JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 4, Nomor 2, April 2020, Page 461-465
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i2.2039

Pengaman File Video Menggunakan Algoritma Merkle Hellman Knapsack

Soeb Aripin[*], Muhammad Syahrizal

[1] Program Studi Manajemen Informatika, STMIK Budi Darma, Medan, Indonesia
[2] Program Studi Teknik Informatika, STMIK Budi Darma, Medan, Indonesia
Email: [1,*]soebaripin0@gmail.com, [2]Syahrizal83.budidarma@gmail.com
Email Penulis Korespondensi: soebaripin0@gmail.com

Abstrak−Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu pesan, data, atau informasi. Dalam hal ini sangat terkait dengan betapa pentingnya pesan, data, atau informasi tersebut dikirim dan di terima oleh pihak atau orang yang berkepentingan, apakah pesan, data, atau informasi masih authenticity. Saat ini banyaknya kemudahan dalam mengunduh dan mengupload video membuat rentannya video untuk dibajak, apalagi jika video itu adalah video yang penting dan sangat rahasia maka diperlukannya suatu aplikasi yang mampu menyandikan video penting tersebut agar keamanannya dapat terjaga dari orang lain yang tidak berkepentingan, kecuali orang yang berhak. Teknik pengamanan yang digunakan penulis didalam penelitian ini, menggunakan teknink kriptografi. Agar dapat dilakukan dengan baik, dibutuhkan suatu algoritma untuk enkripsi dan dekripsi. Algoritma yang digunakan disini adalah Algoritma Merkle Hellman. Algortman ini dapat digunakan pada suatu file video merupakan hal yang perlu diperhatikan dalam menjaga kerahasiaan data itu sendiri, terutama bila file video tersebut hanya boleh diketahui pihak yang tertentu saja.terdapat banyak cara pendekatan yang dilakukan untuk mewujudkan kerahasian data tersebut dimulai dari pengamanan atau perlindungan secara fisik hingga kedalam bentuk algoritma berbasis matematika yang membuat data menjadi tidak terbaca.Sehingga data yang ada di dalamnya tidak dapat mudah diketahui oleh pihak-pihak yang tidak berhak dan hanya penerima file video yang dimaksud mampu menguraikan file video tersebut.

Kata Kunci: Merkle dan Hellman, File video, Algoritma Merkle Hellman

Abstract−The issue of security and confidentiality is one important aspect of a message, data or information. In this case it is closely related to how important the message, data, or information is sent and received by parties or people concerned, whether the message, data, or information is still authenticity. At present there are many conveniences in downloading and uploading videos that make videos vulnerable to hijacking, especially if the video is an important and highly confidential video, so an application that is able to encode this important video is needed so that its security can be protected from unauthorized people, except for people who are entitled to. The security technique used by the author in this study uses cryptographic technology. To be able to do well, we need an algorithm for encryption and decryption. The algorithm used here is the Merkle Hellman Algorithm. This Algortman can be used on a video file is something that needs to be considered in maintaining the confidentiality of the data itself, especially if the video file can only be known by certain parties. There are many ways of approach taken to realize the confidentiality of the data starting from security or protection. physical to the form of a mathematical-based algorithm that makes the data illegible. So that the data in it cannot be easily known by unauthorized parties and only the intended video file recipient is able to decipher the video file.

Keywords: Merkle and Hellman, Video files, Merkle Hellman Algorithm.

1. PENDAHULUAN

Menjaga keamanan dan kerahasiaan data merupakan hal yang sangat penting untuk melakukan sebuah proses pengiriman data, baik itu data teks dan video melalui jaringan internet yang sudah terkoneksi dengan sangat luas. Telah banyak model dari keamanan data yang telah dikembangkan untuk kepentingan dari proses mengamankan data yang akan dikirim, salah satunya adalah algoritma kriftografi. Dalam hal ini tentunya suatu jaringan dalam berkomunikasi sangat rawan terhadap pencurian, penyadapan serta pemalsuan informasi. Pada proses pengiriman data yang melalui suatu jaringan tentunya harus menjamin tingkat keamanan dan keutuhan yang kokoh, sehingga data yang akan dikirim tidak di sadap dan dapat terkirim ke tujuannya. Maka dari itu salah satu cara dalam mengamankan data dari kejadian tersebut, diperlukan penyandian agar data yang dikirim dapat terjaga keamanan dan keasliannya.

