjadinya kejahatan seperti penyadapan data, pencurian informasi, dan penyalahgunaan data pribadi yang merupakan masalah yang paling ditakuti oleh para pengguna jaringan komunikasi. Maka diperlukan suatu sistem keamanan yang dapat melindungi suatu informasi untuk menyembunyikan atau mengamankan suatu pesan ke dalam bentuk pesan lain. Untuk menyelasikan permasalah tersebut terdapat sebuah pembelajaran tentang kriptografi yang dapat mengenkripsikan pesan atau teks kedalam bentuk *chipertext* sehingga dapat menyembunyikan pesan asli yang dikirimkan. Tujuan penelitian ini untuk melakukan pengaman data teks pada aplikasi chatting menggunakan metode *Modular Multiplication-Based Block Chiper (MMB)* dengan mengetahui berapa lama waktu enkripsi sebuah pesan dan untuk mengetahui panjang karakter pesan setelah dienkripsi. Dari pengujian tersebut diperoleh bahwa rata-rata waktu enkripsi dan dekripsi pesan membutuhkan waktu sebesar 1.87 detik. Untuk panjang pesan setelah dienkripsi karakter yang dihasilkan sebanyak 32 Hexadesimal atau 16 karakter *chiphertext*.**

***Kata kunci*—** *Kriptografi, Modular Multiplication-Based Block Chiper , MMB, Aplikasi chatting, chiphertext*.

.

Abstract*— *Chatting applications become a digital communication used by every group, it making easier for humans to send messages and receive messages. The messages conveyed sometimes in the form of messages that are confidential so that not all parties can see the message. However, the frequent occurrence of crimes such as data eavesdropping, information theft, and misuse of personal data are the problems most feared by communication network users. So we need a security system that can protect information to hide or secure a message in the form of another message. To solve this problem there is a learning about cryptography that can encrypt messages or text into ciphertext so that it can hide the original message sent. The purpose of this study is to protect text data in chat applications using the Modular Multiplication-Based Block Ciper (MMB) method by knowing how long it takes to encrypt a message and to determine the character length of the message after it has been encrypted. From these tests, it was found that the average time for message encryption and decryption was 1.87 seconds. The length of the message after being encrypted is 32 Hexadecimal or 16 characters of ciphertext.

***Keywords*—** *Cryptography, Modular Multiplication-Based Block Ciper, MMB, Chatting application, Ciphertext.*

I. PENDAHULUAN

Perkembangan teknologi membuat komunikasi semakin mudah. Salah satu media komunikasi yang sering digunakan berupa aplikasi chatting. Aplikasi chatting telah menjadi media komunikasi digital yang digunakan oleh setiap kalangan, mempermudah manusia dalam mengirim pesan maupun menerima pesan. Dengan adanya aplikasi tersebut komunikasi menjadi lebih efektif dan efisien dibandingkan dengan cara komunikasi lainnya. Pesan yang disampaikan ada kalanya berupa pesan yang bersifat rahasia sehingga tidak semua pihak dapat melihat pesan tersebut [1].

Namun tidak semua perkembangan teknologi komunikasi memberikan dampak yang positif dan menguntungkan. Beberapa dampak negatif dalam perkembangan teknologi adalah adanya penyadapan data, pencurian informasi, dan penyalahgunaan data pribadi yang merupakan masalah yang paling ditakuti oleh para pengguna jaringan komunikasi [2]. Sejak tahun 2013 kasus penyalahgunaan data mulai meningkat. Saat itu, Yahoo mengalami pelanggaran data pengguna. Akibat insiden ini, 3

miliar akun Yahoo diretas dan data tersebut digunakan untuk tujuan yang tidak semestinya. Pada tahun 2018 terjadi lagi penyalahgunaan data terbesar yaitu penyalahgunaan data pribadi pengguna Facebook. Sampai 9 miliar akun seseorang disalahgunakan oleh pihak tertentu. Penyalahgunaan data dimulai dari pencurian data yang dilakukan oleh hacker, kemudian data yang dicuri digunakan untuk kepentingan lainnya. Seperti pembobolan ATM, pelecahan seksual, dan pencemaran nama baik [3].

