Journal of Computation Science And Artificial Intelligence

Journal homepage:
https://jcsai.xjurnal.com/index.php/journal/index

e-ISSN: 3032-4653

Vol. 2, No. 1, 2025

KOMBINASI ALGORITMA BASE64 DAN CAESAR CHIPHER UNTUK KEAMANAN DATA PENYANDANG DISABILITAS PADA DINAS SOSIAL PEMBERDAYAAN PEREMPUAN DAN PERLINDUNGAN ANAK (DSPPPA) KOTA CIREBON

Wahyu Ariandi[1], Yuhano[2], Naufal Imaanullah[3]
Sekolah Tinggi Ilmu Komputer Poltek Cirebon
wahyuariadi@mail.ugm.ac.id , yuhano@stikompoltekcirebon.ac.id, nimaanullah@gmail.com

Abstrak

Keamanan merupakan aspek penting dari suatu data atau informasi, dimana pengiriman data atau informasi membutuhkan keamanan yang tinggi. ada beberapa cara untuk melakukan pengamanan data ataupun pesan, diantaranya adalah dengan menggunakan teknik kriptografi. Kriptografi merupakan seni dan ilmu memproteksi data atau informasi. terdapat dua konsep yang sangat penting yaitu, enkripsi dan dekripsi. Dinas Sosial, Pemberdayaan Perempuan dan Perlindungan Anak (DSPPPA) Kota Cirebon merupakan organisasi perangkat daerah. penelitian ini dilakukan untuk mengolah data disabilitas, dimana pengolahan data masih menggunakan cara manual dan belum data sistem untuk keamanan data disabilitas, yang dimana dalam hal ini yang akan diamankan yaitu berupa nama dan NIK. sistem keamanan data pada penelitian ini menggunakan metode Base64 dan Caesar Chipher. Algoritma Base64 merupakan teknik enkripsi suatu data ke format ASCII yang didasarkan pada bilangan 64, sedangkan algoritma Caesar Chipher merupakan teknik enkripsi yang berjenis subtitusi pengimplementasian pengamanan data tersebut dapat memproteksi data yang dimiliki oleh Dinas Sosial, Pemberdayaan Perempuan dan Perlindungan Anak (DSPPA) Kota Cirebon dari tindak kejahatan siber. Data yang telah melewati 2 kali proses enkripsi akan menghasilkan data acak berupa kombinasi huruf, angka, dan simbol.

Kata kunci: Keamanan Data, Kriptografi, Base64, Caesar Chipher

COMBINATION OF BASE64 AND CAESAR CIPHER ALGORITHM FOR SECURITY OF DATA OF PERSONS WITH DISABILITIES AT THE DEPARTMENT OF SOCIAL SERVICES FOR WOMEN'S EMPOWERMENT AND CHILD PROTECTION (DSPPPA) OF CIREBON CITY

Abstract

Security is an important aspect of data or information, where sending data or information requires high security. There are several ways to secure data or messages, including using cryptography techniques. Cryptography is the art and science of protecting data or information. There are two very important concepts, namely, encryption and decryption. The Office of Social Affairs, Women's Empowerment and Child Protection of Cirebon City is a regional apparatus organization. This research was conducted to process disability data, where data processing still uses manual methods and there is no system data for disability

data security, which in this case will be secured in the form of names and NIK. The data security system in this study uses the Base64 and Caesar Chipher methods. The Base64 algorithm is a data encryption technique to ASCII format which is based on the number 64, while the Caesar Chipher algorithm is an encryption technique that is of the substitution type for implementing data security to protect data owned by the Cirebon City Social, Women's Empowerment and Child Protection Service from cyber crime. Data that has passed 2 times the encryption process will generate random data in the form of a combination of letters, numbers, and symbols.

Kata kunci: *Data Security*, *Cryptography*, *Base64*, *Caesar Chipher*.

1. PENDAHULUAN

Keamanan merupakan aspek penting dari suatu data atau informasi, dimana pengiriman data atau informasi membutuhkan keamanan yang tinggi. Ada beberapa cara melakukan pengamanan data ataupun pesan, diantaranya adalah dengan menggunakan Teknik penyamaran data yang disebut dengan kriptografi.