Penyandian ini tentunya sangat penting, apalagi dalam strategi bisnis, sebuah perusahaan dan pemerintahan sangat memerlukan teknologi penyandian data atau informasi. Ilmu penyandian adalah ilmu yang sudah banyak dikenal di kalangan umum bahkan dari semenjak zaman Julius Caesar (sebelum masehi). Ilmu penyandian ini tentunya mencakup dari teknik-teknik untuk membongkar sandi dan juga sebagai proses untuk mengubah Plainbyte, sehingga Plainbyte berubah menjadi sebuah kode salah satunya pada file video.

Untuk menjaga keamanan informasi yang ada pada video. Ada beberapa teknik pengamanan yang sering di terapkan salah satu nya adalah teknik kriptografi dengan tujuan agar informasi tidak dapat diakses oleh orang tidak berkepetingan terhadap file video tersebut. Algoritma teknik kriptografi yang digunakan oleh penulis didalam penelitian ini adalah algoritma Merkle Hellman dengan diterapkannya algoritma ini maka file teks disandikan sehingga tidak dapat dilihat secara jelas [1]. Merkle-Hellman Knapsack merupakan kriptosistem yang menggunakan algoritma asymmetries. Implementasi Merkle- Hellman Knapsack yang digunakan menggunakan logika xor. Panjang kunci yang digunakan antara 8 sampai 72 bit. Karena dalam bahasa pemrograman Borland C++ tipe data yang paling tinggi adalah long double yang bisa menampung 18 digit. Misalnya saja dalam perhitungan perkalian antara 2 (dua) bilangan dengan panjang 9 digit akan menghasilkan bilangan dengan panjang

Submitted: **26/02/2020**; Accepted: **10/04/2020**; Published: **25/04/2020**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 4, Nomor 2, April 2020, Page 461-465
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i2.2039

18 digit yang akan ditampung dalam tipe long double, kemudian dengan fungsi modulo akan dihasilkan kembali bilangan dengan panjang 9 digit [2]. Berdasarkan penelitian yang dilakukan sebelumnya oleh memaparkan bahwa untuk menjaga keamanan data yang di simpan, maka akan menyulitkan dan memperkecil kemungkinan pihak-pihak yang tidak berkepentingan untuk mengetahui suatu data rahasia[3]. Dengan demikian, data yang terenkripsi pada database tidak akan diketahui arti yang sebenarnya dan sulit untuk dirubah ataupun diganti. Demikian halnya penelitian yang dilakukan oleh Akik hidayat dkk menyatakan pentingnya penyandian bukan hanya merubah bentuk dari data tersebut, tetapi mampu juga menghilangkan makna dari pada data itu sendiri pada saat berubah menjadi informasi bagi yang menggunakannya[4]. Serta menyandikan data sebuah informasi penting untuk di jaga agar tidak dapat di akses dan disalahgunakan oleh orang-orang yang tidak berhak untuk mengaksesnya [5].

2. METODE PENELITIAN

2.1 Video

Video Video adalah salah satu objek representasi data yang telah diolah. Bentuk data video merupakan hasil penggabungan dari pada gambar dan suara. Media video juga dapat diartikan seperangkat komponen atau media yang mampu menampilkan gambar sekaligus suara dalam waktu bersamaan.cecep Kustandi mengungkapkan bahwa video adalah alat yang dapat menyajikan informasi, memaparkan proses, menjelaskan konsep-konsep yang rumit, mengajarkan keterampilan, menyingkat atau memperlambat waktu dan mempengaruhi sikap[6].

