JURNAL SINTAKS LOGIKA Vol. 2 No.3 , September 2022, **E-ISSN : 2775-412X**
https://jurnal.umpar.ac.id/index.php/sylog

PENERAPAN KRIPTOGRAFI PADA FILE TEKS DENGAN MENGGUNAKAN MERKLE HELLMAN KNAPSACK BERBASIS ANDROID

Desi Ratna Sari[1*], A. Irmayani Pawelloi[2]

[1*]Program Studi Teknik Informatika, [2]Teknik Elektro, Universitas Muhammadiyah Parepare, Indonesia
desiratnasari444999@gmail.com ,irmahakzah@gmail.com

InformasiArtikel

Riwayat Artikel:

Dikirim *Author* : 15-9-2022
Diterima Redaksi : 16-9-2022
Revisi *Reviewer* : 20-9-2022
Diterbitkan *online* : 27-09-2022

Keywords: *Cryptography ; Merkle Hellman Knapsack; File Data.*

ABSTRACT

Exchanging information remotely which is often done so as to make it easier for someone to get data easily, whether general or confidential, causes data to be scattered which can be misused by several parties without the data owner being aware of it. The security of a data must be a big concern. Cryptographic or encryption systems can be used for data security. The Merkle Hellman-Knapsack algorithm is included in asymmetric cryptography because it uses different keys for the encryption and decryption process. The advantage of this asymmetric algorithm is that the process of distributing keys on insecure media such as the internet, does not require confidentiality. Because the distributed key is the public key. So that if this key is lost or known by unauthorized persons, the password message sent will remain safe. While the private key (secret) is kept (not distributed). Encryption is a method of converting message data (plaintext) into ciphertext data (ciphertext), while decryption is a method of changing ciphertext into plaintext. Merkle Hellman-Knapsack algorithm has the stages of key generation, encryption, and decryption. This application uses the Javascript Programming Language The results of this study secure text files from theft by storing text files in the form of ciphertext.

Kata kunci: *Kriptografi; Algoritma; Merkle Hellman-Knapsack;* File Teks.

ABSTRAK

Bertukar Informasi jarak jauh yang sering dilakukan sehingga memudahkan seseorang untuk mendapat data dengan mudah baik yang bersifat umum ataupun rahasia menyebabkan data tercecer yang dapat disalahgunakan oleh beberapa pihak tanpa disadari oleh pemilik data. Keamanan sebuah data harus menjadi perhatian besar. Sistem kriptografi atau enkripsi dapat digunakan untuk keamanan data. Algoritma Merkle Hellman-Knapsack termasuk dalam kriptografi asimetris karena menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsiKelebihan algoritma asimetris ini adalah proses pendistribusian kunci pada media yang tidak aman seperti internet, tidak memerlukan kerahasiaan. 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 (rahasia) tetap disimpan (tidak didistribusikan). Enkripsi adalah metode merubah data pesan (*plaintext*) menjadi data sandi (*ciphertext*), sedangkan dekripsi adalah metode merubah *ciphertext* menjadi *plaintext*. Algoritma Merkle Hellman-Knapsack memiliki tahapan pembangkit kunci, enkripsi, dan dekripsi. Aplikasi ini menggunakan Bahasa Pemrograman Javascript. Hasil dari penelitian ini mengamankan file teks dari pencurian dengan cara menyimpan file teks dalam bentuk chipertext.

Penulis Korespondensi:

Desi Ratna Sari,
Program Studi Teknik Informatika,
Universitas Muhammadiyah Parepare,
Alamat institusi Jl. Ahmad Yani Km.6
Email: desiratnasari444999@gmail.com

I. PENDAHULUAN

Bertukar informasi merupakan hal yang biasa kita lakukan. Bertukar informasi jarak jauh dapat dilakukan melalui kantor pos, surat dan surel (surat elektronik). Surel (Surat Elektronik) memungkinkan kita untuk bertukar informasi jarak jauh tanpa membutuhkan waktu yang lama, namun keamanan informasi (data) dalam pengiriman informasi melalui surat elektronik (e-mail) dipertaruhkan. Oleh karena itu dibutuhkan berbagai cara untuk mengamankan informasi tersebut agar sampai ketujuan dengan aman. Salah satu metode yang digunakan untuk mengamankan data adalah kriptografi. 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. Dalam kriptografy dibutuhkan kunci yaitu kode untuk melakukan Enkripsi dan Dekripsi. Berdasarkan kuncinya kriptografi dibagi menjadi dua tipe yaitu algoritma simetris dan algoritma asimetris. Algoritma simetris adalah algoritma yang mempunyai kunci enkripsi dan dekripsi yang sama, sedangkan algoritma asimetris merupakan algoritma yang terdiri atas dua buah kunci yaitu kunci publik untuk melakukan enkripsi dan kunci privat untuk melakukan dekripsi. Kedua algoritma tersebut mempunyai kelebihan dan kekurangan masing-masing.

