Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) p-ISSN: 2355-7699
Vol. 11, No. 3, Juni 2025, hlm. 539-548 e-ISSN: 2528-6579

IMPLEMENTASI ALGORITMA CLEFIA 128 DAN TIME-BASED ONE TIME PASSWORD SEBAGAI TWO-FACTOR AUTHENTICATION UNTUK MENINGKATKAN KEAMANAN PADA PROSES AUTENTIKASI

Munjin Nasyih Annaisaburi[*1], Ari Kusyanti[2], Fariz Andri Bakhtiar[3]

[1,2,3] Universitas Brawijaya, Malang
Email: [1]miinjunn_@student.ub.ac.id, [2]ari.kusyanti@ub.ac.id, [3]fariz@ub.ac.id
*Penulis Korespondensi

(Naskah masuk: 29 November 2024, diterima untuk diterbitkan: 18 Juni 2025)

Abstrak

Autentikasi merupakan proses verifikasi data dengan cara memastikan bahwa pengguna atau *users* adalah pemilik akses yang sah pada sistem. Proses autentikasi sederhana menggunakan metode *single-factor authentication* (SFA) dengan menggunakan *password* atau PIN. SFA memiliki kelemahan karena rentan terhadap serangan seperti *brute force* dan *sniffing*. Efek dari serangan ini berimbas pada kebocoran data. Badan Siber dan Sandi Negara (BSSN) mencatat pada tahun 2023 terdapat 103 insiden dugaan kebocoran data. Insiden ini terjadi karena prosedur pengamanan masih rendah, terutama dalam mengamankan PIN, aplikasi, dan keamanan internet yang menggunakan SFA. Solusi untuk meningkatkan keamanan pada proses autentikasi dilakukan dengan mengkombinasikan kriptografi berupa algoritma Clefia-128 dengan *two-factor authentication* berupa TOTP. Penelitian ini mengimplementasikan algoritma Clefia-128 yang ditulis dalam bahasa pemrograman Python versi 3 untuk proses enkripsi dan dekripsi *secret key* token TOTP pada sistem yang dibangun menggunakan bahasa pemrograman PHP dengan *web-server* XAMPP. Implementasi Clefia-128 dan TOTP pada sistem berhasil meningkatkan keamanan data ketika proses autentikasi *login website*. Hal ini dibuktikan dengan pengujian keamanan dengan metode *cipher-only attack* menggunakan wireshark yang dikombinasikan dengan *brute force* menunjukkan bahwa *ciphertext* yang didapat tidak berhasil dipecahkan. Pengujian berdasarkan *test vector* menunjukkan bahwa Clefia-128 memberikan hasil yang konsisten dan akurat, serta hasil pengujian performa Clefia-128 untuk enkripsi memerlukan waktu 0.0012277 detik dan dekripsi memerlukan waktu 0.0012895 detik.

Kata kunci: *autentikasi, clefia, kriptografi, time-based one-time password, two-factor authentication*

IMPLEMENTATION OF CLEFIA 128 ALGORITHM AND TIME-BASED ONE TIME PASSWORD AS TWO-FACTOR AUTHENTICATION TO IMPROVE SECURITY IN THE AUTHENTICATION PROCESS

Abstract

Authentication is the process of verifying data by ensuring that users are the legitimate owners of access to the system. Simple authentication process uses single-factor authentication (SFA) methods, such as password or PIN. SFA has the disadvantage of being vulnerable to attacks such as brute force and sniffing. The effect of these attacks leads to data leakage. The National Cyber and Crypto Agency, often known as BSSN noted that in 2023 there were 103 incidents of suspected data leakage. These incidents occur because security procedures are still low, especially in securing PINs, applications, and internet security that use SFA. The solution to improve security in the authentication process is to combine cryptography, specifically the Clefia-128 algorithm, with TOTP as two-factor authentication. This study implements the Clefia-128 algorithm written in the Python version 3 for the encryption and decryption process of the secret key in the TOTP token generation which is implemented on the system using the PHP programming language with the XAMPP web-server. The implementation of Clefia-128 and TOTP on the system successfully increases the security of user data during the website login authentication process. This is proven by security testing with the cipher-only attack method using wireshark combined with brute force showing that the ciphertext was not successfully cracked. Test vector show that Clefia-128 provides consistent and accurate results, and the results of Clefia-128 performance testing for encryption takes 0.0012277 seconds and decryption takes 0.0012895 seconds.

Keywords: *authentication, clefia, cryptography, time-based one-time password, two-factor authentication*

1. PENDAHULUAN

Autentikasi merupakan proses verifikasi data untuk memastikan keamanan suatu akun atau sistem (Coding Studio, 2023). Autentikasi digunakan untuk memastikan bahwa pengguna atau *users* merupakan pemilik akses yang sah pada sistem. Autentikasi berperan sebagai lapisan keamanan utama dalam melindungi data sensitif saat proses *login* sistem dengan menggunakan *password* atau PIN. Proses autentikasi ini disebut *single-factor authentication* (Ometov, et al., 2018).

Metode S*ingle-factor authentication* dinilai tidak aman karena rentan terkena serangan, seperti *brute force* dan *sniffing* yang menargetkan informasi atau kredensial penting (Gunson, et al., 2011). *Brute force* merupakan serangan yang mencoba semua kombinasi *input* berupa karakter, angka, maupun simbol untuk mendapatkan kombinasi yang tepat (Sinaga & Nuraisana, 2021). Sedangkan *Sniffing* merupakan teknik serangan yang menargetkan proses autentikasi dengan cara mengamati dan mencuri pada *traffic data* jaringan (Kulshrestha & Dubey, 2014). Efek dari serangan-serangan ini berimbas pada kebocoran data sistem.

Pada tahun 2023, terdapat adanya 103 dugaan insiden kebocoran data. Total insiden terbanyak yaitu 20 kasus kebocoran data yang terjadi pada bulan Maret dan 15 kasus yang terjadi pada bulan Desember 2023 yang menyerang individu, perusahaan, hingga instansi pemerintah (BSSN, 2023).Target utama dari *sniffing* adalah informasi sensitif seperti *username* dan *password*. Kasus tersebut terjadi karena pengamanan akun pribadi masih rendah, khususnya dalam mengamankan sandi PIN, aplikasi, dan keamanan pada internet (Wulandari, 2020).

