Bulletin of Artificial Intelligence
Volume 2, No 1, April 2023 Page: 100-103
ISSN 2962-3944 (media online)
https://journal.grahamitra.id/index.php/buai

Penerapan Algoritma Rabin-Public Key Untuk Pengamanan File Audio

Rusdianto[1]*, [2]Natalia Silalahi, [3]Norenta Sitohang

Fakultas Ilmu Komputer dan Teknologi Informasi, Program Studi Teknik Informatika, Universitas Budi Darma, Medan, Indonesia
Email: [1,*]Rusdiantoarrem017@gmail.com, [2]nataliasilalahi@gmail.com, [3]norentasitohang@gmail.com
Email Penulis Korespondensi: Rusdiantoarrem017@gmail.com

Abstrak−Masalah penyandiaan data seperti file teks, gambar, audio dan video dalam penggunaannya lebih sering dijadikan sebagai pesan atau informasi. Akan tetapi dengan kemajuan teknologi yang semakin berkembang, semakin memungkinkan pesan atau informasi disimpan dalam bentuk file lain seperti gambar, audio dan video. Dimisalkan Sebuah perusahaan rekaman musik ingin mengeluarkan album terbaru dan mereka ingin mendapatkan keuntungan besar dari hasil penjualan CD atau download secara legal (berbayar) melewati situs. Sebelum album keluar secara resmi ke public mereka ingin memastikan bahwa tidak ada satu pihak yang mendapatkan bocoran ataupun mendengarkan file audio tersebut terlebih dahulu. Salah satu solusi teknik yang dapat digunakan untuk menjaga kerahasiaan file audio adalah kriptografi dengan menerapkan algoritma Rabin-Public Key. Algoritma Rabin-p merupakan algoritma yang menerapkan kunci asimetris. Kunci asimetris adalah kunci yang menggunakan dua jenis kunci yaitu kunci publik (public key) yang digunakan untuk mengenkripsi pesan dan kunci rahasia (secret key) yang digunakan untuk mendekripsi pesan. Rabin-p dinamai rabin dengan tambahan p yang melambangkan bahwa skema yang diusulkan hanya menggunakan satu prima p sebagai kunci dekripsi. Hasil pada penyandian file audio dibuat berdasarkan sistem kriptografi asimetris yang menggunakan kunci public dan kunci privat untuk penyandian file audio (kunci yang digunakan untuk proses enkripsi dan dekripsi) menjadi sebuah chipper sehingga keamanan dan kerahasian pesan terjaga. Analisa file audio merupakan tahapan dimana dilakukannya análisa terhadap file-file apa saja yang diolah dalam sistem atau prosedur sebuah rancangan, dalam hal ini file audio yang akan dienkripsi dan dekripsi pada aplikasi kriptografi adalah berupa file audio berformat wave (*.WAV).

Kata Kunci: Penerapaan; Pengamanan File Audio; Rabin Public-Key

Abstract−*Data encoding problems such as text files, images, audio and video are used more often as messages or information. However, with advances in technology that are increasingly developing, it is increasingly possible for messages or information to be stored in the form of other files such as images, audio and video. For example, a music recording company wants to release the latest album and they want to get a big profit from selling CDs or downloading legally (paid) through the site. Before the album officially goes out to the public, they want to make sure that no one party gets a leak or listens to the audio file first. One of the technical solutions that can be used to protect the confidentiality of audio files is cryptography by applying the Rabin-Public Key algorithm. The Rabin-p algorithm is an algorithm that implements an asymmetric key. An asymmetric key is a key that uses two types of keys, namely the public key which is used to encrypt the message and the secret key which is used to decrypt the message. Rabin-p is named rabin with an additional p which symbolizes that the proposed scheme uses only one prime p as the decryption key. The results for encoding audio files are based on an asymmetric cryptographic system that uses a public key and a private key for encoding audio files (the key used for the encryption process). and decryption) into a cipher so that the security and confidentiality of messages are maintained. Audio file analysis is the stage where analysis is carried out on any files that are processed in a design system or procedure, in this case the audio files to be encrypted and decrypted in cryptographic applications are audio files in wave format (*.WAV).*