2.2 Algoritma Merkle Hellman Knapsack

Algoritma merkle hellman knapsack salah satu algoritma asimetris. Yaitu algoritma yang memliki kunci publik dan kunci privat pada proses enkripsi dan dekripsinya. Algoritma merkle hellman knapsack mempunyai tiga proses mekanisme yaitu proses pembangkitan kunci publik dan kunci privat, proses enkripsi dan proses dekripsi[7]. Merkle Hellman adalah salah satu sistem kriptografi yang menggunakan tipe kunci asimetri. Pada sistem Merkle Hellman ini, kunci yang digunakan adalah 2 kunci yang berbeda.Satu kunci untuk mengenkrip dan satu kunci untuk mendekripsi[8].

Secara umum dapat digambarkan cara kerja sistem kriptografi Merkle-Hellman sebagai berikut :

a. Pesan dikonveri ke dalam bilangan biner yang kemudian dikalikan dengan kunci pblik. Hasil perkalian dijumlahkan lalu dikirim ke penerima pesan.
b. Penerima pesan menggunakan kunci rahasia untuk mencari terget sum. Dengan menggunakan algoritma target sum, penerima mendapatkan nilai pesan yang masih berupa bilangan biner {0,1}*. Untuk mendapatkan pesan aslinya, konversi bilangan biner ini ke karakternya [9]:.

Langkah-langkah penjelasan Matematika sebagai berikut[10]:

a. Memilih urutan superincreasing dari jumlah bilangan bulat positif . Urutan superincreasing adalah salah satu di mana setiap nomor lebih besar dari jumlah semua sebelumnya angka .s = (s1 , s2 , s3 , ... sn)
b. Untuk mengkonversi semua karakter dari pesan ke biner . Urutan biner diwakili oleh variabel b .
c. Untuk memilih dua nomor - integer (a) yang lebih besar dari pada jumlah semua nomor di urutan dan co -prime (r).
d. Urutan dan nomor dan r membentuk kolektif kunci pribadi cryptosystem tersebut.
e. Semua elemen - s1 , s2 , s3 , ... sn, dari urutan s adalah dikalikan dengan jumlah r dan modulus dari beberapa diambil dengan membagi dengan angka .
f. Oleh karena itu , pi = r * si mod a
g. Semua elemen p1 , p2 , p3 , ... pn urutan p adalah dikalikan dengan dengan unsur-unsur yang sesuai dari biner urutan b.
h. Angka-angka tersebut kemudian ditambahkan untuk membuat pesan terenkripsi Mi

$$Mi \sum_{i=1}^{n} P_i * b_i \qquad (1)$$

i. Urutan M = (M1 , M2 , M3 ... Mn) membentuk kunci kunci cryptosystem[11].

3. HASIL DAN PEMBAHASAN

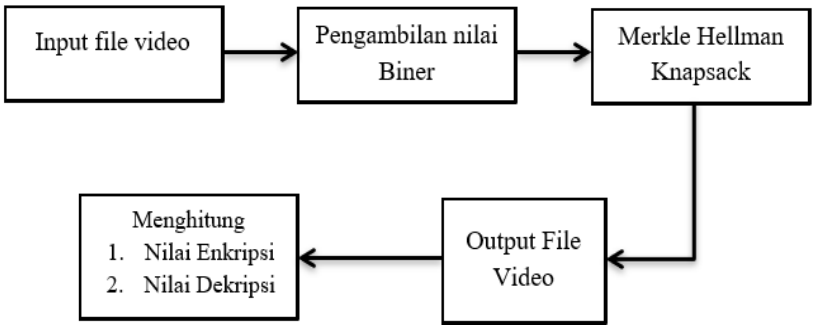
3.1 Analisa Masalah

Analisa masalah dilakukan untuk mendapatkan solusi dalam menyelesaikan permasalahan yang telah dijelaskan pada penelitian ini yang bertujuan untuk mencapai sistem yang baik agar mendapatkan hasil yang akurat. Adapun masalah yang diangkat penulis dalam penelitian ini adalah bagaimana mengamankan file video dengan menggunakan algoritma merkle hellman knapsack. File video format MP4 merupakan sebuah *format file* yang umumnya digunakan untuk *format file* pada audio dan juga video. Selain itu, juga bisa digunakan untuk

