Journal Global Tecnology Computer
Vol 4, No. 1, Desember 2024, Hal 93-103
ISSN: 2809-6118 (Online - Elektronik)
DOI: 10.47065/jogtc.v4i1.6900
Website https://ejurnal.seminar-id.com/index.php/jogtc

Analisis dan Perancangan Sistem Kriptografi Merkle-Hellman Knapsack Untuk Mengamankan File Text

Arief Budiman[1], Yunita Sari[1,*]

[1]Fakultas Teknik dan Komputer, Teknik Informatika, Universitas Harapan Medan, Medan, Indonesia
JL. HM. Jhoni No. 70, Medan Kota, Kota Medan, Indonesia
Email: [1]ariefbudiman@unhar.ac.id, [2,*]yunitasari@unhar.ac.id
Email Penulis Korespondensi: yunitasari@unhar.ac.id

Abstrak−Kriptografi merupakan bidang yang sangat dibutuhkan pada era globalisasi saat ini dimana keamanan dan kerahasiaan informasi menjadi hal yang sangat sulit dijaga mengingat akses komunikasi yang luas dan terbuka. Kriptografi saat ini telah banyak memiliki berbagai macam metode dan teknik yang terbagi menjadi dua kategori yaitu kriptografi simetris dan kriptografi asimetris dimana penggunaanya bergantung pada kebutuhan dan kondisi. Metode *Merkle Hellman Knapsack* merupakan metode kriptografi asimetris yang menggunakan kunci *public* dan kunci *private* sehingga penyadapan dan *cracking* menjadi lebih sulit akibat dari penggunaan kunci yang berbeda baik pada saat enkripsi maupun pada saat dekripsi. Pengembangan aplikasi menggunakan metode *Merkle Hellman Knapsack* membangkitkan kunci *public* dan kunci *private* dengan menggunakan nilai deretan *super increasing* dan *inverse* modulo sehingga lebih menyulitkan proses kriptanalisis. Sistem yang dikembangkan mampu memberikan alternatif dalam mengamankan data teks.

Kata Kunci: Kriptografi; Asimetris; *Merkle Hellman Knapsack*.

Abstract−*Cryptography is a field that is really needed in the current era of globalization where security and confidentiality of information are very difficult to maintain considering wide and open communication access. Cryptography currently has a variety of methods and techniques which are divided into two categories, namely symmetric cryptography and asymmetric cryptography where their use depends on needs and conditions. The Merkle Hellman Knapsack method is an asymmetric cryptography method that uses a public key and a private key so that tapping and cracking becomes more difficult due to the use of different keys both during encryption and during decryption. Application development using the Merkle Hellman Knapsack method generates public keys and private keys using super increasing and inverse modulo series values, making the cryptanalysis process more difficult. The system developed is able to provide an alternative in securing text data.*

Keywords*: Cryptography; Asymmetric; Merkle Hellman Knapsack.*

1. PENDAHULUAN

Perkembangan ilmu dan teknologi komputer telah mempengaruhi segala aspek kehidupan manusia seperti di bidang pendidikan. Teknologi informasi jaringan komputer memegang peranan yang sangat penting [1]. Informasi dan data dapat dengan mudah dan cepat untuk dikirim ke konsumen melalui jaringan komputer. Perlu diketahui jaringan komputer adalah dua atau lebih perangkat komputer yang saling terhubung atau terkoneksi antara satu dengan yang lain dan digunakan untuk berbagai sumber data [2]. Salah satu bidang ilmu untuk menjaga keamanan informasi adalah Kriptografi.[3] Dimana keamanan tersebut disebut dengan kriptografi. kriptografi (Cryptography) berasal dari bahasa Yunani, yaitu kryptos yang berarti tersembunyi dan graphein yang berarti tulisan [4]. Dimana kriptografi adalah sebuah cabang ilmu dalam ilmu komputer yang berfungsi untuk mengamankan data. Secara terminologi, kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya kedalam bentuk yang tidak dapat dipahami maknanya sehingga tidak dapat dibaca oleh orang yang tidak berkepentingan [5].

Pesan rahasia penting ini adalah sesuatu yang perlu dipertimbangkan ketika berbagi informasi di media, dengan pesan-pesan yang tidak menyadari bahwa pesan rahasia dapat disalahgunakan oleh mereka yang tidak memiliki hak untuk mengaksesnya, dengan tujuan untuk merugikan individu tertentu [6]. Untuk melakukan pesan rahasia Terdapat berbagai bentuk pesan rahasia seperti pesan teks (dalam bentuk *file*), pesan citra, pesan audio dan pesan video yang tentu saja menimbulkan risiko jika informasi dan data yang dikirim bisa diakses oleh pihak yang tidak berhak sehingga mengakibatkan kebocoran data. Kriptografi bertujuan untuk informasi yang bersifat rahasia yang dikirim melalui telekomunikasi umum tidak dapat diketahui atau dimanfaatkan dengan orang yang tidak berkepentingan atau yang tidak berhak menerimanya [7]. dengan menggunakan kriptografi maka suatu data dapat diamankan dengan mengaburkan / mengubah/ mengacakisi dari suatu data melalui proses enkripsi [8].

Keamanan data merupakan hal penting dalam menjaga kerahasiaan data-data tertentu yang hanya boleh diketahui oleh pihak yang memiliki hak saja, salah satu cara untuk menjaga keamanan dan kerahasiaan suatu data dengan enkripsi dan dekripsi untuk membuat data agar tidak dapat dibaca atau dimengerti oleh sembarang orang [9]. Dalam penelitian ini penulis tertarik untuk mengamankan file teks, dalam mengamankan sebuah file teks terdapat berbagai macam cara, salah satunya menggunakan teknik kriptografi. Kriptografi yang dapat mengenkripsikan pesan atau teks kedalam bentuk chipertext sehingga dapat menyembunyikan pesan asli yang dikirimkan [10]. Keamanan sistem data merupakan seluruh betuk mekanisme yang wajib dijalankan dalam suatu sistem yang diperuntukan supaya sistem tersebut bebas dari seluruh ancaman yang membahayakan keamanan informasi data serta keamanan pelakon sistem [11].

Ada banyak metode yang digunakan dalam kriptografi, salah satunya adalah algoritma *Merkle-Hellman Knapsack* [12]. MerkleHellman Knapsack dapat menggunakan ukuran kunci yang lebih kecil dibandingkan dengan kriptosistem seperti RSA [13]. *Merkle-Hellman Knapsack* merupakan kriptosistem kunci asimetris, artinya untuk komunikasi,

Journal Global Tecnology Computer
Vol 4, No. 1, Desember 2024, Hal 93-103
ISSN: 2809-6118 (Online - Elektronik)
DOI: 10.47065/jogtc.v4i1.6900
Website https://ejurnal.seminar-id.com/index.php/jogtc

diperlukan dua kunci: kunci publik dan kunci pribadi [14]. Panjang kunci yang digunakan antara 8 sampai 72 bit. Selain itu *Merkle-Hellman Knapsack* merupakan algoritma kriptografi asimetris, di mana terdapat dua kunci yang akan digunakan yaitu, kunci publik (public key) dan kunci rahasia (private key). Mekanisme pengerjaan Merkle- 3 Hellman Knapsack adalah dengan menentukan key generation dari barisan superincreasing [15]. Barisan superincreasring merupakan barisan di mana setiap nilai di dalam barisan lebih besar daripada jumlah semua nilai sebelumnya. Dalam kriptosistem *Merkle-Hellman Knapsack*, 'penyamaran' diakhiri dengan penelusuran diberikan s1, s ,.., sn merupakan sebuah ukuran himpunan *super-increasing*. Memilih suatu bilangan prima p yang lebih besar dari pada jumlah semua si, dan suatu bilangan b dengan $1 < b < p$.

