

# **IMPLEMENTASI CAESAR CIPHER PADA ALGORITMA KRIPTOGRAFI KLASIK DALAM PENYANDIAN PESAN**

**SKRIPSI**



**Oleh**

**Krisma Budi Ziliwu**

**180210119**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNIK & KOMPUTER  
UNIVERSITAS PUTERA BATAM  
2022**

# **IMPLEMENTASI CAESAR CIPHER PADA ALGORITMA KRIPTOGRAFI KLASIK DALAM PENYANDIAN PESAN**

**SKRIPSI**

**Untuk memenuhi salah satu syarat  
memperoleh gelar Sarjana**



**Oleh**

**Krisma Budi Ziliwu**

**180210119**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNIK & KOMPUTER  
UNIVERSITAS PUTERA BATAM  
2022**

## SURAT PERYATAAN ORISINALITAS

Yang bertanda tangan di bawah ini saya:

Nama : Krisma Budi Ziliwu

NPM : 180210119

Fakultas : Teknik dan Komputer

Program Studi : Teknik Informatika

Menyatakan bahwa "Skripsi" yang saya buat dengan judul:

### IMPLEMENTASI CAESAR CIPHER PADA ALGORITMA KRIPTOGRAFI KLASIK DALAM PENYANDIAN PESAN

Adalah hasil karya sendiri dan bukan "duplikasi" dari karya orang lain. Sepengetahuan saya, di dalam naskah Skripsi ini tidak terdapat karya ilmiah atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis dikutip didalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila ternyata di dalam naskah Skripsi ini dapat dibuktikan terdapat unsur-unsur PLAGIASI, saya bersedia naskah Skripsi ini digugurkan dan gelar akademik yang saya peroleh dibatalkan, serta diproses sesuai dengan peraturan perundang-undangan yang berlaku.

Demikian pernyataan ini saya buat dengan sebenarnya tanpa ada paksaan dari siapapun.

Batam, 08 Agustus 2022



Krisma Budi Ziliwu

180210119

**IMPLEMENTASI CAESAR CIPHER PADA ALGORITMA  
KRIPTOGRAFI KLASIK DALAM PENYANDIAN PESAN**

**SKRIPSI**

Untuk memenuhi salah satu syarat  
memperoleh gelar Sarjana

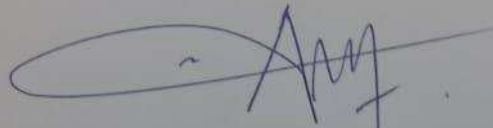
Oleh

Krisma Budi Ziliwu

180210119

Telah disetujui oleh Pembimbing pada tanggal  
seperti tertera di bawah ini

Batam, 08 Agustus 2022

A handwritten signature in blue ink, appearing to read 'Andi Maslan', with a large, sweeping flourish on the left side.

Andi Maslan, S.T., M.Si

Pembimbing



## ABSTRAK

Kejahatan *cyber* menjadi hal yang sangat dikhawatirkan oleh pengguna jaringan internet dalam berkomunikasi. Oleh karena itu, setiap pesan yang akan dikirimkan harus diamankan dengan teknik kriptografi. Caesar cipher adalah satu salah metode pengamanan pesan dalam ilmu kriptografi. Dalam pengamanan pesan menggunakan caesar cipher setiap karakter akan ditukarkan posisinya sehingga makna dari isi pesan susah untuk dimengerti. Tujuan menggunakan caesar cipher untuk mencegah pihak yang tidak berkepentingan mencuri informasi yang bersifat rahasia dalam pesan. Cara mengaplikasi pengamanan pesan pada penelitian ini dengan merancang aplikasi berbasis desktop menggunakan bahasa pemrograman vb.net. Pengamanan pesan dengan menggunakan algoritma caesar cipher yaitu dengan menukarkan setiap karakter pada pesan asli menjadi cipherteks. Karakter pada plainteks akan disubstitusikan berdasarkan penjumlahan urutan abjad pada plainteks dengan kunci yang telah ditentukan. Proses pengamanan pada caesar cipher disebut enkripsi sedangkan proses mengubah kembali pesan tersandi menjadi plainteks disebut deskripsi. Kegiatan deskripsi dilakukan dengan cara mengurangkan urutan setiap abjad dengan kunci yang digunakan saat melakukan enkripsi. Pengamanan pesan menggunakan caesar cipher mampu mengamankan isi pesan dengan cara menyamarkan isi pesan atau mengubah bentuk isi pesan asli dengan bentuk yang lain sehingga susah untuk dimengerti oleh pihak yang tidak bertanggung jawab. Keamanan yang bisa didapatkan berupa kerahasiaan, keaslian isi pesan dan juga anti penyangkalan.