Langkah yang digunakan untuk meningkatkan keamanan dari serangan *brute force* dan *sniffing* pada proses autentikasi adalah dengan menerapkan *two-factor authentication* (2FA). Mekanisme ini bertujuan untuk menambah lapisan keamanan dengan cara mengirimkan token kepada pengguna sebagai bagian dari proses autentikasi. Beberapa contoh implementasi 2FA adalah penggunaan *One-time Password* (OTP), teknologi biometrik seperti pemindaian sidik jari dan pengenalan wajah, serta aplikasi tambahan seperti *Google Authenticator* (Fruhlinger, 2024). Berdasarkan contoh yang telah disebutkan, *Time-based One Time Password* (TOTP) merupakan bentuk pengamanan yang lebih canggih daripada OTP dan memiliki kelebihan dengan tidak menyimpan token pada *database*. TOTP menghasilkan token sekali pakai, serta memiliki interval waktu hingga token kedaluwarsa untuk menghasilkan token baru. Token diperoleh dengan cara menggabungkan *secret key* dengan *current time* yang diubah kedalam bentuk *unix timestamp* (Ungkawa, et al., 2017). Meskipun terlihat aman, terdapat celah pada *secret key* pada metode TOTP yang menggunakan *base32 encoder* sebagai fitur keamanan yang memungkinkan diserang dengan metode *brute force*. Oleh karena itu, perlu adanya mekanisme enkripsi untuk melindungi *secret key* tersebut.

Enkripsi merupakan metode untuk menyembunyikan informasi dengan cara mengubahnya menjadi bentuk-bentuk yang tidak dapat dibaca (Loshin, 2020). Dalam kesepakatan internasional, AES ditetapkan sebagai standar algoritma enkripsi (NIST, et al., 2001). Selain itu, terdapat algoritma enkripsi lain yaitu Clefia. Algoritma Clefia memiliki tingkat efisiensi yang lebih tinggi daripada AES dan telah ditetapkan sebagai standar internasional untuk kategori *lightweight cryptography* pada tahun 2012. Clefia dikembangkan oleh Sony dan diluncurkan ke publik pada tahun 2007. Clefia memiliki tingkat keamanan *block cipher* yang tinggi karena algoritma ini memiliki ukuran blok 128 bit, serta variasi panjang kunci 128 bit, 192 bit, dan 256 bit. Selain faktor keamanan, waktu komputasi merupakan faktor yang menentukan seberapa cepat dan efisien suatu algoritma dalam mengamankan data (Sony Corporation, 2007). Algoritma enrkipsi telah diuji menggunakan superkomputer dari National University of Defense Technology di China yang mampu memproses 33,86 x 2^{50} operasi *floating point* per detik. Dengan demikian, diperlukan waktu (2^{128} / (33,86 x 2^{50}) x 365 x 24 x 60 x 60) detik untuk melakukan *brute force* algoritma enkripsi 128 bit (Cox, 2018).

Berdasarkan uraian di atas, penelitian ini akan difokuskan pada peningkatan keamanan pada proses autentikasi dengan mengimplementasikan algoritma Clefia-128 dan TOTP sebagai *two-factor authentication.*

2. LANDASAN KEPUSTAKAAN

2.1 Kajian Pustaka

Kajian pustaka memuat objek studi yang serupa yaitu algoritma Clefia dan TOTP sebagai dasar dan referensi, serta sebagai bahan perbandingan untuk memperkuat analisis dan hasil yang diperoleh.

Penelitian pertama berjudul "*Implementasi TOTP (Time-Based One-Time Password) untuk Meningkatkan Keamanan Transaksi E-Commerce*" yang dilakukan oleh Ibnu Daqiqil Id, Sukamto, dan Evfi Mahdiyah pada tahun 2016 (Id, et al., 2016). Penelitian tersebut menggunakan pendekatan beorientasi objek berupa *Unified Approach* untuk pengembangan sistem dengan menerapkan TOTP sebagai 2FA saat melakukan pembayaran. Client harus memasang *authentication app* yaitu Google Authenticator untuk mendapatkan token TOTP, token diperoleh dengan cara *scan* QRCode atau memasukkan *key*, tetapi terdapat kelemahan dalam mengamankan *secret key* yaitu dengan menggunakan *base32 encoder* yang memiliki risiko terhadap serangan *sniffing* dan *brute force*. Berdasarkan hasil penelitian tersebut, dapat dikembangkan untuk

memperkuat proses autentikasi dengan melakukan enkripsi pada *secret key* TOTP menggunakan algoritma Clefia sebagai lapisan keamanan tambahan.

Penelitian kedua berjudul *"Implement Time-Based One Time Password and Secure Hash Algorithm 1 for Security of Website Login Authentication"* yang dilakukan oleh Henki Seta, Theresia Wati, dan Ilham Cahya Kusuma pada tahun 2019 (Seta, et al., 2019). Penelitian tersebut mengaplikasikan 2FA dengan cara mengkombinasikan TOTP dan SHA-1 pada *website* yang bertujuan untuk menangani pencurian data pengguna. Dilakukan tes sebanyak 100 kali menggunakan Wireshark untuk mendapatkan kesimpulan bahwa dengan menggunakan TOTP dan SHA-1 yang memiliki interval waktu 30 detik tiap token sudah cukup untuk mencegah pencurian akun, namun terdapat kelemahan pada *secret key* karena hanya menggunakan *base32 encoder*. Hasil dari penelitian tersebut dapat dikembangkan dengan cara mengganti *base32 encoder* dengan algoritma enkripsi sehingga hasil yang ingin dicapai dari penelitian ini terpenuhi, yaitu memperkuat proses autentikasi dengan menambahkan proses enkripsi untuk *secret key* TOTP menggunakan algoritma Clefia sebagai layer keamanan tambahan.

Penelitian ketiga berjudul *"Analisis Algoritma CLEFIA 128 Bit Jenis Block Cipher untuk Pengamanan Teks"* yang dilakukan oleh Rivalri Kristanto Hondro pada tahun 2020 (Hondro, 2020). Penelitian tersebut menggunakan Clefia-128 dengan bahasa pemrograman C++ yang bertujuan untuk mengamankan teks. Penelitian tersebut menjelaskan cara kerja Clefia, menguji Clefia untuk enkripsi teks, serta menguji performa Clefia 128 bit. Hasil pengujian menunjukkan bahwa Clefia memberikan nilai kebingungan (confusion) yang baik, serta rata-rata waktu 0,101 ms untuk proses enkripsi yang menunjukkan bahwa Clefia merupakan algoritma yang efisien. Berdasarkan hasil penelitian tersebut, dapat dikembangkan untuk meningkatkan keamanan pada proses autentikasi dengan mengimplementasikan algoritma Clefia dan TOTP sebagai *two-factor authentication* (2FA).

Jurnal berjudul *"The 128-bit Blockcipher CLEFIA - Algorithm Specification"* yang dipublikasikan oleh Sony Corporation pada tahun 2007 (Sony Corporation, 2007), menguraikan spesifikasi secara detail dari algoritma Clefia sebagai *lightweight block cipher*, serta kelebihan dari Clefia yang menawarkan *high-level security* dan performa tinggi pada *software* dan *hardware* untuk masing-masing 128, 192, dan 256 bit key. Penelitian tersebut digunakan sebagai referensi utama dalam pembuatan algoritma Clefia serta sebagai jurnal acuan untuk mendapatkan hasil yang ingin dicapai dalam penelitian ini, yaitu meningkatkan keamanan proses autentikasi dengan mengimplementasikan algoritma Clefia dan TOTP sebagai 2FA.