Submitted: **26/02/2020**; Accepted: **10/04/2020**; Published: **25/04/2020**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 4, Nomor 2, April 2020, Page 461-465
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i2.2039

menyimpan *subtitle* dan bahkan gambar, yang bersifat rahasia maka diperlukan sebuah pengamanan. Adapun skema alur implementasi metode yang digunakan dalam penelitian ini adalah sebagai berikut:



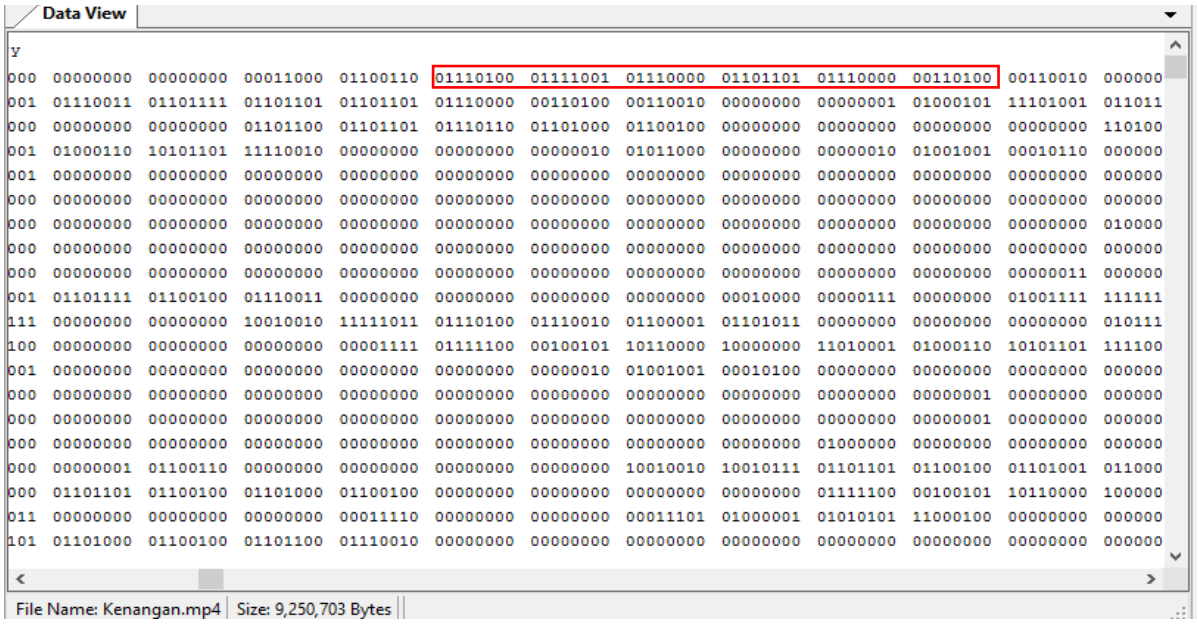
Gambar 1. Skema Analisa Yang Dilakukan.

3.1 Pembahasan Algoritma Merkle Hellman Knapsack

Pembahasan algoritma merkle hellman knapsack dalam tahapan ini dibentuk sesuai dengan pengamanan file video menggunakan algoritma merkle hellman knapsack. Sedangkan untuk penerapan metode knapsack mempunyai tiga proses mekanisme yaitu proses pembangkitan kunci publik dan kunci privat, proses enkripsi dan proses dekripsi file video. File video yang sesuai dengan analisa yang dilakukan berikutnya hanya file video berformat MP4 dengan alasan memperkecil ruang lingkup pembahasan.

Data file MP4 yang dienkripsi dan dekripsi pada analisa hanya sebanyak 6 Byte. Bagian pertama data file MP4 tersebut juga menyertakan digital signature file itu sendiri tetapi pengubahan dari ekripsi menyebabkan file MP4 tidak dapat diputar atau dijalankan dari pemutar video. Pengembalian data cipher dari proses analisa dekripsi tetap sama dengan enkripsi yaitu 6 Byte data cipher file MP4 pada bagian pertama.

