**Jurnal Manajemen Informatika Jayakarta**
Volume 6, Nomor 2, April 2026: halaman 221-230

P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v6i2.2387

# PENGUATAN AUTENTIKASI REGISTER PENGGUNA MELALUI ENKRIPSI OTP BERBASIS CAESAR CIPHER

**Mokhammad Hadi Prayitno[1], Hendarman Lubis[2]***

Program Studi Informatika, Fakultas Ilmu Komputer
Universitas Bhayangkara Jakarta Raya
Jakarta, Indonesia

*Correspondent Author : hendarman.lubis@dsn.ubharajaya.ac.id,

**Abstrak**

Evolusi ekosistem digital yang cepat meningkatkan risiko keamanan informasi, terutama selama proses registrasi pengguna di mana data sensitif dikirimkan. Meskipun teknologi *One-Time Password* (OTP) menyediakan autentikasi dinamis, transmisi kode dalam bentuk teks biasa (*plaintext*) melalui SMS atau email tetap rentan terhadap penyadapan. Penelitian ini bertujuan untuk memperkuat proses registrasi dengan menerapkan sistem keamanan berlapis yang menggabungkan algoritma klasik *Caesar Cipher* dengan mekanisme OTP. Menggunakan pendekatan *Research and Development* (R&D), sebuah prototipe dikembangkan untuk mengenkripsi 6 digit OTP alfanumerik sebelum dikirimkan. Sistem ini menggunakan formula $C = (P + K) \mod 26$ atau penyesuaian tabel ASCII untuk mengubah *plaintext* OTP menjadi *ciphertext*. Pengujian melalui metode *Black Box* dan *Avalanche Effect* mengonfirmasi bahwa sistem berhasil mengamankan data tanpa mengorbankan pengalaman pengguna. Simulasi Python menunjukkan bahwa kode asli (contoh: "AZ29B1") dikirimkan sebagai *ciphertext* (contoh: "DC52E4"), dengan dekripsi otomatis yang terjadi pada sisi aplikasi. Penelitian ini memberikan kontribusi solusi praktis dengan komputasi rendah untuk mencegah pencurian identitas dan akses tidak sah selama tahap pembuatan akun

**Kata kunci:** Caesar Cipher, OTP, Autentikasi, Pendaftaran, Kriptografi

***Abstract***

The rapid evolution of digital ecosystems increases information security risks, particularly during user registration where sensitive data is submitted. Although One-Time Password (OTP) technology provides dynamic authentication, transmitting codes as plaintext via SMS or email remains vulnerable to interception. This study aims to strengthen the registration process by implementing a multi-layered security system combining the classic Caesar Cipher algorithm with OTP mechanisms. Using a Research and Development (R&D) approach, a prototype was developed to encrypt a 6-digit alphanumeric OTP before transmission. The system uses the formula $C = (P + K) \mod 26$ or ASCII table adjustments to convert the plaintext OTP into ciphertext. Testing through Black Box and Avalanche Effect methods confirmed that the system successfully secures data without compromising user experience. Python simulations demonstrated that an original code (e.g., "AZ29B1") is transmitted as ciphertext (e.g., "DC52E4"), with automated decryption occurring on the application side. This research contributes a practical, low-computation solution to prevent identity theft and unauthorized access during the account creation stage

***Keywords:*** *Caesar Cipher, OTP, Authentication, Registration, Cryptography*

DOI: https://doi.org/10.52362/jmijayakarta.v6i2.2387

*http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta*

**Jurnal Manajemen Informatika Jayakarta**
Volume 6, Nomor 2, April 2026: halaman 221-230
P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v6i2.2387