Jurnal berjudul *"The 128-bit Blockcipher CLEFIA - Design Rationale"* yang dipublikasikan oleh Sony Corporation pada tahun 2007 (Sony Corporation, 2007), menguraikan desain algoritma Clefia dengan mempertimbangkan aspek fundamental seperti keamanan, kecepatan, dan biaya implementasi. Penelitian tersebut digunakan sebagai referensi pendukung untuk menambah pemahaman mengenai algortima Clefia, terutama dalam hal desain, sehingga hasil yang ingin dicapai dari penelitian ini terpenuhi, yaitu mengimplementasikan algoritma Clefia dan TOTP sebagai *two-factor authentication* untuk meningkatkan keamanan proses autentikasi.

2.2 Kriptografi

Kriptografi merupakan Teknik untuk menghasilkan kerahasiaan pesan. Jika pada Bahasa Yunani memiliki arti khusus, yaitu *secret writing* (Sharma, et al., 2017). Orang secara global menggunakan kriptografi untuk melindungi data maupun informasi penting (Katz & Lindell, 2014). Algoritma kriptografi yang ditetapkan secara internasional sebagai algoritma standar adalah AES-128 (NIST, et al., 2001). Namun, bukan berarti tidak terdapat algoritma enkripsi lain yang lebih baik dari AES.

Dalam kriptografi, informasi yang ingin disembunyikan disebut *plaintext*. Proses menyembunyikan *plaintext* disebut enkripsi. Hasil enkripsi disebut *ciphertext* yang memiliki sifat acak dan rahasia. Proses mengubah *ciphertext* menjadi *plaintext* disebut dekripsi. Semua proses tersebut dibungkus dengan aturan yang diatur dalam algoritma enrkipsi. (Piper & Murphy, 2002).

2.3 Two-Factor Authentication (2FA)

Two-Factor Authentication merupakan fitur keamanan yang menggunakan dua metode untuk proses autentikasi, artinya pengguna harus memasukkan informasi tambahan agar dapat mengakses sumber daya pada sistem (Liu, et al., 2023). Proses autentikasi pengguna menjadi ganda berawal dari memasukkan *username* dan *password* saat *login*, kemudian autentikasi dilanjutkan dengan memasukkan token yang dikirimkan ke nomor telepon atau *email* yang terhubung dengan akun pengguna (Olbinson & Jonifan, 2022).

2.4 One-Time Password (OTP)

One-Time Password merupakan metode yang dapat menghasilkan token untuk sekali pakai. OTP berfungsi sebagai mekanisme untuk autentikasi tambahan, oleh karena itu termasuk kedalam 2FA (Rosano, et al., 2018).

HMAC-based One-time Password (HOTP) merupakan metode OTP yang menggunakan teknik kriptografi untuk memastikan integritas dan keaslian data dengan menggunakan *hash function* dan *secret*

key. HOTP menggunakan *counter value* yang dimulai dari 0 sebagai *moving factor*. Token HOTP setidaknya terdiri dari 6 digit angka. HOTP menghasilkan token dengan cara menggabungkan *secret key* dengan *sequence value*, kemudian dilakukan *hashing* untuk menghasilkan *digest* sebesar 160 bit, lalu dipotong secara dinamis agar keluaran menjadi 6 hingga 8 digit angka (M'Raihi, et al., 2005).

Time-based One-time Password (TOTP) merupakan sebuah metode OTP yang mengunakan *counter value* berupa interval waktu. TOTP menghasilkan *output* berupa token baru tiap interval waktu yang ditetapkan (M'Raihi, et al., 2011). Standar interval waktu TOTP adalah 30 detik. TOTP menghasilkan token dengan cara meggabungkan *secret key* dengan *current time* yang diubah kedalam bentuk *unix timestamp*. Cara kerja ini memungkinkan TOTP untuk tidak menyimpan token pada database (Sony Corporation, 2007).

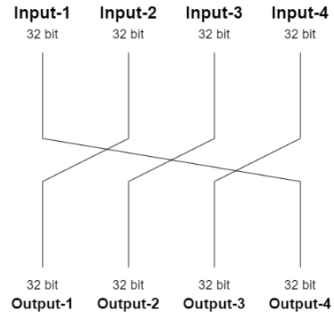
2.5 Clefia

Clefia merupakan algoritma kriptografi berbasis *block cipher* yang dikembangkan oleh Sony pada tahun 2007. Clefia ditetapkan sebagai Standar Internasional untuk kategori *lightweight cryptography* pada tahun 2012. Clefia diklaim merupakan algoritma yang efisien dan memiliki tingkat keamanan *block cipher* yang tinggi. Algoritma ini memiliki ukuran 128 bit blok, sedangkan untuk kuncinya memiliki panjang 128 bit, 192 bit, dan 256 bit (Sony Corporation, 2007).

Clefia memiliki total *round* yang bervariasi. Clefia dengan kunci 128 bit, 192 bit, dan 256 bit secara berurutan memiliki total 18 *round*, 22 *round*, dan 26 *round*. Clefia memiliki *rate gate efficiency* tinggi dan performansi cepat sehingga ideal digunakan pada perangkat keras dan lunak (Sony Corporation, 2007).

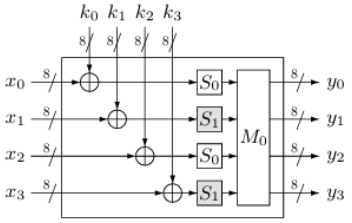
Clefia terdiri dari dua proses utama yaitu *key scheduling* dan *data processing*. Clefia memiliki struktur fundamental yaitu *Generalized Feistel Network* (GFN). Clefia menggunakan 4-*branch* GFN untuk kunci 128 bit, sedangkan 192 bit dan 256 bit menggunakan 8-*branch*. GFN pada algoritma Clefia disimbolkan dengan $GFN_{(d,r)}$ di mana d merupakan banyak *line* atau *branch* pada *feistel network* dan r merupakan banyak *round*. Setiap *input line* memiliki ukuran 32 bit yang menghasilkan *output* sebesar 32 bit tiap *line*.

Gambar 1 merupakan GFN dengan 4-*line*. Tiap round (r) pada Clefia dapat memiliki beberapa variabel yaitu *Whitening Key* (WK), *Round Key* (WK), dan *F-function*. WK pada proses enkripsi dan dekripsi hanya terdapat pada *round* pertama dan terakhir, sedangkan *F-function* terdapat pada setiap *round*. *F-function* pada Clefia terdiri dari dua fungsi yaitu F0 dan F1.