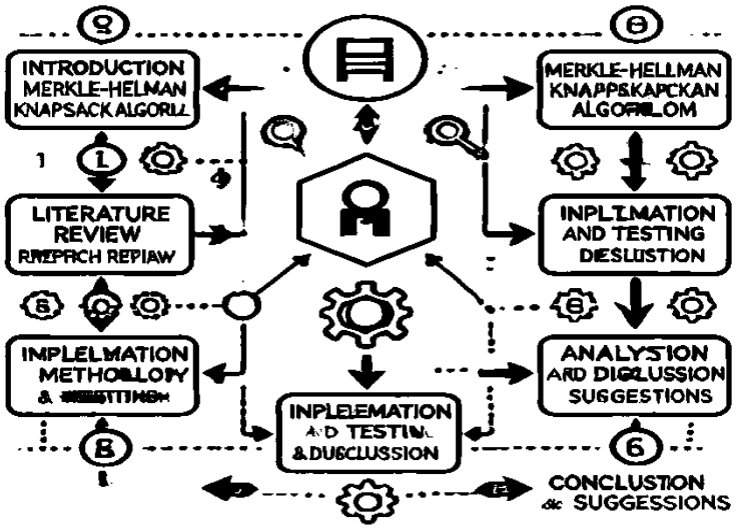
Perlu diketahui dilakukan saat informasi akan dikirimkan dengan disandikan sehingga informasi tersebut akan sulit terbaca. Pesan merupakan bagian dari unsur-unsur komunikasi, Hafied Cangara dalam bukunya Pengantar Ilmu Komunikasi [8]. Dekripsi dilakukan saat penerimaan informasi dengan cara mengubah kembali menjadi bentuk aslinya. Proses Dekripsi tersebut hanya bisa dilakukan oleh penerima dengan menggunakan kunci rahasia yang telah disepakati bersama sebelumnya [16]. Berdasarkan penelitian "*Cryptography Asymmetries Merkle-Hellman Knapsack* Digunakan untuk Enkripsi dan Dekripsi Teks" disimpulkan bahwa metode *Merkle-Hellman Knapsack* memiliki kelebihan dalam proses pendistribusian kunci pada media yang tidak aman seperti internet dan tidak memerlukan kerahasiaan. Karena kunci yang didistribusikan adalah kunci public [17].

Sehingga jika kunci ini sampai hilang atau diketahui oleh orang lain yang tidak berhak, maka pesan sandi yang dikirim akan tetap aman, karena kunci *private* tidak didistribusikan. Penelitian lainnya yang dibuat oleh "Keamanan Data dengan Metode Kriptografi Kunci Publik" disimpulkan metode ini mampu menggabungkan algoritma kunci publik dengan algoritma simetrik untuk memperoleh keunggulan-keunggulan pada masing-masing algoritma. Selanjutnya yaitu penelitian oleh "Kriptografi Gabungan Menggunakan Algoritma *Mono Alphabetic* dan *One Time Pad*" disimpulkan bahwa keamanan algoritma pengenkripsian ini sangat bergantung pada kerahasiaan kunci rahasia (*secret key*) dan *pad* yang digunakan baik dalam mengenkripsi maupun mendekripsi data dan informasi.

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Latar belakang masalah: Menjelaskan perkembangan ilmu dan teknologi komputer, serta peran kriptografi dalam keamanan informasi Rumusan masalah: Mengidentifikasi masalah yang akan diteliti, misalnya bagaimana metode Merkle-Hellman Knapsack digunakan untuk enkripsi dan dekripsi teks Tujuan penelitian: Menjelaskan tujuan utama penelitian, seperti mengamankan file teks menggunakan kriptografi Merkle-Hellman Knapsack Manfaat penelitian: Menguraikan manfaat dari hasil penelitian bagi pengembangan keamanan data dan teknologi informasi. Berikut kami lampirkan tahapan



Gambar 1. Tahapan Penelitian

Diagram terdiri dari enam langkah utama, yang masing-masing saling terhubung dengan panah untuk menunjukkan alur penelitian secara sistematis:

a. Pendahuluan
Menjelaskan latar belakang penelitian tentang pentingnya keamanan data menggunakan kriptografi. Merumuskan masalah yang akan dikaji dalam penelitian ini. Menyampaikan tujuan dan manfaat penelitian.

b. Kajian Pustaka
Mengumpulkan teori dan referensi terkait kriptografi serta algoritma Merkle-Hellman Knapsack. Membahas penelitian terdahulu yang relevan untuk mendukung penelitian ini. Metodologi Penelitian

Journal Global Tecnology Computer
Vol 4, No. 1, Desember 2024, Hal 93-103
ISSN: 2809-6118 (Online - Elektronik)
DOI: 10.47065/jogtc.v4i1.6900
Website https://ejurnal.seminar-id.com/index.php/jogtc

c. **Menjelaskan jenis penelitian yang digunakan (misalnya eksperimen).**
Menyusun langkah-langkah yang akan dilakukan, termasuk metode enkripsi dan dekripsi teks dengan algoritma Merkle-Hellman Knapsack. Menentukan parameter dan alat yang digunakan dalam penelitian.
d. **Implementasi dan Pengujian**
Mengembangkan program atau sistem untuk mengenkripsi dan mendekripsi teks. Melakukan pengujian dengan berbagai skenario untuk melihat efektivitas algoritma.
e. **Analisis dan Pembahasan**
Menganalisis hasil pengujian dan mengidentifikasi kelebihan serta kekurangan metode yang digunakan. Membandingkan hasil dengan metode lain dalam kriptografi.
f. **Kesimpulan dan Saran**
Merangkum temuan utama penelitian. Memberikan saran untuk pengembangan lebih lanjut, seperti optimasi algoritma atau penerapan pada skala yang lebih luas.

2.1 Kriptografi

Kriptografi adalah ilmu dan teknik untuk mengamankan informasi dengan cara menyandikannya agar hanya bisa dibaca oleh pihak yang berhak. Proses ini melibatkan enkripsi (mengubah data asli menjadi sandi) dan dekripsi (mengembalikan sandi ke bentuk asli) untuk menjaga kerahasiaan, integritas, dan keaslian data.

2.3 Merkel Hellmen knapsack

Merkle-Hellman Knapsack adalah algoritma kriptografi asimetris yang dikembangkan oleh Ralph Merkle dan Martin Hellman pada tahun 1978. Algoritma ini didasarkan pada masalah knapsack (rucksack problem) dalam matematika kombinatorik dan menggunakan barisan superincreasing untuk proses enkripsi dan dekripsi. Prinsip Kerja Merkle-Hellman Knapsack. Pembuatan Kunci:
a. Memilih barisan superincreasing: Setiap elemen dalam barisan lebih besar dari jumlah semua elemen sebelumnya.
b. Memilih bilangan prima (p) yang lebih besar dari jumlah semua elemen dalam barisan.
c. Memilih bilangan pengali (b) yang relatif prima terhadap p.
d. Menghitung barisan publik dengan rumus:

$$wi = (si \times b) \bmod p$$

Adalah elemen dalam barisan superincreasing. Proses Enkripsi. Pesan yang akan dienkripsi dikonversi ke dalam bentuk biner. Setiap bit pesan dikalikan dengan elemen dalam barisan publik dan dijumlahkan untuk membentuk ciphertext. Proses Dekripsi. Ciphertext dikalikan dengan invers modulo dari b terhadap p. Hasilnya dipecah kembali menggunakan barisan superincreasing untuk mendapatkan kembali pesan asli dalam bentuk biner.