Kriptografi merupakan seni dan ilmu untuk memproteksi data/informasi dengan mengubahnya menjadi kode tertentu dan ditujukan untuk orang yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali yang berfungsi dalam menjaga kerahasiaan data/informasi. Dalam bidang kriptografi terdapat dua konsep yang sangat penting atau utama yaitu enkripsi dan dekripsi.

Enkripsi adalah proses dimana data/informasi yang hendak diinput diubah menjadi bentuk yang hampir tidak dikenali sebagai data/informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi data/informasi awal [1].

Cybercrime atau kejahatan melalui jaringan internet saat ini semakin tak terbendung. Di Indonesia, kejahatan ini dilakukan untuk pencurian kartu kredit, *hacking* beberapa situs, menyadap transmisi data orang lain, misalnya *email*, dan memanipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki ke dalam program komputer [2]. *Data Forgery*, kejahatan ini dilakukan dengan tujuan memalsukan data pada dokumen-dokumen penting yang ada di internet. Dokumen-dokumen ini biasanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasis *website* [2].

Karena itu pentingnya mengubah data fisik ke data digital yaitu untuk memudahkan pengolahan data, karena data yang sudah berupa data digital dapat mengefisien waktu ketika data sedang diolah, akan tetapi data digital juga mempunyai ancaman dari luar seperti kejahatan siber, dalam hal ini pihak yang tidak bertanggung jawab berusaha untuk melakukan pencurian data yang tersimpan didalam komputer, oleh sebab itu diperlukannya keamanan data secara digital, untuk mengamankan data digital maka diperlukan Teknik kriptografi.

Adapun Teknik kriptografi yang digunakan pada penelitian ini yaitu kombinasi algoritma Base64 dan algoritma Caesar Chipher. Algoritma Base 64 cocok digunakan digunakan sebagai algoritma pembentukan kunci publik yang akan digunakan pada proses enkripsi dan dekripsi data. Dikarenakan sifat algoritma ini yang dapat melakukan penyandian terhadap berbagai jenis data ke dalam format *chiphertext*, sehingga dapat digunakan untuk meningkatkan keamanan pada data [3]. Kemudian algoritma Caesar Chipher metode enkripsi yang populer. Kode ini terdiri dari semua huruf pada teks asli (*plaintext*) disubtitusi dengan kode kemudian berubah menjadi huruf lain yang mempunyai selisih posisi tertentu dalam alfabet, algoritma ini pun dapat digunakan untuk mengamankan data [4].

Dinas Sosial Pemberdayaan Perempuan dan Perlindungan Anak (DSPPPA) Kota Cirebon terletak di Jl. Brigjend Dharsono, Kertawinangun, Kedawung, Cirebon, Jawa

Barat 45153, merupakan Organisasi Perangkat Daerah yang terbentuk pada tanggal 13 September 2016. Dinas Sosial Pemberdayaan Perempuan dan Perlindungan Anak (DSPPPA) Kota Cirebon mempunyai tugas pokok melaksanakan urusan Pemerintahan Daerah berdasarkan asas otonomi dan tugas pembantuan bidang sosial, bidang pemberdayaan perempuan, bidang perlindungan anak dan bidang pemberdayaan masyarakat.

Penelitian ini dilakukan untuk mengolah data disabilitas di Dinas Sosial Pemberdayaan Perempuan dan Perlindungan Anak (DSPPPA) Kota Cirebon. Dimana pengolahan data masih menggunakan cara manual, seperti pengumpulan data disabilitas yang masih berupa *Microsoft Excel* dan pengelompokan data disabilitas juga belum menggunakan aplikasi serta data tersebut belum ada keamanan secara digital.

Permasalahan yang teridentifikasi sebagai berikut :

1. Pengumpulan dan pengolahan data disabilitas yang masih menggunakan *Microsoft Excel* sehingga sulitnya menemukan data disabilitas yang diinginkan memakan banyak waktu.
2. Tidak ada penyimpanan data disabilitas secara sistem.
3. Tidak ada perlindungan untuk data disabilitas itu sendiri sehingga rentan data hilang atau dicuri.

Tujuan dari penelitian ini adalah sebagai berikut :

1. Pembuatan *Website* data Disabilitas.
2. Pengolahan data Disabilitas menggunakan *website*.
3. Pengamanan data disabilitas secara digital menggunakan kombinasi algoritma Base64 dan Caesar Chipher.

