Terakreditasi SINTA Peringkat 2
Surat Keputusan Dirjen Penguatan Riset dan Pengembangan Ristek Dikti No. 10/E/KPT/2019
masa berlaku mulai Vol. 1 No. 1 tahun 2017 s.d Vol. 5 No. 3 tahun 2021

Terbit online pada laman web jurnal: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 5 No. 3 (2021) 483 - 488 ISSN Media Elektronik: 2580-0760

Kriptografi Audio MP3 Menggunakan RSA dan Transposisi Kolom

Cinantya Paramita[1], Usman Sudibyo[2]
[1,2]Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
[1]cinantya.paramita@dsn.dinus.ac.id, [2]usman.sudibyo@dsn.dinus.ac.id

Abstract

Mp3 is one form of audio file extension that is widely used today. With a variety of uses in a variety of mp3 systems become one of the audio extensions that are commonly found in technology systems of the Internet of Things era. However, with the many uses of the .mp3 file extension, there is a new problem, namely the security of the data itself. From these problems, the author aims to examine the security of the mp3 file by designing cryptographic science-based applications. The cryptographic algorithm used in the application is a combination of the asymmetric RSA 2048 algorithm and symmetric columnic transpositions. RSA 2048 algorithm was chosen because it has a key length in accordance with NIST standards in securing data. By combining the two algorithms, the application system will have the ability to manage mp3 files and encrypt mp3 files with the results of data that cannot be played like mp3 files in general. This application system will be developed by prototype method which is the best method in developing a system with trial and error in algorithm development.

Keywords: MP3, RSA, transposition, cryptography

Abstrak

Mp3 merupakan salah satu bentuk ekstensi file audio yang banyak digunakan saat ini. Dengan beragam penggunaan dalam beragam sistem mp3 menjadi salah satu ekstensi audio yang banyak ditemui dalam sistem – sistem teknologi era *Internet Of Things*. Tetapi, dengan banyaknya kegunaan dari file berekstensi .mp3 terdapat masalah baru yaitu keamanan dari data itu sendiri. Dari permasalahan tersebut, penulis bertujuan untuk meneliti tentang pengamanan dari file mp3 tersebut dengan merancang aplikasi berbasis ilmu kriptografi. Algoritma kriptografi yang digunakan dalam aplikasi tersebut merupakan algoritma kombinasi dari algoritma asimetris RSA 2048 dan simetris transposisi kolumnar. Algoritma RSA 2048 dipilih karena memiliki panjang kunci yang sesuai dengan standar NIST dalam pengamanan suatu data. Dengan menggabungkan kedua algoritma tersebut, sistem aplikasi akan memiliki kemampuan untuk mengelola file mp3 dan mengenkripsi file mp3 dengan hasil data yang tidak dapat di putar layaknya file mp3 pada umumnya. Sistem aplikasi ini akan dikembangan dengan metode *prototype* yang menjadi metode terbaik dalam mengembangkan sistem dengan trial dan *error* dalam pengembangan algoritma.

Kata kunci: MP3, RSA, transposisi, kriptografi.

1. Pendahuluan

Pada perkembangan teknologi saat ini yang memasuki era *Internet of Things*, perangkat – perangkat yang digunakan saat ini memiliki pengembangan yang cukup signifikan daripada perangkat sebelumnya. Teknologi saat ini memiliki kemampuan untuk menerima input atau data yang berbagai macam bentuknya untuk dikelola menjadi informasi atau bentuk luaran lainnya. Salah satu masukkan tersebut adalah data yang berbentuk suara atau audio. Salah satu pengembangan dari jenis file dari audio tersebut adalah MP3 yang menjadi format file yang paling banyak digunakan dalam penggunaan sistem teknologi terkini. MP3 merupakan format yang memiliki kompresi yang baik serta memiliki jumlah bit yang dikurangi sehingga menghasilkan ukuran file yang lebih kecil daripada format file audio yang lain. Keamanan data menjadi salah satu prioritas utama dalam penggunaan sistem terutama sistem yang dapat menerima banyak masukkan, otentikasi dari data pengguna yang digunakan sistem harus terjamin. Metode keamanan data tersebut disebut kriptografi yang memiliki berbagai macam algoritma yang telah mengalami perkembangan sehingga terdapat algoritma klasik dan algoritma modern [1]. Pengembangan dari algoritma kriptografi terus mengalami pembaharuan seperti penggabungan algoritma modern dan klasik yang menjadikan algoritma *hybrid* [2]. Algoritma klasik transposisi merupakan salah satu algoritma yang masih mengalami pembaharuan terutama pada pengembangan