2.4 Analisis Permasalahan

Masalah yang diangkat dari penelitian tugas akhir ini adalah pembuatan sistem pengamanan *file* teks menggunakan algoritma *Merkle-Hellman Knapsack*. Dimana algoritma *Merkle-Hellman Knapsack* merupakan metode yang digunakan untuk mengenkripsi *file* teks yang berekstensi txt dan rtf. Metode *Merkle-Hellman Knapsack* merupakan kriptosistem yag menggunakan algoritma asimetris. Kelebihan algoritma asimetris ini adalah proses pendistribusian kunci pada media yang tidak aman seperti internet, tidak memerlukan kerahasian. Karena kunci yang didistribusikan adalah kunci publik. Sehingga jika kunci ini sampai hilang atau diketahui oleh orang lain yang tidak berhak, maka pesan sandi yang dikirim akan tetap aman. Sedangkan kunci *private* tetap disimpan (tidak didistribusikan).

3. HASIL DAN PEMBAHASAN

3.1 Proses Enkripsi Merkle-Hellman Knapsack

Proses enkripsi algoritma *Merkle-Hellman Knapsack* menggunakan kunci *public* yang diberikan oleh pengguna. Adapun proses enkripsi pada algoritma *Merkle-Hellman Knapsack* adalah sebagai berikut:
Diketahui bilangan super-increasing (s):

s = {2,7,11,21,42,89,180,354}

Diketahui public key (t):

218-763-417-725-668-317-70-268

Perhitungan Public Key (t):
t1 = a*s1 mod p = 109 * 2 mod 782 =218
t2 = a*s2 mod p = 109 * 7 mod 782 = 763
t3 = a*s3 mod p = 109 * 11 mod 782 = 417
t4 = a*s4 mod p = 109 * 21 mod 782 = 725

3.2 Proses Deskripsi Algoritma *Merkle-Hellman Knapsack*

Journal Global Tecnology Computer
Vol 4, No. 1, Desember 2024, Hal 93-103
ISSN: 2809-6118 (Online - Elektronik)
DOI: 10.47065/jogtc.v4i1.6900
Website https://ejurnal.seminar-id.com/index.php/jogtc

Proses dekripsi algoritma *Merkle-Hellman Knapsack* adalah kriptosistem yang menggunakan algoritma asimetris menggunakan kunci *private* yang di-input oleh pengguna. [18]Pada proses deskripsi akan digunakan variable tambahan yang disebut dengan variable a^{-1} *inverse* yang diperoleh dari proses modulo *inverse* antara variabel $a$dan variabel p. Adapun proses deskripsi pada algoritma *Merkle-Hellman Knapsack* adalah sebagai berikut:

a. Menghitung nilai modulo inverse dari variabel a dan variabel p
   Diperoleh nilai modulo inverse adalah sebesar 617 dikarenakan memenuhi syarat berikut:
   (617*109) mod 782 = 1
b. Menghitung nilai plaintext sementara
   P(1) = (1826 * 617) mod 782 = 562
   P(2) = (1805 * 617) mod 782 = 117
   P(3) = (1805 * 617) mod 782 = 117
   P(4) = (1431* 617) mod 782 = 49
c. Berikutnya adalah mendekomposisikan nilai *plaintext* sementara dengan mengurangi nilai *plaintext* sementara dengan nilai *super-increasing* (s) yang paling dekat dan lebih kecil:
   P(1):
   562-354 = 208 dikurangi dengan 354 dikarenakan paling dekat dan lebih kecil dibandingkan dengan nilai lain dari *super-increasing* (2)
   208 -180 = 28
   28-21 = 7
   7-7 = 0

3.3 Perancangan Sistem

Pada tahapan perancangan sistem ini akan di jelaskan proses keseluruhan dari program yang akan di buat, agar proses alurnya lebih jelas dan sesuai dengan *standart Unified Modern Language* (UML) yang akan di rancang dimana UML adalah merupakan metode pemodelan berorientasi objek dan berbasis visual [19]. Dibawah ini akan digambarkan rancangan f*lowchart* Proses Enkripsi Algoritma *Merkle-Hellman Knapsack*, dimana perlu diketahui *flowchart* adalah cara penulisan algoritma dengan menggunakan notasi grafis.[20]

Gambar 2. Proses Enkripsi

3.4 Tampilan Program Menu Utama *Merkle-Hellman Knapsack*

Journal Global Tecnology Computer
Vol 4, No. 1, Desember 2024, Hal 93-103
ISSN: 2809-6118 (Online - Elektronik)
DOI: 10.47065/jogtc.v4i1.6900
Website https://ejurnal.seminar-id.com/index.php/jogtc

Pada tampilan menu utama terdapat lima menu utama yaitu menu pembangkit kunci, enkripsi, dekripsi, *about* dan *exit*. Adapun tampilan dari menu utama dapat dilihat pada gambar 2 seperti dibawah ini.

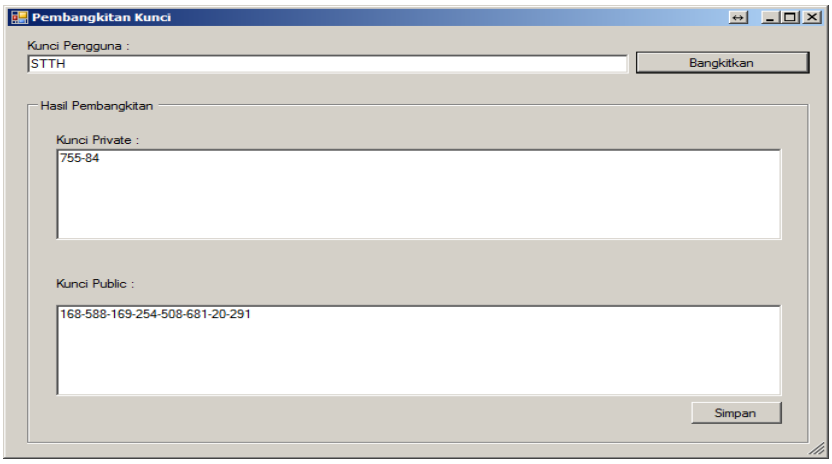
Gambar 3. Menu Utama

Adapun bagian – bagian dari menu utama yaitu:

a. Pembangkit Kunci
   Fungsi dari menu pembangkit kunci adalah untuk menampilkan tampilan pembangkit kunci yang digunakan untuk membangkitkan kunci publik dan kunci *private* untuk proses enkripsi dan dekripsi.
b. Enkripsi
   Fungsi dari menu enkripsi adalah untuk menampilkan tampilan enkripsi yang digunakan untuk mengenkripsi pesan dari pengguna.
c. Dekripsi
   Fungsi dari menu dekripsi adalah untuk menampilkan tampilan dekripsi yang digunakan untuk mengdekripsi pesan dari pengguna.
d. *About*
   Fungsi dari menu *about* adalah untuk menampilkan tampilan *about* yang menampilkan informasi penulis.
e. *Exit*
   Fungsi dari menu *exit* adalah untuk keluar dan menutup aplikasi.