2. BAHAN DAN METODE

Aplikasi Kriptografi Keamanan Data Menggunakan Base64
(Azlin, Fitriah Musadat, Jabal Nur, 2018)

Penerapan Kombinasi Algoritma Base64 dan ROT 47 untuk enkripsi database pasien rumah sakit jiwa Prof. DR. Muhammad Ildrem (Rachmat Aulia, Ahmad Zakir, Dian Agung Purwanto, 2018).

Penerapan kriptografi caesar chipher pada fitur chatting sistem informasi freelance (Yuningrat Dwi Putri, Rosihan, Salkin Lutfi, 2019).

Three-Pass Protocol Implementation in Caesar Chipher Classic Cryptography (Boni Oktaviana, Andysah Putera Utama Siahaan, 2016).

Implementation of Base64 algorithm for securing SMS on smartphones (Ros Minarmi, 2018).

1. Pengembangan Perangkat Lunak

1. Metode *prototype*

   Metode *prototype* ini pengembang dan pelanggan dapat saling berinteraksi selama proses pembuatan sistem. Sering terjadi seorang pelanggan hanya mendefinisikan ssecara umum apa yang dikehendakinya tanpa menyebutkan secara detail *output* apa saja yang dibutuhkan, pemrosesan dan data-data apa saja yang dibutuhkan [1].
2. *Unified Modeling Language (UML)*

   Unified Modeling Language merupakan kumpulan diagram-diagram yang sudah memiliki standar untuk membangun perangkat lunak berbasis objek [2].
3. *Use Case Diagram*

Use Case Diagram merupakan diagram yang harus dibuat pertama kali saat pemodelan perangkat lunak berorientasi objek [2].

4. *Activity Diagram*

   Activity Diagram merupakan penggambaran *workflow* (aliran kerja) atau aktivitas dari sebuah sistem atau proses bisnis [2].
5. *Class Diagram*

   Class Diagram merupakan menjelaskan hubungan apa saja yang terjadi antara pada suatu objek dengan objek lainnya sehingga terbentuklah suatu sistem aplikasi [2].

2. Teori Penelitian

1. Keamanan Data

   Secara umum data dikategorikan menjadi data yang bersifat rahasia dan data tidak rahasia. Data yang tidak bersifat rahasia biasanya tidak terlalu penting, data yang penting adalah data

yang bersifat rahasia, dimana setiap informasi yang ada di dalamnya sangat berharga [3].

2. Kriptografi

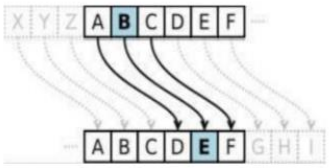
   Cryptography berasal dari bahasa Yunani, menurut bahasanya, istilahnya tersebut terdiri dari kata *crypto* dan *graphia*. Kripto berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan). Kriptografi adalah ilmu atau seni untuk menjaga keamanan pesan, ketika suatu pesan dikirim dari suatu tempat ke tempat lain, isi pesan tersebut kemungkinan dapat disadap oleh pihak lain [4].

3. Algoritma Base64

   Algoritma Base64 merupakan salah satu algoritma *encoding* dan *decoding* suatu data ke dalam format ASCII, yang didasarkan pada bilangan dasar 64 atau bisa dikatakan sebagai salah satu metoda yang digunakan untuk melakukan *encoding* (penyandian) terhadap data *binary* [5].

4. Algoritma Caesar Chipher

   Metode penyandian ini dinamakan Caesar Chipher, merupakan teknik enkripsi yang banyak digunakan. Chipher ini berjenis subtitusi, dimana setiap huruf pada *plaintext* digantikan dengan huruf lain yang tetap pada posisi alfabet [6].



Gambar 3. Pergeseran Huruf

3. HASIL DAN BAHASAN

Hasil Uji Coba Metode

1. Enkripsi Base64
   a. Menentukan *plaintext* yang akan dienkripsi. *Plaintext :* **Naufal.**
   b. Pecah *plaintext* menjadi 3 *bytes.*
      Nau Fal.
   c. Ubah *plaintext* ke dalam bentuk desimal sesuai kode ASCII.

		ASCII			**ASCII**
N	=	**78**	f	=	**101**
a	=	**97**	a	=	**97**
u	=	**117**	l	=	**108**

   a. Ubah desimal ASCII menjadi biner, kemudian gabungkan menjadi 24bit.