Diterima Redaksi: 03-03-2021 | Selesai Revisi: 22-05-2021 | Diterbitkan Online: 20-06-2021

algoritma *hybrid*. Algoritma klasik yang telah dipakai sebelum era digital memiliki kelemahan yaitu terlalu sederhana dan dapat dengan mudah dilakukannya penembusan keamanan dikarenakan kompleksitas yang tidak seperti algoritma modern. Dengan pengembangan algoritma *hybrid* antara algoritma modern dan algoritma klasik, Algoritma kombinasi yang tercipta dari gabungan algoritma tersebut dapat meningkatkan kelemahan tiap – tiap algoritma tersebut. Algoritma modern seperti RSA menjadi salah satu algoritma modern yang paling banyak digunakan dalam pengamanan data pada berbagai macam sistem saat ini [3]. Keunggulan dari algoritam RSA yakni merupakan algoritma asimetris yang berarti kunci atau *key* dari enkripsi dan dekripsi yang berbeda, sehingga keamanan data menjadi lebih kompleks karena diperlukan 2 kunci untuk mengetahui isi dari data yang telah dienkripsi tersebut [4]. Pada penelitian "Penerapan Algoritma RSA Pada Sistem Kriptografi File Audio MP3" disebutkan pula bahwa algoritma RSA terbukti efektif dalam melakukan enkripsi maupun dekripsi pada file audio MP3 [5].

2. Metode Penelitian

2.1. Penelitian Terkait

Dalam melakukan sebuah penelitian diperlukan referensi-referensi dari penelitian terkait yang telah dilakukan sebelumnya. Dasar pemahaman dari penelitian ini diperoleh dengan mengumpulkan berbagai macam studi literatur yang dapat dijadikan dasar penelitian ini.

Tabel 1.Penelitian Terkait

Peneliti	Judul	Tahun	Metode	Hasil
Tin Za Nwe, S Wai Phy [6]	*Performance Analysis of RSA and ElGamal for Audio Security*	2015	RSA + El Gamal	Pada penelitian ini membuktikan bahwa kebutuhan untuk ukuran *key* yang lebih panjang dan kecepatan keamanan dari suatu algoritma yang menjadikan public *key* menjadi yang terbaik dalam manajemen dari *key* tersebut. Dalam penelitian ini juga menunjukkan. bahwa RSA lebih cepat dalam melakukan enkripsi dan dekripsi daripada algoritma El Gamal
Abdul Ghaffar Khan, Sana Basharafn Muhamm d Usam Riaz [7]	*Analysis of Asymmetric Cryptography in Information Security Based on Computational Study to Ensure Confidentiality During Information Exchange*	2018	RSA	Penelitian untuk menentukan *confidentiality* dari algoritma kriptografi asimetris yang terbukti dalam penelitian menggukanan algoritma asimetris RSA
Ahmad Jawahir, Haviluddin [8]	*An Audio Encryption Using Transposition Method*	2015	Transposisi	Hasil penelitian menunjukkan bahwa randomnisasi dari algoritma dapat digunakan dalam pengamanan file audio.
Shireen Nisha, Mohamm d Farik [9	*RSA Public Key Cryptography Algorithm A Review*	2017	RSA	Algoritma RSA yang sudah menjadi algoritma yang paling digunakan dalam pengamanan data masih perlu ditingkatkan dalam ketahanan terhadap serangan
Sura I Yousif [10]	*Encryption and Decryption of Audio Signal Based On RSA Algorithm*	2018	RSA	Kriptosistem yang diimplementasikan menggunakan algoritma RSA menghasilkan sinyal audio yang telah didekripsi masih memiliki kualitas yang baik sesuai dengan kualitas asal.
Achmad Fauzi, Novriyeni i, Yar Maulita, Akim M.H. Pardede [11]	*Analysis Hybrid Cryptosystem* Algoritma RSA dan *Triple* DES	2018	RSA + DES	Hasil penelitian menunjukkan keberhasilan algoritma RSA menjadi dasar dari algoritma *hybrid* yang digunakan dalam pengamanan data

2.2. RSA

Algoritma RSA salah satu algoritma asimmetris yang diciptakan Ron Rivest, Adi Shamir dan Leonard Adleman pada tahun 1978. Algoritma RSA mengimplementasikan *encoding block* dan *key* dengan ukuran yang bervarian. Algoritma ini berdasarkan proses matematika yang dilakukan untuk menghasilkan *key* yang dapat disebarkan secara publik dan *key* privat yang hanya dapat dimiliki oleh penerima dan pengirim. Dasar perhitungan matematika yang digunakan pada algoritma ini adalah memfaktorkan bilangan menjadi faktor – faktor prima.