Berdasarkan permasalahan tersebut maka aspek keamanan dalam pertukaran informasi dianggap penting, karena suatu komunikasi jarak jauh belum tentu memiliki jalur transmisi yang aman dari penyadapan dan kejahatan cyber lainnya. Maka diperlukan suatu sistem keamanan yang dapat melindungi suatu informasi untuk menyembunyikan atau mengamankan suatu pesan ke dalam bentuk pesan lain. Untuk menyelasikan permasalah tersebut terdapat sebuah pembelajaran tentang Kriptografi yang dapat mengenkripsikan pesan atau teks kedalam bentuk chipertext sehingga dapat menyembunyikan pesan asli yang dikirimkan.

Menurut Dewandaru dalam penelitannya pada tahun 2016, ilmu kriptografi yang mempelajari tentang cara merahasiakan sebuah pesan teks dan mengembalikan pesan tersebut ke bentuk semula, memeiliki beberapa metode yang dapat digunakan untuk mengamankan data, salah satunya adalah metode MMB (Modular Multiplication-based Block Cipher) [1]. Proses yang dilakukan pada penelitian ini dengan mengenkripsi data teks dengan kunci acak menggunakan metode Modular Multiplication-based Block Cipher (MMB). Metode MMB dapat digunakan untuk mengamankan data yang berbasis Block Cipher yang digunakan untuk mengenkripsi dan mendekripsi suatu pesan atau informasi.

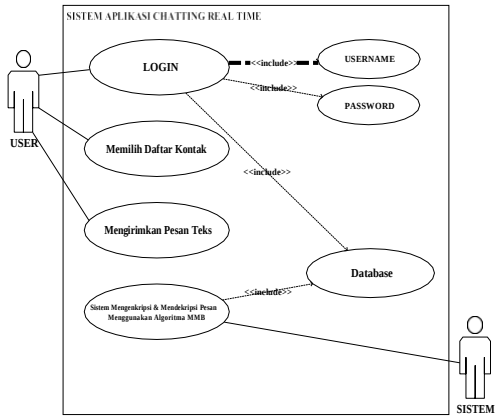
II. METODOLOGI PENELITIAN

A. Perancangan Sistem

Perancangan sistem digunakan untuk menjelaskan gambaran mengenai perancangan sistem yang akan dibuat. Perancangan sistem pada tugas akhir ini terdiri dari perancangan *Use Case* diagram, diagram *activity*, dan *flowchart*.

1. *Use Case* diagram

Use Case diagram sistem yang bertujuan untuk memberikan gambaran serta penjelasan mengenai sistem yang akan dibuat. *Use Case* diagram sistem dapat dilihat pada gambar 1.

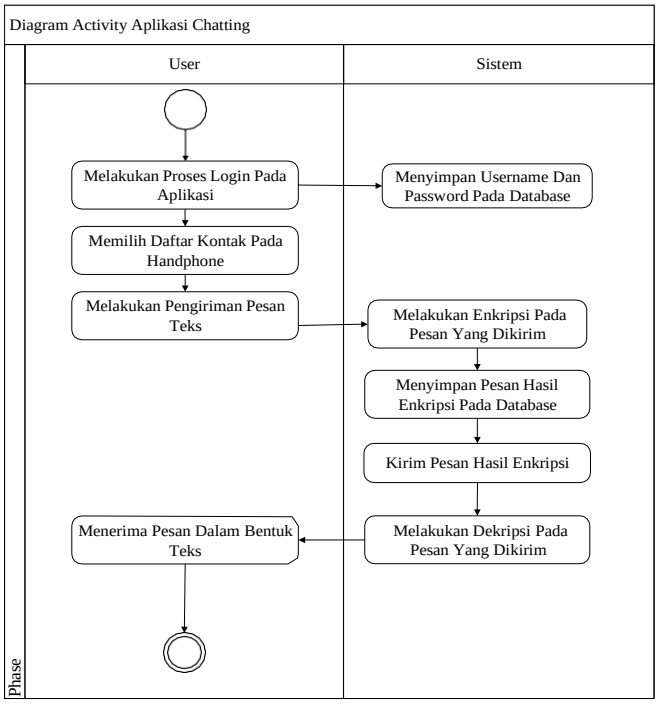


Gambar 1 *Use Case* Diagram

Pada use case diagram diatas mmenjelaskan terdapat dua orang entitas berupa *user* dan *system*. *User* akan melakukan *login* kedalam aplikasi dengan menggunakan *usename* dan *password* yang akan tersimpan kedalam table database. Kemudian user dapat memilih daftar kontak untuk melakukan *chatting*. Setelah mengirimkan pesan, sistem akan menyimpn pesan yang dikirimkan dan menyimpampan hasil enkripsi dan dekripsi kedalam database.