## 1 Pendahuluan

Kemajuan teknologi informasi yang pesat telah mendorong transformasi signifikan dalam interaksi manusia, bertransformasi dari sistem konvensional menuju lingkungan digital yang terus berkembang. Karena perubahan ini melibatkan pembagian data dalam jumlah besar melalui sistem publik, hal tersebut membuat informasi menjadi lebih rentan terpapar risiko keamanan dan kelemahan sistem bawaan [1][2]. Dalam konteks ini, perlindungan data telah bergeser dari sekadar keuntungan tambahan menjadi bagian krusial bagi keberlangsungan organisasi dan upaya menjaga kepercayaan pengguna. Kebutuhan ini semakin ditekankan oleh meningkatnya kompleksitas ancaman yang menargetkan sistem informasi manajemen, baik dari sumber internal maupun eksternal. Dalam sistem digital saat ini, formulir pendaftaran adalah tempat utama di mana informasi pribadi yang penting dikumpulkan, seperti nama, nomor telepon, dan alamat email [3]. Tanpa aturan keamanan yang kuat, langkah ini menjadi risiko yang besar. Hal tersebut dapat dimanfaatkan untuk pencurian informasi pribadi, penyadapan oleh peretas, dan pembuatan akun palsu secara otomatis oleh robot. [4].
Ketergantungan semata-mata pada autentikasi kata sandi statis menciptakan celah keamanan yang besar, sebagaimana dibuktikan oleh maraknya serangan berbasis kredensial. Pengguna sering kali menggunakan kata sandi mudah yang sama untuk berbagai akun daring, sehingga ketika satu akun berhasil diretas, hal tersebut dapat memicu masalah pada seluruh aset daring mereka lainnya. Kelemahan sistemik ini mengharuskan integrasi mekanisme perlindungan yang ketat, seperti yang ditetapkan oleh ISO/IEC 27001:2022, untuk mengautentikasi pendaftar secara efektif dan menyelaraskannya dengan strategi mitigasi risiko organisasi saat ini [5]. alah satu cara terbaik untuk menjaga keamanan adalah dengan menggunakan Autentikasi Dua Faktor (2FA) atau Autentikasi Multi-Faktor (MFA) [6]. Dengan menggunakan pemeriksaan kedua, seperti menyandingkan identitas pengguna dengan kode yang berubah-ubah, kemungkinan seseorang masuk tanpa izin menjadi jauh lebih rendah, bahkan jika orang lain mengetahui kata sandi utamanya [7].

Keamanan informasi, terutama dalam hal menjaga kerahasiaan dan memastikan keakuratan data, sangat bergantung pada alat-alat yang ditawarkan oleh kriptograf [1]. Di antara teknik-teknik tersebut, *Caesar Cipher* merupakan teknik yang sangat dikenal dan masih digunakan di beberapa aplikasi perpesanan modern [8][9]. Sistem mengubah setiap karakter menggunakan metode penggantian sederhana berdasarkan kunci tertentu [10][11]. Daya tarik luasnya disebabkan oleh kesederhanaan operasional dan penggunaan sumber daya yang minimal (*overhead* rendah), yang sangat menguntungkan bagi sistem dengan sumber daya terbatas [10]. Meskipun pergeseran tetapnya mudah diprediksi, algoritma ini dapat dipatahkan menggunakan analisis frekuensi kecuali jika digunakan bersama dengan algoritma yang lebih kuat [9][11]. Saat ini, berbagai studi tengah berfokus pada penggabungan metode ini dengan *Hill Cipher* atau *Vigenere Cipher* guna mempersulit pihak yang tidak memiliki izin untuk memecahkan kode pesan tersebut [12][11].

Autentikasi dinamis, terutama yang menggunakan teknologi *One-Time Password* (OTP), telah mulai digunakan untuk mengurangi risiko penggunaan kata sandi tetap. Identitas unik ini memiliki masa berlaku yang terbatas, biasanya kedaluwarsa setelah satu kali penggunaan atau dalam waktu yang sangat singkat, yang bertujuan untuk mencegah serangan *replay* meskipun transmisi datanya disadap [6]. Walaupun OTP membantu membangun kepercayaan lebih besar dan menjaga keamanan layanan keuangan digital, desainnya tidak sepenuhnya kebal. Pengiriman kode-kode ini dalam bentuk teks biasa (*plain text*) melalui SMS atau email merupakan risiko keamanan yang besar karena pihak lain dapat memperoleh detail masuk sebelum diterima oleh orang yang tepat. Oleh karena itu, mengenkripsi kode OTP sebelum transmisi—menggunakan teknik seperti *Caesar Cipher* atau menggabungkannya dengan algoritma *One-Time Pad* (OTP)—adalah langkah krusial dalam memperkuat integritas data [12].

Kekuatan dari jenis enkripsi ini dapat dilihat melalui *Avalanche Effect* (Efek Longsoran), yang berarti bahwa perubahan kecil pada input atau kunci akan menghasilkan perbedaan besar pada output [13]. Mengevaluasi efek longsoran sangat penting untuk memastikan bahwa OTP yang terenkripsi tetap tangguh terhadap serangan kriptografi, serupa dengan standar kinerja yang terlihat pada algoritma modern seperti AES dan RSA [14] [15]. Dengan menggunakan metode kriptografi ini, penelitian ini

**Jurnal Manajemen Informatika Jayakarta**
Volume 6, Nomor 2, April 2026: halaman 221-230
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v6i2.2387

mengkaji 'Penguatan Autentikasi Registrasi Pengguna melalui Enkripsi OTP Berbasis Caesar Cipher' untuk menciptakan cara pendaftaran pengguna yang lebih aman. Penelitian ini bertujuan untuk menawarkan perlindungan data yang lebih baik dengan tetap menjaga efisiensi proses dalam hal komputasi..