3.5 Tampilan Form Pembangkit Kunci

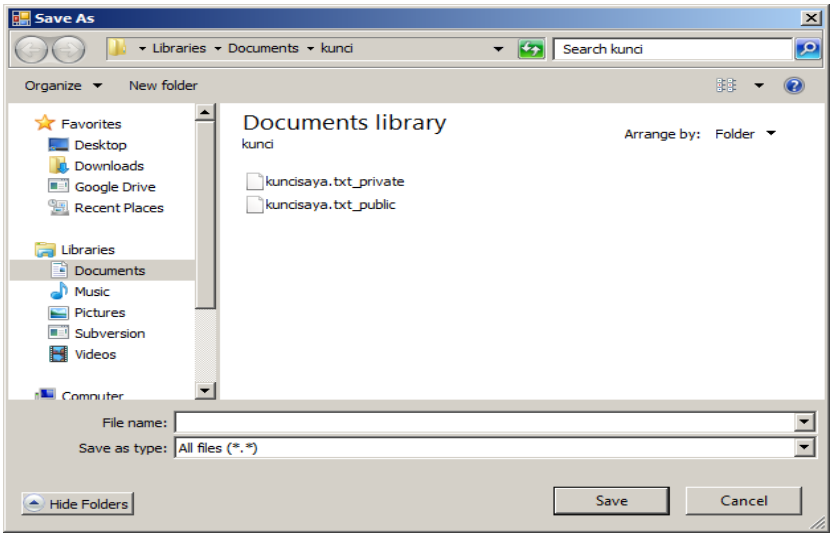
Form ini digunakan untuk melakukan pembangkitan kunci publik dan kunci *private* yang digunakan dalam proses enkripsi dan dekripsi. Pengguna pertama sekali mengisi kunci untuk pengguna yang kemudian pembangkitan kunci dilakukan dengan meng-klik tombol "Bangkitkan". Adapun tampilan dari *form generate* kunci dapat dilihat pada gambar 4.



Gambar 4. Pembangkit Kunci

Setelah kunci dibangkitkan pengguna selanjutnya dapat menyimpan kunci yang dibangkitkan agar dapat digunakan untuk proses enkripsi dan dekripsi dengan mengklik tombol "Simpan".

Journal Global Tecnology Computer
Vol 4, No. 1, Desember 2024, Hal 93-103
ISSN: 2809-6118 (Online - Elektronik)
DOI: 10.47065/jogtc.v4i1.6900
Website https://ejurnal.seminar-id.com/index.php/jogtc

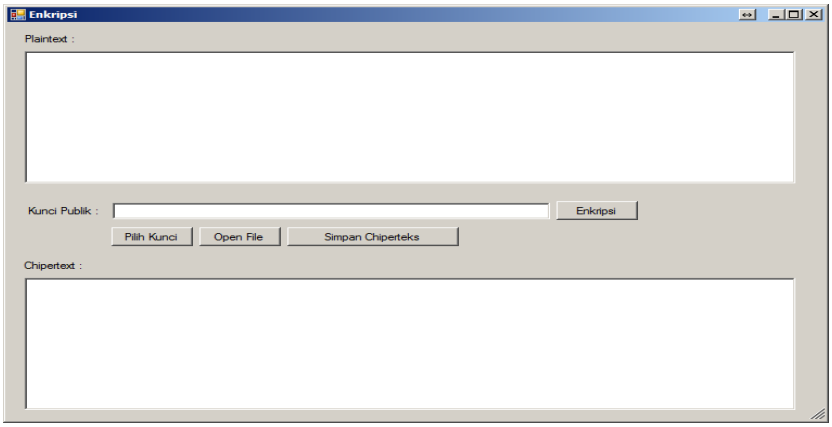


Gambar 5. Penyimpanan Kunci

Kunci yang tersimpan akan memiliki nama berkas dengan akhiran *_public* dan *_private* untuk membedakan berkas kunci publik dan kunci *private*. Selanjutnya kunci – kunci tersebut dapat digunakan untuk proses enkripsi dan dekripsi.

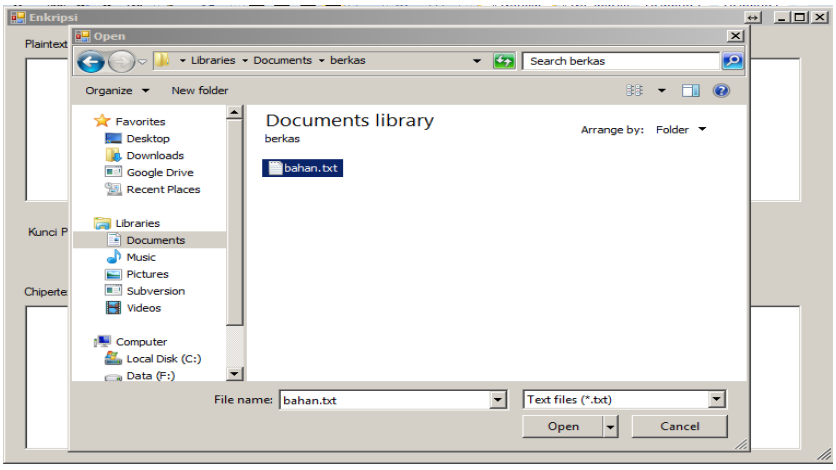
3.6 Tampilan Form Enkripsi

Form ini digunakan untuk melakukan enkripsi terhadap pesan plainteks. Pengguna pertama sekali membuka berkas plainteks yang akan dienkripsi atau mengetikkan langsung pesan plainteks yang akan dienkripsi pada kolom plainteks.



Gambar 6. Form Enkripsi

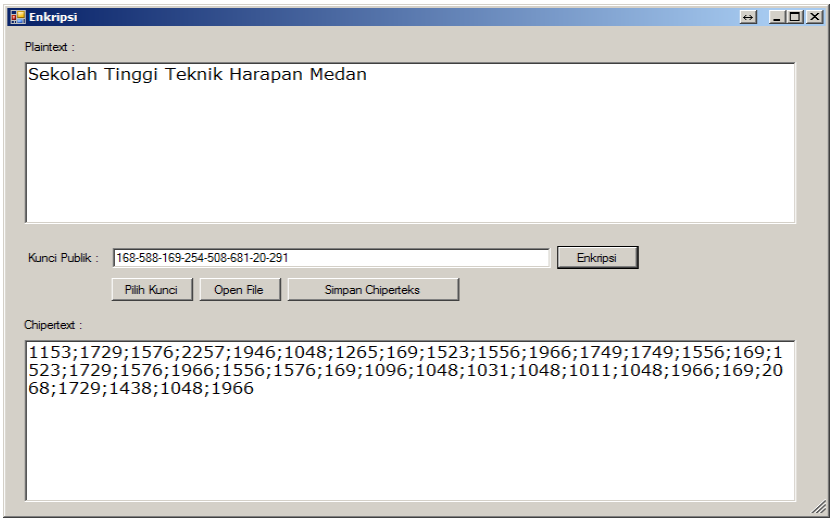
Berkas plainteks dapat dibuka dengan menggunakan tombol “Open File” yang kemudian akan menampilkan dialog untuk memilih *file* plainteks yang akan dienkripsi. Tampilan dialog untuk memilih *file* plainteks dapat dilihat pada gambar 6.