2. Diagram *Activity*

Diagram *Activity* sistem yang bertujuan untuk memberikan gambaran aktivitas *user* dalam penggunaan sistem serta penjelasan mengenai sistem yang akan berjalan. Diagram *Activity* dari sistem dapat dilihat pada gambar 2.



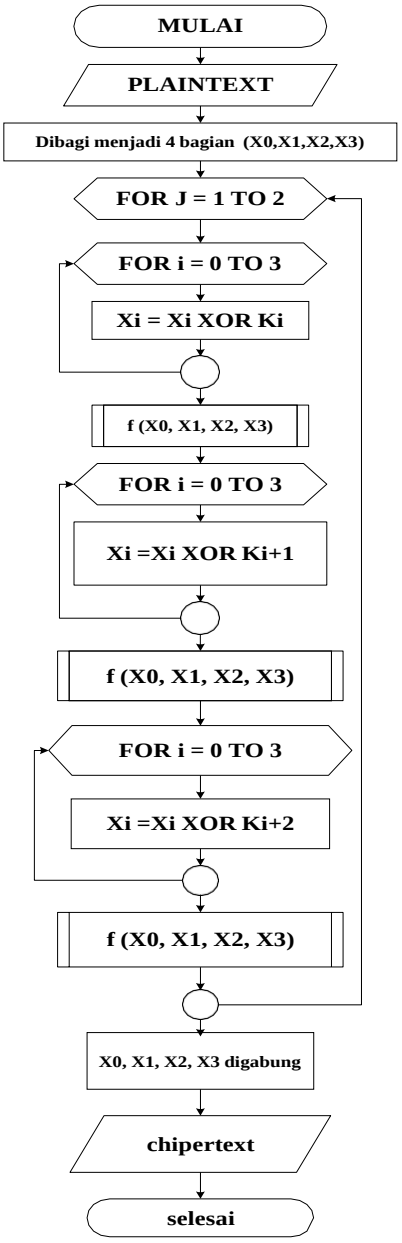
Gambar 2 Diagram *Activity* system

Pada *Activity Diagram* ini menjelaskan aliran kerja pengguna saat login pada aplikasi *chatting* kemudian *user* melakukan proses *login/register* kemudian *user* memilih daftar kontak yang tersedia. Kemudian *user* dapat memilih daftar kontak untuk melakukan *chatting*. Setelah mengirimkan pesan, sistem akan menyimpn pesan yang dikirimkan dan menyimpampan hasil enkripsi dan dekripsi kedalam *database*. Kemudian sistem melakukan proses dekripsi pesan yang dikirim. Pada saat pesan di dekripsi proses yang dilakukan terjadi pada database, database akan menyimpan pesan asli dan dan hasil enkripsi dalam bentuk *chipertext.*

3. *Flowchart*

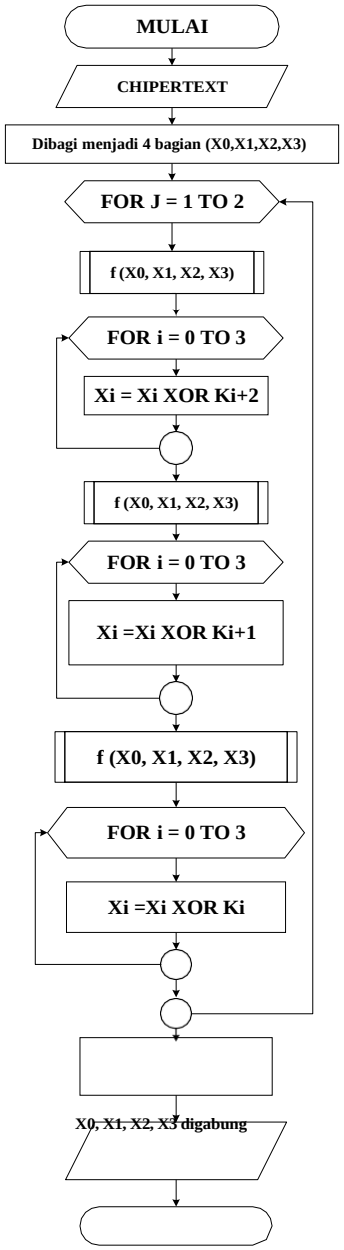
Flowchart akan menjelaskan alur kerja atau urutan jalannya suatu sistem secara keseluruhan pada pengaplikasian metode Modular Multiplication-based Block Cipher (MMB) yang akan diterapkan pada aplikasi *Chatting dan proses penggunaan aplikasi Chatting*. *Flowchart* tersebut terdiri dari *flowchart* proses enkripsi, *flowchart* proses dekripsi dan *flowchart* fungsi *f*. *Flowchart* proses enkripsi, *flowchart* proses dekripsi dan *flowchart* fungsi *f* dapat dilihat pada gambar 3, 4, dan 5.

