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

Aplikasi Pengamanan Data Menggunakan Algoritma Modular Multiplication Based Block Chiper (MMB)

Safriadi[1], Mursyidah[2], Umri Erdiansyah[3], Muhammad Davi[4]

[1,2,3,4] *Jurusan Teknologi Informasi dan Komputer Politeknik Negeri Lhokseumawe Jln. B.Aceh Medan Km.280 Buketrata 24301 INDONESIA*

[1]safriadi@pnl.ac.id

***Abstrak*— Teknologi informasi dan komunikasi yang sangat berkembang saat ini dianggap semakin mempermudah proses pengolahan, penyimpanan dan pendistribusian data dan informasi sehingga mempermudah dalam mengakses data dan informasi. Seperti halnya penyimpanan dokumen, dapat disimpan di cloud, yang mana kita dapat mengakses file tersebut dimana saja akan tetapi muncul beberapa permasalahan seperti penyimpanan dokumen serta data-data penting, apabila data dan informasi penting tersebut dapat diakses oleh pihak yang tidak berwenang maka dapat berakibat kerugian bagi pihak pemilik dari dokumen tersebut. Untuk itu, salah satu cara yang dapat digunakan untuk mengamanan data atau menjaga kerahasiaan data dan informasi penting tersebut adalah dengan mengubahnya kedalam bentuk sandi yang tidak bermakna yang hanya diketahui oleh pihak terkait. Aplikasi pengamanan data teks ini dibangun menggunakan algoritma Modular Multiplication Based Block Chiper (MMB). Tahapan penelitian yang akan diteliti ini terdiri dari pengumpulan data, Analisa sistem pembuatan aplikasi.**

dan implementasi.*Kata kunci*— *Kriptografi, Modular Multiplication-Based Block Chiper , MMB.*

.

Abstract*— *Information and communication technology that is currently highly developed is considered to make it easier to process, store and distribute data and information so as to make it easier to access data and information. As with document storage, it can be stored in the cloud, where we can access the file anywhere, but problems arise such as storing documents and important data, if this important data and information can be accessed by unauthorized parties it can result in losses. for the owner of the document. For this reason, one way that can be used to secure data or maintain the confidentiality of important data and information is to convert it into a meaningless code that is only known by the parties concerned. This text data security application was built using the Modular Multiplication Based Block Chiper (MMB) algorithm. The stages of the research that will be examined consist of data collection, analysis of the application making system.

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

I. PENDAHULUAN

Teknologi informasi dan komunikasi yang sangat berkembang saat ini dianggap semakin mempermudah proses pengolahan, penyimpanan dan pendistribusian data dan informasi sehingga mempermudah dalam mengakses data dan informasi. Seperti halnya penyimpanan dokumen, dapat disimpan di cloud, yang mana kita dapat mengakses file tersebut dimana saja. Namun tidak semua perkembangan teknologi informasi memberikan dampak yang positif dan menguntungkan. Masalah keamanan informasi menjadi hal yang sangat penting dalam suatu sistem informasi untuk keamanan bersama maupun keamanan pribadi. Untuk itu diperlukan suatu system keamanan yang dapat melindungi suatu informasi. Beberapa permasalahan maupun dampak negatif dari perkembangan teknologi informasi ini adalah seperti penyadapan data, pencurian informasi maupun penyalahgunaan data. 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 [1].

Permasalahan lainnya adalah terkait penyimpanan dokumen serta data-data penting, apabila data dan informasi penting tersebut dapat diakses oleh pihak yang tidak berwenang maka dapat berakibat kerugian bagi pihak pemilik dari dokumen tersebut. Untuk itu, salah satu cara yang dapat digunakan untuk mengamanan data atau menjaga kerahasiaan data dan informasi penting tersebut adalah dengan mengubahnya kedalam bentuk sandi yang tidak bermakna yang hanya diketahui oleh pihak terkait. Keamanan data merupakan salah satu hal penting dalam pertukaran data, khususnya pertukaran data didunia maya yang didalamnya terdapat banyak ancaman untuk proses itu sendiri. Bagi suatu organisasi keamanan data bernilai sangat rahasia. Suatu hal yang dirasa perlu dan penting bagi pengguna adalah teknik dalam keamanan data, hal ini menunjukkan bahwa tingkat keamanan data haruslah ditingkatkan.