Gambar 7. Dialog Plainteks

Journal Global Tecnology Computer
Vol 4, No. 1, Desember 2024, Hal 93-103
ISSN: 2809-6118 (Online - Elektronik)
DOI: 10.47065/jogtc.v4i1.6900
Website https://ejurnal.seminar-id.com/index.php/jogtc

Setelah plainteks dibuka selanjutnya pengguna dapat melakukan proses enkripsi dengan memasukkan kunci yang telah dibangkitkan sebelumnya dan melakukan proses enkripsi dengan menekan tombol "Enkripsi" sehingga proses enkripsi akan dilakukan dan menampilkan chiperteks seperti yang terlihat pada gambar 7.

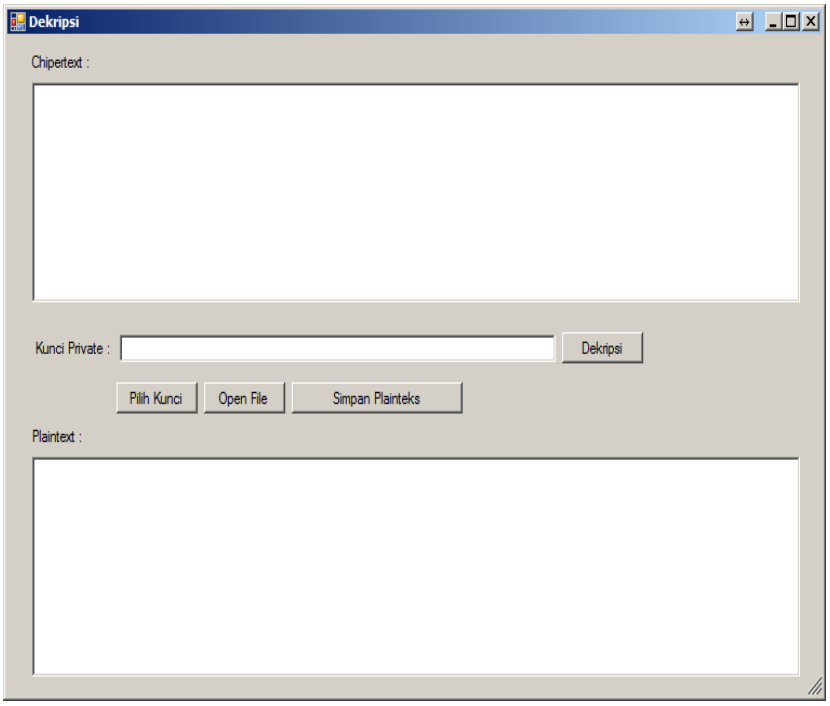


Gambar 8. Proses Enkripsi

Chiperteks hasil enkripsi kemudian dapat disimpan menjadi file menggunakan tombol "Simpan Chiperteks" sehingga dapat di dekripsi kembali menggunakan *form* dekripsi yang akan dijabarkan pada sub bab berikutnya.

3.7 Tampilan Form Dekripsi

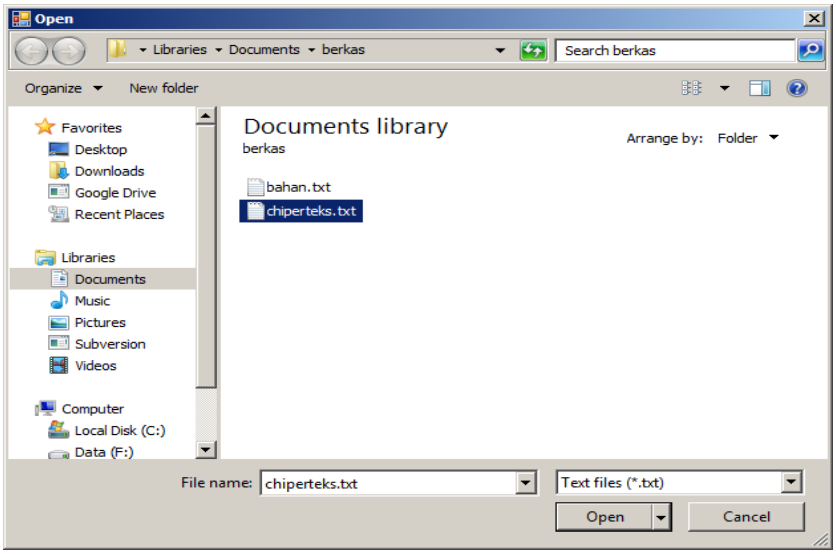
Form ini digunakan untuk melakukan dekripsi terhadap pesan chiperteks yang di masukkan oleh pengguna. Pengguna pertama sekali membuka berkas chiperteks yang akan didekripsi. Adapun tampilan dari *form* dekripsi dapat dilihat pada gambar 8.



Gambar 9. Form Dekripsi

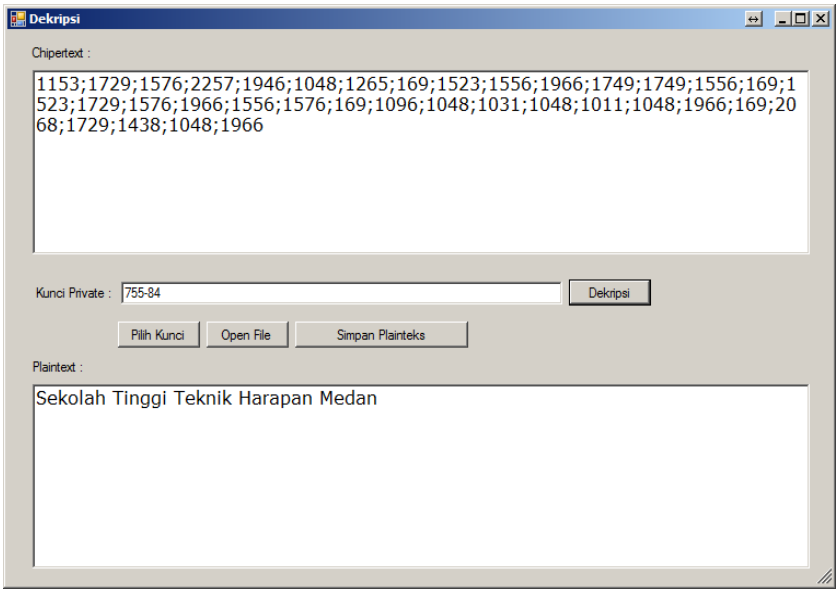
Berkas chiperteks dapat dibuka dengan menggunakan tombol "Open File" yang kemudian akan menampilkan dialog untuk memilih *file* chiperteks yang akan didekripsi. Tampilan dialog untuk memilih *file* chiperteks dapat dilihat pada gambar 9.

Journal Global Tecnology Computer
Vol 4, No. 1, Desember 2024, Hal 93-103
ISSN: 2809-6118 (Online - Elektronik)
DOI: 10.47065/jogtc.v4i1.6900
Website https://ejurnal.seminar-id.com/index.php/jogtc



Gambar 10. Berkas Chiperteks

Setelah plainteks dibuka selanjutnya pengguna dapat melakukan proses dekripsi dengan memasukkan kunci yang telah dibangkitkan sebelumnya dan melakukan proses dekripsi dengan menekan tombol "Dekripsi" sehingga proses dekripsi akan dilakukan dan akan menampilkan plainteks seperti yang terlihat pada gambar 10.

