Implementasi Algoritma Merkle Hellman Dalam Mengamankan Pesan Teks

Implementation of The Merkel Hellman Algortihm in Securing Text Message

Rita Novita Sari[1], Ivi Lazuly[2], Daifiria[3]
[1]Fakultas Teknik dan Ilmu Komputer,
[1]Universitas Potensi Utama
e-mail: *[1]rita.ns89@gmail.com, ivilazuly@potensi-utama.ac.id, daifiria@potensi-utama.ac.id

Abstrak

Pada jaman sekarang ini menjaga kerahasian dan melindungi suatu data pesan adalah hal yang sangat perlu diperhatikan. Banyak cara untuk melindungi atau mengamankan data pesan agar tidak dapat dibaca dan diketahui oleh orang lain yang tidak berkepentinganyaitu dengan memberikan pengamanan secara fisik atau data pesan dirubah kedalam bentuk algoritma berbasis matematika agar pesan tersebut tidak mudah dibaca. Algoritam kriptografi merupakan salah satu cara yang digunakan untuk melindungi / mengamankan data pesan. Dengan algoritma kriptografi ini maka data pesan yang dilindungi / diamankan dengan proses enkripsi dan dekripsi pesan. Hasil dari dilaksanakan penelitian ini adalah dengan menggunakan algoritma Merkle Hellman dapat melindungi data pesan teks. Dengan algoritma ini memanfaatkan kunci public dan kunci privet untuk proses enkripsi dan dekripsi sehingga data pesan teks yang dilindungi tidak akan dengan gampang diketahui oleh orang – orang yang tidak memiliki akses.

Kata Kunci : Keamanan, Kriptografi, Merkle Hellman

.

Abstract

In this day and age, maintaining confidentiality and protecting message data is something that really needs to be considered. There are many ways to protect or secure message data so that it cannot be read and known by other people who are not interested, namely by providing physical security or changing the message data into a mathematical-based algorithm so that the message is not easy to read. Cryptographic algorithm is one way that is used to protect / secure message data. With this cryptographic algorithm, the message data is protected / secured by the encryption and decryption process of the message. The result of this research is that using the Merkle Hellman algorithm can protect text message data. With this algorithm, it utilizes the public key and private key for the encryption and decryption process so that protected text message data will not be easily known by people who do not have access.

Keywords: Security, Cryptography, Merkle Hellman

1. PENDAHULUAN

Pada jaman sekarang ini menjaga kerahasian dan keamanan suatu data pesan merupakan hal yang sangat perlu diperhatikan. Banyak cara untuk melindungi atau mengamankan data pesan agar tidak dapat dibaca dan diketahui oleh orang lain yang tidak berkepentinganyaitu dengan memberikan pengamanan secara fisik atau data pesan dirubah kedalam bentuk algoritma berbasis matematika agar pesan tersebut tidak mudah dibaca. Data pesan yang sudah diamankan tidak aakn diketahui oleh pihak – pihak yang tidak berhak dan hanya orang yang berhak saja yang dapat membaca data pesan tersebut.

Algoritam kriptografi adalah beberapa cara yang diciptakan untuk melindungi / mengamankan data pesan. Dengan algoritma kriptografi ini maka data pesan yang dilindungi / diamankan dengan proses enkripsi dan dekripsi pesan. Ada banyak algoritma kriptogradi yang digunakan untuk melindungi / mengamankan data pesan dengan menggunakan proses enkripsi dan dekripsi pesan.

Algoritma kriptografi Merkle Hellman merupakan salah satu algoritma yang dapat digunakan untuk melindungi / mengamankan data pesan. Dengan menggunakan diskrit logatihtmics pada algoritma markle hellmen untuk proses enkripsi dan deskripsi para hacker tidak akan bisa membaca data pesan tersebut. Untuk mengetahui / membaca data pesan seorang hacker harus mengetahui private key, kunci public, urutan super meningkat. [1]

Pada tahun 1978 Merkle dan Hellman menemukan algoritma krpitografi Mekel Hellman. Untuk proses enkripsi dan dekripsi pesan teks pada algoritma kriptografi Merkle Hellman menggunakan kunci Asimetris. Algoritma kriptografi Merkle Hellman mudah dipelajari karena menerapkan konseptual dan Teknik desain.[2]