Algoritma kriptografi dapat dibagi ke dalam kelompok algoritma simetris dan algoritma asimetris. Algoritma simetris (symmetric algorithm) adalah suatu algoritma dimana kunci enkripsi yang digunakan sama dengan kunci dekripsi sehingga algoritma ini disebut juga sebagai single-key algorithm. Algoritma asimetris (asymmetric algorithm) adalah suatu algoritma dimana kunci enkripsi yang digunakan tidak sama dengan kunci dekripsi. Pada algoritma ini menggunakan dua kunci yakni kunci publik (public key) dan kunci privat (private key). Kunci publik disebarkan secara umum sedangkan kunci privat disimpan secara rahasia oleh si pengguna. Walau kunci publik telah diketahui namun akan sangat sukar mengetahui kunci privat yang digunakan Algoritma kriptografi yang dikategorikan ke dalam algoritma Asimetris salah satunya adalah algoritma MARKLE-HELLMAN KNAPSACK. Merkle Hellman Knapsack merupakan algoritma klasik untuk menyandikan sebuah plaintext dengan cara substitusi sehingga dalam memecahkan pesan tersebut akan terasa susah. Algoritma Merkle Hellman merupakan salah satu metode kriptografi berbasis protokol. Protokol adalah aturan yang berisi tentang langkah-langkah yang melibatkan dua kunci yang dibuat untuk menyelesaikan suatu kegiatan. Dalam kriptografi, protokol digunakan oleh orang-orang yang terlibat, seperti untuk proses otentifikasi, pengaktifan bilangan acak, bahkan untuk berbagi dan bertukar informasi yang bersifat rahasia. Dalam penelitian ini untuk penggunaan algoritma Merklee Hellman menyimpulkan Pada proses enkripsi dengan metode Merkell Hellman, kunci public harus di jumlahkan lalu untuk kunci private harus lebih besar nilainya dari kunci public. Kunci yang dipakai pada proses enkripsi dan deskripsi hanya 8 kunci.

Berdasrakan peneletian terdahulu yang membahas tentang pengamanan file data dengan menggunakan algoritma merkel hellman knapsack salah satunya tahun(2020) Soeb Arifin yang berhasil merancang " pengamanan file video dengan menggunakan algoritma merkel hellman knapsack " bertujuan untuk menjaga informasi yang ada pada file video(10).Pada tahun (2016) Martinus Dias, dan CucuSuhery melakukan peneletian dengan judul "Penerapan Kriptografi Menggunakan Algoritma Knapsack, Algoritma Genetika dan Algoritma Arnolds Catmap pada Citra". Pada penelitian ini peneliti membuat sebuah aplikasi keamanan yang dimana itu adalah citra. Citra merupakan salah satu bentuk data atau informasi yang disajikan secara visual(7).Pada tahun(2018) Indra Gunawan melakukan penelitian yang berjudul "Kombinasi Algoritma Caesar Chiper dan Algoritma RSA untuk pengamanan file Dokumen dan Pesan Teks". Pada penelitian ini peneliti menggunakan 2 gabungan algoritma untuk menbangun keaamanan pada sebuah dokumen dan pesan teks Dengan meningkatkan keamanan data menggunakan kombinasi algoritma, dapat menjaga keamanan data lebih terjamin dari serangan-serangan yang dapat membahayakan isi dari data yang tersimpan, terutama data dalam bentuk berkas dokumen dan pesan teks(6).

Perbedaan penelitian dengan penelitian terdahulu adalah dimana peneliti membuat sebuah keaamanan file teks dengan menggunakan algoritma merkle hellman knapsack.

Adapun tujuan penelitian ini adalah untuk mengamankan sebuah file teks agar informasi yang ada pada file tersebut terjaga keaamanannya.

II. METODOLOGI PENELITIAN

A. Jenis Penelitian

Untuk membantu Penelitian ini dilakukan melalui buku-buku dan internet yang dapat memberikan sumber data dan pengetahuan mengenai kelancaran pengumpulan data, maka penulis menggunakan metode :Penelitian Pustaka (Library Research) sistem yang diteliti, kemudian mencocokkan dengan kemungkinan yang terjadi dalam usaha penyelesaian masalah.

B. Waktu Penelitian

Penelitian ini dilakukan dalam kurung waktu yang dipergunakan untuk pelaksanaan penelitian ini berlangsung selama ± 1 bulan tahun 2022.

C. Metode Pengumpulan Data

Untuk memperoleh data-data yang dibutuhkan dalam rangka melakukan penelitian, maka penulis mengumpulkan data melalui beberapa cara yaitu :

1 Pengumpulan Data

Metode pengumpulan data menggunakan Metode Kepustakaan yaitu metode atau teknik pengumpulan data yang bersumber dari literatur buku-buku penunjang dan jurnal untuk konsep teori yang berhubungan dengan objek permasalahan penelitian.

2 Analisis Data

Menganalisa data-data yang sebelumnya telah dikumpulkan dengan cara menganalisis cara kerja sistem yang akan dirancang, mengidentifikasi masalah, dan menganalisa kebutuhan sistem.

3 Perancangan Program

Sebagai pedoman dalam penulisan program atau kode-kode agar berjalan sesuai rencana.

4 Uji Coba Program

Pengujian program dilakukan untuk memastikan bahwa program yang dibuat dapat berjalan dengan baik dengan cara membuat *Flowchart* Sistem dan kemudian akan digunakan untuk membuat Desain Sistem.

5 Evaluasi

Sistem yang telah selesai dibangun perlu adanya evaluasi untuk menemukan kelemahan yang terdapat pada program yang telah dibangun tadi, yang nantinya bisa digunakan sebagai acuan untuk memperbaiki program sehingga lebih sempurna.