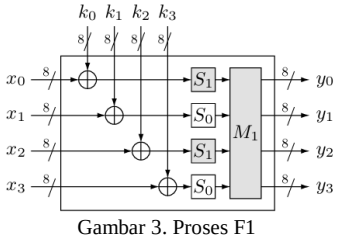


Gambar 1. GFN 4-branch

Pada GFN dengan 4 *line*, F0 mengambil *input line-1* yang diproses dengan RK[2i], sedangkan F1 mengambil *input line-3* yang diproses dengan RK[2i+1]. Pada *F-function* terdapat proses substitusi yaitu sbox dan permutasi yaitu *diffusion matrix*.



Gambar 2. Proses F0



Gambar 3. Proses F1

Diffusion matrix pada algoritma Clefia-128 digunakan untuk memperkuat pertahanan dari serangan salah satunya adalah *Diffusion Switch Mechanism* (Sony Corporation, 2007).

$$M0 = \begin{pmatrix} 0x01 & 0x02 & 0x04 & 0x06 \\ 0x02 & 0x01 & 0x06 & 0x04 \\ 0x04 & 0x06 & 0x01 & 0x02 \\ 0x06 & 0x04 & 0x02 & 0x01 \end{pmatrix}$$

$$M1 = \begin{pmatrix} 0x01 & 0x08 & 0x02 & 0x0a \\ 0x08 & 0x01 & 0x0a & 0x02 \\ 0x02 & 0x0a & 0x01 & 0x08 \\ 0x0a & 0x02 & 0x08 & 0x01 \end{pmatrix}$$

Proses perkalian vektor dan matrix pada diffusion matrix menggunakan prinsip Galois fields $GF(2^8)$ primitive polynomial $z^8 + z^4 + z^3 + z^2 + 1$.

Key Scheduling

Proses *key scheduling* menghasilkan *whitening key* (WK) dan *round key* (RK) yang digunakan untuk *data processing*. *Key scheduling* memiliki dua tahap yaitu membuat *intermediate key* (L), lalu membuat WK dan RK. *Constant value* digunakan untuk mendapatkan L dan RK. Satu blok *constant value* pada Clefia-128 bit memiliki 60 *constant* yang dibagi

menjadi 24 *constant* untuk mendapatkan L dan 36 *constant* untuk RK. Tahap selanjutnya adalah membuat *Intermediate Key* (L) yang diperoleh dari *Key* dan *constant value* melalui proses $GFN_{(4,12)}$.

Pseudocode 1. Intermediate Key

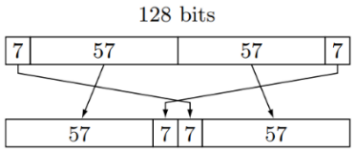
```
GFN(4,12) ← ((Key), (constant_value)):
Input:
    -   Input dibagi 4 bagian masing-masing 32 bit.
    -   24 Constant yang masing-masing 32 bit
Output:
    -   X0, X1, X2, X3 yang masing-masing 32 bit
    -   L ← [X0 + X1 + X2 + X3]
Langkah-1:
  X0 = Key[0]
  X1 = Key [1]
  X2 = Key [2]
  X3 = Key [3]
Langkah-2:
  for i=0 in range(12):
    X1 ← X1 xor F0(X0, constant_value[2*i])
    X3 ← X3 xor F1(X2, constant_value[2*i+1])
Langkah-3:
  L0, L1, L2, L3 ← X1, X2, X3, X0
  L ← L3 + L0 + L1 + L2
```

Tahap terakhir dari *key scheduling* adalah menghasilkan WK dan RK. Tahap ini melibatkan *Key* (K) dan *Intermediate Key* (L), serta *constant value* sesuai algoritma Clefia yang digunakan.

Pseudocode 2. Whitening Key

```
Input:    128 bit Key (16 karakter ascii)
Output:   128 bit WK
Langkah-1:
  Key ← [ int( hex(i)[2:], base=16 ) for i in keytext ]
  Key ← decimal: input berupa key
Langkah-2:
  WK ← []
  for i = 0 sampai 3:
    WK ← Key[ i*4 : i*4+4 ]
```

Sebelum masuk pada proses pembuatan RK, terdapat fungsi penting yang digunakan adalah *Double Swap Function*. Fungsi ini menukar 128 bit data yang dibagi menjadi 4 bagian, tiap bagian mengandung sejumlah bit data.



Gambar 4. Struktur Double Swap Function

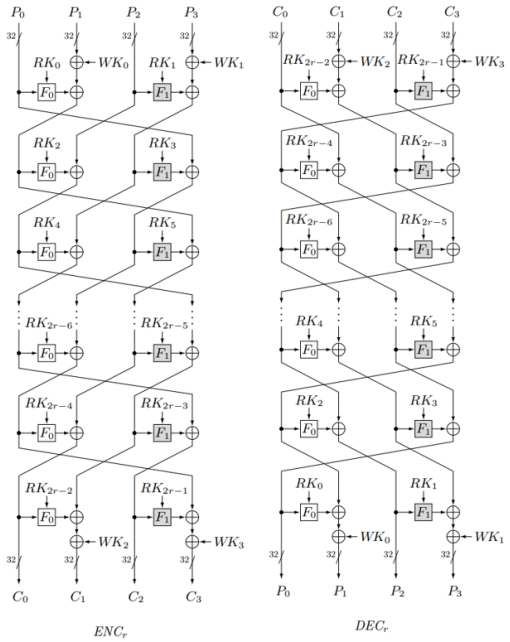
Proses *double swap* diimplementasikan dalam fungsi bernama Sigma yang memiliki input adalah *intermediate key* (L) untuk Clefia-128. Penggunaan fungsi Sigma(X) adalah untuk memperbarui nilai dari *Intermediate Key* (L) tiap dua *round* pada saat proses pembuatan RK. Tujuan utama dari fungsi *double swap* adalah untuk menambah kompleksitas relasi antar RK. Langkah terakhir adalah pembuatan RK.

Pseudocode 3. Round Key

```
generate_rk ← ((Key), (L), (constant_value)):
Input:
    -   Input berupa key sebesar 128 bit
    -   Intermediate key sebesar 128 bit
    -   36 constant yang masing – masing 32 bit
Output:   36 Round Key
Langkah:
  RK ← []
  For i = 0 sampai 8:
    T ← L XOR (con128[24+4i] + con128[24+4i+1]
        + con128[24+4i+2] + con128[24+4i+3])
    L ← Sigma(L)
    if i = ganjil: T ← T XOR K
    For j = 0 sampai 3:
      RK ← T[j*4 : j*4+4]
```

Data Processing

Data Processing memiliki struktur dasar GFN dengan *4-branch* yang disimbolkan dengan GFN(4,r). *Input* enkripsi berupa *plaintext* sebesar 128 bit dan menghasilkan *output* berupa *ciphertext* sebesar 128 bit. Sebaliknya *input* dekripsi berupa *ciphertext* 128 bit dan menghasilkan *output* 128 bit. Clefia-128 memiliki 18 *round* dengan 36 *round key*. Struktur enkripsi dan dekripsi GFN(4,r) direpresentasikan pada Gambar 5.



