IMPLEMENTASI ALGORITMA *ONE TIME PAD COUPLE LINEAR CONGRUENTIAL GENERATOR* DAN *RIVEST SHAMIR ADLEMAN - CHINESE REMAINDER THEOREM* DALAM PENGAMANAN *CODING FILE*

SKRIPSI

Diajukan untuk memenuhi syarat untuk memperoleh gelar Sarjana Matematika

Oleh:

Nabila Nurul Anisa Az Zahra

1906249

PROGRAM STUDI MATEMATIKA

FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS PENDIDIKAN INDONESIA

2023

LEMBAR HAK CIPTA

IMPLEMENTASI ALGORITMA *ONE TIME PAD COUPLE LINEAR CONGRUENTIAL GENERATOR* DAN *RIVEST SHAMIR ADLEMAN - CHINESE REMAINDER THEOREM* DALAM PENGAMANAN *CODING FILE*

Oleh:

Nabila Nurul Anisa Az Zahra

NIM 1906249

Diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar Sarjana Matematika pada Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam

Universitas Pendidikan Indonesia

Agustus 2023

LEMBAR PENGESAHAN

NABILA NURUL ANISA AZ ZAHRA

IMPLEMENTASI ALGORITMA *ONE TIME PAD COUPLE LINEAR CONGRUENTIAL GENERATOR* DAN *RIVEST SHAMIR ADLEMAN - CHINESE REMAINDER THEOREM* DALAM PENGAMANAN *CODING FILE*

Disetujui dan disahkan oleh pembimbing :

Pembimbing I

Dra. Rini Marwati, M.S

NIP. 196606251990012001

Pembimbing II

Ririn Sispiyati, S.Si, M.Si

NIP. 198106282005012001

Mengetahui,

Ketua Program Studi Matematika

Dr. Kartika Yulianti, S.Pd, M.Si

NIP. 198207282005012001

ABSTRAK

Seiring dengan perkembangan jaman, media untuk berkomunikasi ikut mengalami perkembangan. Komunikasi dapat dilakukan di mana pun dengan memanfaatkan perkembangan digital seperti *WhatsApp, Line* dan *E-mail*. Bentuk pesan yang dikirim pun ada berbagai macam. Salah satunya adalah *coding file* yang umumnya digunakan pada bidang IT khususnya oleh *programmer*. Pengiriman *coding file* menggunakan server publik dapat beresiko karena *file* yang dikirim dapat diretas. Kriptografi mampu untuk menyandikan pesan agar pesan yang dikirim menjadi teramankan. Pada penelitian ini diambil algoritma *One Time Pad* (OTP) dan *Rivest Shamir Adleman* (RSA) untuk digabungkan dengan tujuan untuk diimplemetasikan pada pengamanan *coding file* dan dibuat sebuah aplikasi menggunakan algoritma yang telah dipilih. OTP dimodifikasi menggunakan *Couple Linear Congurential Generator* (CLCG) untuk pembangkitkan kunci OTP dan RSA dimodifikasi menggunakan *Chinese Remainder Theorem* (CRT) untuk mempersingkat proses pengembalian isi pesan. Kunci OTP CLCG dipilih oleh kedua belah pihak sedangkan RSA publik dan privat RSA CRT dipilih oleh penerima *file*. Proses enkripsi menggunakan algoritma OTP CLCG, lalu dilanjutnya dengan algoritma RSA. Untuk mengembalikan isi konten *file, file* terenkripsi didekripsi menggunakan algoritma RSA CRT, lalu dilanjutkan dengan OTP CLCG. *Python* dipilih untuk mengkonstruksi aplikasi karena merupakan bahasa pemrograman bersifat *open source* yang mudah dipahami. Aplikasi pengamanan *coding file* dikonstruksi menggunakan library *math* dan Tkinter.

Kata Kunci : Kriptografi, *One Time Pad*, *Couple Linear Congurential Generator*, *Rivest Shamir Adleman*, *Chinese Remainder Theorem*, *Coding file*

ABSTRACT

Along with the development of the era, the media for communication also experienced development. Communication can be done anywhere by utilizing digital developments such as WhatsApp, Line and E-mail. There are various forms of messages. One of them is coding files which are generally used in information and technology's field, especially by programmer. Delivering coding file using public server can be risky because the sending file can be hacked. Cryptography is able to encode messages so that the messages sent are secured. In this study, the algorithm of One Time Pad (OTP) and Rivest Shamir Adleman is combined for the purpose of securing coding file and made an application based on the selected algorithm. OTP is modified using Couple Linear Congurential Generator (CLCG) to generate the OTP key and RSA is modified using Chinese Remainder Theorem (CRT) to reducing the time for the decryption process. The CLCG OTP key is chosen by both parties while the public RSA and private RSA CRT are chosen by the file's recipient. The encryption process use OTP's algorithm then followed by RSA's algorithm. In order to return the file's contents, the encrypted gile is decrypted using RSA CRT's algorithm then followed by OTP CLCG's algorithm. Python was chosen to construct the application because it is an open source programming language that is easy to understand. The coding file security's application is constructed by using math and tkinter's library.