D. Alat dan Bahan

Dalam aktifitas penelitian, penulis membutuhkan alat dan bahan yang mendukung kegiatan penelitian tersebut. Alat dan bahan yang diperlukan antara lain :

1. Alat Penelitian
   a. Alat penelitian yang digunakan selama proses penelitian yaitu alat kendali berbasis elektronika dengan spesifikasi *Hardware* alat penelitian yang digunakan dapat dilihat pada table berikut:

Tabel 1 Perangkat Keras

Nama	Spesifikasi
Laptop	Acer
Processor	Intel R CPU 1.50GH
Memory	4 GB
Hardisk	

   b. Perangkat Lunak yang digunakan untuk membuat aplikasi ini tercantum dalam tabel di bawah ini.

Tabel 2 Perangkat Lunak

Nama	Spesifikasi
Sistem Operasi	Windows 7
Bahasa Pemrograman	javascript
Tools	Framework cordova Android Studio

2. Bahan Penelitian

Bahan yang digunakan dalam penelitian ini berupa data-data yang telah dikumpulkan melalui observasi maupun wawancara.

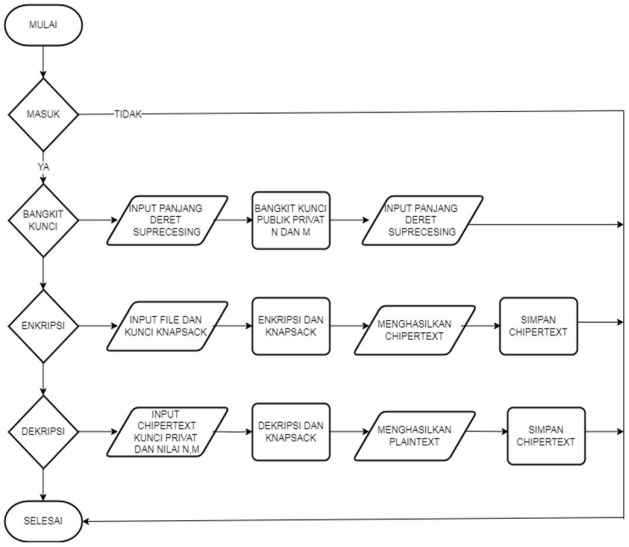
E. Teknik Pengumpulan Data

Metode Pengumpulan data dilakukan melalui studi pustaka, terutama yang berhubungan data-data sekunder. Sementara data primer dilakukan melalui studi lapangan yaitu berupa:

1. *Observasi*, yaitu mengumpulkan data dengan cara mengetahui informasi dan data awal tentang keadaan objek penelitian.
2. *Dokumentasi*, yaitu mengumpulkan data dalam bentuk dokumen atau catatan tertulis.