Merkle Hellman digunakan subset masalah untuk membuat Kriptografi untuk mengenkripsi data, Superincreasing S ransel vektor diciptakan dan Properti superincreasing tersembunyi dengan membuat kedua vektor M oleh perkalian Modular dan permutasi, Vektor M adalah kunci umum kriptografi dan S digunakan untuk mendekripsi pesan.[3]

Penelitian dengan judul Pengaman File Video Menggunakan Algoritma Merkle Hellman Knapsack yang dilakukan oleh Soeb Aripin dan Muhammad Syahrizal (2020). Pada penelitian ini menggunakan Algoritma Merkle-Hellman Knapsack untuk melindungi file video dan dapat melindungi video agar video tidak mudah digunakan oleh orang yang tidak bertanggungjawab karena video – video yang dikirim sudah dilakukan proses enkripsi dengan menggunakan algoritma Merkle Hellman. Proses enkripsi dan dekripsi dengan menggunakan algoritma Merkle Hellman menghasilkan sebuah ciperteks, dimana ciperteks yang dihasilkan berbentuk barisan bilangan dan membentuk plainteks, dimana plainteks awal tersebut sama dengan plainteks akhir dari proses dekripsi. [4]

Penelitian yang dilakukan oleh Magdalena Simanjuntak dengan judul Implementasi Algoritma Merkle Hellman untuk Keamanan Database (2019). Pada penelitian ini melindungi database dengan menggunakan proses enkripsi sehingga menghasilkan pesan yang tidak dapat diaca (cipherteks), namun setelah dijalankan proses dekripsi maka database akan kembali menjadi bentuk awal (plainteks) yang dapat dibaca dengan menerapkan algoritma Merkle Hellman. [5]

Penelitian yang dilakukan oleh Murdani (2017) dengan judul Perancangan Aplikasi Keamanan Data Teks Menggunakan Algoritma Merkle Hellman Knapsack. Pada penelitian ini menggunakan kunci privat dan kunci public untuk untuk memberikan perlindungan ganda dalam mengamankan data teks sehingga data teks tidak dapat dengan mudah dibaca oleh pihak yang tidak bertanggungjawab. Dengan menggunakan algoritma Merkle Hellman Knapsack proses enrkripsi dan deksripsi melahirkan ciperteks, dimana ciperteks yang dilahirkan berbentuk dereta angka, dimana dereta angka ini menciptakan plainteks awal yang sama dengan plainteks akhir dari proses dekripsi. Dengan menggunakan algoritma ini data pesan teks lebih terlindungi dibandingan dengan menggunakan algoritma kriptografi yang lain, karena algoritma Merkle Hellman menghasilkan enrkipsi berupa angka sedangkan algortima kriptografi menghasilkan berupa teks. [6]

Penelitian yang dilakukan oleh Lamrianto Purba (2019) dengan judul Aplikasi Enkripsi dan Dekripsi Teks Menggunakan Algoritma Merkle Hellman. Pada penelitian ini penulis menggunakan algoritma Merkel Hellman yang bertujuan untuk melindung data – data yang ingin dilindungi oleh *user* agar tidak dapat dibaca/ digunakan oleh orang yang tidak bertanggungjawab. Dengan menggunakan algoritma Merkle Hellman data – data akan dienkripsi secara ganda (2 x) untuk menghasilkan symbol – symbol yang berbeda dengan data awal yang telah diinputkan. Symbol –

symbol yang dihasilkan tadi akan dirubah kembali menjadi data – data yang dapat dibaca oleh *user* seperti data awal dengan menggunakan kunci yang telah ditentukan oleh *user*. [7]

Penelitian yang dilakukan oleh Aminudin, Ahmad Faisal Helmi, dan Sofyan Arifianto (2018) yang berjudul Analisa Kombinasi Algoritma Merkle-Hellman Knapsack Dan Algoritma Diskrit Pada Aplikasi Chat. Pada penelitian ini penulis mengamankan data pesan pada aplikasi pesan chat sehingga pengguna dapat dengan tenang mengirim pesan tanpa perlu merasa takut pesannya akan dibaca oleh pihak – pihak yang tidak bertanggungjawab. Pesan teks yang dikirim melalui aplikasi chat akan diubah dengan menggunakan kunci public untuk menghasilkan pesaan yang berbentuk ciperteks. Pesan teks yang berbentuk ciperteks selanjutnya akan diubah kembali menjadi pesan teks dengan menggunakan kunci privat.[8]