Teknologi keamanan data terus berkembang mulai dari penyandian data sampai kepenyisipan data. Salah satu teknik yang dapat digunakan untuk mengamankan data adalah dengan membangun sebuah aplikasi pengamanan data. Aplikasi pengamanan data yang akan dikembangkan ini hanya berfokus pada dokumen yang berisikan hanya file teks. Gambaran dari sistem pengamanan data yang akan dibangun ini menggunakan algoritma Modular Multiplication Based Block Chiper (MMB). Proses yang dilakukan pada penelitian ini proses enkripsi data teks dengan kunci acak dan proses dekripsi dengan kunci acak berbasis block chipper.

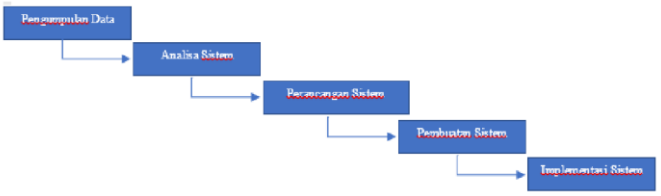
II. METODOLOGI PENELITIAN

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

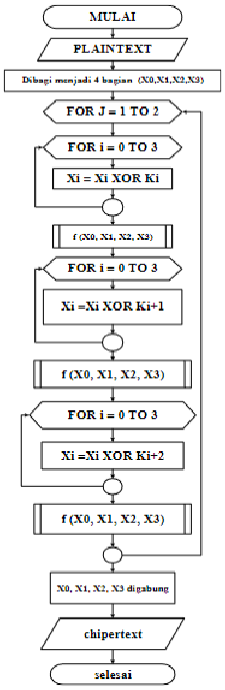
Use Case diagram sistem yang bertujuan untuk memberikan gambaran serta penjelasan mengenai sistem yang akan dibuat. *Use Case* diagram sistem dapat dilihat pada gambar 1.



Gambar 1 *Tahapan Penelitian*

1. Pengumpuan Data
   Dalam penelitian ini data dikumpulkan di Politeknik Negeri Lhokseumawe pada program studi Teknologi Rekayasa Komputer Jaringan. Teknik pengumpulan data yang digunakan pada penelitian pengamanan data teks pada penelitian ini ini menggunakan 2 jenis data :
   a. Data primer berupa data yang didapat oleh peneliti secara langsung.Dalam penelitian ini teknik pengumpulan data yang akan dilakukan menggunakan Quetsioner. Pengumpulan data ini dilakukan untuk mengetahui jenis file apa saja yang akan dilakukan pengamanan data.
   b. Dalam pengumpulan data sekunder teknik pengumpulan data yang digunakan berupa Observasi dari penelitian yang telah dilakukan. Pada tahap ini peneliatan banyak menggunakan data dari penelitian terdahulu. Seperti pencarian referensi yang dilakukan di perpustakan, di internet, artikel, jurnal dan buku.
2. Analisa Sistem
   Tahapan ini merupakan tahapan untuk mempertimbangkan dalam membangun sebuah sistem pengamanan data teks. Analisa sistem disini terdiri dari Analisa kebutuhan dari sisi hardware dan Analisa kebutuhan software.

3. Perancangan Sistem



4. Pembuatan Sistem
Pada tahapan ini merupakan tahapan pembuatan aplikasi pengamanan data mobile yang akan dibagun sesuai dengan tahapan dari perancangan sistem. Dan sistem pengamanan data teks yang akan dibangun dengan mengimplementasikan algoritma MMB.