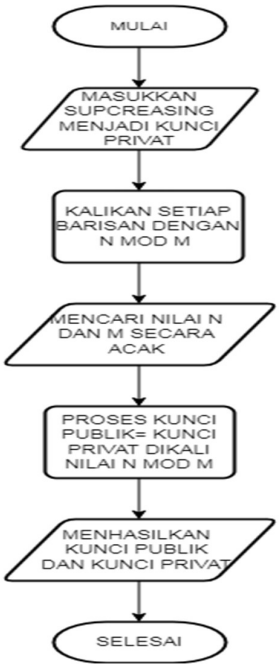
F. ***Rancangan Sistem***

1. Flowchart system



Gambar 1. Flowchart System

2. Flowchart Pembangkit Kunci

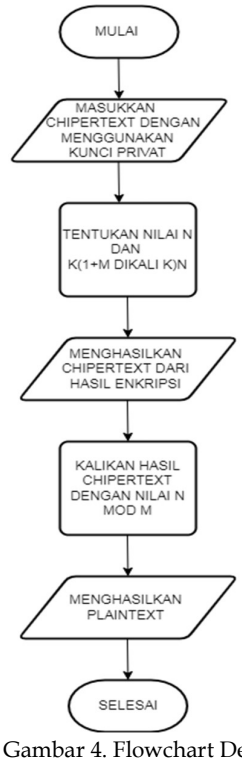


Gambar 2. Flowchart Pembangkit kunci

3. Flowchart Enkripsi

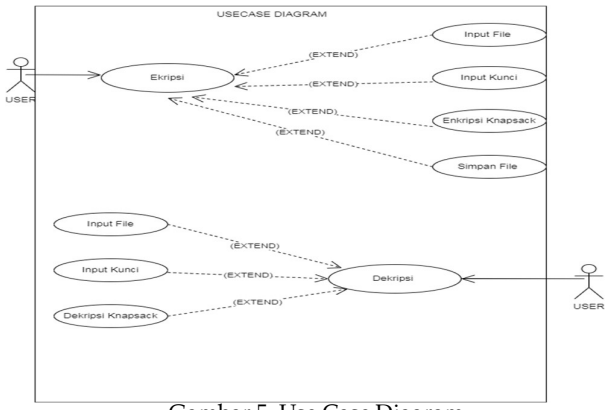
Gambar 3. Flowchart Enkripsi

4. Flowchart Dekripsi



Gambar 4. Flowchart Dekripsi

5. Use case Diagram

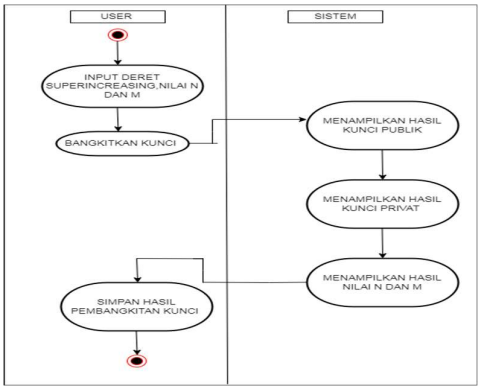


Gambar 5. Use Case Diagram

Tabel 4. Penjelasan Use Case Diagram

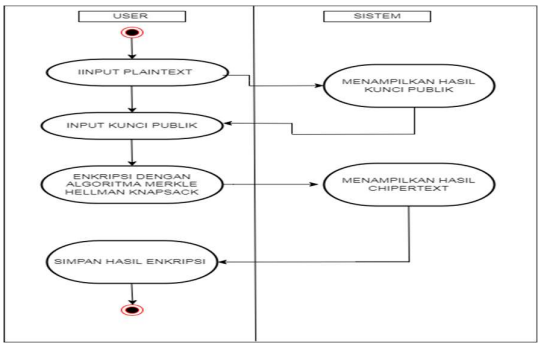
Nama *Usecase*	Deskripsi *Usecase*
Enkripsi	*Use case* ini menjelaskan tentang proses *enkripsi*file teks menggunakan kunci privat.
Input File	Ini menjelaskan user bisa menginput file terlebih dahulu .
Input Kunci	Menjelaskan user menginput Kunci untuk proses enkripsi Merkle
Dekripsi	Menjelaskan tentang proses *dekripsi*teks yang menggunakan kunci privat yang berbeda dengan kunci publik.

6. Activity Diagram Pembangkit kunci



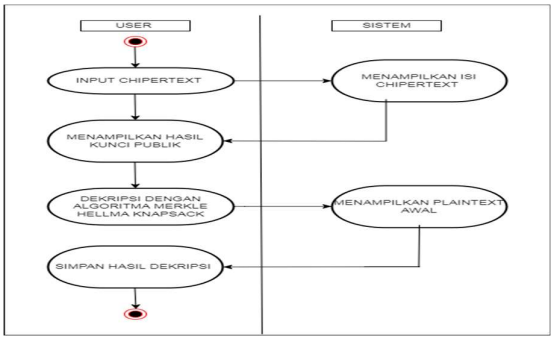
Gambar 6. Activity Diagram Pembangkit Kunci

7. Activity Diagram Enkripsi



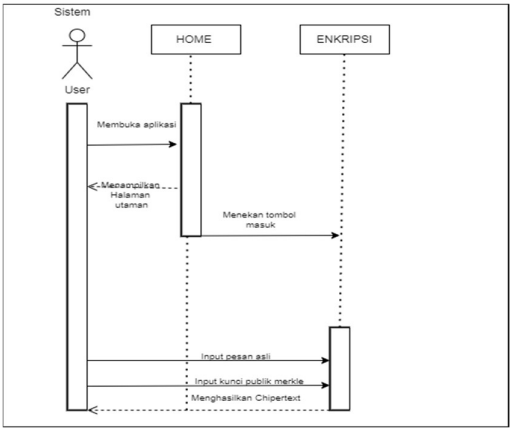
Gambar 7. Activity Diagram Enkripsi

8. Activity Diagram Dekripsi



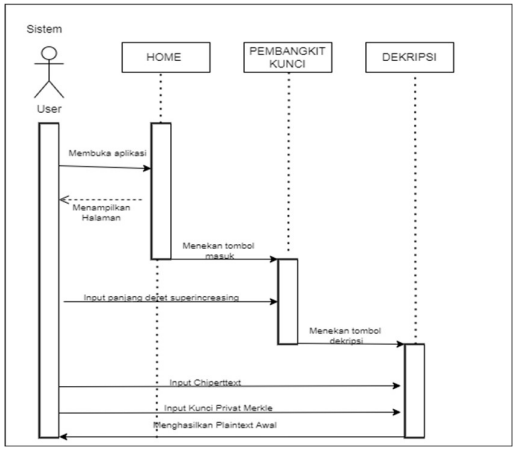
Gambar 8. Activity Diagram Dekripsi

9. Squence Diagram Enkripsi



Gambar 9. Squence Diagram Enkripsi

10. Sequence Diagram Dekripsi



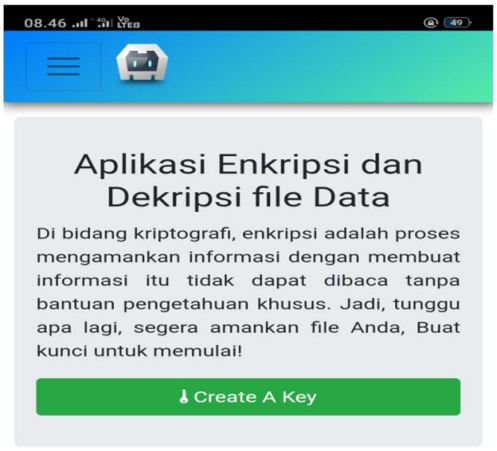
Gambar 10. Squence Diagram Dekripsi

III. HASIL DAN PEMBAHASAN

A.. Tampilan Aplikasi

Tampilan aplikasi sebagai tampilan antarmuka antara sistem dan pengguna.