Pada penelitian ini algoritma RSA – 2048 bit menjadi algoritma utama dalam pengembangan algoritma kombinasi yang akan diimplementasikan dalam sistem pengamanan data audio berbasis python. Algoritma RSA – 2048 yang akan digunakan terbukti sesuai dengan standar NIST terkait dengan kemampuan untuk

DOI: https://doi.org/10.29207/resti.v5i3.2996

melakukan pengamanan data. Sebelum perhitungan enkripsi dan dekripsi dalam algoritma RSA, diperlukan perhitungan *public key* (e) dan *private key* (d), *Euler tottient function* ϕ (n) dimodelkan beberapa persamaan seperti berikut (Yousif, 2018):

$$n = p\ x\ q \quad (1)$$

$$\phi\ (n) = (p-1)(q-1) \quad (2)$$

$$GCG\ \big(e, \varphi\ (n)\big) = 1 \quad (3)$$

Dimana *e* harus lebih besar dari 1 dan kurang dari dan lebih φ (n)(n), d mod $\phi(n) = e - 1\ mod\ \phi\ (n) \rightarrow \phi(n) = e\phi\big(\phi(n)\big) - 1 \rightarrow\ \phi(n) = e - 1 mod\ \phi\ (n)$. Proses enkripsi dilakukan setelah melakukan perhitungan public *key* dan private *key* yang dimodelkan dengan perhitungan matematika (4).

$$C = M\phi\ mod\ n \quad (4)$$

Dimana M sebagai encipher dan $n = p\ x\ q$. Proses dekripsi dimodelkan dengan rumus matematika (5).

$$M = \ C^{-1}\ mod\ n \quad (5)$$

Dimana C sebagai cipher dan $d = (\phi(n-1))mod\ \phi(n)$.

2.3. Transposisi Kolom

Algoritma Transposisi merupakan teknik enkripsi dengan menggantikan atau menata ulang posisi tiap bit tertentu pada tiap *block* menjadi *cipher*. Penerapan metode tersebut membuat data awal sebelum terenkripsi menjadi tidak dapat terbaca sebelumnya. Algoritma transposisi merupakan algoritma simetris dimana penggunaan *key* dapat digunakan untuk melakukan enkripsi maupun dekripsi. Pada penelitian ini metode transposisi akan disisipkan kedalam algoritma RSA yang akan mengenkripsi data audio dalam sistem yang akan diimplementasikan.

Metode transposisi yang digunakan pada penelitian ini adalah transposisi kolom yang dimodelkan dalam perhitungan sebagai berikut :