## 2 Tinjauan Literatur

Secara ringkas, penuls memiiki lteratur yang digunakan pada penelitian, antara lain :

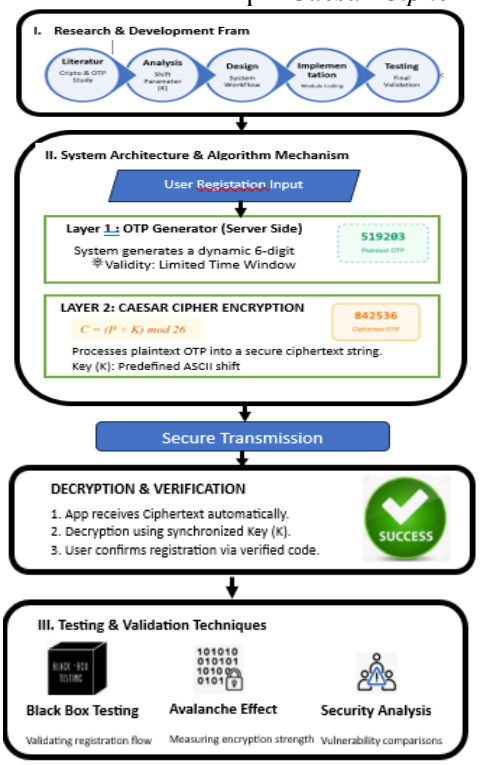
(1) Enkripsi untuk Keamanan Data,
Enkrip**si** adalah proses teknis yang mengubah informasi atau data asli (*plaintext*) menjadi format yang tidak dapat dibaca (*ciphertext*) menggunakan algoritma matematis dan kunci tertentu. Tujuan utamanya adalah untuk menjamin kerahasiaan (*confidentiality*), integritas (*integrity*), dan autentikasi data, sehingga meskipun data tersebut berhasil disadap saat dikirimkan melalui jaringan publik, pihak yang tidak berwenang tidak dapat memahami isinya [16].

(2) Caesar Cipher: Merupakan algoritma kriptografi klasik yang menggunakan teknik substitusi sederhana dengan menggeser posisi karakter dalam alfabet berdasarkan nilai kunci tertentu. Meskipun mudah diimplementasikan, metode ini rentan terhadap serangan *brute-force* karena ruang kuncinya yang terbatas [17]

(3) One-Time Pad (OTP): Sebuah metode autentikasi dan enkripsi yang menghasilkan kode unik dan dinamis yang hanya berlaku untuk satu kali penggunaan dalam jangka waktu tertentu. Secara teoritis, OTP dianggap sebagai teknik enkripsi yang sempurna jika kuncinya benar-benar acak [18].

## 3 Metode Penelitian

Penelitian ini menggunakan metode penelitian dan pengembangan (*Research and Development*) dengan model pengembangan sistem berbasis mesin. Fokus utamanya adalah merancang modul keamanan yang mengintegrasikan OTP dan enkripsi *Caesar Cipher* ke dalam proses pendaftaran.




Gambar 1 : Metode Penelitian

**Jurnal Manajemen Informatika Jayakarta**
Volume 6, Nomor 2, April 2026: halaman 221-230
P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v6i2.2387

a) Kerangka Penelitian:
   (1) Studi Literatur: Meninjau kriptografi, mekanisme OTP, dan ancaman autentikasi.
   (2) Analisis Kebutuhan: Menentukan parameter pergeseran untuk *Caesar Cipher* dan metode transmisi.
   (3) Desain Sistem: Merancang diagram alur (*workflow*) untuk pendaftaran dan verifikasi.
   (4) Implementasi: Melakukan pengodean pada modul enkripsi dan generator OTP.
   (5) Pengujian: Mengevaluasi fungsionalitas dan keamanan.

b) Desain Algoritma:
   (1) Lapisan 1 (Generator OTP): Menghasilkan kode acak 6 digit yang dinamis dengan masa berlaku terbatas.
   (2) Lapisan 2 (Enkripsi Caesar Cipher): Memproses OTP teks biasa (*plaintext*) menggunakan formula $C = (P + K) \mod 26$ atau penyesuaian ASCII.

c) Arsitektur Sistem:
   (1) Input Data: Pengguna memasukkan detail pendaftaran.
   (2) Generasi OTP: Server membuat kode unik.
   (3) Tahap Enkripsi: Server mengenkripsi OTP menggunakan kunci ($K$) yang telah ditentukan.
   (4) Transmisi: Kode terenkripsi dikirimkan kepada pengguna.
   (5) Dekripsi & Verifikasi: Aplikasi secara otomatis mendekripsi kode, dan pengguna memasukkannya untuk verifikasi.

d) Teknik Pengujian:
   (1) Black Box Testing: Memastikan alur pendaftaran berjalan lancar bagi pengguna.
   (2) Avalanche Effect: Mengukur sejauh mana perubahan kecil pada kunci atau *plaintext* memengaruhi *ciphertext* untuk mengevaluasi kekuatan enkripsi.
   (3) Analisis Keamanan Deskriptif: Membandingkan kerentanan transmisi antara teks terenkripsi dengan teks biasa (*plaintext*).

Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 2, April 2026: halaman 221-230
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v6i2.2387

## 4 Hasil dan Pembahasan

Temuan dari penelitian ini mengkonfirmasi bahwa mekanisme *One-Time Password* (OTP) telah bertransformasi dari fitur keamanan tambahan menjadi kebutuhan kritis bagi ekosistem registrasi pengguna modern. Berdasarkan analisis fungsional dan teknis, implementasi OTP memberikan perlindungan utama bagi sistem:

(1) Keamanan Berlapis (Penjagaan Ganda): Enkripsi kode OTP menggunakan *Caesar Cipher* sebelum transmisi memberikan pendekatan *Two-Factor Authentication* (2FA) yang melindungi identitas melalui sifat dinamis OTP sekaligus menjaga integritas kode melalui enkripsi kriptografi.

(2) Efisiensi Komputasi: Sistem ini menciptakan lingkungan pendaftaran yang aman namun tetap efisien karena memiliki beban komputasi yang rendah, sehingga cocok untuk aplikasi dengan sumber daya terbatas.

(3) Transformasi Teknis yang Teruji: Dalam simulasi, kode asli (contoh: "AZ29B1") berhasil diubah menjadi *ciphertext* (contoh: "DC52E4") menggunakan kunci pergeseran $K=3$.

Secara ringkas, temuan ini menunjukkan bahwa mengenkripsi kode OTP menggunakan *Caesar Cipher* sebelum transmisi memberikan pendekatan "penjagaan ganda" (2FA): melindungi identitas melalui sifat dinamis dari kode OTP, dan menjaga integritas kode itu sendiri melalui enkripsi kriptografi. Hal ini menciptakan lingkungan pendaftaran yang aman namun tetap efisien dalam hal beban komputasi.

Implementasi aplikasi pendaftaran pengguna menggunakan algoritma *Caesar Cipher* untuk mengenkripsi OTP yang dihasilkan. Logika inti dari modul enkripsi disusun seperti yang ditunjukkan pada Tabel 1. Kode Algoritma Aplikasi, ditulis dalam bahasa pemrograman:

Tabel 1. Kode Algoritma Aplikasi

```
func caesarCipherEncrypt(input string) string {
var result strings.Builder
// Shift parameter K = 4
shift := 4

for _, r := range input {
//Checking for alphabetical
characters
if (r >= 'a' && r <= 'z')
|| (r >= 'A' && r <= 'Z')
{
base := 'a'
    if r>='A' && r<='Z' {
    base = 'A'
    }

    // Applying the Caesar Cipher formula: (P+K)mod 26

    shifted := ((int(r) –
    int(base) + shift) % 26)  + int(base)
    result.WriteRune(rune(shifted))
    } else {
    // Non-alphabetical
    characters are written
    without modification
```

Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 2, April 2026: halaman 221-230
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v6i2.2387

```
    result.WriteRune(r)
    }
    }
    return result.String()
                                        }
```

Kode di atas mendemonstrasikan mekanisme pergeseran di mana setiap karakter dari *plaintext* OTP diubah menjadi karakter *ciphertext* berdasarkan nilai pergeseran tertentu. Hal ini memastikan bahwa kode yang ditransmisikan melalui jaringan telah dikaburkan (*obfuscated*), sehingga memenuhi lapisan kedua dari kerangka keamanan yang diusulkan.

Untuk mendemonstrasikan penerapan praktis dari persyaratan teoritis ini, simulasi sistem keamanan dua lapis yang diusulkan disajikan di bawah ini, yang mengilustrasikan bagaimana integrasi OTP dan *Caesar Cipher* beroperasi dalam proses registrasi di dunia nyata.

Guna mengevaluasi efektivitas kerangka keamanan dua lapis yang diusulkan, sebuah simulasi teknis terkendali dilakukan dengan menggunakan dataset representatif. Simulasi ini menjelaskan transisi sistematis mulai dari pendaftaran pengguna awal hingga pembuatan dan transmisi kredensial autentikasi yang terenkripsi.