**Kata kunci:** Kejahatan *cyber*; Caesar cipher; Kriptografi; Keamanan; Pesan

## ***ABSTRACT***

*Cyber crime is a matter of great concern for internet network users in communicating. Therefore, every message to be sent must be secured with cryptographic techniques. Caesar cipher is a method of securing messages in cryptography. In securing messages using Caesar cipher, each character will be exchanged in position so that the meaning of the message content is difficult to understand. The purpose of using caesar cipher is to prevent unauthorized parties from stealing confidential information in messages. How to apply message security in this study by designing a desktop-based application using the vb.net programming language. Message security using the Caesar cipher algorithm is by exchanging each character in the original message into ciphertext. The characters in the plaintext will be substituted based on the sum of the alphabetical order in the plaintext with a predetermined key. The process of securing the Caesar cipher is called encryption while the process of converting the encrypted message back into plaintext is called description. The description activity is carried out by subtracting the order of each alphabet with the key used when encrypting. Securing messages using Caesar cipher is able to secure the contents of the message by disguising the content of the message or changing the form of the original message in another form so that it is difficult for irresponsible parties to understand. Security that can be obtained in the form of confidentiality, authenticity of the message content and also anti-denial.*

***Keywords:*** *Cyber crime; Caesar cipher; Criptography; Security, Message*





## KATA PENGANTAR

Puji Tuhan kami ucapkan syukur karena telah dengan baik memberikan keberkahan kepada penulis sehingga bisa menyelesaikan tugas akhir yang menjadi syarat utama untuk menyelesaikan progran studi strata satu (S1) pada Program Studi Teknik Informatika Universitas Putera Batam.

Penulis sadar bahwa penulisan skripsi ini sangat sederhana dan jauh dari kata sempurna. Oleh sebab itu kritik dan saran akan selalu penulis menerimanya dengan senang hati. Dengan segala keterbatasan, penulis menyadari bahwa skripsi ini tidak akan terselesaikan tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, segala kerendahan hati, penulis menyampaikan terima kasih kepada:

1. Ibu Dr. Nur Elfi Husda, S.Kom., M.SI. selaku Rektor Universitas Putera Batam;
2. Bapak Welly Sugianto, S.T., M.M. selaku Dekan Fakultas Teknik dan Komputer;
3. Bapak Andi Maslan, S.T., M.SI. selaku Ketua Program Studi Teknik Informatika dan juga selaku pembimbing skripsi penulis;
4. Bapak Koko Handoko, S.Kom., M.Kom. Selaku pembimbing Akademik pada Program Studi Teknik Informatika Universitas Putera Batam;
5. Dosen dan Staff Universitas Putera Batam;
6. Orang tua dan adik kandung penulis yang memberikan dukungan dan doa agar penulis dapat menyelesaikan skripsi ini;
7. Istri tercinta yang selalu memberi dukungan dan doa agar penulis dapat menyelesaikan skripsi ini;
8. Dan teman-teman seperjuangan yang tidak bisa penulis sebutkan semuanya terimakasih untuk saran dan dukungannya;

Kiranya Tuhan saja yang membalas kebaikan setiap orang yang telah membantu penulis dan semoga skripsi ini dapat memberikan manfaat untuk penulis maupun setiap orang membutuhkan.