Gambar 5. Struktur Enkripsi dan Dekripsi GFN(4,r)

2.6 XAMPP

XAMPP merupakan perangkat lunak gratis yang bersifat *open source*. XAMPP juga dikenal sebagai *cross-platform web server* yang memiliki kemampuan untuk menjalankan *web server* secara lokal (Lubis, 2016). XAMPP sebagai *server* yang berjalan secara lokal digunakan untuk menjalankan dan mengetes *website* maupun aplikasi berbasis web serta interaksi *server* dengan *client*.

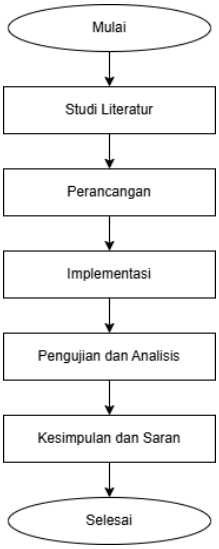
2.7 Model Serangan

Model serangan kriptografi terbagi menjadi 8 tipe, yaitu *brute force, cipher only attack, known plaintext attack, chosen plaintext attack, chosen ciphertext attack, key and algorithm attack, side channel attacks*, dan *replay attacks* (Burge, 2024).

3. METODOLOGI PENELITIAN

3.1 Tahapan Penelitian

Tahapan penelitian dimulai dari mengkaji studi literatur yang berhubungan dengan pemanfaatan algoritma Clefia-128 maupun TOTP, dilanjutkan dengan perancangan, implementasi, pengujian dan analisis, terakhir adalah pengambilan kesimpulan dan saran. Tahapan penelitian ini ditunjukkan pada diagram alur yang tercantum pada Gambar 6.



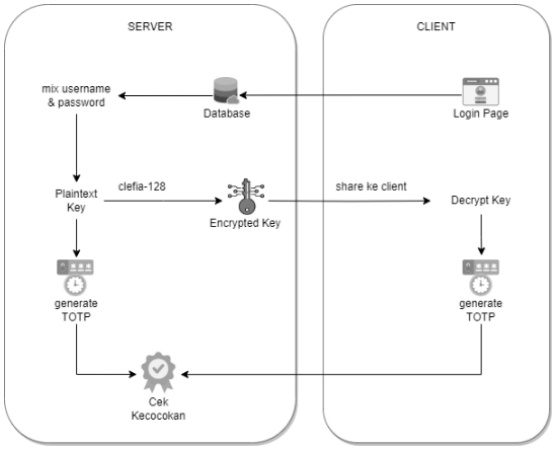
Gambar 6. Diagram Alur Metodologi Penelitian

3.2 Perancangan Sistem

Perancangan sistem membahas mengenai gambaran umum dari sistem yang dibangun pada penelitian ini. Sistem dibuat pada *localhost* menggunakan *database* MySQL, diakses melalui phpMyAdmin yang disediakan oleh *software* XAMPP. Bahasa pemrograman yang digunakan adalah Python dan PHP. Rancangan arsitektur pada sistem direpresentasikan pada Gambar 7.

Langkah awal adalah pengguna mendaftar untuk mendapatkan akun, informasi akun pengguna tersimpan pada *database*. Setelah itu pengguna dapat *login* pada halaman *login website* dan akan dilakukan validasi akun, jika valid maka server akan melakukan *mix username* dan *password* sebagai *key* TOTP. *Key* TOTP dalam bentuk *plaintext* ini yang akan dienkripsi menggunakan Clefia-128. *Key* Clefia sendiri diambil dari *password* akun pengguna.

Ciphertext hasil enkripsi *key* TOTP akan dibagikan ke pengguna dengan cara ditampilkan pada *website* dalam bentuk string dan qr code sebagai alternatif. Kemudian pengguna menuju halaman untuk mendapatkan token TOTP dengan cara memasukkan ciphertext atau *scan qr code* serta memasukkan *password* akun. Token akan diperbarui secara otomatis setiap 30 detik.

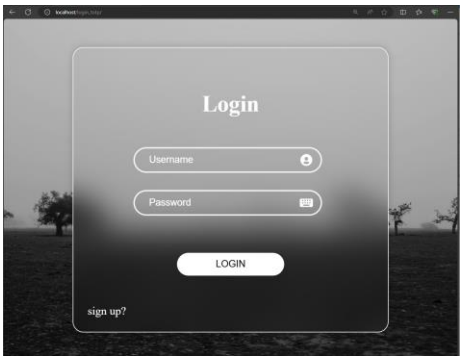


Gambar 7. Rancangan Arsitektur Sistem

Setelah mendapatkan token TOTP yang berjumlah 6 digit, pengguna memasukkan token tersebut pada halaman web lalu menekan tombol *submit*. Saat itulah *web server* menghasilkan TOTP lalu mencocokannya dengan TOTP dari pengguna, jika cocok maka pengguna diarahkan pada *homepage website*.

4. IMPLEMENTASI

Implementasi algoritma Clefia-128 dan TOTP pada sistem yang dibangun pada penelitian ini memiliki tampilan awal seperti pada Gambar 8.

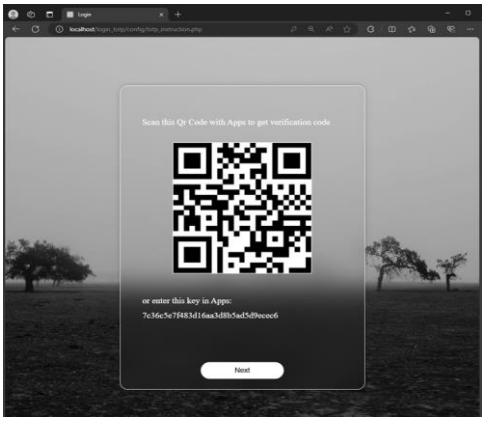


Gambar 8. Tampilan Halaman *Login Website*

Tampilan *secret key* yang sudah dienrkipsi dengan Clefia-128 direpresentasikan pada Gambar 9.

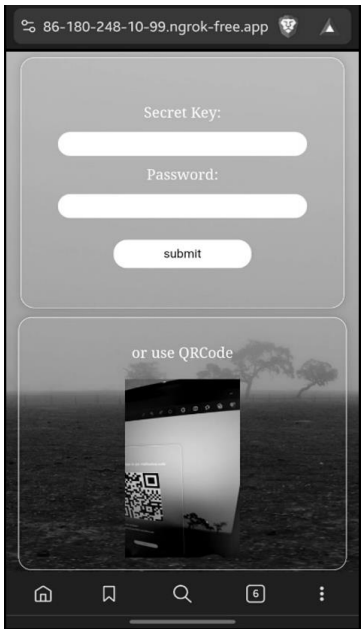
Nilai dari secret key pada gambar diatas adalah: 7c36c5e7f483d16aa3d8b5ad5d9ecec6.