		Dec	**Biner**
N	=	78	0100 1110
a	=	97	0110 0001
u	=	117	0111 0101
f	=	102	0110 0110
a	=	97	0110 0001
l	=	108	0110 1100
24bit	Nau	=	0100 1110, 0110 0001, 0111 0101
24bit	fal	=	0110 0110, 0110 0001, 0110 1100

   a. 24bit dipecah menjadi 4 kelompok bit
      Nau = 010011, 100110, 000101, 110101
      fal = 011001, 100110, 000101, 101100
   b. Masing-masing kelompok diubah kenilai desimal

      Nau = 010011, 100110, 000101, 110101
      = 19, 38, 5, 53
      fal = 011001, 100110, 000101, 101100
      = 25, 38, 5, 44
   c. Nilai desimal tersbut menjadi indeks untuk memilih karakter penyusun dari Base64.

Tabel 1. Tabel Base64

Value	Char	Value	Char	Value	Char	Value	Char
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+

15	P	31	f	47	v	63	á.

Nau = 19, 38, 5, 53
= T, m, F, 1
fal = 25, 38, 5, 44
= Z, m, F, s.

Didapat hasil enkripsi menggunakan algoritma Base64 yaitu, **TmF1ZFs**.

2. Enkripsi Caesar Chipher
   a. Menentukan *plaintext*, hasil enkripsi Base64 menghasilkan **TmF1ZFs** akan menjadi *plaintext* pada proses algoritma Base64.
   b. Menentukan jumlah geser (*key*) dan mengganti setiap huruf yang ada dengan jumlah pergeseran huruf yang ditentukan.

Tabel 1 Tabel Indeks Abjad

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

Rumus Enkripsi => C = (P + K) Mod 26

C = *Chiphertext*

P = *Plaintext* (indeks abjad)

K = Pergeseran (*Key*)

Chiphertext = **TmF1zmFs** (hasil enkripsi *Base64*)

K = 7 (*Key* / Pergeseran)

T = (19+7) *mod* 26 = 0 (A)

m = (5+7) *mod* 26 = 19 (t)

F = (5+7) *mod* 26 = 12 (M)

1 = (1+7) *mod* 26 = 8

Z = (25+7) *mod* 26 = 32 (G)

m = (12+7) *mod* 26 = 18 (t)

F = (5+7) *mod* 26 = 12 (M)

s = (18+7) *mod* 26 = 25 (z)

Maka didapat hasil dari enkripsi algoritma Caesar Chipher **AtM8GtMz**.

C. Dekripsi Caesar Chipher

Menentukan *plaintext* dan *key*, hasil dari enkripsi Caesae Chipher akan menjadi *plaintext* kali ini **AtM8GtMz**, *key* = 7.

P = *Plaintext* (indeks abjad)

C = *Chiphertext*

K = Pergeseran (*key*)

C = Atm8GtMz (hasil dekripsi *Caesar Chipher*)

K = 7 (pergeseran / Key)

A = (0 – 7) *mod* 26 = 19 (T)

t = (19 – 7) *mod* 26 = 12 (m)

M = (12 – 7) *mod* 26 = 5 (F)

8 = (8 – 7) *mod* 26 = 1

G = (6 – 7) *mod* 26 = 25 (Z)

t = (19 – 7) *mod* 26 = 12 (m)

M = (12 – 7) *mod* 26 = 5 (F)

z = (25 – 7) *mod* 26 = 18 (s)

Maka didapat hasil dekripsi algoritma Caesar Chipher yaitu **TmF1ZmFs**.

3. Dekripsi Base64
   a. *Plaintext* menggunakan hasil dekripsi Caesar Chipher. Yaitu **TmF1ZmFs**.
   b. Cari nilai desimal setiap karakter dengan menggunakan tabel indeks penyusun Base64.

T = 19
m = 38
F = 5
1 = 53
Z = 25
m = 38
F = 5
s = 44

   c. Ubah masing-masing nilai desimal menjadi bilangan biner lalu kelompokan menjadi panjang 24bit.

