JURNAL SITEBA
Volume 2, No. 1, 2023
https://journal.iteba.ac.id/index.php/jurnalsiteba/index

IMPLEMENTASI ALGORITMA CAESAR CIPHER UNTUK KEAMANAN DATA ANGGOTA PERPUSTAKAAN DI UNIVERSITAS XYZ

Alvendo Wahyu Aranski [1], Reni Wahdini [2], Fadillah Anggraini [3], Feby Khairani [4], Iswandani S [5], Meyrina Tamaryska [6]

Institut Teknologi Batam

alvendo@iteba.ac.id

Abstrak

Perkembangan teknologi kini sudah berkembang begitu pesat dan canggih, menyebabkan permasalahan baru dimana kejahatan sudah beralih menjadi kejahatan digital. Sehingga keamanan data harus lebih ditingkatkan untuk menghindari hal-hal yang tidak diinginkan. Universitas XYZ memiliki perpustakaan yang dimana data anggota perpustakaan harus dijaga kerahasiaan nya agar tidak jatuh di tangan yang salah. Saat ini data anggota perpustakaan yang ada pada universitas XYZ masih dilakukan secara manual yaitu dengan menggunakan media kertas, hal ini dirasa masih kurang efisien dan efektif bagi para petugas perpustakaan. Sehingga keamanan data yang ada pada perpustakaan saat ini masih memiliki risiko rusak dan hilang yang masih tinggi. Salah satu langkah yang diambil oleh pihak perpustakaan di universitas XYZ untuk melindungi data anggota perpustakaan yaitu dengan menerapkan algoritma Caesar chipper pada saat anggota perpustakaan melakukan login pada saat mengakses website. Tujuan dari diimplementasikan nya algoritma Caesar chipper ini adalah untuk meminimalisir kerusakan atau kehilangan data anggota perpustakaan yang ada di universitas XYZ, selain itu pekerjaan anggota perpustakaan juga lebih efisien dan efektif.

Key Words: Keamanan data, Enkripsi, Deskripsi, Algoritma Caesar Chipper

1. PENDAHULUAN

Teknologi telah menjadi bagian penting dari kehidupan sehari-hari kita. Teknologi telah membantu dalam berbagai aspek kehidupan kita untuk mempermudah dan mempercepat proses yang sebelumnya dilakukan secara manual. Namun, masih ada beberapa pekerjaan yang belum menggunakan teknologi dengan baik misalnya, data anggota perpustakaan

Universitas XYZ masih dikelola menggunakan media kertas. Untuk membuat kegiatan lebih terorganisir dan efisien, hal ini harus diselesaikan. Dengan menggunakan sistem informasi pengelolaan data perpustakaan berbasis website serta penerapan algoritma Caesar Cipher sebagai metode pengamanan.

Salah satu teknik enkripsi sederhana yang masih digunakan hingga hari ini adalah algoritma Caesar Cipher, yang dibuat oleh Julius Caesar pada era Romawi kuno. Prinsip dasar algoritma ini adalah mengubah setiap huruf dalam pesan dalam urutan alfabet sebanyak langkah tertentu. Misalnya, huruf "A" dapat digeser menjadi "D", huruf "B" dapat digeser menjadi "E", dan seterusnya. Dengan menggunakan algoritma Caesar Cipher sebagai metode pengamanan dalam sistem pengelolaan data anggota perpustakaan Universitas XYZ dapat melindungi data pribadi dan menjaga kerahasiaan data.

Di Indonesia, algoritma Caesar Cipher telah dibahas sebagai metode pengamanan dalam beberapa jurnal. Sebagai contoh, Sumarsono dan Widodo (2017) meneliti penggunaan algoritma Caesar Cipher dalam sistem keamanan data jaringan komputer. Selain itu, Prayudi dan Fatimah (2020) membahas penggunaan algoritma ini pada sistem keamanan pesan teks dalam komunikasi online. Hasil penelitian menunjukkan bahwa algoritma Caesar Cipher dapat digunakan secara efektif sebagai metode pengamanan dalam berbagai situasi.