Penelitian yang dilakukan oleh Muhammad Fadlan, Hadriansa (2017) dengan judul Rekayasa Aplikasi Kriptografi Dengan Penerapan Kombinasi Algoritma Knapsack Merkle Hellman Dan Affine Cipher. Pada penelitian ini penulis menggabungkan algoritma Knapsack Merkle Hellam dengan algoritma Affine Cipher. Penggabungan algoritma ini diawali dengan menggunakan algoritma affine cipher untuk proses enkripsi dimana pada proses ini merubah pesan awal yang bisa dibaca menjadi pesan yang tidak bisa dibaca oleh orang lain jika tidak memiliki kunci. Pesan yang sudah dienkripsi disebut ciperteks. Selanjutnya dengan menggunakan algoritma Knapsack Merkle Hellman merubah ciperteks menjadi pesan awal yang dapat dibaca dengan proses dekripsi. [9]

Penelitian yang dilakukan oleh Mardalius (2018) dengan judul Implementasi Aplikasi Enrkipsi dan Dekripsi Text Dengan Menggunakan Algoritma Merkle Hellman Knapsack. Pada penelitian ini menerapkan Metode Algoritma Merkle Hellman dalam melindungi text dengan menggunakan Bahasa pemograman Visual Basic. Net. Hasil enkripsi dan dekripsi yang didapat akan dibandingkan dengan yang dilakukan secara manual dan menggunakan software yang dibangun dengan Bahasa pemograman Visual Basic. Net. [10]

Penelitian yang dilakukan oleh Deski Helsa Pane (2020) dengan judul Implementasi Kriptografi Keamanan Data Resi Pada PT JNE Perbaungan Menggunakan Metode Merkle Hellman (2020). Pada penelitian ini peneliti Deski menggunakan algoritma Kriptografi Merkle Hellman untuk melindungi data resi pada PT. JNE. Implementasi algoritma ini yang dituangkan kedalam Bahasa pemograman dan melakukan proses pengujian aplikasi sesuai dengan data yang telah ditambahkan dan untuk melindungi data resi para customer pada PT. JNE. [11]

Penelitian yang dilakukan oleh Akik Hidayat, Rudi Rosyadi, Erick Paulus (2016) dengan judul Aplikasi Merkle-Hellman Knapsack Untuk Kriptografi File Teks. Pada peneltian ini Akik beserta teman – teman melakukan penelitian dengan menggunakan algoritma Merkle Hellman. Dimana pada algoritma ini menggunakan kunci Asimetris untuk melindungi file teks. Akik beserta teman – teman menerapkan algoritma Merkle Hellman dan Bahasa pemograman C^{++} untuk melindungi file teks.

2. METODE PENELITIAN

Algoritma kriptografi Merkle Hellman merupakan sandi, dimana sandi ini bermulai dari algoritma kriptografi one time pad, merupakan kunci yang dibangun secara acak dan ukuran kunci harus sama dengan jumlah teks awal yang akan dilakukan proses enkripsi. Tetapi dengan algoritma kriptografi menggunakan pembangkit kunci – kunci yang sudah ditentukan secara spontan dengan teknik berikatan[10].

Algoritma kriptografi Merkle Hellman ini mempunyai metode penggantian berdasarkan pada algoritma Caesar cipher yaitu dengan pemindahan karakter – karakter. Kemampuan sepasang algoritma terletak di deretan angka – angka yang bermanfaat menjadi pengali beserta kunci.

Deretan angka – angka tercantum dapat berbentuk angka tertentu seperti barisan angka ganjil, angka genap, barisan fibonanci, barisan angka prima, serta barisan angka yang dilakukan sendiri[11].

Faktnya penggantian sandi dilakukan sebagai suatu hal yang rumit, yaitu bersama melakuan proses enrkripsi secara *double* (proses enkripsi dilakukan sebanyak dua kali), jadi pesan awal akan dienkripsi dengan cipher pertama, selanjutnya hasil enkripsi pertama dienkripsi kembali dengan cipher kedua yang arah II kebalikan arah I. Untuk itu maka normalnya untuk cipher ini adalah cipher ganda yaitu cipher yang melakukan enkripsi secara double, yaitu dengan memuat pola enkripsi pertama dengan merunjung kearah kanan dan enkripsi kedua merunjung ke arah kiri.