Keywords : *Cryptography, One Time Pad, Couple Linear Congurential Generator, Rivest Shamir Adleman, Chinese Remainder Theorem, Coding File*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR PUSTAKA

Anton, H., & Rorres, C. (2004). *Aljabar Linear Elementer*. Erlangga.

Arief, A., & Saputra, R. (2016). Implementasi Kriptografi Kunci Publik dengan Algoritma RSA-CRT pada Aplikasi Instant Messaging. *Scientific Journal of Informatics*. https://doi.org/10.15294/sji.v3i1.6115

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi.* Penerbit Andi.

Biantara, I. M. D., Sudana, I. M., Alfa Faridh Suni, S., & Hangga, A. (2015). Modifikasi Metode Linear Congruential Generator Untuk Optimalisasi Hasil Acak. *SemNaSIF*, *2015*(November), 182–186.

Burton, D. M. (2007). *Elementary Number Theory - Sixth Edition*. *Elementary Number Theory*.

Burton, D. M. (2010). *Elementary Number Theory - Seventh Edition. In Paper Knowledge . Toward a Media History of Documents*.

Firdaus, I. L., Marwati, R., & Sispiyati, R. (2017). Aplikasi Kriptografi Komposisi One Time Pad Cipher Dan Affine Cipher. *Eurematika*, *5*(2), 42–51.

Hardikushwawa. (2020). *Difference Between a Script file and a Binary file*. GreeksforGreeks. Diakses dari https://www.geeksforgeeks.org/difference-between-a-script-file-and-a-binary-file/

Ibnutama, K., & Panjaitan, M. G. S. Z. (2019). Penggunaan Chinese Reminder Theorem (CRT) pada Algoritma RSA. 18.

Munir, I. R. (2010). *Algoritma RSA dan ElGamal*. Kriptografi.

Pandey, O. (2017). *Lecture 2 : Shannon and Perfect Secrecy Instructor : Omkant Pandey We discussed some historical ciphers.* 2017(Cse 594), 1–32.

Perkovic, L. (2012). *Introduction to computing using python*.

Ristiana, M. G. (2017). *Algoritma Hybrid Kriptografi RSA dengan Kriptografi One Time Pad*. (Skripsi). Fakultas Pendidikan dan Ilmu Pengetahuan Alam, Universitas Pendidikan Indonesia, Bandung.

Ruslida, A. M., Sapri, & Sartika, D. (2022). Implementasi Algoritma Byte Pair Encoding Untuk Kompresi File. 18(2), 253–260.

Schneier, B. (2010). *Applied Cryptography Second Edition.* Dr.Johon Dsan.

Simargolang, M. Y. (2017). Implementasi Kriptografi RSA dengan PHP. *Jurnal Teknologi Informasi*. https://doi.org/10.36294/jurti.v1i1.1

Sitohang, T. R., Marwati, R., & Yusnitha, I. (2019). Kriptosistem Gabungan S-Ecies Dan Rsa. *Jurnal EurekaMatika*, *7*(1), 93–102.

Stinson, D. R. (2005). *Cryptography: Theory and practice, third edition. In Cryptography: Theory and Practice, Third Edition* (pp. 1–582).

Stinson, D. R., & Paterson, M. B. (2019). *Shannon's Theory, Perfect Secrecy, and the One-Time Pad In Cryptography*. https://doi.org/10.1201/9781315282497-3

Suhardi. (2016). Aplikasi Kriptografi Data Sederhana Dengan Metode Exlusive-or (Xor). *Jurnal Teknovasi*, *03*(2), 23–31.

Syahputra, A. (2021). Implementasi Algoritma Freivlds Untuk Pembangkitan Kunci Algoritma RSA Pada Pengamanan Data Video. *Pelita Informatika : Informasi Dan Informatika*, *10*(2), 70–77.

Triwibowo, D. N., & Ariyus, D. (2020). Penerapan Algoritma Coupled Linear Congurential Generator (CLCG) pada Algortima Kriptografi One Time Pad (OTP) dalam Proses Mengamankan Pesan. *Jurnal Media Informatika Budidarma*, *4*(3), 841. https://doi.org/10.30865/mib.v4i3.2244

Wagstaff, S. S., & Rosen, K. H. (1987). *Elementary Number Theory and Its Applications. Mathematics of Computation*. https://doi.org/10.2307/2007902