Plain text = 11001010111100010101110101011101

Key = GBECDAF

Susunan kolom = 7 2 5 3 4 1 6

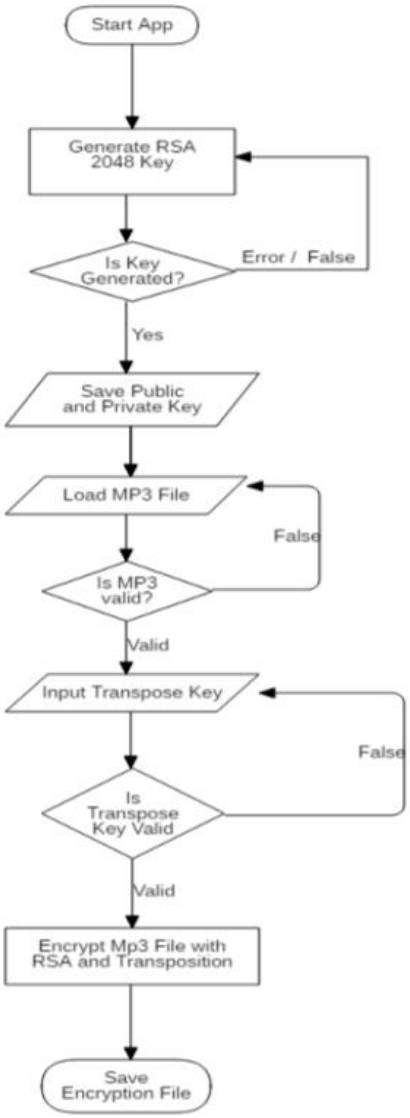
Proses Enkripsi =

7 2 5 3 4 1 6
1 1 0 0 1 0 1
0 1 1 1 1 0 0
0 1 0 1 0 1 1
1 0 1 0 1 0 1
1 1 0 1

Hasil enkripsi = 0010 11101 01101 1101 01010 1011 10011

2.4. Usulan Metode

Pada analisis algoritma kombinasi dilakukan penelitian tentang penggabungan algoritma yang akan diimplementasikan di sistem enkripsi dan dekripsi audio. Algoritma kriptografi RSA merupakan algoritma asimetri yang memiliki kunci *private* dan *public* yang dibangkitkan menggunakan perhitungan matematika. Untuk alur penelitian, telah dilakukan seperti tampak pada Gambar 1.



Gambar 1. Skema Usulan Metode

Algoritma transposisi merupakan algoritma simetri yang dalam melakukan enkripsi dan dekripsi menggunakan metode memindahkan letak bit secara kolumnar dengan tahapan sebagai berikut:

1. Pembangkitan *private key* dan *public key* untuk algoritma kombinasi RSA – 2048 dan transposisi kolumnar menggunakan bilangan prima desimal yang lebih dengan ukuran p dan q berukuran 1024 bit untuk

DOI: https://doi.org/10.29207/resti.v5i3.2996

menghasilkan *key length* yang sebesar 2048 bit untuk menjaga keamanan dari kunci tersebut.

2. Susunan file berekstensi .mp3 memiliki susunan bit tiap frame yang akan di enkripsi terlebih dahulu menggunakan algoritma transposisi kolum sesuai dengan *key*.

3. Setelah tiap frame dari mp3 yang akan dienkripsi akan dilakukan enkripsi seluruh file menggunakan algoritma RSA – 2048 bit dan *public key* yang dilakukan ke seluruh file dengan mempartisi frame dari sesuai dengan padding dan batasan *byte* yang dapat diproses algoritma RSA 2048.

4. Hasil akhir berupa file mp3 yang telah diubah susunan bit tiap framenya terlebih dahulu oleh transposisi kemudian di enkripsi menggunakan algoritma RSA.

5. Dekripsi menggunakan private *key* yang telah dibangkitkan untuk mendekripsi file mp3 yang telah dienkripsi menjadi file mp3 yang terenkripsi oleh transposisi kolom terlebih dahulu.

6. File mp3 kemudian di didekripsi menggunakan *key* yang sama dengan enkripsi menggunakan algoritma transposisi kolumnar ketika dienkripsi.

7. Hasil dari dekripsi tersebut merupakan hasil akhir atau plain *text* dari file mp3 semula yang sebelum dilakukan enkripsi.

2.5. Pengujian Metode

Tahapan pengujian dilakukan untuk melakukan pembuktian dari implementasi algoritma kombinasi yang telah dibuat sebelumnya sesuai dengan tujuan penelitian yang dilakukan dan menentukan kesimpulan dari penelitian ini. Metode pengujian algoritma yang digunakan pada penelitian ini adalah *avalanche effect* dam penghitungan entropi. Avalanche effet adalah uji coba terhadap algoritma kriptografi yang akan menguji tingkat perubahan hasil enkripsi yang didapat ketika melakukan perubahan pada bagian perhitungan enkripsi. Uji coba ini akan memberikan hasil tentang pengaruh perubahan susunan *key* akan menghasilkan perubahan kepada susunan bit hasil enkripsinya. Pada pengujian ini akan dilakukan pemeriksaan tentang spesifikasi dari aplikasi tersebut dan fitur – fitur yang dibutuhkan dalam sistem aplikasi kriptografi transposisi kolumnar dan RSA– 2048 bit pada file mp3. Hasil dari tahapan pengujian ini dapat dilakukan siklus ulang terhadap salah satu tahapan penelitian jika hasil pengujian belum sesuai dengan tujuan penelitian atau dapat dilanjutkan ke tahap akhir yaitu hasil dari penelitian dari implementasi algoritma kombinasi tersebut.