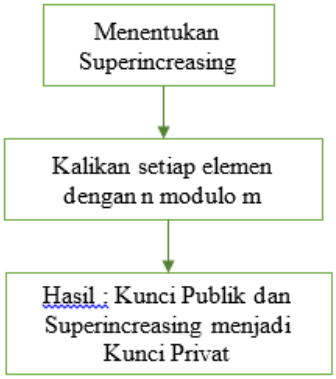
Merkle Hellman merupakan bagian dari algoritma kriptografi yang menerapkan mode kunci asimetri. Dengan algoritma Merkle Hellman, kunci yang diterapkan adalah dua kunci yang tidak sama dengan kunci yang lainnya. Kunci pertama bakal digunakan pada proses enkripsi dan satu kunci untuk melakukan proses dekripsi. Umumnya akan dijelaskan sistem prosedur algoritme kriptografi Merkle Hellman sebagai berikut :

a. Data Pesan Teks dirubah menjadi angka biner yang setelah itu dilakukan proses pengalian pada kunci publik. Hasil pengalian ini kemudian akan ditotalkan lalu dikirim ke orang yang dituju.
b. Orang yang dituju memakai secret key untuk melacak terget sum. Dengan menggunakan metode target sum, orang yang dituju memperoleh hasil pesan yang sudah berbentuk angka biner {0,1}*. Demi memperoleh pesan awal, dilakuan proses perubahan angka biner ini ke karakternya.

Merkle Hellman Knapsack memiliki keunggulan lain pada kemampuan yaitu memiliki total kunci publik. ketika ditemukan n pengguna, yang sekedar memiliki satu kunci publik, oleh karena itu untuk total pengguna yang jumlahnya cukup banyak, metode ini akan sangat berguna. Dengan menerapkan pergantian kunci pada proses enkripsi dan dekrispi data pesan teks dengan menggunakan algoritma kripto adalah melindungi data pesan seperti teks untuk menjauhi terhadap pengintaian yang dibuat oleh orang – orang yang tiada bertanggung jawab[5]. Tahapan – tahapan penjelasan Matematika yaitu :

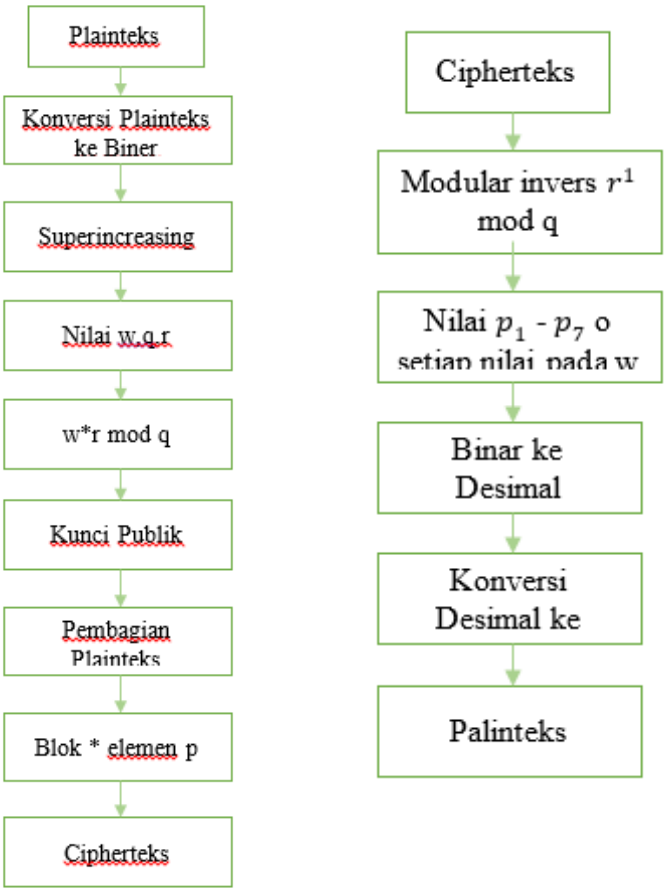
1. Menentukan deretan superincreasing dari total angka integral positif. deretan super increasing adalah salah satu dimana setiap bilangan lebih besar dari total jumlah sebelumnya angka. s = (s1, s2, s3, ….sn)
2. Perlu merubah semua huruf dari pesan ke biner. Dereta angka biner pengantar oleh peubah b.
3. Untuk menentukan dua angka bulat (a) yang makin besar dari pada total semua angka pada deretan dan co-prime (r).
4. deretan dan angka dan r membuat bersama – sama kunci pribadi kriptografi tersebut.
5. Seluruh anggota – s1, s2, s3, … sn, dari deretan s dilakukan proses pengalian dengan jumlah r dan modulus dari sebagian diperoleh dengan memaruh dengan bilangan. Oleh sebab itu, pi = r si mod a
6. Semua anggota p1, p2, p3, …. pn dereta p adalah dilakukan proses pengalian dengan elemen – elemen yang sesuai dari biner urutan b.
7. Kemudian bilangan – bilangan tersebut akan dijumlahkan untuk menghasilkan pesan yang sudah dienrkipsi. Deretan M = (M1, M2, M3…Mn) membuat kunci-kunci kriptografi.