a. *Flowchart* Proses Enkripsi



Gambar 3 *Flowchart* proses enkripsi

b. *flowchart* proses dekripsi



Gambar 4 *Flowchart* proses dekripsi

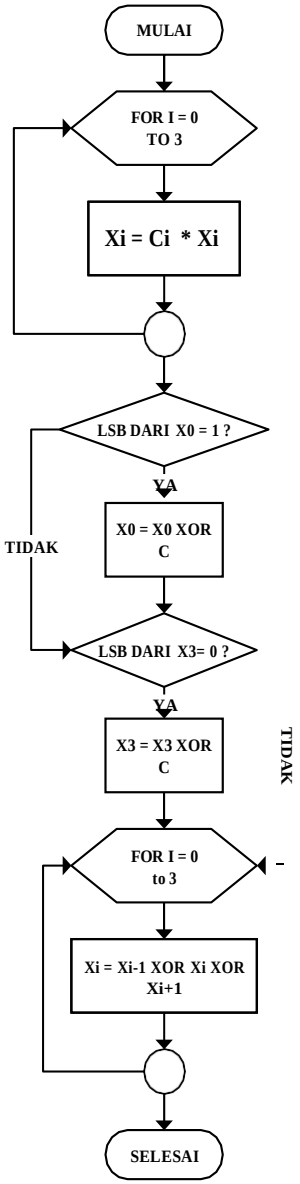
Pertama – tama, plaintext 64 bit dibagi menjadi 4 buah sub blok dengan panjang 16 bit, yaitu X_1, X_2, X_3, X_4. Empat sub blok ini menjadi masukan bagi iterasi tahap pertama algoritma. Total terdapat 8 iterasi. Pada setiap iterasi, 4 sub blok di-XOR-kan, ditambahkan, dikalikan dengan yang lain dan dengan 6 buah subkey 16 bit. Diantara iterasi sub blok kedua dan ketiga saling dipertukarkan. Akhirnya 4 buah sub blok dikombinasikan dengan 4 subkey dalam transformasi output. Pada setiap tahapan, urutan berikut ini dikerjakan :

1) Kalikan X_1 dengan K_1 mod $(2^{16} + 1)$.
2) Tambahkan X_2 dengan K_2 mod 2^{16} .
3) Tambahkan X_3 dengan K_3 mod 2^{16} .
4) Kalikan X_4 dengan K_4 mod $(2^{16} + 1)$.
5) XOR hasil dari step 1 dan 3.
6) XOR hasil dari step 2 dan 4.

Algoritma yang digunakan pada proses dekripsi agak sedikit berbeda dengan proses enkripsi. Inti proses dekripsi dari metode MMB dapat dijabarkan seperti berikut :

1. Cipherteks dibagi menjadi 4 subblock yang sama besar (P_0…….P_3).
2. Melakukan operasi XOR antara cipherteks dengan kunci yang keempat (K_3), kemudian gunakan fungsi f.
3. Melakukan operasi XOR antara cipherteks dengan kunci yang ketiga (K_2), kemudian gunakan fungsi f.
4. Melakukan operasi XOR antara cipherteks dengan kunci yang kedua (K_1), kemudian gunakan fungsi f.
5. Melakukan operasi XOR antara cipherteks dengan kunci yang pertama (K_1), kemudian gunakan fungsi f.
6. Ulangi langkah 2 sampai 5 sebanyak satu kali.
7. Gabungkan 4 subblock sehingga didapatkan plainteks.