Proses selanjutnya adalah untuk mendapatkan token TOTP. Form Secret key diisi dengan ciphertext yang sudah dihasilkan dari proses diatas, kemudian form password diisi dengan password pengguna. Penulis menambah fitur QRCode yang bersifat optional untuk memudahkan penelitian dalam memasukkan secret key.



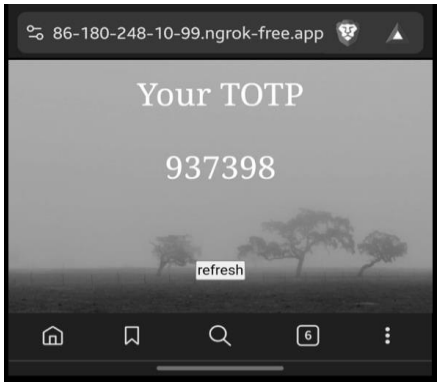
Gambar 9. Tampilan *Secret Key* pada *Website*

Tampilan *website* untuk *generate* token TOTP direpresentasikan pada Gambar 10.



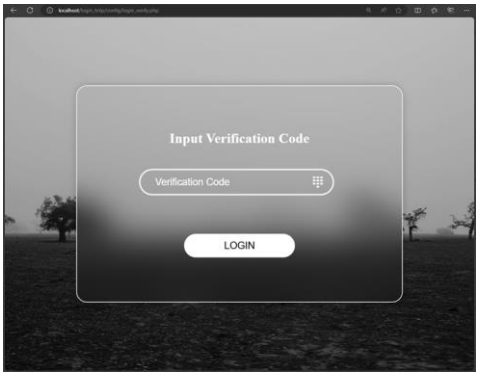
Gambar 10. Tampilan *Generate* Token TOTP

Pengguna menekan *submit* untuk mendapatkan token TOTP. Token secara otomatis diperbarui dalam interval waktu 30 detik. Terdapat tombol untuk *refresh* jika sistem gagal memperbarui token secara otomatis. Token ditampilkan seperti pada Gambar 11.



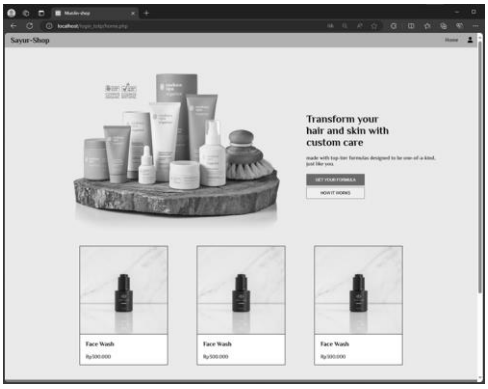
Gambar 11. Tampilan Token TOTP

Pada sistem *website* utama, pengguna memasukkan token TOTP yang telah dibuat sebelumnya pada *form verification code*.



Gambar 12. Tampilan Halaman *Verification Code*

Server melakukan validasi token. Tampilan *homepage website* setelah pengguna berhasil masuk seperti pada Gambar 13.



Gambar 13. Tampilan *Homepage Website*

5. PENGUJIAN DAN ANALISIS

5.1 Pengujian *Test Vector*

Pengujian *test vector* membahas tentang penggunaan data *test vector* yang representatif berdasarkan jurnal acuan. Hal ini untuk memastikan bahwa sistem dapat menghasilkan nilai enkripsi dan dekripsi yang konsisten dan akurat terhadap berbagai jenis *input* data.

Tabel 1. Pengujian Test Vector

Tipe	Test Vector sistem	Test Vector jurnal acuan
Plaintext	0001020304050607 08090a0b0c0d0e0f	0001020304050607 08090a0b0c0d0e0f
Key	ffeeddccbbaa9988 7766554433221100	ffeeddccbbaa9988 7766554433221100
Ciphertext	de2bf2fd9b74aacd f1298555459494fd	de2bf2fd9b74aacd f1298555459494fd

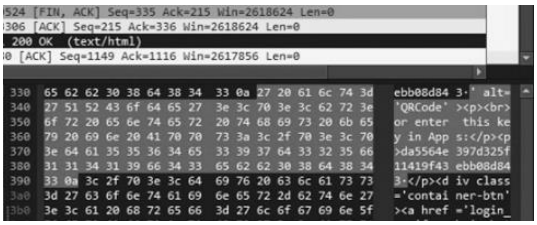
5.2 Pengujian Keamanan

Pengujian keamanan berfokus pada upaya memahami tingkat keamanan yang dimiliki oleh algoritma Clefia-128. Spesifikasi host untuk pengujian direpresentasikan pada Tabel 2.

Tabel 2. Spesifikasi *Host*

Komponen	Spesifikasi
Processor	3,4 GHz AMD Ryzen 7 5700X 8-Core Processor
Graphics	AMD Radeon RX 6700 XT 12 GB
Memory	16 GB 3200 MHz DDR4
Disk	SSD Adata 1000 GB
OS	Windows 10

Pengujian keamanan menggunakan *software* Wireshark untuk melihat *traffic* data.



Gambar 14. Pengujian Keamanan dengan Wireshark

Gambar 14 menunjukkan hasil berupa didapatkan *key* untuk *generate* TOTP, namun *key* dalam bentuk *ciphertext* karena sudah terenkripsi oleh algoritma Clefia-128.

Berdasarkan informasi yang diperoleh, pengujian selanjutnya adalah dengan serangan *Cipher-only attack* yang digabung dengan *brute force.* Pengujian dilakukan dengan program yang dibuat menggunakan Python untuk melakukan *brute force* dengan tujuan mendapatkan *plaintext* dan *key* dari *ciphertext* yang diketahui. Pengujian ditampilkan pada Gambar 15.

Gambar 15. Pengujian Keamanan dengan Brute Force

Pengujian dilakukan selama 24 menit karena sistem *website* dibuat menggunakan PHP yang memiliki *session default timeout* sebesar 24 menit. Hasilnya menunjukkan bahwa program tidak berhasil melakukan *brute force*.

Pengujian selanjutnya adalah *Avalanche Effect* untuk mengetahui pengaruh perubahan bit *plaintext* pada *ciphertext*. Hasil dari pengujian direpresentasikan pada Tabel 3.