1. Inisiasi Pendaftaran dan Mekanisme Generasi OTP
   a. Inisiasi dan Penggabungan Data Unik
      Protokol keamanan dimulai saat pengguna memasukkan identitas unik (misalnya "mhp1970"). Sistem tidak hanya menggunakan ID tersebut, tetapi juga menangkap *Unix Timestamp* dalam resolusi milidetik tepat saat tombol pendaftaran ditekan. Penggabungan identitas dan penanda waktu yang presisi ini menciptakan variabel masukan unik yang mustahil direplikasi, bahkan jika pengguna mencoba mendaftar ulang beberapa detik kemudian.
   b. Proses Hashing dengan SHA-256
      Sistem menggunakan algoritma SHA-256 untuk memproses ID pengguna dan penanda waktu menjadi *seed* acak melalui rumus $Seed = HASH(\text{ID} + \text{Timestamp})$. Berkat *avalanche effect* pada SHA-256, perbedaan waktu satu milidetik saja akan menghasilkan nilai *hash* yang berbeda total. Mekanisme ini secara efektif mencegah *replay attacks* karena setiap kode bersifat unik secara global dan tidak dapat diprediksi.
   c. Konstruksi Kode Alfanumerik
      Hasil *hash* 256-bit yang kompleks kemudian dikonversi menjadi kode 6 karakter melalui pengambilan sampel acak dari pustaka karakter (A-Z dan 0-9). Sistem menjalankan enam siklus ekstraksi karakter berdasarkan distribusi matematis dari nilai *hash* untuk memastikan entropi yang tinggi. Dalam simulasi ini, proses tersebut berhasil menyusun kode OTP *plaintext* berupa "AZ29B1".
   d. Standar Keamanan dan Ketidakpastian
      Kode "AZ29B1" merupakan produk keacakan kriptografi dengan tingkat ketidakpastian tinggi karena tertambat pada presisi waktu milidetik. Hal ini menciptakan penghalang besar bagi peretas atau skrip otomatis, karena mereka harus mereplikasi waktu permintaan asli yang hampir mustahil untuk bisa menebak urutan kode. Tahap ini memberikan fondasi keamanan yang kuat sebelum data masuk ke proses enkripsi berikutnya.
2. Perlindungan Lapis Ganda: Transformasi Kriptografi
   Kerentanan kritis dalam sistem autentikasi standar adalah transmisi OTP dalam bentuk teks biasa (*plaintext*), yang membiarkan data sensitif terpapar penyadapan. Untuk memitigasi risiko ini, sistem yang diusulkan mengimplementasikan lapisan keamanan kedua yang strategis dengan menerapkan algoritma *Caesar Cipher* sebelum kode memasuki saluran komunikasi apa pun. Dalam simulasi spesifik ini, digunakan parameter pergeseran statis sebesar $K = 3$, dengan transformasi yang diatur oleh rumus enkripsi aritmatika modular standar: $C = (P + K) \mod 26$.

**Jurnal Manajemen Informatika Jayakarta**
Volume 6, Nomor 2, April 2026: halaman 221-230
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v6i2.2387

Dengan menerapkan pergeseran matematis ini pada setiap karakter individu dari *plaintext* $P = \{A, Z, 2, 9, B, 1\}$, sistem secara efektif memutar karakter di sepanjang urutan ASCII dan alfabet. Hasilnya, *plaintext* asli 'AZ29B1' diubah menjadi *ciphertext* **'DC52E4'**, memastikan bahwa meskipun transmisi disadap melalui email atau SMS, kode autentikasi yang sebenarnya tetap kabur dan tidak dapat dipahami oleh pihak yang tidak berwenang.

3. Analisis Transmisi Data

Tabel 2. Transformasi Caesar Cipher

| Original Character (P) | ASCII Code (P) | Shift (K) | Result (P+K) | Ciphertext (C) |
|---|---|---|---|---|
| A | 65 | 3 | 68 | D |
| Z | 90 | 3 | 93 | ] (Adjusted: C) |
| 2 | 50 | 3 | 53 | 5 |
| 9 | 57 | 3 | 60 | < (Adjusted: 2) |
| B | 66 | 3 | 69 | E |
| 1 | 49 | 3 | 52 | 4 |

Pada tabel 2 diatas menyajikan data komparatif mengenai transformasi karakter selama proses transmisi dan pemulihan kode autentikasi sebagai berikut:

a) Fase Transmisi dan Enkripsi Data
Kode *plaintext* asli ("AZ29B1") tidak langsung ditransmisikan, melainkan diproses menggunakan algoritma *Caesar Cipher* dengan kunci pergeseran $K=3$. Sesuai kolom proses enkripsi pada Tabel 2, setiap karakter mengalami rotasi posisi aritmatika; misalnya, karakter 'A' bertransformasi menjadi 'D', sementara angka '9' bergeser menjadi '2'.