Algoritma Merkle-Hellman digunakan pada tahapan untuk proses enkripsi dan dekripsi pesan teks. Langkah pertama yang harus dilakukan pada algoritma Merkle Hellman adalah dengan menentukan kunci publik dan privat. Adapun algoritma untuk menentukan kunci tersebut dapat dilihat pada Gambar 1.



Gambar 1. Algoritma Pembangkit Kunci

Pada bagian ini akan dilakukan proses enkripsi dan dekripsi teks yang dapat dilihat pada gambar 2.



Gambar 2. Proses Eknripsi dan Dekripsi Teks Merkle Hellman

3. HASIL DAN PEMBAHASAN

Pada pembahasan ini peneliti melakukan beberapa langkah – langkah dalam penelitian ini yaitu yang pertama peneliti menentukan data teks yang akan dilindung. Data teks yang akan dilindungi ini akan disebut sebagai plainteks. Plainteks yang sudah ditentukan selanjutnya akan dirubah ke dalam table ASCII dan selanjutnya diubah menjadi angka / bilangan biner. Langkah ke dua peneliti melakukan proses enkripsi. Pada penelitian ini dengan menggunakan metode algoritma kriptografi Markle Hellman proses enkripsi dilakukan sebanyak 2 kali yaitu enkripsi ke satu dan enkripsi ke dua. Dengan dilakukan dua kali proses enkripsi maka diperoleh lah data teks yang tidak dapat dibaca, data teks tersebut kemudian disebut sebagai cipher. Langkah terakhir setelah cipher diperoleh, cipher yang diperoleh dilakukan proses dekripsi agar cipher kembali ke pesan awal. Proses pada penelitian ini dapat dilihat pada contoh langkah – langkah penelitian. Pada penelitian ini peneliti mengambil melakukan enkripsi dan dekripsi dengan menggunakan plainteks Potensi Utama. Langkah – langkah penelitian yang dilakukan oleh peneliti adalah Plaintek dari kata Potensi Utama dirubah ke table ASCII sehingga menjadi {80, 111, 116, 101, 110, 115, 105, 32, 85, 116, 97, 109, 97} Setelah ditentukan plainteknya kemudian diubah kedalam bentuk biner sehingga menjadi :