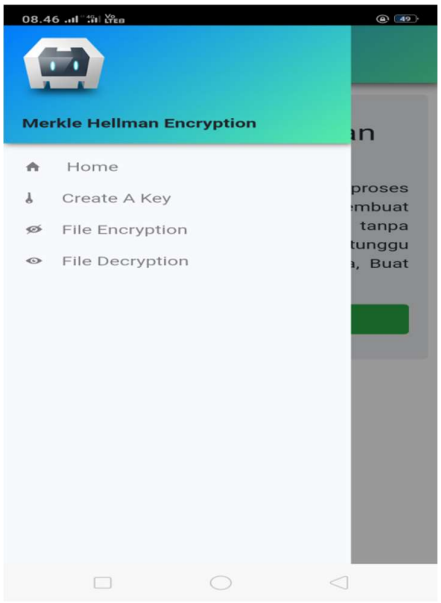
1) Tampilan Halaman Utama



Gambar 1. Tampilan Halaman Utama

2) Tampilan Menu Home

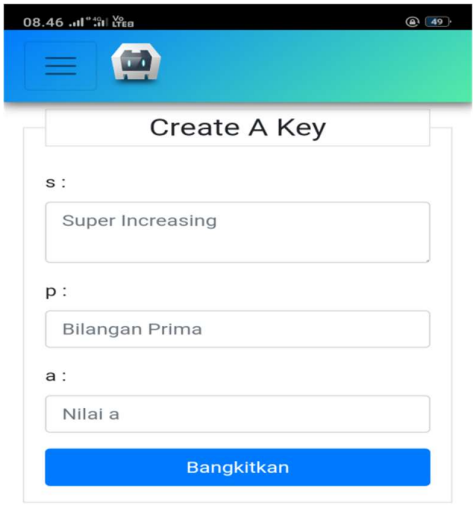
Pada tampilan menu home muncul apabila kita mengklik menu home menu home ini terdapat pada bagian kanan atas halaman utama pada halaman utama dan menu home menampilkan menu home, pembangkitan kunci, enkripsi, dan dekripsinya.



Gambar 2. Tampilan Menu Home

3) Tampilan Menu Pembangkit Kunci

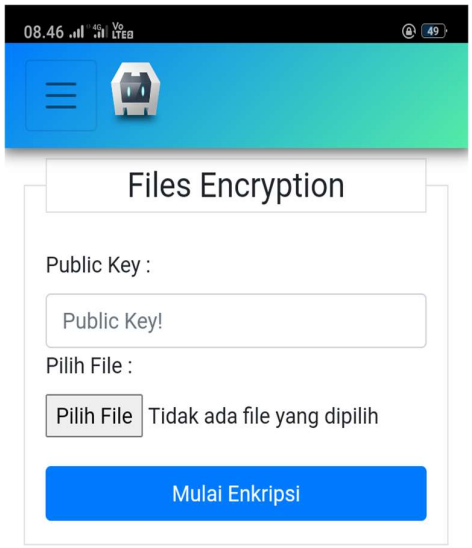
Pada tampilan ini menentukan nilai superincreasing, nilai a atau disebut bilangan pembagi,dan nilai p atau disebut bilangan prima.dan menampilkan tombol menu bangkitkan.



Gambar 3. Tampilan menu pembangkit kunci

4) Tampilan Menu Enkripsi

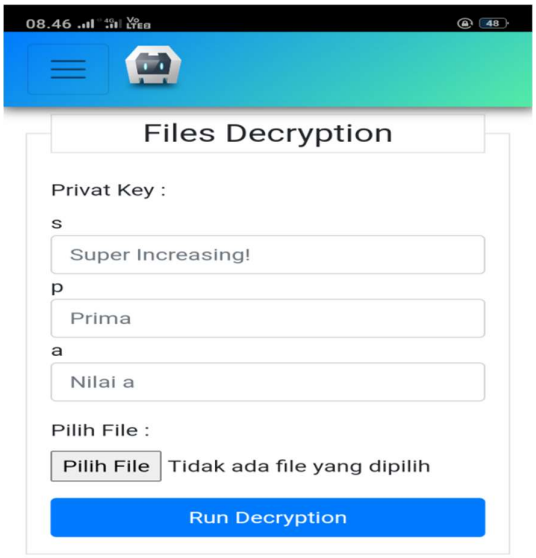
Pada tampilan menu enkripsi terdapat kolom untuk menambahkan kunci publik, pemilihan file untuk memasukkan file yang akan di enkripsi, dan tombol untuk memulai enkripsi.



Gambar 4. Menu Enkripsi

5) Tampilan Menu Dekripsi

Pada tampilan menu dekripsi terdapat beberapa kolom seperti superincreasing,prima dan nilai yang terdapat pada ketiga kolom tersebut adalah kunci privat dan terdapat pemilihan file yang sudah di enkripsi apabila sudah mendapat file terdapat tombol deskripsi.



Gambar 5. Tampilan Menu Dekripsi

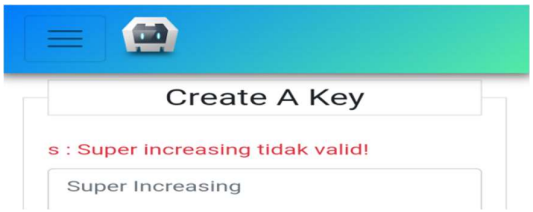
B. *Pengujian Aplikasi*

Pengujian aplikasi dilakukan dengan menggunakan metode pengujian yaitu pengujian *blackbox* dan pengujian *whitebox*.