3. Hasil dan Pembahasan

Algoritma klasik yang digunakan hanya algoritma simetri transposisi kolumnar yang memiliki inputan sampai 1024 karakter dan algoritma modern asimetri RSA dengan nilai modulus N 2048 bit atau 256 *byte* yang menggunakan *padding* standar PKCS v1.5. 2. Data yang diuji untuk diamankan adalah data audio berformat mp3 dengan ukuran maksimal 5 *megabyte* secara keseluruhan isi file yang diambil dari file-example.com. Pengujian algoritma kriptografi peningkatan keamanan menggunakan pengujian *avalanche effect*, perhitungan *entropy* hasil enkripsi dan kecepatan algoritma dieksekusi.

Hasil dari penelitian ini berupa perbandingan dari algoritma yaitu kombinasi, RSA, dan transposisi dari segi kecepetan dalam melakukan enkripsi dan dekripsi, perbandingan hasil akhir enkripsi dan dekripsi, sebagai berikut:

3.1. Perhitungan Kecepatan

Dalam sistem aplikasi ini telah dilakukan berbagai percobaan enkripsi maupun dekripsi dengan variable yang berbeda baik secara kunci atau ukuran objek yang dikelola. Dengan banyaknya *variable* yang diuji coba semakin banyak data percobaan yang dapat dijadikan acuan dalam mengukur performa algoritma kombinasi yang telah dibuat ketika digunakan untuk melakukan proses enkripsi dan dekripsi.

Dari pengujian sistem berikut dengan kunci publik yang sama, menggunakan ukuran berkas yang berbeda dan kunci transposisi yang bervariasi. Pengujian dilakukan dengan melakukan enkripsi berulang kali sehingga mendapatkan hasil yang di rata-rata. Hasil percobaan tersebut menghasilkan perhitungan kecepatan rata-rata sesuai Tabel 2 dan Tabel 3.

Tabel 2. Waktu Enkripsi

Ukuran Data	Panjang Kunci Transposisi	Tranposisi	RSA	Total
741 kb	256	00 : 2.74	00 : 19.81	00 : 22.5
741 kb	512	00 : 3.34	00 : 19.84	00 : 23.18
741 kb	1024	00 : 3.90	00 : 19.82	00 : 23.72
1063 kb	256	00 : 3.01	00 : 30.16	00 : 33.17
1063 kb	512	00 : 3.84	00 : 30.14	00: 33.98
1063 kb	1024	00 : 4.12	00 : 30.17	00 : 34.29
2065 kb	256	00 : 4.30	00 : 59.98	01 : 04.28
2065 kb	512	00 : 4.76	00 : 59.99	01 : 04.75
2065 kb	1024	00 : 5.09	01 : 00.02	01 : 05.11
5166 kb	256	00 : 11.10	02 : 15.03	02 : 26.13
5166 kb	512	00 : 14.24	02 : 15.05	02 : 29.29
5166 kb	1024	00 : 17.12	02 : 15.04	02 : 32.16

Tabel 3. Waktu Dekripsi

Ukuran Data	Panjang Kunci	Tranposisi	RSA	Total
741 kb	256	02 : 28.04	00 : 2.72	00 : 22.5
741 kb	512	02 : 28.03	00 : 3.37	00 : 23.18
741 kb	1024	02 : 28.05	00 : 3.94	00 : 23.72
1063 kb	256	03 : 22.09	00 : 3.02	00 : 33.17
1063 kb	512	03 : 22.09	00 : 3.82	00: 33.98
1063 kb	1024	03 : 22.11	00 : 4.14	00 : 34.29
2065 kb	256	06 : 39.89	00 : 4.35	01 : 04.28
2065 kb	512	06 : 39.90	00 : 4.80	01 : 04.75
2065 kb	1024	06 : 39.89	00 : 5.16	01 : 05.11
5166 kb	256	16 : 25.03	00 : 11.09	16 :36.12

DOI: https://doi.org/10.29207/resti.v5i3.2996

5166 kb	512	16 : 25.04	00 : 14.14	16 : 39.18
5166 kb	1024	16 : 25.05	00 : 17.01	16 : 42.06

3.2. Perhitungan Ukuran Data

Pengujian ini dilakukan untuk mengetahui ada perubahan ukuran yang dihasilkan dari proses enkripsi file dengan kunci *public* yang sama dan panjang kunci transposisi yang di variasi. Hasil dari perbandingan ukuran file dapat dilihat pada Tabel 4.