TmF1 = 19, 38, 5, 53
= 010011, 100110, 000101, 110101
ZmFs = 25, 38, 5, 44
= 011001, 100110, 000101, 101100

   d. Dalam 24bit dipecah menjadi 3 kelompok
TmF1 = 01001110, 01100001, 01110101
ZmFs = 01100110, 01100001, 01101100
   e. Ubah setiap kelompok kedalam bilangan desimal

TmF1 = 01001110, 01100001, 01110101
= 78, 97, 117

ZmFs = 01100110, 01100001, 01101100
= 102, 97, 108

f. Gunakan bilangan desimal untuk mencari karakter pada tabel ASCII
78 = N
97 = a
117 = u
102 = f
97 = a
108 = l

Maka didapat hasil dekripsi algoritma Base64 yaitu, **Naufal**.

4. KESIMPULAN

Dengan menggunakan kombinasi algoritma Base64 dan Caesar Chipher data yang terenkripsi sulit dibaca, karena pada proses algoritma Base64 ada konversi bilangan desimal menggunakan tabel ASCII, yang menghasilkan data acak berupa kombinasi huruf, angka, dan simbol.

Jika hanya menggunakan algoritma Caesar Chipher hasil dari proses enkripsi data, hanya menghasilkan kombinasi huruf dan angka. Sehingga data yang terenkripsi mudah dibaca, karena pada proses enkripsi Caesar Chipher hanya menggeaser angka, oleh sebabitu keamanan data akan diperkuat dengan algoritma Base64.

Kombinasi algoritma Base64 dan Caesar Chipher dapat diimplementasikan dengan baik ke dalam *website* DSPPPA Kota Cirebon. Berdasarkan hasil penelitian yang telah dilakukan, penulis memberikan saran sebagai berikut :

1. Disarankan untuk mengembangkan metode yang penulis implementasikan pada *website* ketahap yang lebih lanjut terutama untuk algoritma Caesar Chipher. Salah satu cara yang disarankan yaitu dengan menambah jumlah geser (*key*), atau mengacaj indeks dari abjad itu sendiri. Karena pada Caesar Chipher menggunakan indeks abjad sesuai dengan ururtan abjad iru sendiri. Jika menggunakan indeks abjad yang masih sesuai dengan urutan abjad itu sendiri hasil enkripsi mudah dibaca.
2. Disarankan untuk mengembangkan metode algoritma Base64. Salah saru cara yang disarankan yaitu dengan memodifikasi nilai desimal pada tabel penyusun indeks Base64. Agar bisa menghasilkan data yang lebih acak dan sulit untuk dibaca.

Disarankan pada *website* DSPPPA Kota Cirebon untuk menambahkan fitur unduh data. Karena pada *website* yang terlah dibuat belum ada fitur unduk data;

5. DAFTAR PUSTAKA

[1] F. Susanto, "Sistem informasi pengolahan data pasien pada puskesmas abung pekurun menggunakan metode prototype," J. Mikrotik, vol. 8, no. 1, pp. 65–73, 2018, [Online]. Available: https://ojs.ummetro.ac.id/index.php/mikrotik/article/view/751/552.

[2] Fitri Ayu and Nia Permatasari, "perancangan sistem informasi pengolahan data PKL pada divisi humas PT pegadaian," J. Infra tech, vol. 2, no. 2, pp. 12–26, 2018, [Online]. Available: http://journal.amikmahaputra.ac.id/index.php/JIT/article/download/33/25.

[3] A. P. N. Nurdin, "Analisa Dan Implementasi Kriptografi Pada Pesan Rahasia," Jesik, vol. 3, no. 1, pp. 1–11, 2017, [Online]. Available: nnurdin69@gmail.com.

[4] Azlin, F. Musadat, and J. Nur, "Aplikasi Kriptografi Keamanan Data Menggunakan Algoritma Base64," J. Inform., vol. 7, no. 2, pp. 1–5, 2018.

[5] R. Aulia, A. Zakir, and D. A. Purwanto, "Penerapan Kombinasi Algoritma Base64 Dan Rot47 Untuk Enkripsi Database Pasien Rumah Sakit Jiwa Prof. Dr. Muhammad Ildrem," InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan), vol. 2, no. 2, pp. 146–151, 2018, doi: 10.30743/infotekjar.v2i2.300.

[6] Y. Dwi Putri, R. Rosihan, and S. Lutfi, "Penerapan Kriptografi Caesar

Cipher Pada Fitur Chatting Sistem Informasi Freelance," JIKO (Jurnal Inform. dan Komputer), vol. 2, no. 2, pp. 87–94, 2019, doi: 10.33387/jiko.v2i2.1319.