

**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

© Nabila Nurul Anisa Az Zahra 2023

Universitas Pendidikan Indonesia

Agustus 2023

Hak cipta dilindungi undang-undang

Skripsi tidak boleh diperbanyak seluruhnya atau sebagian dengan dicetak ulang,
difotokopi, atau cara lainnya tanpa izin penulis

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 Sispiwati, 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 dilanjutkan 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 Congruential 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 file 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 Congruential Generator, Rivest Shamir Adleman, Chinese Remainder Theorem, Coding File*

DAFTAR ISI

LEMBAR PENGESAHAN	i
SURAT PERNYATAAN.....	ii
KATA PENGANTAR	iii
UCAPAN TERIMAKASIH.....	iv
ABSTRAK	v
ABSTRACT.....	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR	ix
DAFTAR TABEL.....	x
BAB I PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Batasan Masalah	4
1.3 Rumusan Masalah.....	4
1.4 Tujuan Penelitian	5
1.5 Manfaat Penelitian.....	5
BAB II LANDASAN TEORI	6
2.1 Teori Dasar Matematika	6
2.1.1 Algoritma Pembagian	6
2.1.2 Bilangan Prima	6
2.1.3 Faktor Persekutuan Terbesar (FPB).....	6
2.1.4 Relatif Prima.....	7
2.1.5 Phi Euler	7
2.1.6 Modulo.....	7
2.1.7 <i>Invers</i> Modulo.....	7
2.1.8 Matriks.....	7
2.1.9 <i>Coupled Linear Congruential Generator</i>	7
2.2 Kriptografi	9
2.2.1 Kriptografi Simetris	10
2.2.2 Kriptografi Asimetris	10
2.2.3 <i>American Standard Code for Information Interchange</i>	10
2.2.4 <i>One Time Pad</i>	11

2.2.5 <i>Rivest Shamir Adleman (RSA)</i>	13
2.2.6 <i>Chinese Remainder Theorem (CRT)</i>	17
2.2.7 <i>Coding File</i>	18
2.3 Bahasa Pemrograman (<i>Python</i>)	18
BAB III METODOLOGI PENELITIAN.....	19
3.1 Identifikasi Masalah	19
3.2 Model Dasar	19
3.2.1 Algoritma OTP	19
3.2.2 Algoritma RSA	20
3.3 Pengembangan Model	21
3.4 Konstruksi Aplikasi	21
3.4.1 <i>Input dan Output</i>	22
3.4.2 Algoritma OTP menggunakan CLCG	23
3.4.3 Algoritma RSA-CRT.....	24
3.5 Rancangan Tampilan	24
3.6 Validasi	25
BAB IV HASIL DAN PEMBAHASAN	26
4.1 Skema Aplikasi Kriptografi <i>Coding File</i> OTP-CLCG RSA-CRT	26
4.2 Aplikasi	27
4.2.1 Tampilan Aplikasi	27
4.2.2 Algoritma Aplikasi	31
4.3 Validasi	37
4.3.1 Validasi Pembangkitan Kunci RSA-CRT	38
4.3.2 Validasi Pembangkitan Kunci OTP CLCG.....	39
4.3.3 Perbandingan hasil <i>running file</i> dekripsi dengan <i>file</i> asli	41
BAB V KESIMPULAN DAN SARAN.....	44
5.1 Kesimpulan.....	44
5.2 Saran	44
DAFTAR PUSTAKA	45
LAMPIRAN.....	47

DAFTAR GAMBAR

Gambar 3.1 Skema kriptografi OTP	20
Gambar 3.2 Skema kriptografi RSA	20
Gambar 3.3 Skema enkripsi dan dekripsi model pengembangan	21
Gambar 3.4 Rancangan Tampilan Menu Utama Aplikasi	24
Gambar 3.5 Rancangan Tampilan Menu Pembangkitan Kunci RSA-CRT	24
Gambar 3.6 Rancangan Tampilan Menu Tipe Data Untuk Input Data Pembangkitan Kunci RSA-CRT.....	25
Gambar 3.7 Rancangan Tampilan Menu Dekripsi <i>File</i>	25
Gambar 3.8 Rancangan Tampilan Menu Enkripsi <i>File</i>	25
Gambar 4.1 Skema Aplikasi Kriptografi <i>Coding File</i> OTP-CLCG RSA-CRT.....	26
Gambar 4.2 Tampilan Menu Utama Aplikasi Kriptografi <i>Coding File</i> OTP-CLCG RSA-CRT.....	27
Gambar 4.3 Tampilan Menu Pembangkitan Kunci RSA-CRT.....	28
Gambar 4.4 Tampilan Menu Enkripsi <i>Coding File</i>	29
Gambar 4.5 Tampilan Fitur <i>Upload</i> dan <i>Save Coding File</i>	29
Gambar 4.6 Tampilan Menu Dekripsi <i>Coding File</i>	30
Gambar 4.7 Tampilan Menu Petunjuk Penggunaan Aplikasi Pengamanan <i>Coding File</i>	30
Gambar 4.8 Tampilan Menu saat kunci yang dipilih tidak valid.....	38
Gambar 4.9 Tampilan <i>Output</i> Pembangkitan Kunci.....	39
Gambar 4.10 Matriks Ukuran 14×16.....	39
Gambar 4.11 Pembangkitan OTP CLCG menggunakan pada aplikasi.....	40
Gambar 4.12 Tampilan hasil <i>running file</i> awal .py.....	41
Gambar 4.13 Tampilan hasil <i>running file</i> dekripsi .py.....	41
Gambar 4.14 Tampilan hasil <i>running</i> .cpp	42
Gambar 4.15 Tampilan hasil <i>running file</i> dekripsi .cpp.....	42
Gambar 4.16 Tampilan hasil <i>running file</i> awal .m.....	42
Gambar 4.17 Tampilan hasil <i>running file</i> dekripsi .m.....	43

DAFTAR TABEL

Tabel 2.1 Tabel Operasi XOR.....	11
Tabel 2.2 Kode ASCII Pesan dalam Blok.....	15
Tabel 2.3 Blok <i>Ciphertext</i> Hasil Enkripsi RSA.....	15
Tabel 2.4 Blok <i>Plaintext</i> Hasil Dekripsi RSA.....	16
Tabel 3.1 <i>Input</i> dan <i>output</i> pada rancangan Aplikasi	22
Tabel 3.2 Matriks Pemilihan Kunci OTP CLCG	23
Tabel 4.1 Pembangkitan Kunci OTP CLCG menggunakan <i>microsoft excel</i>	40

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 Remainder 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 Exclusive-or (Xor). *Jurnal Teknovasi*, 03(2), 23–31.
- Syahputra, A. (2021). Implementasi Algoritma Feivlds 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 Congruential Generator (CLCG) pada Algoritma 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>