Tabel 3. Pengujian Avalanche Effect

Plaintext	Ciphertext
Quick yellow fox	768a1d8fee81c814f461e98053542b40
Wuick yellow fox	3e5ad8d0a7ac34cf843c70ffe0bb5aad
Quick Tellow fox	6d77fbe48b6d925e4885131b2724c7f9
Quick yellow foc	e9d1ed669728e7b8326fc6af7da8b89a

Berdasarkan tabel diatas, mengubah 1 *byte plaintext* mengakibatkan perubahan *ciphertext* secara keseluruhan. Hal ini menunjukkan bahwa algoritma memiliki proses perputaran *key* yang kompleks dan relasi yang kuat antar *round* (Aumasson, 2017). Sehingga dapat disimpulkan bahwa Cleifa-128 memiliki struktur algoritma *block cipher* yang kuat.

5.3 Pengujian Waktu Komputasi

Pengujian waktu komputasi menggunakan sampel bersifat acak sebanyak 31 sampel sesuai dengan *Central Limit Theorem* (CLT) yaitu n >= 30 sampel. Karakteristik sampel yang digunakan memiliki panjang *plaintext* acak, sedangkan panjang *key* maksimal 128 bit.

Tabel 4. Pengujian Waktu Komputasi

Memory (MB)	Enkripsi (detik)	Dekripsi (detik)
10.3320313	0.0005022	0.0004979
10.4179688	0.0007203	0.0007211
10.7304688	0.0004936	0.0005003
10.4062500	0.0004953	0.0005013
10.4453125	0.0004950	0.0004968
10.4023438	0.0004929	0.0004950
10.2851563	0.0011689	0.0012055
10.3320313	0.0007152	0.0007132
10.3671875	0.0017628	0.0017694
10.3164063	0.0007227	0.0007127
10.3085938	0.0004939	0.0005040
10.3320313	0.0004943	0.0004945
10.3945313	0.0004885	0.0004973
10.3320313	0.0004904	0.0004924
10.2773438	0.0009211	0.0009348
10.5000000	0.0057751	0.0067744
10.3945313	0.0004954	0.0004942
10.4101563	0.0004921	0.0005000
10.3320313	0.0004966	0.0005028
10.3554688	0.0004907	0.0005075
10.2734375	0.0004985	0.0005048
10.3515625	0.0011755	0.0012465
10.3437500	0.0007137	0.0007233
10.3320313	0.0005107	0.0005153
10.4179688	0.0137468	0.0143657
10.3593750	0.0007019	0.0007129
10.3281250	0.0004946	0.0005473
10.3281250	0.0005053	0.0005149
10.2890625	0.0004948	0.0005081
10.3906250	0.0004964	0.0005025
10.2929688	0.0005135	0.0005179

Berdasarkan pengujian waktu komputasi yang telah dilakukan, didapatkan rata-rata waktu komputasi algoritma Clefia-128 yang direpresentasikan pada Tabel 5.

Tabel 5. Pengujian Performa Algoritma Clefia-128

Waktu komputasi enkripsi Clefia-128	
Physical Memory usage	10.3670615 MB
Execution time	0.0012277 detik
Waktu komputasi dekripsi Clefia-128	
Physical Memory usage	10.3790454 MB
Execution time	0.0012895 detik

Tabel 6. Perbandingan Clefia-128 dan AES-128

Proses	Clefia-128	AES-128
Enkripsi (detik)	0.0012277	0.0027244
Dekripsi (detik)	0.0012895	0.0028403

Langkah selanjutnya dalam pengujian waktu komputasi adalah melakukan perbandingan antara algoritma Clefia-128 dengan AES-128. Pengujian ini

bertujuan untuk mengetahui algoritma enkripsi mana yang lebih optimal dan sesuai untuk penelitian ini.

Tabel 6 menunjukkan rata-rata waktu komputasi tiap algoritma. Hasil pengujian menunjukkan bahwa algoritma Clefia-128 memiliki waktu komputasi yang lebih cepat serta performa yang lebih baik dibandingkan dengan AES-128 sehingga penggunaan algoritma Clefia-128 dalam penelitian ini sudah tepat.

5.4 Analisis

Hasil pengujian *test vector* algoritma Clefia-128 pada sistem menghasilkan nilai yang sama dengan nilai *test vector* pada jurnal acuan, menunjukkan bahwa sistem yang dibangun dapat menghasilkan output yang konsisten dan akurat.

Hasil pengujian keamanan menunjukkan bahwa implementasi algoritma Clefia-128 dan TOTP yang digunakan sebagai 2FA dapat meningkatkan keamanan ketika proses autentikasi *login* pada *website*. Hal ini dibuktikan saat pengujian keamanan menggunakan *Wireshark* dimana *plaintext* yang merupakan *secret key* untuk menghasilkan token TOTP tidak dapat dibaca karena telah terenkripsi. Selain itu, algoritma Clefia-128 juga mampu bertahan dari serangan *ciphertext only attack* berupa *brute force* dan pengujian *avalanche effect*.

Hasil pengujian waktu komputasi untuk proses enkripsi algoritma Clefia-128 pada sistem adalah 0.0012277 detik, sedangkan proses dekripsi memiliki rata-rata 0.0012895 detik. Hasil ini menunjukkan bahwa proses enkripsi lebih cepat dibandingkan dekripsi, dengan perbandingan sebesar 0.0000618 detik, serta proses enkripsi menggunakan *physical memory* yang lebih sedikit. Selanjutnya, hasil perbandingan waktu komputasi Clefia-128 dengan AES-128 menegaskan bahwa Clefia-128 merupakan pilihan yang lebih optimal untuk penelitian ini.

6. PENUTUP

6.1 Kesimpulan

Berdasarkan hasil penelitian dan analisis yang telah dilakukan menghasilkan kesimpulan sebagai berikut:

1. Penerapan algoritma Clefia-128 untuk mengamankan TOTP pada proses autentikasi terbukti dapat meningkatkan keamanan. Dibuktikan dengan sistem yang mampu bertahan dari berbagai pengujian keamanan.
2. Berdasarkan pengujian waktu komputasi, algoritma Clefia-128 memerlukan waktu 0.0012277 detik untuk proses enkripsi dan 0.0012895 detik untuk proses dekripsi.
3. Penggunaan 2FA berupa TOTP secara *default* mengamankan *secret key* dengan format *base32*. Namun, dengan mengimplementasikan algoritma enkripsi Clefia-128, meskipun terjadi penambahan waktu, sistem dapat menawarkan tingkat keamanan yang lebih tinggi.

6.2 Saran

Saran yang dapat diberikan oleh penulis untuk penelitian selanjutnya adalah sebagai berikut:

1. Penelitian sekarang menggunakan maksimal *input username* 8 karakter dan *password* 8 karakter karena menyesuaikan 1 *block* Clefia sebesar 16 bytes. Penelitian selanjutnya dapat dikembangkan untuk topik serupa dengan menambahkan maksimal kombinasi *input username* dan *password* lebih dari 16 karakter sehingga sistem lebih fleksibel dan dapat menyimpan data yang lebih bervariasi.
2. Penelitian selanjutnya dapat diperluas dengan mengimplementasikan algoritma Cleifa-128 pada sistem dan perangkat yang berbeda karena terbukti akurat, dapat meningkatkan keamanan sistem, dan merupakan algortima yang efisien.