1. Pengujian Blackbox

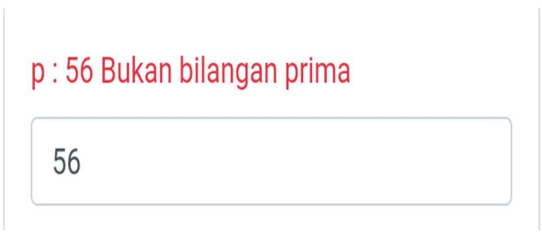
Tabel 1. Nilai superincreasing tidak terisi

Test	Hasil	Kesimpulan
Nilai superincreasing tidak terisi	✓	Berhasil, ada muncul pesan validasi.
Screenshot		



Tabel 2. *Nilai bilangan prima tidak di isi dengan bilangan prima*

Test	Hasil	Kesimpulan
Nilai bilangan prima tidak di isi dengan bilangan prima	✓	Berhasil, karena ada muncul pesan validasi.
Screenshot		



Tabel 3. *Pembuatan Kunci Berhasil*

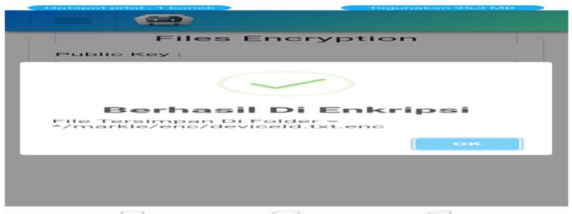
Test	Hasil	Kesimpulan
Pembuatan Kunci berhasil	✓	Berhasil, karena tidak muncul pesan validasi

Screenshot

Tabel 4. *Enkripsi Berhasil*

Test	Hasil	Kesimpulan
Enkripsi Berhasil	✓	Berhasil, karena tidak muncul pesan validasi

Screenshot



Tabel 5. *Dekripsi Berhasil*

Test	Hasil	Kesimpulan
Dekripsi berhasil	✓	Berhasil, karena tidak muncul pesan validasi

Screenshot

Tabel 6. Pengujian Enkripsi dan Dekripsi

No	File teks	Hasil Enkripsi (Chipertext)	Hasil Dekripsi (Plaintext)
1	Sistem kriptografi knapsack Merkle-Hellman adalah salah satu kriptosistem kunci publik paling awal. Diterbitkan oleh Ralph Merkle dan Martin Hellman pada tahun 1978. Serangan waktu polinomial diterbitkan oleh Adi Shamir pada tahun 1984. Akibatnya, sistem kriptografi sekarang dianggap tidak aman.	1859$2086$2231 $1490$1331$173 8$1013$1097$14 76$248$1621$11 58$1331$868$10 13$1766$1387$1 158$952$807$13 31$248$1621$11 86$952$868$173 8$952$1242$162 1$248$1228$109 7$1158$1621$89 6$1097$1352$50 3$1097$896$896 $1476$952$1186 $248$952$517$9 52$896$952$751 $248$173$8$952$ 896$952$751$24 8$1738$952$101 3$1593$248$162 1$1158$1331$86 8$1013$1766$17 38$1331$1738$1 013$1097$1476$ 248$1621$1593$ 1186$1242$1331 $248$868$1593$ 662$896$1331$1 621$248$868$95 2$896$1331$118 6$1387$248$952 $1883$952$896$ 1062$248$269$1 331$1013$1097$ 1158$662$1331$ 1013$1621$952$ 1186$248$1766$ 896$1097$751$2 48$910$952$896 $868$751$248$1 228$1097$1158$ 1621$896$1097$ 248$517$952$11 86$248$1228$95 2$1158$1013$13 31$1186$248$50 3$1097$896$896 $1476$952$1186 $248$868$952$5 17$952$248$101 3$952$751$1593 $1186$248$1324 $1703$1759$112 3$1062$248$149 0$1097$1158$95 2$1186$1387$95 2$1186$248$188 3$952$1621$101 3$1593$248$868 $1766$896$1331 $1186$1766$147	Sistem kriptografi knapsack Merkle-Hellman adalah salah satu kriptosistem kunci publik paling awal. Diterbitkan oleh Ralph Merkle dan Martin Hellman pada tahun 1978. Serangan waktu polinomial diterbitkan oleh Adi Shamir pada tahun 1984. Akibatnya, sistem kriptografi sekarang dianggap tidak aman.