Tabel 4. Waktu Dekripsi

Ukuran Data	Panjang Kunci	Tranposisi	RSA	Total
741 kb	256	02 : 28.04	00 : 2.72	00 : 22.5
741 kb	512	02 : 28.03	00 : 3.37	00 : 23.18
741 kb	1024	02 : 28.05	00 : 3.94	00 : 23.72
1063 kb	256	03 : 22.09	00 : 3.02	00 : 33.17
1063 kb	512	03 : 22.09	00 : 3.82	00: 33.98
1063 kb	1024	03 : 22.11	00 : 4.14	00 : 34.29
2065 kb	256	06 : 39.89	00 : 4.35	01 : 04.28
2065 kb	512	06 : 39.90	00 : 4.80	01 : 04.75
2065 kb	1024	06 : 39.89	00 : 5.16	01 : 05.11
5166 kb	256	16 : 25.03	00 : 11.09	16 :36.12
5166 kb	512	16 : 25.04	00 : 14.14	16 : 39.18
5166 kb	1024	16 : 25.05	00 : 17.01	16 : 42.06

Dari Tabel 4, dapat terlihat bahwa proses enkripsi RSA mengubah ukuran file menjadi lebih besar dibanding dengan ukuran file asli. Hal ini terjadi karena metode RSA 2048 dengan standar PKCS#1 v1.5 menggunakan *padding* yang disisipkan tiap enkripsi dengan 214 byte, sedangkan pada metode transposisi kolum, tidak terjadi perubahan ukuran dikarenakan transposisi kolumnar hanya merubah susunan dan urutan tiap elemen byte array tanpa menambah jumlah elemen *byte array* tersebut.

3.3 Perhitungan Entropy

Perhitungan nilai *entropy* digunakan untuk mengetahui tingkat keacakan dan kualitas dari hasil proses enkripsi. Metode kriptografi dikatakan berkualitas, jika memiliki nilai *entropy* mendekati 8 [12]. Berikut merupakan hasil dari perhitungan nilai *entropy* pada file mp3 yang telah terenkripsi sesuai Tabel 5.

Tabel 5. Pengujian *Entropy*

Ukuran Data	Panjang Kunci Transposisi	Transposisi	RSA+ Transposisi
741 kb	256	7.881448603654222	7.999778156673427
741 kb	512	7.881448603654222	7.999800420888501
741 kb	1024	7.881448603654222	7.999796352423447
1063 kb	256	7.873715708053562	7.999857521123294
1063 kb	512	7.873715708053562	7.999831933916985
1063 kb	1024	7.873715708053562	7.999928488083420 5
2065 kb	256	7.875414125214095	7.999918817412766
2065 kb	512	7.875414125214095	7.999910422248671
2065 kb	1024	7.875414125214095	7.999928488083420 5
5166 kb	256	7.872488827205234	7.999957657451292
5166 kb	512	7.872488827205234	7.999962157533926
5166 kb	1024	7.872488827205234	7.999976500911441

3.2. Perhitungan *Avalanche* Effect

Pengujian *avalanche effect* ini dengan melihat struktural *byte* dari file mp3 ketika diinputkan dengan *public key* yang sama tetapi memiliki susunan *transpose key* yang berbeda dari segiri posisi beberapa karakter saja. Dari pengujian seperti yang disebutkan sebelumnya pada file mp3 berukuran 741 kb, 1mb, 2mb, dan 5mb dan panjang kunci transposisi kolom yang dirubah. Seperti contoh dengan kunci awal "udinusudinusudin" akan dirubah pada bagian awal menjadi "ddinusudinusudin", pada bagian tengah "udinusuuinusudin", dan terakhir "udinusudinusudii" seperti terlihat pada Tabel 6.

Tabel 6. Pengujian *Avalanche Effect*

Ukuran Data	Panjang Kunci Transposisi	Transposisi	RSA+ Transposisi
741 kb	49.97965837 %	50.006995 %	49.9883918 %
1063 kb	49.95959979 %	50.01256019 %	49.99454155 %
2065 kb	49.9865780 %	49.9792368 %	50.00624379 %
5166 kb	50.00054317 %	49.98717325 %	49.99524774 %

Dari Tabel 6 pada pengujian *avalanche effect*, kita dapat melihat bahwa rata-rata dari hasil perhitungan menunjukkan nilai mendekati 50%. Dari hasil tersebut, algoritma dapat disimpulkan bahwa algoritma usulan memiliki kualitas yang baik.