DAFTAR PUSTAKA

AUMASSON, J. P., 2017. *Serious Cryptography: A Practical Introduction to Modern Encryption.* 1st ed. s.l.:No Starch Press.

BASRI, 2016. Kriptografi Simetris dan Asimetris dalam Perspektif Keamanan Data dan Kompleksitas Komputasi. *Jurnal Ilmiah Ilmu Komputer,* 2(2), pp. 16-23.

BSSN, 2023. *Lanskap Keamanan Siber Indonesia 2023*, s.l.: s.n.

BURGE, S., 2024. *8 Types of Attack in Cryptography*. [Online] Tersedia di: <https://internationalsecurityjournal.com/types-of-attack-in-cryptography/#8_Types_of_Attack_in_Cryptography> [Diakses 25 April 2024].

Coding Studio, 2023. *Apa itu Autentikasi? Pengertian, Fungsi dan Cara Kerjanya bagi Keamanan Data.* [Online] Tersedia di: <https://codingstudio.id/blog/autentikasi-adalah/> [Diakses 27 Juli 2024].

COX, G., 2018. *Quora.* [Online] Tersedia di: <https://www.quora.com/How-long-does-it-take-to-break-40-bit-56-bit-128-bit-128-bit-192-bit-and-256-bit-through-a-brute-force-attack> [Diakses 12 January 2022].

FRUHLINGER, J., 2024. *Two-factor authentication (2FA) explained: How it works and how to enable it.* [Online] Tersedia di: <https://www.csoonline.com/article/563753/two-factor-authentication-2fa-explained.html>

GUNSON, N., Marshall, D., Morton, H. & Jack, M., 2011. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers & Security,* Volume 30, pp. 208-220.

HAPSARI, N. S., FATMAN, Y. & I., 2020.

Implementasi Metode One Time Password pada Sistem Pemesanan Online. *Media Informatika Budidarma*, Volume 4, pp. 930-939.

HONDRO, R. K., 2020. Analisis Algoritma CLEFIA 128 Bit Jenis Block Cipher Untuk Pengamanan Teks. Volume 1, pp. 35-38.

ID, I. D., S. & MAHDIYAH, E., 2016. *Implementasi TOTP (Time-Based One-Time Password) Untuk Meningkatkan Keamanan Transaksi E-Commerce*. Batam, s.n.

KATZ, J. & LINDELL, Y., 2014. *Introduction to Modern Cryptography*. 2nd ed. s.l.:CRC Press.

KULSHRESTHA, A. & DUBEY, S. K., 2014. A Literature Review on Sniffing Attacks in Computer Network. *International Journal of Advanced Engineering Research and Science (IJAERS)*, 1(2), pp. 32-37.

KUSTONO, A. S., MAS'UD, I. & NANGGALA, A. Y. A., 2020. Determinants of the Use of E-Wallet for Transaction Payment among College Students. *Journal of Economics, Business, and Accountancy Ventura*, Volume 23, pp. 85 - 95.

KWAK, S. G. & KIM, J. H., 2017. Central limit theorem: the cornerstone of modern statistics. *Korean Journal of Anesthesiology*, 70(2), p. 144–156.

LIU, K. et al., 2023. A Robust and Effective Two-Factor Authentication (2FA) Protocol Based on ECC for Mobile Computing. *Applied Sciences.*

LOSHIN, P., 2020. *TechTarget.* [Online] Tersedia di: <https://www.techtarget.com/searchsecurity/definition/encryption> [Diakses 12 January 2022].

LUBIS, R. P., 2016. *Belajar Web Multimedia Berbasis PHP MySQL XAMPP*. [Online] Tersedia di: <https://adoc.pub/belajar-dengan-xampp-mysql.html> [Diakses 11 January 2022].

MIRONOV, I., 2005. Hash functions: Theory, attacks, and application.

M'RAIHI, D. et al., 2005. *HOTP: An HMAC-Based One-Time Password Algorithm.* [Online] Tersedia di: <https://www.rfc-editor.org/info/rfc4226> [Diakses 27 February 2024].

M'RAIHI, D., Rydell, J., Pei, M. & Machani, S., 2011. *TOTP: Time-Based One-Time Password Algorithm.* [Online] Tersedia di: <https://datatracker.ietf.org/doc/html/rfc6238> [Diakses 27 February 2024].

NIST, et al., 2001. Advanced Encryption Standard (AES). *Federal Inf. Process. Stds. (NIST FIPS).*

OLBINSON, J. & JONIFAN, 2022. Implementasi Teknologi Two Factor Authentication Dengan Menggunakan Metode Time-Based One Time Password (TOTP) Pada Website Private Cloud Storage untuk Guru Bimbingan Konseling. *Jurnal Ilmiah KOMPUTASI*, Volume 21.

OMETOV, A. et al., 2018. Multi-Factor Authentication: A Survey. *Cryptography*, 2(1).

PIPER, F. & MURPHY, S., 2002. *Cryptography: A Very Short Introduction.* s.l.:Oxford University Press.

ROSANO, A., FARABI, N. A. & KUSUMANINGRUM, A., 2018. Perancangan Sistem Internet Banking (IBank) Menggunakan One. *Ilmu-ilmu Sosial*, Volume 3, pp. 1-12.

SETA, H., WATI, T. & KUSUMA, I. C., 2019. 2019 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS). *Implement Time Based One Time Password and Secure Hash Algorithm 1 for Security of Website Login Authentication*, pp. 115-120.

SHARMA, N., PRABHJOT, P. & KAUR, H., 2017. A Review of Information Security Using Cryptography Technique. *International Journal of Advanced Research in Computer Science*, Volume 8.

SINAGA, A. & NURAISANA, 2021. Implementasi Algoritma Brute Force Dalam Pencarian Menu Pada Aplikasi Pemesanan Coffee (Studi Kasus : Tanamera Coffee). *JIKOMSI (Jurnal Ilmu Komputer dan Sistem Informasi)*, 4(1), pp. 6-15.

Sony Corporation, 2007. *Clefia: The 128-bit Blockcipher.* [Online] Tersedia di: <https://www.sony.net/Products/cryptography/clefia/> [Diakses 12 January 2022].

UNGKAWA, U., DEWI, I. A. & PUTRA, K. R., 2017. Implementasi Algoritma Time-Based One Time Password dalam Otentikasi Token Internet Banking.

WULANDARI, G., 2020. Pengaruh Persepsi Manfaat, Kepercayaan Terhadap Minat Penggunaan Kembali E-Money (Ovo, Dana, Go-Pay) pada Mahasiswa. *Repositori Universitas Sumatera Utara.*