c. Flowchart Fungsi *F*



Gambar 5 *Flowchart* Fungsi *f*

Fungsi *f* yang digunakan memiliki tiga langkah yaitu :

a. For i = 0 to 3
   Xi = Ci * Xi
   next i
b. Jika LSB (Least Significant Bit) dari $X_0 = 1$, maka $X_0 = X_0$ XOR C.
c. Jika LSB dari $X_3 = 0$, maka $X_3 = X_3$ XOR C.
d. For i = 0 to 3
   Xi = Xi-1 XOR Xi XOR Xi+1
   next i

Operasi perkalian yang digunakan merupakan operasi perkalian modulo $2^{32} - 1$. Sedangkan konstanta yang digunakan dapat dirincikan sebagai berikut:

- $C = (2AAAAAAA)_{16}$
- $C_0 = (025F1CDB)_{16}$
- $C_1 = 2 * C_0$
- $C_2 = 2^3 * C_0$
- $C_3 = 2^7 * C_0$

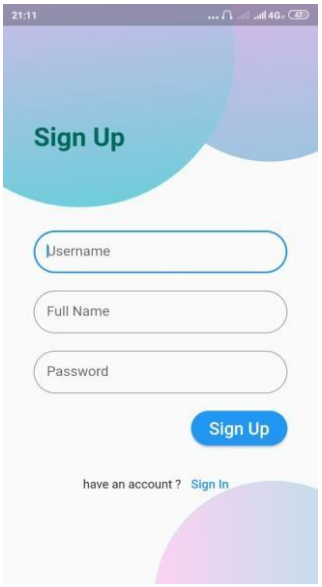
III. HASIL DAN PEMBAHASAN

A. Implementasi Aplikasi

Aplikasi yang dibangun memiliki beberapa antarmuka seperti tampilan *Login* dan *register/ sign in*, tampilan *profile*, tampilan *list chat*, dan tampilan *room chat*. Penjelasan penggunaan dan fungsi dari masing masing tampilan tersebut akan diuraikan sebagai berikut.

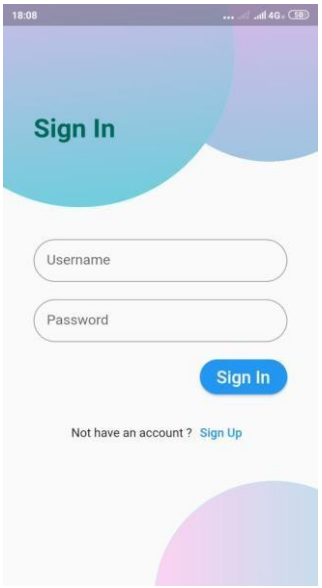
1. Halaman *Register* dan *Login*

Tampilan register/sign up, user dapat melakukan proses mendaftar untuk mendapatkan hak akses pada aplikasi dengan memasukkan identitas berupa *username* pengguna, *full name* atau nama lengkap dan kata sandi agar dapat menggunakan aplikasi tersebut. Implementasi halaman register dapat dilihat pada gambar 6.



Gambar 6 Tampilan Halaman Register

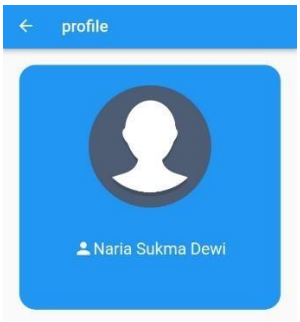
Selanjutnya tampilan *Sign In*, pada tampilan *Sign In user* dapat melakukan proses autentikasi untuk masuk pada aplikasi *Chatting* berbasis *mobile*. Tampilan login dari aplikasi yang dibangun dapat dilihat pada gambar 7 berikut:



Gambar 7 Tampilan Halaman *Sign In*

2. Halaman *Profile*

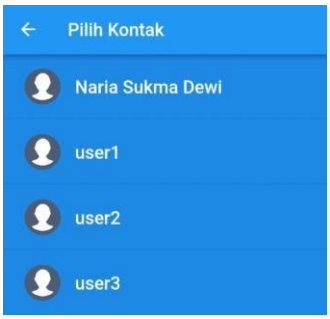
Tampilan *profile*, pada bagian tampilan *profile User* dapat mengedit foto profil dan nama. Tampilan *Profile* pada aplikasi *chatting* dapat dilihat pada gambar 4.3 berikut:



Gambar 8 Tampilan *Profile* pada aplikasi *Chatting*

3. Halaman *List Contact*

Terdapat tampilan list contact pada aplikasi chatting, untuk dapat melihat berapa banyak contact yang tersedia. Tampilannya *List Contact* dapat dilihat pada gambar 9 berikut:



Gambar 9 Tampilan *List Contact*

4. Halaman *Room Chat*

Selain tampilan list contact terdapat tampilan *Room Chat* pada aplikasi chatting, yang menampilkan balon percakapan antar pengguna. Berikut tampilannya *Room Chat* pada aplikasi dapat dilihat pada gambar 10 dibawah:

Gambar 10 Tampilan *Room Chat* pada aplikasi *Chatting*

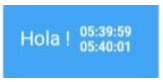
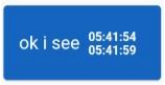
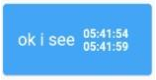
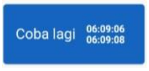
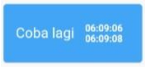
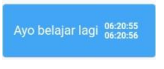
B. Pengujian Metode *Modular Multiplication-Based Block Chiper* (MMB)

Berikut pengujian yang dilakukan sesuai dengan rumusan masalah pada penelitian ini berupa lama waktu yang dibutuhkan untuk proses enkripsi dan dekripsi pesan yang dikirim dari aplikasi *chatting*, dan panjang karakter sebelum dan setelah dienkripsi.

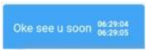
a. Pengujian Waktu Pengiriman Pesan

Berikut akan dilakukan pengujian waktu yang dibutuhkan dalam proses enkripsi dan dekripsi pesan mengggunakan metode *Modular Multiplication-Based Block Chiper (MMB).* Pada pengujian ini akan dilakukan pengujian sebanyak 8 kali dengan teks yang berbeda-beda untuk melihat berapa lama waktu yang dibutuhkan untuk proses enkripsi dan dekripsi dapat dilihat pada tabel 1 brikut ini :

TABEL I
HASIL PENGUJIAN WAKTU PENGIRIMAN PESAN

Pesan User1	Pesan User 2	Size	Waktu
		6 Bytes	2 detik
		15 Bytes	1 detik
		8 Bytes	5 detik
		10 Bytes	2 Detik
		16 bytes	1 Detik
		9 Bytes	2 Detik
		16 Bytes	1 Detik

P-ISSN : 2797-054X
E-ISSN : 2777-001X

		16 Bytes	1 Detik

Hasil pengujian pada tabel 1 diatas adalah berapa lama waktu yang di butuh kan untuk mengenkripsi pesan teks dalam proses mengirim pesan dari aplikasi *chatting*. Pada tabel diatas dapat dilihat durasi waktu yang paling lama dibutuhkan untuk melakukan proses enkripsi dan dekripsi sebuah pesan adalah 5 detik dan durasi waktu yang paling cepat untuk proses enkripsi dan dekripsi adlah 1 detik. Hal tersebut bias terjadi karna beberapa faktor salah satunya adalah karna kecepatan koneksi internet/ wifi dan panjang dan pendeknya karakter yang dienkripsi. Adapun Rata-rata durasi waktu yang dibutuhkan dalam proses enkripsi dan dekripsi dapat diperoleh dari perhitungan berikut :

Rata-rata waktu = 15 / 8
= 1,87 Detik

Dari sampel diatas dapat disimpulkan rata-rata waktu yang dibutuhkan dalam proses enkripsi dan dekripsi pada aplikasi *chatting* menggunakan metode *Modular Multiplication-Based Block Chiper (MMB)* 1,87 detik. Hasil rata rata wktu yang didapatkan dengan menjumlahkan waktu yang diperoleh dari setiap pengujian kemudian dibagi banyaknya pengujian. Setelah melakukan pengujian diatas dapat dilihat perbedaan perbedaan size pesan yang dikirimkan dan waktu yang dibutuhkan, pada teks “ini naria sukma” dengan ukuran size 15 Bytes membutuhkan waktu enkripsi yang lebih singkat yaitu 1 detik. Dan pada sampel teks “ok i see” yang memiliki size 8 Bytes lebih kecil dari pada teks “ini naria sukma” sebelumnya. Hal tersebut bisa terjadi dikarnakan algoritma *Modular Multiplication-Based Block Chiper (MMB)* tetap mengeksekusi 16 karakter, walaupun size teks yang dikirimkan lebih kecil algoritma ini akan menambahkan NULL agar panjang teks yang dieksekusi tetap terdiri dari 16 karakter sehingga waktu yang dibutuhkan akan lebih besar dikarnakan algoritma akan melakukan pengecekan terhadap ukuran teks dan ditambahkan dengan NULL jika teks tersebut kurang dari 16 karkater, oleh karena itu dibutuhkan waktu yang lebih panjang untuk melakukan proses enkripsi pada teks yang size kecil daripada teks yang dikirimkan dengan ukuran 16 karakter.