4. Kesimpulan

Setelah melakukan pengembangan sistem aplikasi kriptografi dengan algoritma kombinasi RSA 2048 dan transposisi kolom penulis dapat menarik kesimpulan bahwa algoritma kombinasi dari algoritma modern asimetri RSA 2048 bit dan algoritma klasik simetri transposisi kolumnar dapat menjalankan proses enkripsi pada file mp3 secara fungsional dengan kecepatan yang berbanding lurus dengan ukuran objek yang akan dienkripsi, serta algoritma kombinasi dapat menghasilkan ukuran yang bervarian dan susunan yang lebih random dan bervarian. Perolehan nilai entropy mendekati angka 8. Pengujian entropy pada RSA-Tranposisi kolom terbukti lebih tinggi dibanding Transposisi saja. Nilai entropy transposisi tertinggi yaitu 7.881448603654222, dan RSA-transposisi memperoleh nilai tertinggi 7.999976500911441. Ukuran file hasil enkripsi membuktikan bahwa file hasil enkripsi transposisi saja tidak berubah, namun pada RSA-transposisi diperoleh ukuran data yang lebih besar.

DOI: https://doi.org/10.29207/resti.v5i3.2996

Daftar Rujukan

[1] N. A. Fauziah, E. H. Rachmawanto, D. Setiadi and C. A. Sari, "Design and Implementation of AES and SHA-256 Cryptography for Securing Multimedia File over Android Chat Application," in 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), Yogyakarta, 2018.

[2] O. G. Abood and S. K. Guirguis, "A Survey on Cryptography Algorithms," International Journal of Scientific and Research Publications, vol. 8, no. 7, pp. 495- 516, 2018.

[3] R. D. Ardy, O. R. Indriani, C. A. Sari, D. Setiadi and E. H. Rachmawanto, "Digital image signature using triple protection cryptosystem (RSA, Vigenere, and MD5)," in International Conference on Smart Cities, Automation & Intelligent Computing Systems (ICON-SONICS) 2017, Yogyakarta, 2018.

[4] E. J. Kusuma, C. A. Sari, E. H. Rachmawanto and D. Setiadi, "A Combination of Inverted LSB, RSA, and Arnold Transformation to get Secure and Imperceptible Image Steganography," Journal of ICT Research and Applications, vol. 12, no. 2, pp. 103-122, 2018.

[5] N. N. Diarse and K. J. Bendi, "Penerapan Algoritma RSA pada Sistem Kriptografi File Audio MP3," Jurnal Hoaq Teknologi Informasi, vol. 7, no. 2, pp. 567 -575, 2016.

[6] T. Z. Nwe and S. W. Phyo, "Performance Analysis of RSA and ElGamal for Audio Securit," International Journal of Scientific Engineering and Technology Research, vol. 3, no. 11, pp. 2494-2498, 2014.

[7] A. G. Khan, S. Basharat and M. U. Riaz, "Analysis of asymmetric cryptography in information security based on computational study to ensure confidentiality during information exchange," International Journal of Scientific & Engineering Research, vol. 9, no. 10, pp. 992-999, 2018.

[8] A. Jawahir and H. Haviluddin, "An audio encryption using transposition method," International Journal of Advances In Intelligent Informatics, vol. 1, no. 2, pp. 98-106, 2015.

[9] S. Nisha and M. Farik, "RSA Public *Key* Cryptography Algorithm – A Review," International Journal of Scientific & Technology Research, vol. 6, no. 7, pp. 187-191, 2017.

[10] S. F. Yousif, "Encryption And Decryption of Audio Signal Based On Rsa Algorithn," International Journal of Engineering Technologies and Management Research, vol. 5, no. 7, pp. 57-64, 2018.

[11] A. Fauzi, Novriyenni, Y. Maulita and A. M. Pardede, "Analisis *Hybrid* Cryptosystem Algoritma Algoritma RSA dan Triple Des," Jtik (Jurnal Teknik Informatika Kaputama), vol. 1, no. 2, pp. 36-44, 2017.

[12] Zhen, P, Zhao, G, Min, L, Jin, X, "Chaos-based image encryption scheme combining DNA coding and entropy," Multimed Tools Appl, vol. 75, pp. 6303–6319, 2016.

DOI: https://doi.org/10.29207/resti.v5i3.2996