KRIPTOGRAFI AUDIO MENGGUNAKAN TRANSPOSISI DAN *AFFINE CIPHER* YANG DIKEMBANGKAN DENGAN ALGORITMA *BLUM BLUM SHUB*

SKRIPSI

Diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar Sarjana Matematika

Oleh:

Muhammad Fakhri Naufal

NIM 1702032

PROGRAM STUDI MATEMATIKA

DEPARTEMEN PENDIDIKAN MATEMATIKA

FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS PENDIDIKAN INDONESIA

2021

LEMBAR PENGESAHAN

MUHAMMAD FAKHRI NAUFAL

KRIPTOGRAFI AUDIO MENGGUNAKAN TRANSPOSISI DAN *AFFINE CIPHER* YANG DIKEMBANGKAN DENGAN ALGORITMA *BLUM BLUM SHUB*

disetujui dan disahkan oleh pembimbing:

Pembimbing I,

Dra. Hj. Rini Marwati M.S.

NIP. 196606251990012001

Pembimbing II,

Ririn Sispiyati, S.Si., M.Si.

NIP. 198106282005012001

Mengetahui,

Ketua Departemen Pendidikan Matematika

Dr. H. Dadang Juandi M.Si.

NIP. 196401171992021001

LEMBAR PERNYATAAN

Dengan ini saya menyatakan bahwa skripsi dengan judul "Kriptografi Audio Menggunakan Transposisi dan *Affine Cipher* yang Dikembangkan Dengan Algoritma *Blum Blum Shub*" ini beserta seluruh isinya adalah benar-benar karya saya sendiri. Saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika ilmu yang berlaku dalam masyarakat keilmuan. Atas pernyataan ini, saya siap menanggung risiko/sanksi apabila di kemudian hari ditemukan adanya pelanggaran etika keilmuan atau ada klaim dari pihak lain terhadap keaslian karya saya ini.

Bandung, 26 November 2020

Yang Membuat Pernyataan,

Muhammad Fakhri Naufal

NIM. 1702032

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Dengan memanjatkan puji syukur kehadirat Allah SWT, serta rahmat shalawat dan salam untuk junjungan besar Nabi Muhammad SAW penulis dapat menyelesaikan skripsi yang berjudul: "Kriptografi Audio Menggunakan Transposisi dan *Affine Cipher* yang Dikembangkan dengan Algoritma *Blum Blum Shub*".

Penulisan skripsi ini diajukan untuk memenuhi sebagian persyaratan untuk memperoleh gelar sarjana di Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam Universitas Pendidikan Indonesia. Penulis menyadari di dalam penulisan ini masih terdapat kekurangan-kekurangan yang disebabkan oleh keterbatasan dan kemampuan penulis. Oleh karena itu, penulis sangat mengharapkan saran dan kritik yang membangun untuk menyempurnakan skripsi ini.

Semoga Allah SWT melimpahkan rahmat dan karunia-Nya serta membalas kebaikan semua pihak yang telah membantu penulis dalam penyusunan skripsi ini. Semoga skripsi ini dapat bermanfaat bagi penulis khususnya dan bagi pembaca pada umumnya.

Wassalamu'alaikum Wr. Wb.

Bandung, 26 November 2020

Muhammad Fakhri Naufal

NIM. 1702032

UCAPAN TERIMA KASIH

Dengan memanjatkan puji syukur kehadirat Allah SWT, serta rahmat shalawat dan salam untuk junjungan besar Nabi Muhammad SAW penulis dapat menyelesaikan skripsi dengan tepat waktu. Selesainya skripsi ini tidak terlepas dari dukungan, bantuan dan doa berbagai pihak. Oleh karena itu, penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Yth. Ibu Dra. Hj. Rini Marwati, M. S. selaku Pembimbing 1 yang telah meluangkan waktunya untuk memberikan arahan yang sangat membantu penyusunan dari awal hingga akhir penulisan skripsi ini;
2. Yth. Ibu Ririn Sispiyati, S.Si.,M.Si. selaku Pembimbing II yang telah meluangkan waktunya untuk memberikan arahan yang sangat membantu penyusunan dari awal hingga akhir penulisan skripsi ini;
3. Yth. Ibu Dr. Khusnul Novianingsing, M.Si. selaku dosen Pembimbing Akademik yang telah memberikan arahan serta motivasi selama penulis menjalani perkuliahan S1;
4. Yth. Bapak Drs. H. Cece Kustiawan, M.Si. selaku Ketua Program Studi Matematika Universitas Pendidikan Indonesia;
5. Yth. Bapak Dr. Dadang Juandi, M.Si. selaku Ketua Departemen Pendidikan Matematika Universitas Pendidikan Indonesia;
6. Yth. Ibu Kartika Yulianti, S.Pd., M.Si. selaku Ketua KBK Terapan Program Studi Matematika Departemen Pendidikan Matematika Universitas Pendidikan Indonesia;
7. Yth. Seluruh dosen Departemen Pendidikan Matematika yang telah memberikan ilmunya selama penulis menjalani perkuliahan S1;
8. Seluruh Civitas Akademika Departemen Pendidikan Matematika dan Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam Universitas Pendidikan Matematika;
9. Kedua orang tua tercinta Ibu Sumiati dan Bapak Zaenudin, kakak serta adik penulis Herdin dan Alya yang telah memberikan dorongan serta doa dan kasih sayang agar selalu berusaha dengan maksimal dan senantiasa bersyukur;

10. Sahabat-sahabat yang selalu ada dalam suka dan duka khususnya Salsabila Ayu Pratiwi serta Ilham Fikriansyah, Fakhri Maulana Nurjaman, Muhammad Agus Hermawan, Deni Septian, Rifky Anugrah, Muhammad Fadhil Rifqi, Yarits Hanifan Fakhruddin, Bagas Hamdanirahman, Wildy Ardan, Michael Alberto, Nugroho Dwi Widodo, dan rekan-rekan mahasiswa Matematika UPI untuk dukungan, bantuan, dan kebersamaan selama menjalani perkuliahan S1.
11. Seluruh Pihak yang tidak dapat penulis cantumkan satu persatu yang telah mendukung dan membantu penulis menyelesaikan skripsi ini.