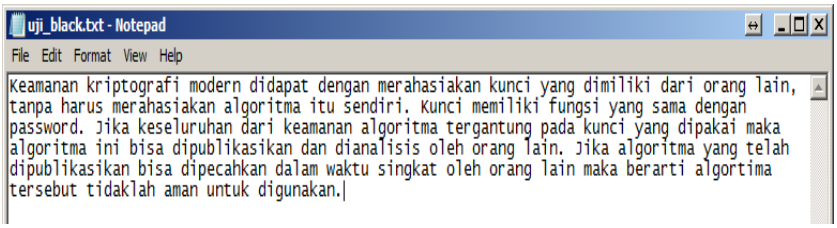


Gambar 11. Proses Dekripsi

Plainteks hasil dekripsi kemudian dapat disimpan menjadi file menggunakan tombol "Simpan Plainteks" sehingga dapat digunakan lebih lanjut oleh pengguna.

3.8 Pengujian Blackbox

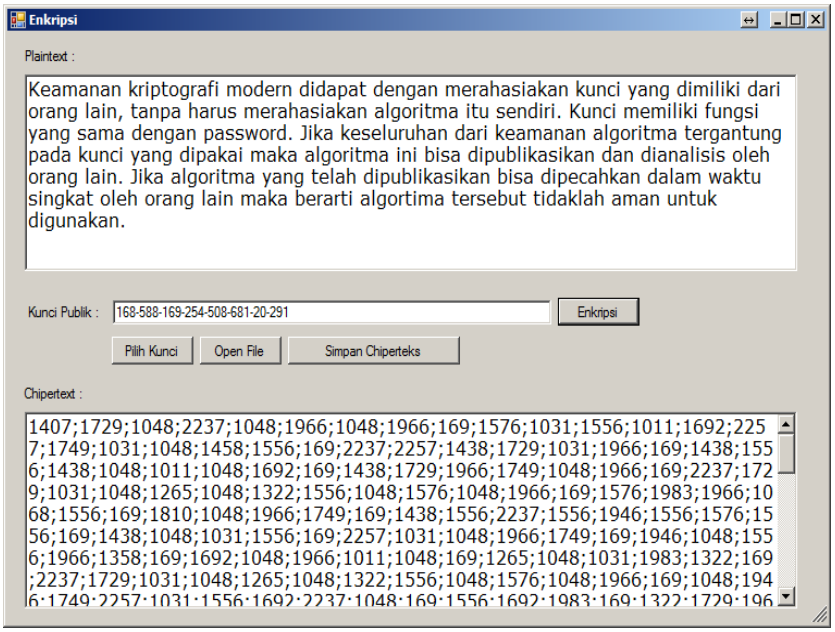
Pengujian *blackbox* dilakukan untuk memperoleh validasi terhadap fungsionalitas yang dimiliki oleh aplikasi yang dikembangkan. Pengujian *blackbox* pada penelitian ini dilakukan dengan menggunakan *input* teks yang akan dienkripsi dan didekripsi kembali. Input teks yang digunakan pada pengujian ini adalah *input* "uji_black.txt" yang mana memiliki teks yang dapat dilihat pada gambar 11 berikut :



Gambar 12. Pengujian *Blackbox*

Journal Global Tecnology Computer
Vol 4, No. 1, Desember 2024, Hal 93-103
ISSN: 2809-6118 (Online - Elektronik)
DOI: 10.47065/jogtc.v4i1.6900
Website https://ejurnal.seminar-id.com/index.php/jogtc

Pengujian *blackbox* yang dilakukan pada penelitian ini dimulai dengan proses enkripsi, kemudian dilanjutkan dengan melihat hasil chiperteks setelah proses enkripsi, pengujian terus dilanjutkan dengan proses dekripsi yang akan memeriksa apakah berkas atau teks dapat dikembalikan ke kondisi saat sebelum di enkripsi. Pengujian enkripsi pada pengujian ini yang dapat dilihat pada gambar 12 berikut.



Gambar 13. Enkripsi Blackbox

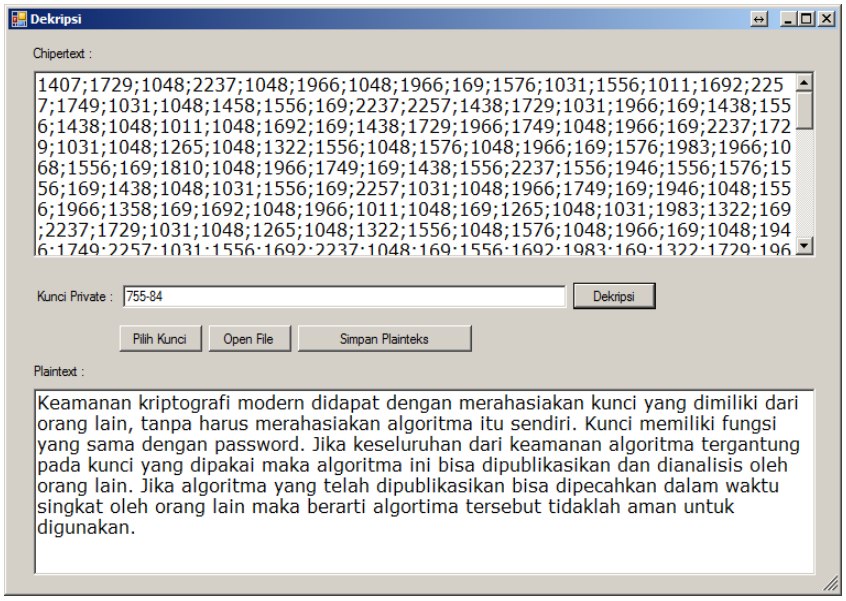
Hasil pengujian enkripsi seperti yang terlihat pada gambar 13 dapat dilihat chiperteks hasil enkripsi telah berubah sehingga proses enkripsi berhasil menerapkan metode *Merkle-Hellman* pada plainteks yang digunakan. Adapun parameter yang digunakan pada proses enkripsi adalah:
Kunci Publik: 168-588-169-254-508-681-20-291

Plainteks:
Keamanan kriptografi modern didapat dengan merahasiakan kunci yang dimiliki dari orang lain, tanpa harus merahasiakan algoritma itu sendiri. Kunci memiliki fungsi yang sama dengan password. Jika keseluruhan dari keamanan algoritma tergantung pada kunci yang dipakai maka algoritma ini bisa dipublikasikan dan dianalisis oleh orang lain. Jika algoritma yang telah dipublikasikan bisa dipecahkan dalam waktu singkat oleh orang lain maka berarti algortima tersebut tidaklah aman untuk digunakan.