Contoh kasus dalam proses ini seperti dijelaskan dalam analisa yaitu file video MP4 (Kenangan.mp4). data yang diambil hanya sebanyak 6 Byte untuk plainteks, cara pengambilan nilai biner data video menggunakan aplikasi Binary Viewer seperti dibawah ini:


Data View

y												
000	00000000	00000000	00011000	01100110	01110100	01111001	01110000	01101101	01110000	00110100	00110010	000000
001	01110011	01101111	01101101	01101101	01110000	00110100	00110010	00000000	00000001	01000101	11101001	011011
000	00000000	00000000	01101100	01101101	01110110	01101000	01100100	00000000	00000000	00000000	00000000	110100
001	01000110	10101101	11110010	00000000	00000000	00000010	01011000	00000000	00000010	01001001	00010110	000000
001	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	000000
000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	000000
000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	010000
000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	000000
000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000011	000000
001	01101111	01100100	01110011	00000000	00000000	00000000	00000000	00010000	00000111	00000000	01001111	111111
111	00000000	00000000	10010010	11111011	01110100	01110010	01100001	01101011	00000000	00000000	00000000	010111
100	00000000	00000000	00000000	00001111	01111100	00100101	10110000	10000000	11010001	01000110	10101101	111100
001	00000000	00000000	00000000	00000000	00000000	00000010	01001001	00010100	00000000	00000000	00000000	000000
000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000001	00000000	000000
000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000001	00000000	000000
000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	01000000	00000000	00000000	000000
000	00000001	01100110	00000000	00000000	00000000	00000000	10010010	10010111	01101101	01100100	01101001	011000
000	01101101	01100100	01101000	01100100	00000000	00000000	00000000	00000000	01111100	00100101	10110000	100000
011	00000000	00000000	00000000	00011110	00000000	00000000	00011101	01000001	01010101	11000100	00000000	000000
101	01101000	01100100	01101100	01110010	00000000	00000000	00000000	00000000	00000000	00000000	00000000	000000

File Name: Kenangan.mp4 | Size: 9,250,703 Bytes

Gambar 2. Nilai Biner Kenangan.mp4

Adapun yang dijadikan sampel dengan nilai biner menggunakan Algoritma Merkle Hellman Knapsack, baik pada proses enkripsi maupun dekripsi sebagai berikut:

a. Plaintext yaitu:
   Biner : 01110100 01111001 01110000 01101101 01110000 00110100
b. Menentukan superincreasing. w : {3,4,9,19,38,76,151,310}
c. nilai w , q dan r : q = 611 r = 31
d. w*r mod q
   w1 = 3 * 31 mod 611 = 93

Submitted: **26/02/2020**; Accepted: **10/04/2020**; Published: **25/04/2020**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 4, Nomor 2, April 2020, Page 461-465
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i2.2039

w2 = 4 * 31 mod 611 = 124
w3 = 9 * 31 mod 611 = 279
w4 = 19 * 31 mod 611 = 589
w5 = 38 * 31 mod 611 = 567
w6 = 76 * 31 mod 611 = 523
w7 = 151 * 31 mod 611 = 404
w8 = 310 * 31 mod 611 = 445