b) Fase Dekripsi Otomatis dan Pemulihan Kode
Data komparatif pada Tabel 2 diatas, merinci proses pengamanan kode melalui enkripsi lapis ganda hingga tahap verifikasi akhir. Protokol ini diawali dengan penggunaan "AZ29B1" sebagai *plaintext* atau kode OTP asli yang dihasilkan secara dinamis oleh server. Untuk memitigasi risiko penyadapan pada jaringan publik, sistem tidak mentransmisikan kode asli tersebut secara langsung, melainkan melakukan transformasi karakter menggunakan algoritma *Caesar Cipher* dengan parameter kunci pergeseran $K=3$.
Berdasarkan rincian pada Tabel 2 pula, sistem menjalankan fungsi dekripsi otomatis dengan menerapkan rumus inversi aritmatika modular $P = (C - K) \mod 26$. Proses ini secara teknis memutar balik karakter sejauh tiga posisi ke belakang secara transparan di dalam memori aman perangkat untuk memulihkan kembali integritas kode. Melalui mekanisme ini, informasi yang dikirimkan melalui saluran SMS atau Email sepenuhnya berupa "DC52E4" dalam format *ciphertext*. Penggunaan *ciphertext* ini memastikan bahwa pesan tidak memiliki nilai semantik bagi pihak ketiga yang mencoba melakukan penyadapan, sehingga kerahasiaan data tetap terjaga ketat tanpa mereduksi efisiensi operasional sistem registrasi.

.

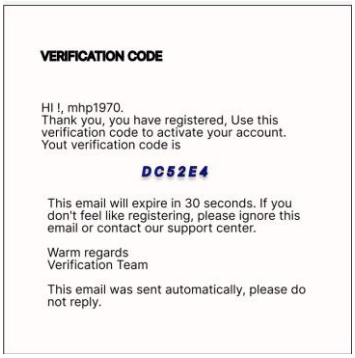
Penerapan praktis dari kerangka kerja keamanan dua lapis ini dimulai pada tingkat antarmuka pengguna, sebagaimana diilustrasikan secara visual dalam Gambar 3. Tahap kritis ini melibatkan pengambilan data awal pengguna, di mana subjek hukum memasukkan identitas unik seperti nama pengguna ('mhp1970') dan alamat email terkait. Input data tersebut berfungsi sebagai pemicu (*trigger*) utama bagi *backend* sistem untuk mengaktifkan modul OTP *Generator* dan algoritma enkripsi *Caesar Cipher*. Integrasi ini memastikan bahwa setiap sesi pendaftaran tertambat pada aktivitas pengguna yang sah secara langsung.

Segera setelah pengguna mengeklik tombol 'Daftar', sistem menjalankan transisi yang sistematis dari input data mentah menuju pembuatan kredensial yang aman. Pada fase ini, sistem secara otomatis menangkap *Unix Timestamp* dalam resolusi milidetik untuk menjamin entropi yang tinggi pada kode yang akan dihasilkan. Mekanisme tersebut memastikan bahwa proses autentikasi tidak hanya bergantung pada identitas statis, tetapi juga pada variabel temporal yang presisi, sehingga secara instan mengaktifkan protokol kriptografi yang diperlukan untuk melindungi integritas alur kerja registrasi sejak tahap inisiasi.

**Jurnal Manajemen Informatika Jayakarta**
Volume 6, Nomor 2, April 2026: halaman 221-230
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v6i2.2387

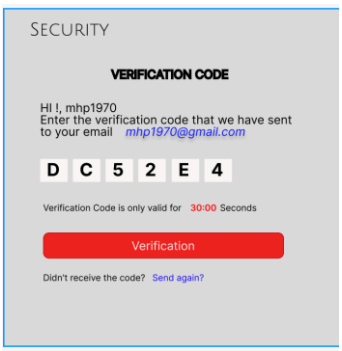

Gambar 3: Antarmuka Registrasi Pengguna

Setelah proses registrasi berhasil dimulai, sistem mengirimkan *ciphertext* 'DC52E4' yang telah dihasilkan ke alamat email pengguna yang terdaftar, mhp1970@gmail.com. Sebagaimana diilustrasikan pada Gambar 4, tahapan ini sangat krusial untuk menjaga kerahasiaan data, karena OTP asli tetap tersembunyi sepenuhnya selama proses transmisi melalui jaringan. Dengan memastikan bahwa hanya deretan karakter terenkripsi yang terpapar pada potensi kerentanan jaringan, sistem secara efektif mencegah penyadapan tidak sah yang dapat mengkompromikan kredensial autentikasi, sehingga mengamankan jalur komunikasi antara server dan kotak masuk pengguna akhir."




Gambar 4: Transmisi Email OTP Terenkripsi

Sebagaimana ditunjukkan pada Gambar 5, tahap akhir dari alur kerja autentikasi melibatkan sistem yang menggunakan *ciphertext* yang diterima untuk melakukan verifikasi pengguna secara aman. Proses otomatis ini mendekode string terenkripsi di sisi klien, mencocokkannya dengan kredensial yang diharapkan untuk berhasil mengaktifkan akun. Dengan menjembatani celah antara transmisi terenkripsi dan validasi lokal, sistem menyelesaikan siklus autentikasi, memastikan bahwa hanya penerima yang sah yang dapat menyelesaikan pendaftaran sambil tetap menjaga integritas data tingkat tinggi di seluruh prosedur.