P = 01010000

o = 01101111

t = 01110100

e = 01100101

n = 01101110

s = 01110011

i = 01101001

<Spasi> = 00100000

U = 01010101

t = 01110100

a = 01100001

m = 01101101

a = 01100001

Selanjutnya tentukan super increasing (w) = {3,4,9,19,38,76,151,310}

q = 611

r = 31

kemudian lakukan cari nilai w * r mod q

$w_1 = 3 * 31 \bmod 611 = 93$

$w_2 = 4 * 31 \bmod 611 = 124$

$w_3 = 9 * 31 \bmod 611 = 279$

$w_4 = 19 * 31 \bmod 611 = 589$

$w_5 = 38 * 31 \bmod 611 = 567$

$w_6 = 76 * 31 \bmod 611 = 523$

$w_7 = 151 * 31 \bmod 611 = 611$

$w_8 = 310 * 31 \bmod 611 = 196$

$w_1 = 3 * 31 \bmod 611 = 93$

$w_2 = 4 * 31 \bmod 611 = 124$

$w_3 = 9 * 31 \bmod 611 = 279$

$w_4 = 19 * 31 \bmod 611 = 589$

$w_5 = 38 * 31 \bmod 611 = 567$

$w_6 = 76 * 31 \bmod 611 = 523$

$w_7 = 151 * 31 \bmod 611 = 611$

$w_8 = 310 * 31 \bmod 611 = 196$

Kunci public untuk dilakukan enkripsi adalah : { 93, 124, 279, 589, 567, 523, 611, 196}

Selanjutnya, dilakukan pembagian plaintext ke dalam blok-blok berdasarkan jumlah elemen p sebagai berikut:

Block 1 = 01010000

Block 2 = 01101111

Block 3 = 01110100

Block 4 = 01100101

Block 5 = 01101110

Block 6 = 01110011

Block 7 = 01101001

Tahap berikutnya, setiap bagian akan dilakukan proses pengalian dengan tiap - tiap bagian p, sehingga diperoleh hasil ciperteks sebagai berikut :

Cipher 1 = (0*93) + (1*124) + (0*279) + (1*589) + (0*567) + (0*523) + (0*611) + (0*196) = 282

Cipher 2 = (0*93) + (1*124) + (1*279) + (0*589) + (1*567) + (1*523) + (1*611) + (1*196)= 1498

Cipher 3 = (0*93) + (1*124) + (1*279) + (1*589) + (0*567) + (1*523) + (0*611) + (0*196)=1515

Cipher 4 = (0*93) * (1*124) + (1*279) + (0*589) + (0*567) + (1+523) + (0*611) + (1*196) = 1122

Cipher 5 = (0*96) + (1*124) + (1*279) + (0*589) + (1*567) + (1*523) + (1*611) + (0*196) =2104

Cipher 6 = (0*96) + (1*124) + (1*279) + (1*589) + (0*567) + (0*523) + (1*611) + (1*196)= 1799

Cipher 7 = (0*96) + (1*124) + (1*279) + (0*589) + (1*567) + (0*523) + (0*611) + (1*196) = 1166

Sehingga diperoleh cipherteks {282, 1498, 1515, 1122, 2104, 1799, 1166}

Selanjutnya cipherteks yang sudah didapat dilakukan deskripsi

P_1 = 282 * 31 mod 611 = 188

P_2 = 1498 * 31 mod 611 = 9

P_3 = 1515 * 31 mod 611 = 529

P_4 = 1122 * 31 mod 611 = 568

P_5 = 2104 * 31 mod 611 = 458

P_6 = 1799 * 31 mod 611 = 168

P_7 = 1166 * 31 mod 611 = 97

nilai P_1 sampai P_7 akan diuraikan dengan memanfaatkan setiap angka pada w. penguraian ini dibuat dengan sistem penyusutan pada angka dari yang terbesar sampai ke terkecil.

P_1 = 188 – 76 = 112 – 76 = 36 – 19 = 17 – 9 = 8 – 4 = 4 – 4 = 0

Plainteks : 01010000

P_2 = 9 – 9 = 0

Plainteks : 01101111

P_3 = 529 – 310 = 219 -151 = 68 – 38 = 30 – 19 = 11 – 3 = 8 – 4 = 4 – 4 = 0

Plainteks : 01110100

P_4 = 568 – 310 = 258 -151 = 107 – 76 = 31 – 19 = 12 – 9 = 3 – 3 = 0

Plainteks : 01100101

P_5 = 458 – 310 = 148 – 76 = 72 – 38 = 34 – 19 = 15 – 9 = 6 – 3 = 3 – 3 = 0

Plainteks : 01101110

P_6 = 168 – 151 = 23 – 19 = 4 – 4 = 0

Palinteks : 01110011

P_7 = 97 – 76 = 21 – 9 = 12 – 4 = 8 – 4 = 4 – 4 = 0

Palinteks 01101001

Sehingga diperoleh plainteks : 01010000, 01101111, 01110100, 01100101, 01101110, 01110011, 01101001. Nilai biner dirubah menjadi nilai decimal dan dikonversikan menjadi karakter sehingga diperoleh : Potensi.