		6$1331$952$896$248$517$1331$1013$1097$1158$662$1331$1013$1621$952$1186$248$1766$896$1097$751$248$704$517$1331$248$1490$751$952$1476$1331$1158$248$868$952$517$952$248$1013$952$751$1593$1186$248$1324$1703$1123$889$1062$248$704$1621$1331$662$952$1013$1186$1827$952$772$248$1738$1331$1738$1013$1097$1476$248$1621$1158$1331$868$1013$1766$1387$1158$952$807$1331$248$1738$1097$1621$952$1158$952$1186$1387$248$517$1331$952$1186$1387$1387$952$868$248$1013$1331$517$952$1621$248$952$1476$1186$1062$248$1104$669$f	

Tabel 7. Pengujian Enkripsi dan Dekripsi

No	File Teks	Hasil Enkripsi (Chipertext)	Hasil Dekripsi (Plaintext)
2	Pengujian Blackbox (blackbox testing) adalah salah satu metode pengujian yang berfungsi pada sisi fungsionalitas yang ada dalam sistem. Kemudian membandingkan hasil keluaran sistem dengan hasil yang diharapkan. Bila hasil yang diharapkan sesuai dengan hasil pengujian, artinya aplikasi sesuai dengan desain yang telah ditentukan sebelumnya. Jika belum sesuai maka perlu dilakukan pengecekan lebih lanjut dan perbaikan.	799$623$651$310$310$310$162$605$563$661$612$535$591$577$563$310$211$507$577$633$647$521$675$486$6$310$324$521$507$577$633$647$521$675$486$310$500$605$640$500$591$563$661$436$310$577$493$577$507$577$479$310$640$577$500$612$310$619$605$500$675$563$493$605$310$472$563$661$591$310$549$612$563$661$640$591$310$472$577$493$577$310$640$591$310$549$612$563$661$640$591$675$563$577$507$591$500$577$640$310$598$577$563$661$310$577$493$577$507$577$619$310$640$591$500$605$619$408$310$337$605$619$612$493$591$577$563$310$619$605$619$521$577$563$493$591$563$661$647$577$563$310$479$577$640$591$507$310$647$605$507$612$577$528$577$563$310$640$591$640$500$605$619$310$493$605$563$661$577$563$310$479$577$640$591$507$310$598$577$563$661$310$493$591$479$577$528$577$472$647$577$563$408$310$211$591$507$577$310$479$577$640$591$507$310$598$577$563$661$310$493$591$479$577$528$577$472$647$577$563$310$640$605$640$612$577$591$310$493$605$563$661$577$563$310$479$577$640$591$507$310$472$605$563$661$612$535$591$577$563$352$310$577$528$500$591$	Pengujian Blackbox (blackbox testing) adalah salah satu metode pengujian yang berfungsi pada sisi fungsionalitas yang ada dalam sistem. Kemudian membandingkan hasil keluaran sistem dengan hasil yang diharapkan. Bila hasil yang diharapkan sesuai dengan hasil pengujian, artinya aplikasi sesuai dengan desain yang telah ditentukan sebelumnya. Jika belum sesuai maka perlu dilakukan pengecekan lebih lanjut dan perbaikan.

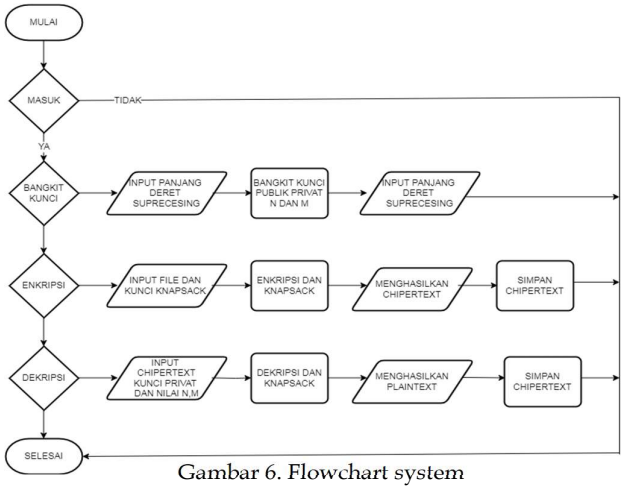
563$598$577$31
0$577$472$507$
591$647$577$64
0$591$310$640$
605$640$612$57
7$591$310$493$
605$563$661$57
7$563$310$493$
605$640$577$59
1$563$310$598$
577$563$661$31
0$500$605$507$
577$479$310$49
3$591$500$605$
563$500$612$64
7$577$563$310$
640$605$521$60
5$507$612$619$
563$598$577$40
8$310$225$591$
647$577$310$52
1$605$507$612$
619$310$640$60
5$640$612$577$
591$310$619$57
7$647$577$310$
472$605$528$50
7$612$310$493$
591$507$577$64
7$612$647$577$
563$310$472$60
5$563$661$605$
633$605$647$57
7$563$310$507$
605$521$591$47
9$310$507$577$
563$535$612$50
0$310$493$577$
563$310$472$60
5$528$521$577$
591$647$577$56
3$408$154$70$1
54$70$ff

2. *Pengujian Whitebox*

Pada tahap pengujian *white box*, dilakukan pengujian terhadap *method source code* yang digunakan pada aplikasi ini. Pengujian *white box* dilakukan untuk memastikan bahwa aplikasi dapat berjalan dengan lancar dan tidak terdapat kesalahan dalam logika pemrograman.