Batam, 08 September 2022

KRISMA BUDI ZILIWU

## Daftar Isi

|   |     |
|---|-----|
| <b>ABSTRAK</b> .....                                | i   |
| <b>ABSTRACT</b> .....                               | ii  |
| <b>KATA PENGANTAR</b> .....                         | iii |
| <b>Daftar Gambar</b> .....                          | vi  |
| <b>Daftar Tabel</b> .....                           | vii |
| <b>BAB I PENDAHULUAN</b> .....                      | 1   |
| <b>1.1 Latar Belakang</b> .....                     | 1   |
| <b>1.2 Identifikasi Masalah</b> .....               | 3   |
| <b>1.3 Batasan Masalah</b> .....                    | 4   |
| <b>1.4 Rumusan Masalah</b> .....                    | 4   |
| <b>1.5 Tujuan Penelitian</b> .....                  | 4   |
| <b>1.6 Manfaat Penelitian</b> .....                 | 4   |
| <b>BAB 2 TINJAUAN PUSTAKA</b> .....                 | 5   |
| <b>2.1 Teori Dasar</b> .....                        | 5   |
| 2.1.1 Sejarah Kriptografi.....                      | 5   |
| 2.1.2 Unsur Dalam Kriptografi .....                 | 7   |
| 2.1.3 Tujuan Kriptografi.....                       | 10  |
| 2.1.4 Jenis Jenis Kriptografi.....                  | 11  |
| 2.1.5 Fungsi Hash.....                              | 13  |
| <b>2.2 Algoritma Caesar Cipher</b> .....            | 14  |
| <b>2.3 Perancangan Sistem</b> .....                 | 14  |
| 2.3.1 VB.net .....                                  | 15  |
| 2.3.2 Node.js .....                                 | 15  |
| 2.3.3 Unified modelling language (UML).....         | 16  |
| 2.3.4 Flowchart.....                                | 18  |
| <b>2.4 Pengujian Aplikasi Penyajian Pesan</b> ..... | 21  |
| <b>2.5 Penelitian Terdahulu</b> .....               | 21  |
| <b>2.6 Kerangka Pemikiran</b> .....                 | 24  |
| <b>BAB III METODE PENELITIAN</b> .....              | 26  |
| <b>3.1 Desain Penelitian</b> .....                  | 26  |
| <b>3.2 Teknik Pengumpulan Data</b> .....            | 28  |
| <b>3.3 Pemodelan Fungsional</b> .....               | 28  |
| 3.3.1 <i>Flowchart caesar cipher</i> .....          | 29  |
| 3.3.2 <i>Diagram Use Case</i> .....                 | 30  |

|  |   |    |
|--|---|----|
| 3.3.3  | <i>Diagram Activity</i> .....                                     | 31 |
| <b>3.4</b>                                     | <b>Perancangan Interface</b> .....                                | 33 |
| 3.4.1  | <i>Halaman Utama</i> .....  | 33 |
| 3.4.2  | <i>Menu Login</i> .....   | 34 |
| 3.4.3  | <i>Menu log out</i> .....   | 34 |
| 3.4.4  | <i>Menu Enkripsi</i> .....  | 35 |
| 3.4.5  | <i>Menu Deskripsi</i> .....                                       | 35 |
| <b>3.5</b>                                     | <b>Perancangan algoritma caesar cipher</b> .....                  | 36 |
| <b>3.6</b>                                     | <b>Implementasi</b> .....   | 41 |
| <b>3.7</b>                                     | <b>Pengujian</b> .....  | 42 |
| <b>3.8</b>                                     | <b>Jadwal Penelitian</b> .....                                    | 42 |
| <b>BAB IV</b>                                  | <b>HASIL DAN PEMBAHASAN</b> .....                                 | 43 |
| <b>4.1</b>                                     | <b>Hasil Penelitian</b> .....                                     | 43 |
| 4.1.1  | Halaman Utama.....  | 43 |
| 4.1.2  | Menu Login.....   | 44 |
| 4.1.3  | Menu Log Out.....   | 44 |
| 4.1.4  | Menu Kirim Wa (Encrypted).....                                    | 45 |
| 4.1.5  | Menu Decryptor.....   | 45 |
| <b>4.2</b>                                     | <b>Pembahasan</b> .....   | 46 |
| 4.2.1  | Implementasi Pengamanan Pesan dengan Algoritma Caesar Cipher..... | 47 |
| 4.2.2  | Pengujian Fungsional Sistem Dengan Blackboxs Testing.....         | 48 |
| 4.2.3  | Pengujian enkripsi dan deskripsi.....                             | 48 |
| <b>BAB V</b>                                   | <b>KESIMPULAN</b> .....   | 52 |
| <b>5.1</b>                                     | <b>Kesimpulan</b> .....   | 52 |
| <b>5.2</b>                                     | <b>Saran</b> .....  | 52 |
| <b>Daftar Pustaka</b>                          | .....   | 53 |
| <b>Lampiran</b>                                | .....   | 56 |
| <b>Lampiran 1. Pendukung Penelitian</b>        | .....   | 56 |
| <b>Lampiran 2. Daftar Riwayat Hidup</b>        | .....   | 58 |
| <b>Lampiran 3. Turnitin Skripsi</b>            | .....   | 59 |
| <b>Lampiran 4. Turnitin Jurnal</b>             | .....   | 60 |
| <b>Lampiran 5. Surat Keterangan Penelitian</b> | .....   | 61 |