Penerapan algoritma Caesar Cipher sebagai metode pengamanan dalam konteks pengelolaan data anggota perpustakaan di Universitas XYZ dapat memberikan perlindungan yang cukup baik. Dengan menggunakan algoritma ini, data sensitif seperti nomor identitas, alamat, atau riwayat peminjaman buku dapat dienkripsi, sehingga hanya pihak yang berwenang yang dapat mengakses dan memahami data tersebut. Oleh karena itu, menggunakan teknologi berbasis web dengan algoritma Caesar Cipher sebagai pengamanan dapat memberikan solusi yang efektif dan efisien untuk mengelola data anggota perpustakaan Universitas XYZ.

2. METODELOGI PENELITIAN

2.1 Extreme Programming (XP)

Metode pengembangan ini bertujuan untuk meningkatkan kualitas perangkat lunak yang adaptif, efektif, dan efisien terhadap kebutuhan pengguna. Nilai yang mendasari metode extreme programming adalah communication, courage, simplicity, feedback, dan quality

work. Extreme programming menggunakan 4 langkah kerja yang dilakukan, yaitu sebagai berikut :

a) Planning adalah perencanaan proses bisnis yang di mulai dengan memahami kebutuhan fungsionalitas dan fitur-fitur sistem yang akan dibuat dengan rekayasa perangkat lunak. Pada tahap ini, stakeholder dan programmer bekerjasama untuk menentukkan bagaimana mengelompokkan cerita ke dalam rilis berikutnya atau peningkatan perangkat lunak selanjutnya, yang akan dibangun oleh tim XP.

b) Desain adalah tahap gambaran perancangan atau permodelan dari tahap perencanaan sebagai panduan dalam implementasi. Gunanya untuk memastikan perangkat lunak yang akan dibuat sesuai dengan anggaran, perencanaan, dan selesai tepat pada waktu yang ditargetkan.

c) Coding adalah pengkodean dari penjabaran tahap extreme programming .

d) Testing adalah pada tahap ini unit test yang dikreasikan harus diimplementasikan menggunakan framework yang memungkinkan mereka menjadi otomatis (karenanya, dapat dieksekusi dengan mudah dan berulang-ulang). Hal ini mendorong strategi regresi testing ketika kode dimodifikasi.

2.2 Teknik Pengumpulan Data

Berikut adalah teknik pengumpulan data yang digunakan pada penelitian ini :

a) Wawancara adalah mengumpulkan informasi dengan melakukan tanya jawab langsung dengan narasumber yang terkait dengan penelitian.

b) Observasi adalah melakukan pengamatan langsung terhadap suatu objek yang berkaitan dengan penelitian.

c) Studi literatur adalah mencari informasi dengan cara membaca, mencatat, dan mengelola bahan penelitian.

2.3 Algoritma Caesar Cipher

Dalam kriptografi, sandi Caesar, atau sandi geser, kode Caesar atau Geseran Caesar adalah salah satu teknik enkripsi paling terkenal. Sandi ini termasuk sandi substitusi dimana setiap huruf pada teks terang (plaintext) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet. Algoritma kriptografi ini awalnya digunakan oleh kaisar Romawi bernama Julius Caesar, untuk menyandikan pesan yang dikirimkan ke para gubernur dengan mensubstitusikan satu karakter dengan karakter lain dalam susunan alfabet.

Misalnya, tiap huruf disubstitusi dengan huruf ketiga berikutnya dari susunan abjad. Dalam hal ini kuncinya adalah jumlah pergeseran huruf (yaitu k = 3). Dengan mengkode kan

setiap huruf abjad dengan integer sebagai berikut: A = 0, B = 1, ...,Z = 25, maka secara matematis caesar chipper menyandikan plainteks pi menjadi ci dengan aturan (enkripsi): C = (P+K) mod 94 (5) P = (C-K) mod 94 (6) Untuk proses dekripsi, rumus di atas hanya digunakan saat indeks cipher lebih besar atau sama dengan kunci yang digunakan (C≥K). Pergeseran huruf yang dapat dilakukan adalah mulai 0 sampai dengan 25 karena hanya ada 26 huruf alfabet. Contoh, huruf A diganti dengan huruf C, huruf E diganti dengan huruf J, dan seterusnya.