b. Pengujian Panjang Karakter Pesan Setelah Enkripsi

Berikut ini merupakan pengujian panjang karakter pesan yang dikirimkan sebelum dienkripsi dan setelah dienkripsi pada aplikasi *chatting*. Tujuan pengujian ini untuk melihat apakah ada perbedaan dan pengacakan pada hasil *chipertext* yang telah dienkripsi pada pengujian ini akan dilakukan sebanyak 7 kali pengiriman pesan, dengan menggunakan kunci yang sama yang terdiri dari 16 karakter yaitu “NARIA SUKMA DEWI” dan karakter pesan yang terdiri dari 16 karakter. Untuk hasil pengujian tersebut dapat dilihat pada Tabel 2.

TABEL 2
HASIL PENGUJIAN PANJANG KARAKTER PESAN

No	**Plaintext**	**Hasil Enkripsi (*Chipertext*)**	**Biner**
1	AYO BELAJAR LAGI	17 0c 16 19 0f 61 0b 08 0f 67 73 1c 00 18 15 00	00000101000111000001100 00110100100001100000001 00000111100000100000001 01101100001000000010111 01010000011100001100000 0011001101001
2	HELLO WORLD !	74 75 67 01 0b 0d 1e 06 61 77 1c 07 07 09 61 01	01110100011101010110011 10000000100001011000011 01000111100000011001100 00101110111000111000000 01110000011100001001011 0000100000001
3	12345678910111213	75 77 64 7d 7b 77 65 71 78 11 63 64 7a 7c 73 11	01110101011101110110010 00111110101111011011101 11011001010111000101111 00000010001011000110110 01000111101001111100011 1001100010001
4	pasti bisa jalan	41 50 42 46 58 12 51 5d 46 41 16 5d 59 55 51 4e	01000001010100000100001 00100011001011000000100 10010100010101110101000 11001000001000101100101 11010101100101010101010 1000101001110
5	Naria Sukma Dewi	7f 50 43 5b 50 12 60 41 5e 4d 57 17 7c 5c 47 49	01111111010100000100001 10101101101010000000100 10011000000100000101011 11001001101010101110001 01110111110001011100010 0011101001001
6	@#$%^&*()!!<>?_ =	71 12 15 17 6f 14 19 1c 1c 01 17 0b 06 06 6f 1d	01110001000100100001010 10001011101101111000101 00000110010001110000011 10000000001000101110000 10110000011000000110011 0111100011101
7	EMPAT + tiga = 7	73 7a 68 78 25 57 4e 52 00 10 47 50 12 0e 14 02	0111001101111101001101 0000111100000100101 01 0101110100111001010 01 0000000000000100000100 0111010100000000100100 0001110000010100000000 10
8	Pengamanan DATa TEKS PADA aplikasi CHATTNG	66 52 56 5e 10 1a 04 1c 15 17 00 75 73 67 55 15	0110011001010010 01010 1100101111000010 00000 0110100000010000 01110 0000101010001011 10000 0000011101010111 00110 1100111010101010 00101 01
9	TUGAS AKHIR	06 07 08 09 41 23 30 35 35 2a 00 70 79 7b 7d 67	0000011000000011100001 0000000100101000001 00 1000110011000000110 10 1001101010010101000 00 0000011100000011110 010 1111011011111010110 01 11

10	qwerty 123456789	47 40 5d 4b 05 0e 45 43 46 4a 14 04 04 04 0c 0c	01000111010000000 1011 10101001011000001 0100 00111001000101010 0001 10100011001001010 0001 01000000010000000 1000 00001000000110000 0011

Berdasarkan tabel 2 Pengujian yang dilakukan dengan mencoba berbagai macam bentuk karakter huruf, angka, symbol untuk melihat apakah hasil enkripsi yang berupa *chipertext* yang dihasilkan berbeda beda atau sama panjangnya pengujian diatas dapat dilihat perbedaan *chipertext* hasil enkripsi yang signifikan daripada karakter asli. Plaintext yang dikirimkan berbeda beda dengan menggunakan kunci yang sama. Jika kunci kurang dari 16 karakter maka proses enkripsi tidak akan berjalan. *Chipertext* yang dihasilkan setelah enkripsi berbentuk nilai hexadecimal yang akan diubah kedalam bentuk biner agar dapat melakukan proses dekripsi kembali sehingga pesan asli akan tersampaikan dalam bentuk *plaintext*.