e. Sehingga diperoleh kunci publik untuk proses enkripsi ini sebagai berikut :{ 93, 124, 279, 589,567, 523, 404, 445 }
f. Selanjutnya, dilakukan pembagian plaintext ke dalam blok-blok berdasarkan jumlah elemen p sebagai berikut:
Blok 1 =01110100
Blok 2 =01111001
Blok 3 =01110000
Blok 4 =01101101
Blok 5 =01110000
Blok 6 = 00110100
g. Selanjutnya, setiap blok akan dikalikan dengan setiap elemen p, sehingga diperoleh chipertext sebagai berikut:
Chiper 1 = (0 * 93) + (1 * 124) + (1 * 279) + (1 *589) + (0 * 567) + (1 * 523) + (0 *404) + (0*445)
= 124 + 279 + 589 + 523 = 1.515
Chiper 2 = (0 * 93) + (1 * 124) + (1 * 279) + (1 *589) + (1 * 567) + (0* 523) + (0 *404) + (1*445)
= 124 + 279 + 589 + 567 + 445 = 2.004
Chiper 3 = (0 * 93) + (1 * 124) + (1 * 279) + (1 *589) + (0 * 567) + (0 * 523) + (0 *404) + (0*445)
= 124 + 279 + 589 = 992
Chiper 4 = (0 * 93) + (0 * 124) + (1 * 279) + (1 *589) + (0 * 567) + (1 * 523) + (0 *404) + (0*445)
= 279 + 589 + 523 =1.938
Chiper 5 = (0 * 93) + (1 * 124) + (1 * 279) + (0 *589) + (1 * 567) + (1 * 523) + (0 *404) + (1*445)
= 124 + 279 + 567 + 523 + 445= 992
Chiper 6 = (0 * 93) + (0 * 124) + (1 * 279) + (1 *589) + (0 * 567) + (1 * 523) + (0 *404) + (0*445)
= 279 + 589 + 523 =1.391
h. Memperoleh chipertext hasil enkripsi sebagai berikut : {1515,2004,992,1938,992,1391}
i. Chipertext Untuk proses dekripsi algoritma merkl hellmanm knapsack ini, digunakan chipertext {1515,2004,992,1938,992,1391}
j. Modular invers nilai modulo invers dari (r -1) sebesar 138, dengan menggunakan nilai r -1 ini, akan dilakukan perkalian seluruh chiperteks dengan nilai r -1 mod q, sehingga diperoleh nilai-nilai sebagai berikut :
P1 = 1515* 138 mod 611 = 108
P2 = 2004 * 138 mod 611 = 380
P3 = 992 * 138 mod 611 = 32
P4 = 1938 * 138 mod 611 = 437
P5 = 992 * 138 mod 611 = 32
P6 = 1391 * 138 mod 611= 104
k. Nilai P1 sampai P7 akan didekomposisi menggunakan setiap nilai pada w. Dekomposisi ini dilakukan dengan cara melakukan pengurangan terhadap nilai terbesar hingga terkecil.
P1 = 108 – 76 =32– 19 = 13 – 9 = 4 – 4 = 0
diperoleh : 01110100
P2 = 380 – 310=70– 38 = 32 – 19 = 13 – 9 = 4 – 4 = 0
diperoleh : 01111001
P3 = 32– 19 = 13 – 9 = 4 – 4 = 0
diperoleh : 01110000
P4 = 437 – 310 =127 – 76 = 51 – 38 = 13 – 9 = 4 – 4 = 0
diperoleh : 01101101
P5 = 32– 19 = 13 – 9 = 4 – 4 = 0
diperoleh : 01110000
P6 = 104 – 76 = 28 – 19 = 9 – 9 = 0
diperoleh : 00110100
l. Sehingga diperoleh pesan awal sebagai berikut : 01110100 01111001 01110000 01101101 01110000 00110100.

Berdasarkan penjelasan pembahasan metode ini memiliki pengamanan ganda sehingga sulit untuk ditembus dan pengamana file video tersebut dapat melindungi video agar video tersebut lebih aman dan tidak mudah dilihat oleh orang yang tidak berhak karena video tersebut ketika dikirim berbentuk video yang sudah dienkripsi menggunakan algoritma Merkle-Hellman Knapsack. Selain itu,pada proses dekripsi juga berhasil mengembalikan cipherteks menjadi bentuk semula data video.