## Daftar Gambar

|                     |  |    |
|---------------------|--|----|
| <b>Gambar 2. 1</b>  | Diagram Enkripsi dan Deskripsi .....   | 8  |
| <b>Gambar 2. 2</b>  | Sistem Kriptografi Simetri .....       | 12 |
| <b>Gambar 2. 3</b>  | Sistem kriptografi nirsimetri .....    | 13 |
| <b>Gambar 2. 4</b>  | Simbol <i>usecase diagram</i> .....    | 17 |
| <b>Gambar 2. 5</b>  | Simbol activity diagram .....          | 18 |
| <b>Gambar 2. 6</b>  | Bagian penting flowchart .....         | 19 |
| <b>Gambar 2. 7</b>  | Simbol Flowchart .....                 | 20 |
| <b>Gambar 2. 8</b>  | Kerangka pemikiran .....               | 24 |
| <b>Gambar 3. 1</b>  | Desain Penelitian .....                | 26 |
| <b>Gambar 3. 2</b>  | Flowchart Caesar Cipher .....          | 29 |
| <b>Gambar 3. 3</b>  | Diagram Usecase .....                  | 30 |
| <b>Gambar 3. 4</b>  | Diagram aktivitas Enkripsi pesan ..... | 31 |
| <b>Gambar 3. 5</b>  | Diagram Activity Enkripsi Pesan .....  | 32 |
| <b>Gambar 3. 6</b>  | Halaman Utama .....                    | 33 |
| <b>Gambar 3. 7</b>  | Menu Login .....                       | 34 |
| <b>Gambar 3. 8</b>  | Menu Logout .....                      | 34 |
| <b>Gambar 3. 9</b>  | Menu Enkripsi .....                    | 35 |
| <b>Gambar 3. 10</b> | Menu Deskripsi .....                   | 35 |
| <b>Gambar 3. 11</b> | Arsitektur Aplikasi .....              | 41 |
| <b>Gambar 4. 1</b>  | Halaman Utama .....                    | 43 |
| <b>Gambar 4. 2</b>  | QR Code .....                          | 44 |
| <b>Gambar 4. 3</b>  | Menu Log Out .....                     | 44 |
| <b>Gambar 4. 4</b>  | Menu Kirim Wa .....                    | 45 |
| <b>Gambar 4. 5</b>  | Menu Decryptor .....                   | 46 |
| <b>Gambar 4. 6</b>  | Enkripsi kunci 1 .....                 | 49 |
| <b>Gambar 4. 7</b>  | Enkripsi Kunci 2 .....                 | 49 |
| <b>Gambar 4. 8</b>  | Enkripsi Kunci 3 .....                 | 50 |
| <b>Gambar 4. 9</b>  | Deskripsi Kunci 1 .....                | 50 |
| <b>Gambar 4. 10</b> | Enkripsi Kunci 2 .....                 | 51 |
| <b>Gambar 4. 11</b> | Deskripsi Kunci 3 .....                | 51 |

## Daftar Tabel

|  |    |
|--|----|
| <b>Tabel 3. 1</b> Plainteks .....          | 37 |
| <b>Tabel 3. 2</b> Cipherteks.....          | 38 |
| <b>Tabel 3. 3</b> Baris plainteks .....    | 38 |
| <b>Tabel 3. 4</b> Baris Cipherteks .....   | 38 |
| <b>Tabel 3. 5</b> Jadwal Penelitian .....  | 42 |
| <b>Tabel 4. 1</b> Pengujian Fungsional     | 48 |
| <b>Tabel 4. 2</b> Pengujian Enkripsi.....  | 48 |
| <b>Tabel 4. 3</b> Pengujian Deskripsi..... | 49 |