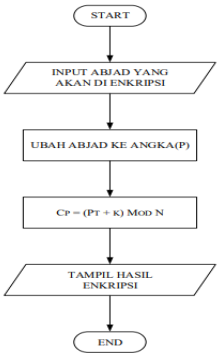
Bagian metode penelitian berisi paparan naratif desain penelitian, sumber data, teknik pengumpulan data, dan analisis data. Isi metode penelitian diketik dengan Baskerville Old Face 12 point, spasi 1,5.

3. ANALISA DAN PERANCANGAN

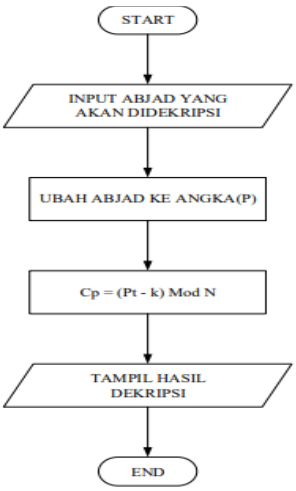
Hasil penelitian menunjukkan bahwa proses enkripsi password saat login aplikasi perpustakaan memberikan tingkat keamanan yang tinggi untuk data-data pengguna. Hal ini mengurangi risiko peretasan yang dilakukan oleh pihak yang tidak bertanggung jawab dan mengurangi potensi adanya penyalahgunaan data pengguna perpustakaan.

Adapun Hasil dan Pembahasan dari penelitian ini sebagai berikut:

a. Flowchart Enkripsi dan Dekripsi



Gambar 1. Flowchart Enkripsi



Gambar 2. Flowchart Deskripsi

b. Algoritma Caesar Chiper

Tabel 1. Tabel deret Alphabet

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19
U	V	W	X	Y	Z				
20	21	22	23	24	25				

Contoh :

Password pengguna perpustakaan dalam bentuk Plaintext (Pi) : 0maribelajar2

Jumlah deret substitusi (key) : 3

Kemudian menentukan index dari Plaintext (Pi) berdasarkan table 1.

Tabel 2. Hasil Konversi index dari Pi

0	M	A	R	I	B	E
0	12	0	17	8	1	4
L	A	J	A	R	2	
11	0	9	0	17	2	

Proses enkripsi dengan Caesar Chiper :

Plaintext : 0maribelajar2

Jumlah deret substitusi (key) : 3

Rumus : Cp = (Pt + k) mod 26

Proses :

0 = (0+3) mod 26 = 3

m = (12+3) mod 26 = 15 (P)

a = (0+3) mod 26 = 3 (D)

r = (17+3) mod 26 = 20 (U)

i = (8+3) mod 26 = 11 (L)

b = (1+3) mod 26 = 4 (E)
e = (4+3) mod 26 = 7 (H)
l = (11+3) mod 26 = 14 (O)
a = (0+3) mod 26 = 3 (D)
j = (9+3) mod 26 = 12 (M)
a = (0+3) mod 26 = 3 (D)
r = (17+3) mod 26 = 20 (U)
2 = (2+3) mod 26 = *5*

Chipertext : 3pdulehodmdu*5*

Proses deskripsi dengan Caesar Chiper :

Chipertext : 3pdulehodmdu*5*
Jumlah deret distribus (key) : 3
Rumus : Cp = (Pt - k) mod 26
Proses :

3 = (3 - 3) mod 26 = 0
p = (15 - 3) mod 26 = 12 (m)
d = (3 - 3) mod 26 = 0 (a)
u = (20 - 3) mod 26 = 17 (r)
l = (11 - 3) mod 26 = 8 (i)
e = (4 - 3) mod 26 = 1 (b)
h = (7 - 3) mod 26 = 4 (e)
o = (14 - 3) mod 26 = 11 (l)
d = (3 - 3) mod 26 = 0 (a)
m = (12 - 3) mod 26 = 9 (j)
d = (3 - 3) mod 26 = 0 (a)
u = (20 - 3) mod 26 = 17 (r)
5 = (5 - 3) mod 26 = 2