Keywords*: Application; Audio File Protection; Rabin Public-Key*

1. PENDAHULUAN

Kriptografi merupakan salah satu cara teknik yang dengan tujuan untuk meningkatkan aspek dalam pengamanan suatu informasi baik berupa pesan, *file image*, teks, audio video dan lain sebagainya agar suatu data tersebut menjadi aman. Dengan berkembangnya teknologi informasi saat ini yang begitu pesat dimana halnya setiap orang akan mudah untuk mendapatkan suatu pesan dengan berbagai cara yang dilakukan orang untuk mendapatkan data dan informasi tersebut. Mulai dari tingkatan yang paling mudah sampai dengan cara yang lebih rumit, dan berbagai cara pula orang berusaha untuk bagaimana caranya untuk melindungi pesan tersebut agar tidak dapat diketahui oleh orang yang tidak memiliki hak akses atas pesan atau data [1]-[2]-[3].

Masalah penyandiaan data seperti *file* teks, gambar, audio dan video dalam penggunaannya lebih sering dijadikan sebagai pesan atau informasi. Akan tetapi dengan kemajuan teknologi yang semakin berkembang, semakin memungkinkan pesan atau informasi disimpan dalam bentuk *file* lain seperti audio dan video. Dimisalkan Sebuah perusahaan rekaman musik ingin mengeluarkan album terbaru dan mereka ingin mendapatkan keuntungan besar dari hasil penjualan CD atau *download* secara legal (berbayar) melewati situs. Sebelum album keluar secara resmi ke *public* mereka ingin memastikan bahwa tidak ada satu pihak yang mendapatkan bocoran ataupun mendengarkan *file* audio tersebut terlebih dahulu. Oleh sebab salah satu teknik yang dapat digunakan untuk menjaga kerahasiaan *file* audio adalah teknik kriptografi dengan menerapkan kunci *Rabin.*

Algoritma *Rabin-p* merupakan algoritma yang menerapkan kunci asimetris. Menurut penelitian sebelumnya M.A Asbullah dan Arifin yang berjudul "*Rabin-key Cryptosystem: Practical and Efficient Method for Rabin based Encryption*" hasil dari penelitian ialah menggunakan dua jenis kunci yaitu kunci publik (*public key*) yang digunakan untuk mengenkripsi pesan dan kunci rahasia (*secret key*) yang digunakan untuk mendekripsi pesan. *Rabin-p* dinamai *rabin* dengan tambahan *p* yang melambangkan bahwa skema yang diusulkan hanya menggunakan satu prima *p* sebagai kunci dekripsi [4]-[5]-[6].

Bulletin of Artificial Intelligence
Volume 2, No 1, April 2023 Page: 100-103
ISSN 2962-3944 (media online)
https://journal.grahamitra.id/index.php/buai

Serta menurut penelitian oleh H.Wandani, A.Budiman yang berjudul "Implementasi sistem keamanan data dengan menggunakan teknik steganografi *end of file* (EOF) dan *rabin public key cryptosystem*" hasil dari penelitian membuktikan beberapa kombinasi *plaintext* dan kunci tertentu dengan hasil dekripsi yang berbeda dari *plaintext* yang sebenarnya karena pada saat sistem memeriksa 4 (empat) kemungkinan nilai *plaintext* terdapat 2 (dua) atau lebih nilai kemungkinan *plaintext* yang memenuhi syarat sebagai *plaintext* yang sebenarnya. Sehingga sistem ini akan mengambil nilai kemungkinan *plaintext* yang pertama sekali memenuhi syarat sebagai *plaintext* yang sebenarnya [6]-[7]-[8].