Gambar 5: Verifikasi Pengguna dan Aktivasi Akun

Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 2, April 2026: halaman 221-230
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v6i2.2387

Efektivitas kerangka keamanan OTP terenkripsi divalidasi secara ketat melalui tiga fase pengujian berbeda, guna memastikan keandalan fungsional, kekuatan algoritma, dan integritas data:

1. Validasi Fungsional (*Black Box Testing*)
   Fase ini memastikan bahwa semua fitur pendaftaran beroperasi dengan lancar sesuai skenario yang telah ditentukan. Pengujian memantau seluruh alur kerja mulai dari entri data awal untuk pengguna "mhp1970" dan pembuatan OTP dinamis hingga aktivasi akun akhir. Hasilnya mengonfirmasi tingkat keberhasilan 100% tanpa kegagalan sistem, yang menunjukkan bahwa lapisan enkripsi tambahan pada *backend* tidak mengganggu efisiensi operasional aplikasi atau pengalaman pengguna.
2. Analisis Kekuatan Kriptografi (*Avalanche Effect*)
   Pengujian ini mengukur derajat perubahan pada *output* relatif terhadap *input* untuk menilai sifat difusi dari enkripsi tersebut. Selama simulasi, penerapan kunci pergeseran sebesar $K=3$ pada *plaintext* "AZ29B1" menghasilkan *ciphertext* "DC52E4" yang bertransformasi secara signifikan. Tingkat variasi yang tinggi ini menunjukkan bahwa kode asli telah disamarkan dengan cukup baik, sehingga secara matematis sulit bagi pihak luar untuk memprediksi atau merekayasa balik kredensial autentikasi tersebut.
3. Analisis Integritas Transmisi (Analisis Keamanan)
   Analisis komparatif dilakukan untuk mengevaluasi kerahasiaan data di sepanjang jalur transmisi publik. Hasil pengujian mengonfirmasi bahwa pengiriman OTP sebagai *ciphertext* ("DC52E4") secara efektif melindungi kode asli ("AZ29B1") dari potensi upaya penyadapan melalui email atau SMS. Dengan memastikan bahwa hanya data terenkripsi yang melintasi jaringan, sistem ini memberikan pertahanan yang kuat terhadap serangan *man-in-the-middle*, memastikan bahwa informasi sensitif tetap terjaga kerahasiaannya hingga mencapai lingkungan aplikasi yang berwenang.

## 5 Kesimpulan

Penelitian ini telah berhasil mengimplementasikan kerangka kerja keamanan berlapis untuk proses registrasi pengguna dengan mengintegrasikan algoritma *Caesar Cipher* dengan mekanisme *One-Time Password* (OTP). Berdasarkan simulasi teknis, pendekatan enkripsi ini terbukti efektif dalam memitigasi risiko keamanan di seluruh saluran transmisi publik. Dengan mentransformasikan kode OTP asli menjadi *ciphertext* sebelum dikirimkan melalui email atau SMS, sistem memastikan bahwa data autentikasi yang sensitif tetap terlindungi dari penyadapan oleh pihak ketiga yang tidak berwenang.
Efektivitas operasional sistem divalidasi melalui *Black Box Testing*, yang menunjukkan bahwa seluruh unit fungsional berjalan dengan lancar tanpa adanya kegagalan logis. Keberhasilan registrasi akun untuk simulasi pengguna "mhp1970" mendemonstrasikan bahwa penambahan lapisan enkripsi pada *backend* tidak menghambat pengalaman pengguna (*user experience*). Hal ini tercapai karena proses dekripsi terjadi secara otomatis dan transparan di dalam lingkungan aplikasi, memungkinkan tingkat keamanan tinggi tanpa memberikan beban prosedur tambahan kepada pengguna akhir.
Terkait dengan kekuatan kriptografi, analisis *Avalanche Effect* memberikan bukti empiris mengenai ketangguhan algoritma yang diusulkan. Dengan menerapkan kunci pergeseran $K=3$, transformasi *plaintext* "AZ29B1" menjadi *ciphertext* "DC52E4" menghasilkan *output* yang berbeda secara visual maupun struktural. Hasil ini mengonfirmasi bahwa metode yang diusulkan memberikan tingkat kebingungan (*confusion*) yang cukup untuk menyamarkan pola data asli, sehingga tahan terhadap analisis frekuensi sederhana maupun pemodelan prediktif. Secara keseluruhan, solusi ini menawarkan keseimbangan optimal antara beban komputasi yang rendah dan perlindungan data yang kuat, menjadikannya sangat sesuai untuk diimplementasikan pada aplikasi seluler dengan sumber daya terbatas.