Semoga Allah SWT membalas semua kebaikan ketulusan dari pihak-pihak yang telah membantu penulis dan mendapat ridho Allah SWT.

ABSTRAK

Di era informasi, teknologi berkembang dengan pesat dan kemudahan dalam bertukar informasi menjadi sangat mudah, namun dengan perkembangan tersebut timbul suatu masalah yaitu keamanan informasi tersebut terutama untuk suatu informasi rahasia. Salah satu bentuk informasi seperti file audio memerlukan sebuah mekanisme untuk mengamankan file audio tersebut, salah satunya dengan kriptografi. Teknik kriptografi audio seperti transposisi membuat data audio teracak sehingga suara yang dihasilkan file audio tersebut tidak dapat dipahami. Namun, untuk meningkatkan keamanan nilai data audio pada file audio diperlukan teknik enkripsi substitusi salah satunya yaitu *Affine Cipher*. Dengan melakukan pengembangan pada *Affine Cipher* menggunakan pembangkit bilangan acak semu *Blum Blum Shub*, dapat memberikan peningkatan yang cukup signifikan pada teknik kriptografi klasik ini. Hasil yang diperoleh dengan mengenkripsi file audio WAV menggunakan *Python* dapat mengamankan file audio sehingga menghasilkan suara acak dan file audio terenkripsi dapat didekripsi untuk mendapatkan informasi asli.

Kata Kunci: Kriptografi, Kriptografi Audio, File Audio, Transposisi, *Affine Cipher, Blum Blum Shub*

ABSTRACT

In this information era, technology is developing rapidly and the ease of exchanging information becomes very easy, but with these developments arises a problem that is the security of such information especially for a secret information. One form of information such as an audio file requires a mechanism to secure the information, one of which is with cryptography. Audio cryptographic techniques such as transposition make the audio data scrambled so that the sound generated by the audio file is incomprehensible. However, to increase the security of the value of audio data in audio files, it is necessary to encrypt substitution techniques, one of which is Affine Cipher. By developing Affine Cipher using a pseudo random number generator Blum Blum Shub, it can provide a significant improvement on this classic cryptographic technique. The results obtained by encrypting WAV audio files using Python can secure the audio file so that it generates scrambled sounds and the encrypted audio file can be decrypted to get the original information.

Keywords: *Cryptography, Audio Cryptography, Audio Files, Transposition, Affine Cipher, Blum Blum Shub*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR PUSTAKA

Alvarado, R. M., dkk. (2020). Simultaneous Audio Encryption and Compression Using Compressive Sensing Techniques. *Electronics,* 9, 863.

Arroyo, J.C.T. & Delima, A.J.P. (2020). An Improved Affine Cipher using Blum Blum Shub Algorithm. *International Journal of Advanced Trends in Computer Science and Engineering, 9,* 3295 – 3298.

Firdaus, I. L. (2017). *Aplikasi Kriptografi Komposisi One Time Pad Cipher dan Affine Cipher.* (Skripsi). Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam, Universitas Pendidikan Indonesia, Bandung.

Gallian, J.A. (1986). *Contemporary Abstract Algebra*. Boston: Cengage Learning

Jawahir, A. & Haviluddin. (2015). An Audio Encryption using Transposition Method. *International Journal of Advances in Intelligent Informatics,* 1, 98-106.

Kordov, K. (2019). A Novel Audio Encryption Algorithm with Permutation-Substitution Architecture. *Electronics,* 8, 530.

Mansi & Chawla, R. (2015). A Review on Audio Cryptography. *International Journal of Modern Communication Technologies & Research (IJMCTR),* 3.

Mitra, P. (2018). *Introductory Chapter: Recent Advances in Cryptography and Network Security.* Guwahati: Department of Computer Science and Engineering.

Munir, R. (2004). *Teori Bilangan (Number Theory)*. Bandung:Departemen Teknik Informatika Institut Teknologi Bandung.

Niven, I., Zuckerman, H.S., & Montgomery, H.L. (1991). *An Intoroduction to the Theory of Numbers*. 5th ed.

Oliphant, T.E., (2007). Python for Scientific Computing. *IEEE: Computing in Science and Engineering. 9,* 10 – 20.

Sinha, N., Bhowmick, A., & Kishore, B. (2015). Encrypted Information Hiding using Audio Steganography and Audio Cryptography. *International nJournal of Computer Applications*, 112, 0975 – 8887.

Sobari, A. I. (2017). *Aplikasi Pengirim Email dengan Penerapan Enkripsi Caesar Cipher yang Telah Ditingkatkan Keamanannya Menggunakan Enkripsi*

Row Transposition Cipher. (Skripsi). Fakultas Pendidikan dan Ilmu Pengetahuan Alam, Universitas Pendidikan Indonesia, Bandung.

Stinson, D. R. & Rosen, K.H. (Penyunting). (2006). *Criptography: Theory and Practice.* 3rd Ed. Chapman & Hall/CRC: Ontario.

Stuart, C. (2004). *Wave PCM Soundfiles Format. [Online]*. Diakses dari http://soundfile.sapp.org/doc/WaveFormat/