Dari beberapa penelitian diatas dapat disimpulkan bahwa enkripsi *file* menggunakan algoritma *rabin-public key* mampu mengenkripsi dalam penyandian *file* audio karena untuk menjaga kerahasian suatu data salah satunya adalah enkripsi (*encryption)*. Pesan biasa atau pesan asli disebut *plain* audio sedangkan pesan yang diubah atau disandikan supaya tidak mudah dibaca disebut dengan *chiper*. Aplikasi dalam penerapan algoritma *rabin publick key* untuk pengamanan *file* audio ditujukan untuk membantu mengatasi masalah keamanan data yang dibuat atau disimpan menggunakan *file* yang berformat *wave* (*.*WAV*) dan lain-lainya dari pencurian *file* baik yang tidak penting maupun yang penting dan rahasia.

2. METODOLOGI PENELITIAN

2.1 Keamanan

Keamanan adalah salah satu aspek yang terpenting dari sebuah sistem informasi. Masalah keamanan sering juga kurang mendapatkan perhatian dari para perancang dan pengelola sstem informasi. Masalah keamanan sering berada diurutan setelah tampilan, atau bahkan diurutan terakhir dalam daftar hal-hal yang dianggap penting [9]-[10]-[11].

2.2 Rabin-Public Key

Rabin Public Key menggunakan kunci asimetris yang menggunakan kunci publik dan kunci privat. Algoritma *Rabin Public Key* merupakan varian algoritma *Rivest Shamir Adleman* (RSA) . Fungsi dasar algoritmanya mirip dengan fungsi dasar dari algoritma RSA. Yang membedakannya hanya komputasinya lebih sederhana dengan dibandingkan algoritma RSA [12]. Pada algoritma Rabin Public Key, proses pembangkitan kuncinya dilakukan sebagai berikut :

1. Memilih 2 (dua) buah bilangan prima besar sembarang yang saling berbeda (p dan q), dimana $p \equiv q \equiv 3 \pmod 4$. Atau dengan kata lain jika p dan q di modulo 4 akan menghasilkan 3.
2. Dengan menghitung nilai n yang merupakan kunci publik dengan rumus $n = p * q$ dengan p dan q adalah kunci privat. Untuk mengenkripsi pesan hanya dibutuhkan kunci publik n dan untuk proses dekripsinya dibutuhkan bilangan p dan q sebagai kunci privat tersebut.

3. HASIL DAN PEMBAHASAN

3.1 Analisa Masalah

Mengenai penerapan dalam pengamanan *file* audio untuk membuat sebuah aplikasi dengan menerapkan metode *Rabin-Public Key* untuk mengamankan suatu *file* audio yang akan diterapkan dalam aplikasi yang akan dibuat. Analisa dalam tahapan yang akan dilakukannya dimana análisa terhadap sebuah *file* apa saja yang akan diproses atau diolah dalam sistem sebuah prosedur rancangan aplikasinya, dalam hal ini proses *file* yang akan dienkripsi dan dekripsi pada aplikasi berupa file audio yang berformat *wave* (*.WAV).

Alasan penelitian dalam pengamanan *file* audio dilakukan karena proses *file* audio untuk menjaga kerahasian data, dari sandi kunci metode yang dibuat berdasarkan dari sistem kriptografi seperti pembangkit kunci dari asimetris yang digunakan kunci public untuk proses enkripsi sedangkan kunci privat untuk proses dekripsi untuk penyandian *file* audio sehingga file akan setelah di enkripsi tersandi menjadi sebuah *chipper* sehingga keamanan dan kerahasian pesan tetap terjaga. Sehingga pesan hasil *chipper* file audio tidak akan dapat diputar dan tersandi dan untuk pengembalian file berbentuk awal dilakukan proses dekripsi. Aplikasi dalam penerapan algoritma *rabin publick key* untuk pengamanan *file* audio ditujukan untuk membantu mengatasi masalah keamanan data baik data yang tidak penting maupun data yang penting dan rahasia, sehingga orang lain tidak akan dapat mengetahui isi *file* audio tersebut.