VI. KESIMPULAN

Berdasarkan hasil pembahasan dan pengujian simpulkan setelah melakukan penelitian mengenai Pengamanan Data Teks Pada Aplikasi *Chatting* Menggunakan *Metode Modular Multiplication-Based Block Chiper (MMB)* Berbasis *Android* yaitu :

a. Berdasarkan hasil pengujian pengiriman pesan pada aplikasi *chatting*, rata-rata waktu yang dibutuhkan untuk proses enrkipsi dan dekrisi pada aplikasi *chatting* menggunakan metode *Modular Multiplication-Based Block Chiper (MMB)* sebanyak 1,87 detik.
b. Pada pengujian panjang karakter yang dihasilkan setelah enkripsi terdiri dari 16 *chiper text* dan dalam bentuk Hexa desimal terdiri dari 32 karakter.
c. Kelemahan metode MMB pada program aplikasi yang telah dibangun, hanya dapat mengenkripsi *plaintext* dengan ukuran 16 karakter dan kunci yang digunakan untuk mengenkripsi dan dekripsi pada aplikasi menggunakan kunci yang sama.

IV.REFERENSI

[1] Dewandaru , Fajar. 2016 (Februari). “Aplikasi Keamanan Data Menggunakan Metode MMB Dan LSB”, *Jurnal Informatika Polinema*. 2, (2), hal. 61-65.

[2] Rudiyanto. 2018 (Mei). “Implementasi Kriptografi Untuk Pengamanan Pesan Teks Pada Aplikasi Chatting Berbasis Android Dengan Metode Vigenere Cipher Pada SMK Negeri 7 ota Tangerang”, Jurnal SKANIKA (Sistem Komputer dan Teknik Informatika). 2,(1), hal 758-765.

[3] Andriyanto , Heru (2018). “Data Bocor, Facebook Terancam Sanksi Berat”. https://www.beritasatu.com/fokus/data-facebook-bocor Diakses 14 Desember 2021.

[4] Kromodimoeljo , Sentot. TEORI & APLIKASI KRIPTOGRAFI. Jil. 1, Cet. Ke-1. Jakarta: SPK IT Consulting.2009.

[5] Situmeang, Sahat Maruli Tua. “Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber”, desember 2021 (online) https://fhukum.unpatti.ac.id/jurnal/sasi/article/view/394/285 Diakses 1 desember 2021

[6] Juliadi, Prihandono, B. & Kusumastuti, N., 2013. “Kriptografi Klasik Dengan Metode Modifikasi Affine Cipher Yang Diperkuat Dengan Vigenere Cipher”. Buletin Ilmiah Mat. Stat. dan Terapannya (Bimaster), 2(2), hal.87–92.

[7] Juliarto, Rendi (2021). “Apa itu UML? Beserta Pengertian dan Contohnya”. https://www.dicoding.com/blog/apa-itu-uml/ . Diakses 14 november 2021.

[8] Ramadhan, A. O., Tolle, H., & Fanani, L. (2018). “Pembangunan Modul Penunjang Pembelajaran di Kelas Untuk Aplikasi Brawijaya Messenger Dengan Platform Firebase”.8, 2(4), 1630–1637.

[9] Wibowo, Dimas Catur. 2019 (Mei). “Apa itu Android? Kenapa Developer Memilih Android ?”. https://www.dicoding.com/blog/apa-itu-androidkenapa-developer-memilih-android/ Diakses 18 Desember 2021.

[10] Endah. (2020).Fungsi Android Studio. https://metodeku.com/fungsi-androidstudio/ . Diakses 22 November 2020.

[11] Latief, Mukhlisulfatih. 2010 (Desember). “Studi Perbandingan Enkripsi Menggunakan Algoritma IDEA Dan MMB” MEDIA ELEKTRIK. 5 (2)

[12] Ibnu. 2022 (Maret). **“**Flutter Adalah Framework Pengembang Aplikasi”. https://accurate.id/teknologi/flutter-adalah/ Diakses 18 Desember 2021.