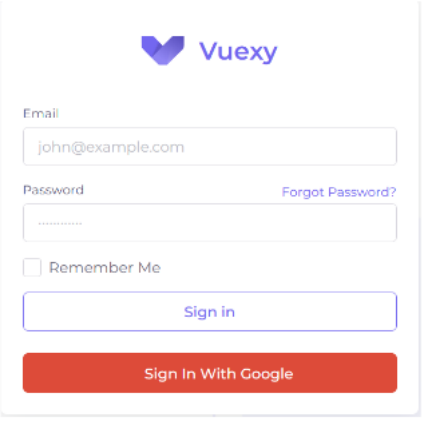
III. HASIL DAN PEMBAHASAN

A. Implementasi Aplikasi

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

1. Halaman *Login*

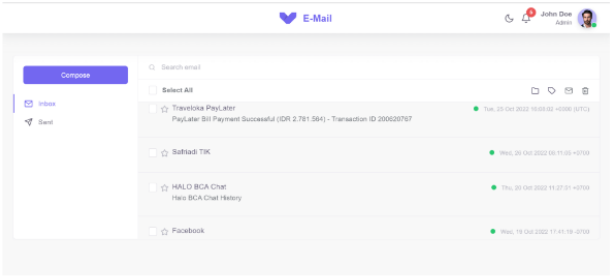
ada halaman Login, pada tampilan Login user dapat melakukan proses autentikasi untuk masuk pada aplikasi email. Tampilan login dari aplikasi yang dibangun dapat dilihat pada gambar berikut



Gambar 2. Halaman Login

2. Halaman Kotak Masuk

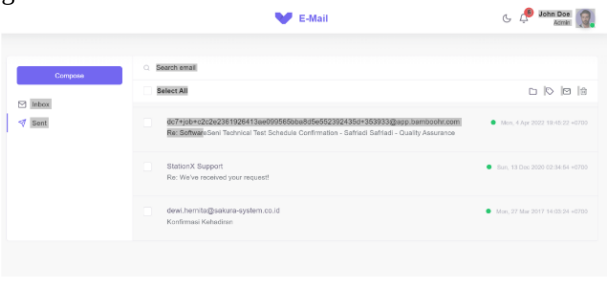
Pada halaman Kotak Masuk, pada tampilan ini user dapat melihat daftar pesan yang diterima oleh user. Tampilan halaman dari aplikasi ini yang dibangun dapat dilihat pada gambar berikut:



Gambar 3. Halaman Kotak Masuk

3. Halaman Terkirim

Pada halaman Pesan terkirim, pada tampilan ini user dapat melihat daftar pesan yang dikirim oleh user. Tampilan halaman dari aplikasi ini yang dibangun dapat dilihat pada gambar berikut



Gambar 4. Halaman Pesan Terkirim

B. Proses Pembentukan Kunci

Pada proses pembentukan kunci, kunci yang akan digunakan terdiri dari 16 karakter, yang diambil dari username dan password user pada aplikasi. Metode MMB ini memiliki input 128 bit kunci (key) yang identik dengan 32 digit heksadesimal ataupun 16 karakter yang akan dipecah menjadi 4 buah sub kunci (subkey) dengan panjang masing-masing sub kunci adalah sebesar 32 bit. Untuk lebih memahami proses pembentukan kunci pada métode MMB.

C. Proses Enkripsi dan Dekripsi

Proses enkripsi dari algoritma MMB ini memiliki input data plainteks 128 bit yang identik dengan 12 digit heksadesimal atau 16 karakter.

D. Hasil Pengujian

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 menggunakan teks dengan panjang maksimal 16 karakter.

VI. KESIMPULAN

Berdasarkan pembahasan sebelumnya, maka dapat diambil kesimpulan-kesimpulan. Adapun kesimpulan-kesimpulan tersebut adalah sebagai berikut:

1. Algoritma modular multiplication based block cipher mengenkripsi data algoritma iteratif yang terdiri dari langkah-langkah linier (seperti XOR dan aplikasi kunci) serta aplikasi parallel dari empat substitusi non linier.
2. Pengujian algoritma modular multiplication based block cipher dilakukan dengan menggunakan program web php dengan memasukkan data teks serta kunci kemudian akan diproses dengan sebuah tombol enkripsi yang telah disisipi algoritma

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

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

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