3.1.1 Penerapan Enkripsi Algoritma *Rabin-public key*

Proses enkripsi pada *Rabin-public key* menggunakan kunci publik *n.* Berikut adalah proses enkripsi dalam pembangkit *public key* menggunakan algoritma *Rabin-public Key* dengan mengambil sebagai contoh sampel data *file* audio. Berikut nilai diambil dari sampel *file* suara 52, 49, 46, 46, 6A, 4C, 37 yang akan enkripsi menggunaakan algoritma *Rabin-public key*. Sebelum di enkripsi konversi terlebih dahulu nilai heksa dari *file* suara ke decimal, berikut tabel konversi dapat dilihat dibawah ini :

Tabel 1. Nilai konversi

Heksa	Desimal
52	82
49	73

Bulletin of Artificial Intelligence
Volume 2, No 1, April 2023 Page: 100-103
ISSN 2962-3944 (media online)
https://journal.grahamitra.id/index.php/buai

46	70
46	70
6A	106
4C	76
37	55

Proses Enkripsi :
Menggunakan pembangkit kunci dua bilangan prima yang berbeda yaitu *p* dan *q* sebagai kunci, nilai *p* = 127 dan nilai *q* = 139 di mana $p \equiv q \equiv 3 \pmod 4$. Hitung nilai kunci *public* berdasarkan nilai kunci *private*, yaitu *n*.
$n = p*q$
$n = 127 * 139$
$n = 17653$
Publikasikan nilai kunci *public n* dan simpan kunci *privat p* dan *q*.
Kunci *n :* 17653
Hitung C1 $= m^2 \bmod n$
$= 82^2 \bmod 17653$
$= 6724$
Hitung C2 $= m^2 \bmod n$
$= 73^2 \bmod 17653$
$= 5329$
Hitung C3 $= m^2 \bmod n$
$= 70^2 \bmod 17653$
$= 4900$
Hitung C4 $= m^2 \bmod n$
$= 70^2 \bmod 17653$
$= 4900$
Hitung C5 $= m^2 \bmod n$
$= 106^2 \bmod 17653$
$= 11236$
Hitung C6 $= m^2 \bmod n$
$= 76^2 \bmod 17653$
$= 5776$
Hitung C7 $= m^2 \bmod n$
$= 55^2 \bmod 17653$
$= 3025$

Tabel 2. Hasil Enkripsi Algoritma *Rabin-public key*

Nilai	**Kode ASCII**	***Chiper***
82	R	6724
73	I	5329
70	F	4900
70	F	4900
106	j	11236
76	L	5776
55	7	3025

3.1.2 Penerapan Dekripsi Algoritma *Rabin-public key*

Proses dekripsi pada *Rabin-public key* menggunakan kunci private *p.* Berikut adalah proses enkripsi dalam pembangkit *private key* sebagai berikut :
Kunci *Private Key (p)* = 5987
Cipher " 6724 " dengan menggunakan *privat key*.
Hitung P1 :
W $\equiv c \pmod p$
$\equiv 6724 \pmod{5987}$
Mp $= w^{\frac{p+1}{4}} \pmod p$
Mp $= 6724^{\frac{5987+1}{4}} \pmod{5987}$
Mp $= 82$
m $= \frac{c - m^2 p}{p}$
i $= \frac{6724 - 8^2}{5987}$

Bulletin of Artificial Intelligence
Volume 2, No 1, April 2023 Page: 100-103
ISSN 2962-3944 (media online)
https://journal.grahamitra.id/index.php/buai

i $= \frac{0}{5987} = 0$
j $= \frac{i}{2mp} (\text{mod } p)$
j $= \frac{0}{130} (\text{mod } 5987)$
j $= 0$
i $= 0$
m_1 $= m_p + jp$
m_1 $= 82 + 0.5987$
m_1 $= 82$
$m_1 < 2^{2k-1}$
$82 < m^{13}$
$82 < 8192$
Sehingga didapat hasillnya $m = 82$

Tabel 3. Hasil Dekripsi Algoritma *Rabin-public key*

Chiper	***Plain***	**Hexa**
6724	82	52
5329	73	49
4900	70	46
4900	70	46
11236	106	6A
5776	76	4C
3025	55	37