4. KESIMPULAN

Kesimpulan dari dilaksanakan penelitian ini adalah dengan menggunakan algoritma Merkle Hellman dapat melindungi data pesan teks. Dengan metode kriptografi ini memanfaatkan kunci public dan kunci privet untuk proses enkripsi dan dekripsi sehingga data pesan teks yang dilindungi tidak akan dengan mudah dibaca oleh orang – orang yang tidak memiliki akses.

5. SARAN

Saran untuk perbaikan penelitian ini adalah menggunakan algoritma steganografi untuk perlindungan double pada data pesan teks yang akan dilindungi sehingga pesan data teks tida bisa dilihat / dibaca oleh orang yang tidak memiliki akses pada data tersebut.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Potensi Utama yang telah memberi dukungan financial terhadap penelitian ini. Dan kepada seluruh pihak yang terlibat sehingga penelitian ini bisa terbit. Dan semoga penelitian ini dapat bermanfaat dan berguna bagi para peneliti – peneliti yang ingin meneliti tentang kriptografi.

DAFTAR PUSTAKA

[1]. Bhat, A. R. S. (2013). "<2013.pdf>." International Journal of Scientific and Research Publications 3(4): 1-5.

[2]. A. F. Helmi, S. Arifianto, J. T. Informatika, and U. M. Malang, “ANALISA KOMBINASI ALGORITMA MERKLEHELLMAN KNAPSACK DAN ANALYSIS OF A COMBINATION OF MERKLEHELLMAN ALGORITHMS AND,” vol. 5, no. 3, pp. 325–334, 2018.

[3]. Agarwal, A. (2011). "<20110502.pdf>." IJCSNS International Journal of Computer Science and Network Security 11: 1-3.

[4]. Aripin, Soeb., 2020, Muhammad Syahrizal, Pengaman File Video Menggunakan Algoritma Merkle Hellman Knapsack, JURNAL MEDIA INFORMATIKA BUDIDARMA, Volume 4, Nomor 2, April 2020, Page 461-465

[5]. S. Magdalena, P. Tioria, dan R. Semiati, ”Implemtasi Algoritma Merkle Helman Untuk Keamanan Data Base”, Media Informasi Analisis Dan Sistem, Vol 4, no1, pp. 46-50, 2019.

[6]. Murdani, “PERANCANGAN APLIKASI KEAMANAN DATA TEKS MENGGUNAKAN ALGORITMA MERKLE HELLMAN KNAPSACK,” Jurnal Pelita Informatika, vol. 16, no. 3, pp. 302-305 , 2017.

[7]. Purba, Lamrianto,. Guidio Leonarde Ginting, Aplikasi Enkripsi dan Dekripsi Teks Menggunakan Algoritma Merkle Hellman, MEANS (Media Informasi Analisa dan Sistem), Volume 4 No. 1, Januari - Juni 2019

[8]. Aminudin, Ahmad Faisal Helmi, dan Sofyan Arifianto, 2018, Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), Vol. 5, No.3, Agustus 2018, hlm. 325-x

[9]. Fadlan, M., & Hadriansa, H, 2017, Rekayasa Aplikasi Kriptografi dengan Penerapan Kombinasi Algoritma Knapsack Merkle Hellman dan Affine Cipher, Jurnal Teknologi Informasi Dan Ilmu Komputer, 4(4), 268–274.

[10]. Mardalius, 2018, Implementasi Aplikasi Enkripsi Dan Dekripsi Text Pada Visual Basic .Net Mengunakan Algoritma Merkle Hellman Knapsack, Seminar Nasional Royal (SENAR) 2018, ISSN 2622-9986

[11]. Deski Helsa Pane, 2020, Implementasi Kriptografi Keamanan Data Resi Pada PT JNE Perbaungan Menggunakan Metode Merkle Hellman, Journal of Information System, Computer Science and Information Technology, Vol.1, No.1 Juni 2020

[12]. A. Hidayat and R. Rosyadi, 2016 “Cryptography Asymmetries Merkle Hellman Knapsack Digunakan untuk Enkripsi dan Dekripsi Teks,” pp. 27–28,

[13]. R. Munir, “Kriptografi,” Inform. Bandung, 2006.