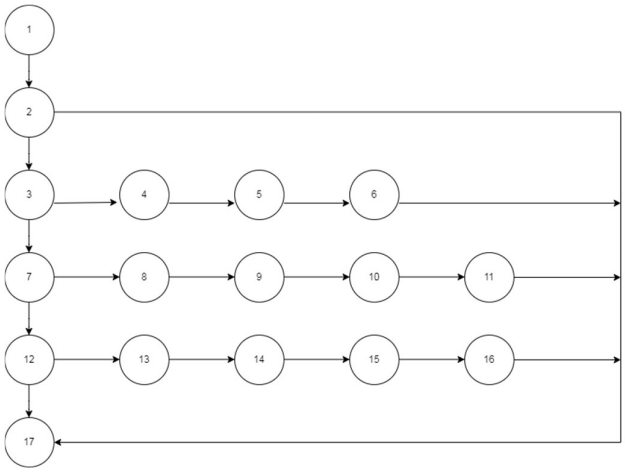
a. Flowchart dan flowgraph system

1) Flowchart system



Gambar 6. Flowchart system

2) Flowgraph system



Gambar 7. Flowgraph system

Dari *flowgraph* menu *login* pada atas dapat dilakukan proses perhitungan sebagai berikut:

1) Menghitung *Cyclomatic Complexcity* V(G) asal *Egde* dan *Node*:

Menggunakan rumus : V(G) = E – N + 2
E (*edge*) = 20
N (*Node*) = 17
P (Predikat *Node*) = 4
Penyelesaian : V(G) = E – N + 2
= 20 – 7 + 2
= 5
Predikat (P) = P + 1
= 4 + 1
= 5

2) Berdasarkan perhitungan *Cyclomatic Complexcity* dari *flowgraph* di atas mempunyai Region = 5

3) *Independentpath* pada *flowgraph* di atas ialah:

Path 1 = 1 – 2 – 3 – 7 – 12– 17
Path 2 = 1 – 2 – 17
Path 3 = 1 – 2 – 3 – 4 – 5 – 6 – 7 – 12 – 17
Path 4 = 1 – 2 – 3 – 7 – 8 – 9 – 10 – 11 – 12 – 17
Path 5 = 1 – 2 – 3 – 7 – 12 – 13 – 14 – 15 – 10 – 17

4) Grafik Matriks Aktivitas Menu

Tabel 8. Grafik Matriks Aktivitas

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	E - 1
1		1																1-1=0
2			1														1	2 - 1 = 1
3				1			1											2 - 1 = 1
4					1													1 - 1 = 0
5						1												1 - 1 = 0
6																	1	1 - 1 = 0
7								1				1						2 - 1 = 1
8									1									1 - 1 = 0
9										1								1 - 1 = 0
10											1							1 - 1 = 0
11																	1	1 - 1 = 0
12													1				1	2 - 1 = 1
13														1				1 - 1 = 0
14															1			1 - 1 = 0
15																1		1 - 1 = 0
16																	1	1 - 1 = 0
17																		
Sum = (E + 1)																		4 + 1 = 5

IV. KESIMPULAN

Pada proses kriptografi dengan algoritma Merkle hellman knapsack memiliki tiga proses mekanisme yaitu proses pembangkitan kunci, enkripsi dan dekripsi. Pada proses kriptografi dengan menggunakan metode Merkle hellman knapsack ini menggunakan kunci Asimetris yang memiliki kunci yang berbeda pada pada proses enkripsi dan deskripsinya dan menggunakan file teks yang berformat txt. File teks yang telah di enkripsi akan tersimpan di media penyimpanan.,Pada proses enkripsi dan dekripsi dengan menggunakan metode MERKLE, file plaintext awal setelah di enkripsi dengan menggunakan kunci publik akan menghasilkan file chipertext, lalu file chipertext di dekripsi kembali dengan kunci privat akan menghasilkan file plaintext awal. Hasil kriptografi dengan menggunakan metode kriptografi MERKLE HELLMAN KNAPSACK menghasilkan chippertext yang tersimpan di media penyimpanan. Chipertext yang dihasilkan berbeda-beda untuk setiap plaintext dan kuncinya. Ini sangat efektif jika digunakan untuk pengamanan suatu file Karena untuk proses Deskripsinya user memerlukan Plain Text dan Kunci. Jika salah satu variabelnya berbeda maka hasil chipper text sudah tentu berbeda

REFERENSI

[1] Andika, D. (2018). Pengertian danSejarah Kriptografi. Diperoleh dari: https://www.it-jurnal.com/pengertian-dan-sejarah-kriptografi/.(Diakses 10Mei 2022).

[2] Dharma.A. K. (2016:2). Kolaborasi dahsyat android dengan php dan mysql.

[3] Nugroho.A. (2010:6) .Bahasa pemodelan UML.

[4] Kurniawan. B. (2020). Pengertian, sejarah, fungsi, karakter dan contoh ASCII Diperolehdari ilmuelektro.id/ascii-adalah/. (Diakses 25 mei 2022)

[5] Munir. R. M.T. (2004) Algoritma Knapsack. Department Teknik Informatika Institut Teknologi Bandung.

[6] Gunawan. I. (2018) .Kombinasi Algoritma Caesar Chiper dan Algoritma RSA untuk pengamanan file dokumen dan pesanteks. Jurnal Nasional Informatika dan Teknologi Jaringan. Medan.

[7] Dias. M.&Suhery. C.(2016).Penerapan Kriptografi menggunakan algoritma knapsack, algoritma genetika, dan algoritma Arnolds Catmap pada citra.Jurnal Coding Sistem Komputer Untan. Pontianak.

[8] Safaat. N. H. (2012). Pemrograman Aplikasi Mobile Smartphone dan Tablet Pc Berbasis Android. Pekan baru, Riau

[9] Santi. R. (2019) Analisa dan pemodelan framework cordova berbasis Anroid.

[10] Arifin. S. (2020). Pengamanan file video menggunakan Algoritma Markle-Hellman Knapsack . Medan.