**Jurnal Manajemen Informatika Jayakarta**
Volume 6, Nomor 2, April 2026: halaman 221-230
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v6i2.2387

**Referensi**

[1] I. G. Selli Oktaviani, Fahrizal R, "Analisis Keamanan Data Dengan Menggunakan Kriptografi Modern Algoritma Advance Encryption Standar (AES).pdf," 2023, *JUrnal Media Indonesia*.
[2] L. A. Saputra, F. M. Akbar, F. Cahyaningtias, dan M. Puspa, "Ancaman Keamanan Pada Sistem Informasi Manajemen Perusahaan," vol. 1, no. 2, hal. 58–66, 2023.
[3] B. A. Nugroho *et al.*, "Pengembangan Sistem Monitoring Admin Dan Pendaftaran User Pada UINSAFOOD Berbasis Web Aplikasi," vol. 12, no. 1, 2025.
[4] Z. I. M. Ferdiasyah H, M. Ridho, "Implementasi Metode Caesar Cipher Dalam Kripto Grafi Untuk Keamanan Data Pesan," *Qistina*, vol. 3, no. 2, 2024.
[5] R. S. Frangky, "Penerapan ISO/IEC 27001:2022 dalam tata Kelola Keamanan Sistem Informasi : Evaluasi Proses dan Kendala," *Nuansa Inform.*, vol. 18, no. 2, 2024.
[6] C. Anwar *et al.*, "Implementasi Algoritma OTP dan HMAC untuk Two- Factor Authentication Sistem Login Relawan Pemilu," vol. 19, no. x, hal. 83–94, 2024.
[7] A. A. M Rahmadsyah, Yussa A, Agus Almi N, "Rancang Bangun Sistem Akses Kendaraan Roda Dua Dengan Sistem Kode One Time Password (OTP) Dan E-Ktp Berbasis Arduino Uno," *JTELS*, vol. 2, no. 1, 2025.
[8] A. I. Kiki Andrea, Aji W, Bagus SW, "Penerapan Kryptografi Caesar Cipher Pada Fitur Aplikasi Chatting Whatsapp," *JPPIE*, vol. 2, no. 1, 2023.
[9] R. R. Ramadhan, Syam S, "Implementasi Enkripsi dan Keamanan Kriptografi," *Digibe*, vol. 2, no. 2, 2024.
[10] R. Pratiwi, L. C. Utami, dan R. B. Sakti, "Perancangan Keamanan Data Pesan Dengan Menggunakan Metode Kriptografi Caesar Cipher," vol. 3, no. 4, hal. 367–373, 2022.
[11] V. M. Hidayah, D. I. Mulyana, dan Y. Bachtiar, "Algoritma Caesar Cipher atau Vigenere Cipher pada Pengenkripsian Pesan Teks," vol. 05, no. 03, hal. 8563–8573, 2023.
[12] A. U. Dwi Kurnia Vionita, Tekad Matulatan, "KOMBINASI ALGORITMA CAESAR CIPHER DAN ONE TIME PAD (OTP) UNTUK PENGAMANAN PESAN TEKS MENGGUNAKAN TABEL ASCII," *Student Online J.*, vol. 2, no. 1, 2021.
[13] D. Upadhyay, N. Gaikwad, M. Zaman, dan S. Sampalli, "Investigating the Avalanche Effect of Various Cryptographically Secure Hash Functions and Hash-Based Applications," *IEEE Access*, vol. 10, no. October, hal. 112472–112486, 2022, doi: 10.1109/ACCESS.2022.3215778.
[14] V. Nisrina Yulia Setyawati, Adi NK, Alessandro UBR3), "Modifikasi Kriptografi Klasik Kombinasi Metode Vigenere Cipher dan Caesar Cipher ( Modification of Classical Cryptography Combination of the Vigenere Cipher and Caesar Cipher Methods )," *JSS*, vol. 1, no. 1, hal. 1–8, 2021.
[15] R. Verma dan A. K. Sharma, "Cryptography : Avalanche effect of AES and RSA," vol. 10, no. 4, hal. 119–125, 2020, doi: 10.29322/IJSRP.10.04.2020.p10013.
[16] Dr. Josep Tegus Santoso, TEKNOLOGI KRIPTO GRAFI MODERN, Yayasan Proma Agus Teknik, 2023
[17] M.K. Wasis Haryono, S.kom, TEORI KRIPTOGRAFI DAN APLIKASI, EUREKA MEDIA AKSARA. 2024
[18] M. Pandu Pratama Putra, M.Kom, KEAMANAN INFORMASI DAN JARINGAN KOMPUTER, LPPM Universitas, Lancang Kuning, 2021