Submitted: **26/02/2020**; Accepted: **10/04/2020**; Published: **25/04/2020**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 4, Nomor 2, April 2020, Page 461-465
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i2.2039

4. KESIMPULAN

Kesimpulan yang dapat diambil setelah melakukan penelitian Implementasi Algoritma Merkle Hellman Knapsack Untuk Mengamankan File Video adalah:

1. Algoritma Merkle-Hellman Knapsack menggunakan kunci privat dan kunci publik dalam proses kriptografinya, metode ini memiliki pengamanan ganda sehingga sulit untuk ditembus.
2. Pengamana file video tersebut dapat melindungi video agar video tersebut lebih aman dan tidak mudah dilihat oleh orang yang tidak berhak karena video tersebut ketika dikirim berbentuk video yang sudah dienkripsi menggunakan algoritma Merkle-Hellman Knapsack.
3. Pengujian algoritma Merkle-Hellman Knapsack dalam enkripsi dan dekripsi menghasilkan chipertext berupa deretan angka dan menghasilkan plaintext input yang sama dengan plaintext output dari proses dekripsi. Enkripsi ini lebih aman dibandingkan metode kriptografi yang menghasilkan enkripsi dalam bentuk teks.

REFERENCES

[1] Murdani, “PERANCANGAN APLIKASI KEAMANAN DATA TEKS MENGGUNAKAN ALGORITMA MERKLE HELLMAN KNAPSACK,” Jurnal Pelita Informatika, vol. 16, no. 3, pp. 302-305 , 2017.
[2] Muhammad Fadlan, 2017.” Rekayasa Aplikasi Kriptografi Dengan Penerapan Kombinasi Algoritma Knapsack Merkle Hellman Dan Af ine Cipher”, Vol. 4, No. 4, Desember 2017, hlm. 268-274 p-ISSN: 2355-7699
[3] F. Muhammad dan H. Hadriansa, “Rekayasa Aplikasi Kriptografi dengan Penerapan Kombinasi Algoritma Knapsack Merkle Hellman dan Affine Cipher,” Jurnal Teknologi Informasi dan Ilmu Komputer, vol. 4, no. 4, pp. 268-274, 2017.
[4] H. Akik , A. Akmal dan R. Rudi , “Cryptography Asymmetries Merkle-Hellman Knapsack Digunakan untuk Enkripsi dan Dekripsi Teks,” dalam Prosiding Seminar Nasional MIPA, Medan, 2016.
[5] Mardalius, 2018.” Implementasi Aplikasi Enkripsi Dan Dekripsi Text Pada Visual Basic .Net Mengunakan Algoritma Merkle Hellman Knapsack”, STMIK Royal – AMIK Royal, hlm. 249 – 252 ISSN 2622-6510 (online), Seminar Nasional Royal (SENAR) 2018 ISSN 2622- 9986 (cetak).
[6] A. Dedy dan N. S. Doni , “IMPLEMENTASI ALGORITMA BLOWFISH DAN METODE LEAST SIGNIFICANT BIT INSERTION PADA VIDEO MP4,” Jurnal Pseudocode, vol. III, no. 2, pp. 137-145, 2016.
[7] A. Ashish , “Encrypting Messages using the Merkle-Hellman Knapsack Cryptosystem,” IJCSNS International Journal of Computer Science and Network Security, vol. 11, no. 5, pp. 12-14, 2011.
[8] 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.
[9] A. Hidayat dan R. Rosyandi,” Cryptography Asynnetries Merkle-Hellman Knapsack Digunakan Untuk Enkripsi Dan Deskripsi Teks”, Prosiding Seminar MIPA, pp 27-28, 2016
[10] Ahmad Suryadi , 2017.” Perancangan Aplikasi Keamanan Data Gambar Menggunakan Algoritma Merkle Hellman Knapsack”, Jurnal Pelita Informatika, Volume 16, Nomor 3, Juli 2017 ISSN 2301-9425 (Media
[11] A. F. Helmi, S. Arifianto, J. T. Informatika, and U. M. Malang, “Analisa Kombinasi Algoritma Merkle-Hellman Knapsack Dan Analysis Of A Combination Of Merkle-Hellman Algorithms,” vol. 5, no. 3, pp. 325–334, 2018.
[12] Munir, Rinaldi, “Kriptografi”, Penerbit Informatika, B{Mamatha.T, 2012 2}andung, 2006.
[13] Aryus, Dony, “Pengantar Kriptografi Teori dan Aplikasi”,Penerbit Andi, Yogyakarta, 2008.

Submitted: **26/02/2020**; Accepted: **10/04/2020**; Published: **25/04/2020**