4. KESIMPULAN

Berdasarkan hasil yang di dapat dalam penelitian dan penyusunan skripsi serta disesuaikan dengan tujuan, maka diperoleh kesimpulan sebagai berikut Proses *Rabin-public key* menggunakan pembangkit kunci seperti kunci yang tidak aturan dari metode rabin, kunci harus menggunakan 2 (dua) bilangan prima yang jika dimodulus 4 (empat) maka sama-sama menghasilkan 3 (tiga) untuk proses enkripsi pada penyandian file audio. Metode *Rabin-public key* memberikan hasil *chipper* dengan kunci public sehingga *file* audio berformat (*.WAV) tidak akan dapat diputar dan sedangkan kunci *privat* menghasilkan *plain* pada saat dekripsi pengembalian awal enkripsi *file* audio sehingga *file* audio dapat diputar atau *play* kembali. Perubahan pada enkripsi pada *file* audio yang dialami *file* audio menjadi *file* yang tersandi dan *file* audio tidak akan dapat diputar, jadi oleh sebab itu sangat berguna didalam menjaga kerahasiaan data sehingga tidak banyak orang yang menyadarinya.

REFERENCES

[1] Dony ariyus, *Pengantar Ilmu Kriptografi*. Yogyakarta: C.V Andi Offiset, 2008.
[2] R. Handayani, "Perancangan Aplikasi Kompresi File Audio Menerapkan Algoritma Universal Codes," *KOMIK (Konferensi Nas. Teknol. Inf. dan Komputer)*, vol. 5, no. 1, 2021.
[3] Y. S. Gustiviana and E. R. Agustina, "Perancangan Spesifikasi Fungsi Keamanan Aplikasi File Encryption (Filtion) Versi 1.0. 0 berdasarkan SNI ISO/IEC 15408: 2014," in *Seminar Nasional Sains dan Teknologi Informasi (SENSASI)*, 2021, vol. 3, no. 1, pp. 108–116.
[4] M. A. Asbullah and M. R. K. Ariffin, "Rabin-p Cryptosystem: Practical and Efficient Method for Rabin based Encryption Scheme," pp. 1–13, 2014.
[5] S. H. Silitonga and S. D. Nasution, "Implementasi Algoritma Boldi-Vigna Codes Untuk Kompresi File Audio Pada Aplikasi Pemutar Audio Berbasis Web," *KOMIK (Konferensi Nas. Teknol. Inf. dan Komputer)*, vol. 6, no. 1, pp. 586–595, 2023.
[6] H. Wandani, M. A. Budiman, M. C. Sc, A. S. S. Si, and M. Kom, "Implementasi Sistem Keamanan Data dengan Menggunakan Teknik Steganografi End of File (EOF) dan Rabin Public Key Cryptosystem."
[7] N. Aisyah and S. Aripin, "Penerapan Algoritma Elias Omega Code Pada Kompresi File Audio Aplikasi Murottal Muzzamil Hasbalah," *Pelita Inform. Inf. dan Inform.*, vol. 9, no. 2, pp. 113–119, 2020.
[8] V. Lusiana, "Implementasi Kriptografi Pada File Dokumen Menggunakan Algoritma Aes-128," 2013.
[9] J. Kurniawan, *Kriptografi, Keamanan Internet, dan Jaringan Komunikasi*. Bandung: Informatika, 2004.
[10] M. Ali, "Analisis Perbandingan Algoritma Even-Rodeh Code dan Algoritma Fibonacci Code untuk Kompresi File Teks," 2018.
[11] U. S. Utara, U. S. Utara, and U. S. Utara, "Analisis Perbandingan Kinerja Algoritma Start-Step-Stop Code dan Gopala-Hemachandra Code 2 (GH-2 (n)) pada Kompresi File Teks," vol. 2, 2019.
[12] M. Elia, M. Piva, and D. Schipani, "The Rabin cryptosystem revisited," *Appl. Algebr. Eng. Commun. Comput.*, vol. 26, no. 3, pp. 251–275, 2015, doi: 10.1007/s00200-014-0237-0.