Chiperteks:
1407;1729;1048;2237;1048;1966;1048;1966;169;1576;1031;1556;1011;1692;2257;1749;1031;1048;1458;1556;169;22
37;2257;1438;1729;1031;1966;169;1438;1556;1438;1048;1011;1048;1692;169;1438;1729;1966;1749;1048;1966;169;2
237;1729;1031;1048;1265;1048;1322;1556;1048;1576;1048;1966;169;1576;1983;1966;1068;1556;169;1810;1048;196
6;1749;169;1438;1556;2237;1556;1946;1556
;1576;1556;169;1438;1048;1031;1556;169;2257;1031;1048;1966;1749;169;1946;1048;1556;1966;1358;169;1692;1048
;1966;1011;1048;169;1265;1048;1031;1983;1322;169;2237;1729;1031;1048;1265;1048;1322;1556;1048;1576;1048;19
66;169;1048;1946;1749;2257;1031;1556;1692;2237;1048;169;1556;1692;1983;169;1322;1729;1966;1438;1556;1031;1
556;1378;169;1407;1983;1966;1068;1556;169;2237;1729;2237;1556;1946;1556;1576;1556;169;1458;1983;1966;1749;
1322;1556;169;1810;1048;1966;1749;169;1322;1048;2237;1048;169;1438;1729;1966;1749;1048;1966;169;1011;1048;
1322;1322;2003;2257;1031;1438;1378;169;1116;1556;1576;1048;169;1576;1729;1322;1729;1946;1983;1031;1983;12
65;1048;1966;169;1438;1048;1031;1556;169;1576;1729;1048;2237;1048;1966;1048;1966;169;1048;1946;1749;2257;1
031;1556;1692;2237;1048;169;1692;1729;1031;1749;1048;1966;1692;1983;1966;1749;169;1011;1048;1438;1048;169;
1576;1983;1966;1068;1556;169;1810;1048;1966;1749;169;1438;1556;1011;1048;1576;1048;1556;169;2237;1048;157
6;1048;169;1048;1946;1749;2257;1031;1556;1692;2237;1048;169;1556;1966;1556;169;777;1556;1322;1048;169;1438
;1556;1011;1983;777;1946;1556;1576;1048;1322;1556;1576;1048;1966;169;1438;1048;1966;169;1438;1556;1048;196
6;1048;1946;1556;1322;1556;1322;169;2257;1946;1729;1265;169;2257;1031;1048;1966;1749;169;1946;1048;1556;19
66;1378;169;1116;1556;1576;1048;169;1048;1946;1749;2257;1031;1556;1692;2237;1048;169;1810;1048;1966;1749;1
69;1692;1729;1946;1048;1265;169;1438;1556;1011;1983;777;1946;1556;1576;1048;1322;1556;1576;1048;1966;169;7
77;1556;1322;1048;169;1438;1556;1011;1729;1068;1048;1265;1576;1048;1966;169;1438;1048;1946;1048;2237;169;2
003;1048;1576;1692;1983;169;1322;1556;1966;1749;1576;1048;1692;169;2257;1946;1729;1265;169;2257;1031;1048;
1966;1749;169;1946;1048;1556;1966;169;2237;1048;1576;1048;169;777;1729;1031;1048;1031;1692;1556;169;1048;1
946;1749;2257;1031;1692;1556;2237;1048;169;1692;1729;1031;1322;1729;777;1983;1692;169;1692;1556;1438;1048;
1576;1946;1048;1265;169;1048;2237;1048;1966;169;1983;1966;1692;1983;1576;169;1438;1556;1749;1983;1966;104
8;1576;1048;1966;1378

Journal Global Tecnology Computer
Vol 4, No. 1, Desember 2024, Hal 93-103
ISSN: 2809-6118 (Online - Elektronik)
DOI: 10.47065/jogtc.v4i1.6900
Website https://ejurnal.seminar-id.com/index.php/jogtc

Pengujian selanjutnya dilakukan dengan melakukan dekripsi terhadap chiperteks yang dihasilkan dari proses enkripsi. Pengujian dekripsi pada pengujian ini yang dapat dilihat pada gambar 13 berikut.



Gambar 14. Dekripsi *Blackbox*

Pengujian dekripsi seperti yang terlihat pada gambar 14 dapat dilihat proses dekripsi balik terhadap berkas chiperteks yang dienkripsi sebelumnya dapat dikembalikan menjadi berkas teks semula dengan sempurna. Adapun parameter proses dekripsi yang digunakan adalah:
Kunci Private: 755-84
Chiperteks:
1407;1729;1048;2237;1048;1966;1048;1966;169;1576;1031;1556;1011;1692;2257;1749;1031;1048;1458;1556;169;22
37;2257;1438;1729;1031;1966;169;1438;1556;1438;1048;1011;1048;1692;169;1438;1729;1966;1749;1048;1966;169;2
237;1729;1031;1048;1265;1048;1322;1556;1048;1576;1048;1966;169;1576;1983;1966;1068;1556;169;1810;1048;196
6;1749;169;1438;1556;2237;1556;1946;1556;1576;1556;169;1438;1048;1031;1556;169;2257;1031;1048;1966;1749;16
9;1946;1048;1556;1966;1358;169;1692;1048;1966;1011;1048;169;1265;1048;1031;1983;1322;169;2237;1729;1031;10
48;1265;1048;1322;1556;1048;1576;1048;1966;169;1048;1946;1749;2257;1031;1556;1692;2237;1048;169;1556;1692;
1983;169;1322;1729;1966;1438;1556;1031;1556;1378;169;1407;1983;1966;1068;1556;169;2237;1729;2237;1556;194
6;1556;1576;1556;169;1458;1983;1966;1749;1322;1556;169;1810;1048;1966;1749;169;1322;1048;2237;1048;169;143
8;1729;1966;1749;1048;1966;169;1011;1048;1322;1322;2003;2257;1031;1438;1378;169;1116;1556;1576;1048;169;15
76;1729;1322;1729;1946;1983;1031;1983;1265;1048;1966;169;1438;1048;1031;1556;169;1576;1729;1048;2237;1048;
1966;1048;1966;169;1048;1946;1749;2257;1031;1556;1692;2237;1048;169;1692;1729;1031;1749;1048;1966;1692;19
83;1966;1749;169;1011;1048;1438;1048;169;1576;1983;1966;1068;1556;169;1810;1048;1966;1749;169;1438;1556;10
11;1048;1576;1048;1556;169;2237;1048;1576;1048;169;1048;1946;1749;2257;1031;1556;1692;2237;1048;169;1556;1
966;1556;169;777;1556;1322;1048;169;1438;1556;1011;1983;777;1946;1556;1576;1048;1322;1556;1576;1048;1966;1
69;1438;1048;1966;169;1438;1556;1
048;1966;1048;1946;1556;1322;1556;1322;169;2257;1946;1729;1265;169;2257;1031;1048;1966;1749;169;1946;1048;
1556;1966;1378;169;1116;1556;1576;1048;169;1048;1946;1749;2257;1031;1556;1692;2237;1048;169;1810;1048;196
6;1749;169;1692;1729;1946;1048;1265;169;1438;1556;1011;1983;777;1946;1556;1576;1048;1322;1556;1576;1048;19
66;169;777;1556;1322;1048;169;1438;1556;1011;1729;1068;1048;1265;1576;1048;1966;169;1438;1048;1946;1048;22
37;169;2003;1048;1576;1692;1983;169;1322;1556;1966;1749;1576;1048;1692;169;2257;1946;1729;1265;169;2257;10
31;1048;1966;1749;169;1946;1048;1556;1966;169;2237;1048;1576;1048;169;777;1729;1031;1048;1031;1692;1556;16
9;1048;1946;1749;2257;1031;1692;1556;2237;1048;169;1692;1729;1031;1322;1729;777;1983;1692;169;1692;1556;14
38;1048;1576;1946;1048;1265;169;1048;2237;1048;1966;169;1983;1966;1692;1983;1576;169;1438;1556;1749;1983;1
966;1048;1576;1048;1966;1378
Plainteks:
Keamanan kriptografi modern didapat dengan merahasiakan kunci yang dimiliki dari orang lain, tanpa harus merahasiakan algoritma itu sendiri. Kunci memiliki fungsi yang sama dengan password. Jika keseluruhan dari keamanan algoritma tergantung pada kunci yang dipakai maka algoritma ini bisa dipublikasikan dan dianalisis oleh orang lain. Jika algoritma yang telah dipublikasikan bisa dipecahkan dalam waktu singkat oleh orang lain maka berarti algortima tersebut tidaklah aman untuk digunakan.