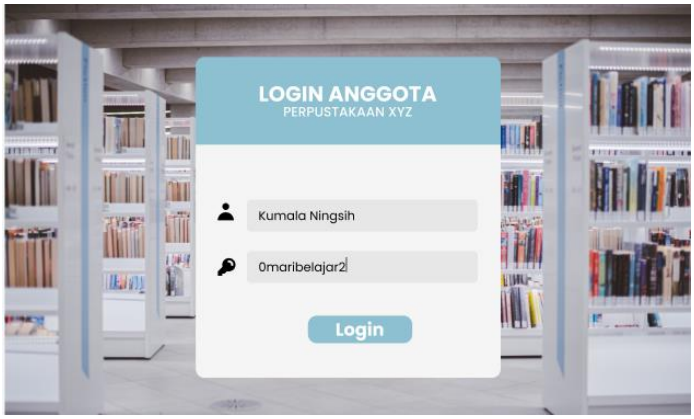
Dengan begini proses enkripsi dan deskripsi menggunakan Algoritma Caesar Chipper dapat bekerja dengan baik untuk membantu mempertahankan keamanan pada password login pengguna perpustakaan

c. Implementasi

Pengguna :

Tampilan Login

Gambar 3. Tampilan Login Pengguna



Database :

Username	Password
Kumala Ningsih	3pdulehodmdu5

Gambar 4. Tampilan Database

Jika dilihat berdasarkan implementasi diatas ketika pengguna mengisikan data login berupa username dan password maka database akan menyimpan data tersebut berdasarkan apa yang telah di input kan pengguna, hanya saja di bagian password database menyimpan datanya ke dalam bentuk yang telah ter enkripsi.

4. KESIMPULAN

Berdasarkan pembahasan diatas dapat disimpulkan bahwa penerapan algoritma caesar chipper memiliki hasil yang efektif untuk digunakan sebagai password login website perpustakaan, sehingga kerahasiaan data anggota mahasiswa dapat terjaga dengan baik.

Diharapkan tingkat keamanan data dapat ditingkatkan dengan menggabungkan dua algoritma untuk memberikan hasil yang lebih baik atau menggabungkan dua pola pergeseran yang berbeda, sehingga sulit untuk menemukan pola dekripsi oleh orang-orang yang ingin menyalah gunakan data tersebut.

REFERENSI

Sumarsono, A., & Widodo, B. (2017). Implementasi Algoritma Caesar Cipher dalam Sistem Keamanan Data pada Jaringan Komputer. Jurnal Teknik Informatika dan Sistem Informasi, 3(2), 77-83.

Prayudi, E., & Fatimah, L. (2020). Penerapan Algoritma Caesar Cipher pada Sistem Keamanan Pesan Teks dalam Komunikasi Online. Jurnal Ilmiah Rekayasa Komputer dan Informatika, 4(2), 58-63.

Angriani, H., & Saharaeni, Y. (2019). Implementasi Algoritma Caesar Cipher pada Keamanan Data Sistem e-voting Pemilihan Ketua Organisasi Kemahasiswaan. Inspiration: Jurnal Teknologi Informasi dan Komunikasi, 9(2), 123-126.

Faqih, F. N., Tahir, M., Ashfarina, Z., Faa'izzani, R. I., Alfarisi, S., & Erfani, F. (2023). Efektivitas Peningkatan Keamanan Login Pada Website Menggunakan Enkripsi Caesar Chipper. Jurnal Adijaya Multidisplin, 1(02), 354-362.

Vebby, V., & Van FC, L. L. (2023). PENERAPAN ALGORITMA CAESAR CIPHER DALAM METODE KRIPTOGRAFI KLASIK PADA PANIC BUTTON. ZONAsi: Jurnal Sistem Informasi, 5(1), 126-136.

Yusup, I. M., Carudin, C., & Purnamasari, I. (2020). Implementasi Algoritma Caesar Cipher Dan Steganografi Least Significant Bit Untuk File Dokumen. Jurnal Teknik Informatika dan Sistem Informasi, 6(3).