Pengujian *blackbox* yang dilakukan menunjukkan bahwa aplikasi yang dikembangkan memiliki fungsi yang sesuai dan dapat beroperasi sesuai dengan yang diharapkan baik pada saat proses enkripsi maupun pada saat proses dekripsi.

4. KESIMPULAN

Berdasarkan proses perancangan kriptografi menggunakan metode *Merkle-Hellman Knapsack* maka dapat diambil beberapa kesimpulan yaitu: Aplikasi ini menerapkan algoritma Merkle-Hellman Knapsack dalam proses enkripsi dan dekripsi pada *file.* Aplikasi ini terdiri dari tiga komponen utama yaitu komponen pembangkit kunci, enkripsi dan dekripsi. *File* yang digunakan pada proses enkripsi dan dekripsi ini berformat rtf dan txt.

REFERENCES

[1] 2Sistem Sujono1, Okkita Rizan2, Hamidah3, Harrizkie Arie Pradana4 1, "PELATIHAN SIMULASI JARINGAN KOMPUTER UNTUK PERSIAPAN UJI KOMPETENSI SISWA SMKN 1 PAYUNG," vol. 2, hal. 17–22, 2021.
[2] K. J. Asyar, "DASAR JARINGAN KOMPUTER," no. May, 2022.
[3] A. I. Zidan BP Tafakur, *Sakina Sudinb, "Aplikasi Enkripsi dan Dekripsi Menggunakan Metode Triple Transppsition Viginere Cipher," vol. 2617, no. 2, hal. 21–27, 2022.
[4] AMELIA VEGA, "ENKRIPSI DAN DEKRIPSI PESAN MENGGUNAKAN POLINOMIAL GALOIS FIELD DENGAN ALGORITMA HILL CIPHER," vol. 9, hal. 356–363, 2022.
[5] D. R. Sari dan A. I. Pawelloi, "Penerapan Kriptografi Pada File Teks Dengan Menggunakan Merkle Hellman Knapsack Berbasis Android," *J. Sintaks Log.*, vol. 2, no. 3, hal. 1–10, 2022, doi: 10.31850/jsilog.v2i3.1845.
[6] Y. Prie, N. Zalukhu, F. T. Waruwu, dan H. K. Siburian, "Penyisipan Pesan Terenkripsi Affine Chiper Pada Citra Digital Dengan Menggunakan Metode Pixel Value Differencing," vol. 01, no. 04, hal. 22–33, 2024.
[7] B. Dina, D. I. Mulyana, dan J. S. Hutagalung, "Algoritma ADFGVX Product Transposition Cipher Pada Pengenkripsian Pesan Text," *J. Pendidik. Sains dan Komput.*, vol. 2, no. 01, hal. 172–183, 2022, doi: 10.47709/jpsk.v2i01.1378.
[8] M. Fadlan dan H. Hadriansa, "Rekayasa Aplikasi Kriptografi dengan Penerapan Kombinasi Algoritma Knapsack Merkle Hellman dan Affine Cipher," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 4, no. 4, hal. 268–274, 2017, doi: 10.25126/jtiik.201744468.
[9] R. Maulana dan R. M. Simanjorang, "Implementasi Kriptografi Pengamanan Data Pribadi Siswa SMA Swasta Jaya Krama Beringin Dengan Algoritma RC4," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 4, no. 6, hal. 377–383, 2021, doi: 10.32672/jnkti.v4i6.3533.
[10] N. S. Dewi, A. Amri, dan S. Safriadi, "Pengamanan Data Teks Pada Aplikasi Chatting Menggunakan Metode Modular Multiplication Based Block Chiper (MMB) Berbasis Android," *J. Artif. Intell. Softw. Eng.*, vol. 2, no. 2, hal. 1–7, 2022, doi: 10.30811/jaise.v2i2.3881.
[11] M. A. Jayana, D. Rafael, dan A. A. Rahman, "Implementasi Pengamanan Data Pengarsipan Dengan Metode Algoritma Kriptografi Aes Studi Kasus Pada Bank Bjb Kcp Pasteur Bandung," *Pros. Semin. Sos. Polit. Bisnis, Akunt. dan Tek.*, vol. 4, hal. 184, 2022, doi: 10.32897/sobat.2022.4.0.1922.
[12] C. Chandra, "Keamanan Data Dengan Metode Kriptografi Kunci Publik," *J. TIMES*, vol. 5, no. 2, hal. 11–15, 2016, doi: 10.51351/jtm.5.2.2016548.
[13] a Hidayat, R. Rosyadi, dan E. Paulus, "Aplikasi Merkle-Hellman Knapsack Untuk Kriptografi File Teks," *Prosiding-Seminar Nas. ...*, vol. 2, no. November, hal. 26–27, 2018, [Daring]. Tersedia pada: http://senter.ee.uinsgd.ac.id/repositori/index.php/prosiding/article/view/senter2016p23
[14] K. E. WIDYASARI, "PERBANDINGAN ALGORITMA RSA DAN MERKLE-HELLMAN DALAM RANCANG BANGUN APLIKASI PENYANDIAN PESAN TEKS," hal. 6, 2022.
[15] C. A. Novianti, M. Khudzaifah, dan M. N. Jauhari, "Kriptografi Hibrida Cipher Block Chaining (CBC) dan Merkle-Hellman Knapsack untuk Pengamanan Pesan Teks," *J. Ris. Mhs. Mat.*, vol. 3, no. 1, hal. 10–25, 2023, doi: 10.18860/jrmm.v3i1.22292.
[16] Fatonah dan Dadang Iskandar Mulyana, "Implementasi Metode Rivest Shamir Adleman untuk Enkripsi dan Dekripsi Text," *J. Inform. dan Teknol. Komput. (J-ICOM)*, vol. 3, no. 1, hal. 32–39, 2022, doi: 10.33059/j-icom.v3i1.4990.
[17] A. Aminudin, A. F. Helmi, dan S. Arifianto, "Analisa Kombinasi Algoritma Merkle-Hellman Knapscak dan Logaritma Diskrit pada Aplikasi Chat," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 5, no. 3, hal. 325, 2018, doi: 10.25126/jtiik.201853844.
[18] A. Usman, Y. D. Lestari, P. Studi, T. Informatika, U. Harapan, dan K. Buatan, "PEMODELAN GERAKAN CHESS KNIGHT DALAM MASALAH," vol. 6, no. 01, 2024.
[19] R. S. Sinukun, R. Pakaya, dan S. Suleman, "Perancangan Sistem Informasi Perjalanan Dinas (SIMPERNAS) Menggunakan Metode UML," *Energy - J. Ilm. Ilmu-Ilmu Tek.*, vol. 12, no. 1, hal. 18–24, 2022, doi: 10.51747/energy.v12i1.1040.
[20] J. R. Fauzi, "Algoritma Dan Flowchart Dalam Menyelesaikan Suatu Masalah Disusun Oleh Universitas Janabadra Yogyakarta 2020," *J. Tek. Inform.*, no. 20330044, hal. 4–6, 2020.