Implementasi Algoritma Base 64 untuk Pengamanan File Teks di PDAM Tirta Jati Sumber

Virgiyanti[a], Erwanto[b]

[a,b] STIKOM Poltek Cirebon

Abstract

Data security is very important in maintaining the confidentiality of information, especially that contain sensitive information that should only be known it by the party entitled to it, especially if they are sent over a public network. If the data is not secured in advance, would be easily intercepted and note the contents of the information by parties that do not have the authority. Currently all information text files that are sent and received by the Company's local water (PDAM) is still easily read by people who are not interested because of the lack of confidentiality in the text file data and the information, and the lack of a way to secure a text file information and data The aim of this study to keep confidential and secure text file data and information. One of the ways used to secure data is to use cryptographic techniques is to provide content information (plaintext) into the content of which is not understood through an encryption process (chiperteks), and to recover the original information, a process description. To build a text file security application author uses Java JDK 7.0 and Netbeans IDE 7.2 as supporting applications. This application is made in the Window platform. In Making the design implementation of cryptographic techniques for safety text file using Base64 algorithm.The results of the research that has been done is a security application that can hide text files and text files to secure data and information docx extension.

Keywords*: Base64, Security, Security of Text Files*

Abstrak

Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi terutama berisi informasi sensitif yang hanya boleh diketahui isinya oleh pihak yang berhak saja, apalagi jika pengirimannya dilakukan melalui jaringan publik. Apabila data tersebut tidak diamankan terlebih dahulu, akan sangat mudah disadap dan diketahui isi informasinya oleh pihak-pihak yang tidak memiliki wewenang. Saat ini semua informasi file teks yang di kirim dan diterima oleh Perusahaan Daerah Air minum (PDAM) masih dengan mudah dibaca oleh orang yang tidak berkepentingan karena kurangnya kerahasiaan pada file teks data dan informasi tersebut dan belum adanya sebuah cara untuk mengamankan file teks data dan inforamsi.Tujuan penelitian ini untuk merahasiakan dan mengamankan file teks data dan informasi.
Salah satu cara yang digunakan untuk pengamanan data adalah menggunakan teknik kriptografi yaitu dengan menyediakan isi informasi (plainteks) tersebut menjadi isi yang tidak dipahami melalui proses enkripsi (*chiperteks*), dan untuk memperoleh kembali informasi yang asli, dilakukan proses deskripsi. Untuk membangun aplikasi keamanan file teks penulis menggunakan Java JDK 7.0 dan Netbeans IDE 7.2 sebagai aplikasi pendukungnya. Aplikasi ini dibuat dalam platform Window. Dalam Pembuatan desain implementasi teknik kriptografi untuk pengaman file teks dengan menggunakan algoritma Base64. Hasil dari penelitian yang telah dilakukan adalah Aplikasi Pengamanan File teks yang dapat merahasiakan dan mengamankan file teks data dan informasi berekstensi docx.

Kata kunci: Base64, Keamanan, Pengamanan File Teks

1. Pendahuluan

1.1. Latar Belakang

Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi terutama yang berisi informasi sensitif yang hanya boleh diketahui isinya oleh pihak yang berhak saja, apalagi jika pengirimannya dilakukan melalui jaringan publik. Apabila data tersebut tidak diamankan terlebih dahulu, akan sangat mudah disadap dan diketahui isi informasinya oleh pihak-pihak yang tidak memiliki wewenang (Rahmawati,A., & Rahman,A, 2011). Salah satu cara yang digunakan untuk pengamanan data adalah menggunakan teknik kriptografi yaitu dengan menyediakan isi informasi (*plainteks*) tersebut menjadi isi yang tidak dipahami melalui proses enkripsi (*chiperteks*), dan untuk memperoleh kembali informasi yang asli, dilakukan proses deskripsi (Raharjo, 2014) Adapun algoritma enkripsi yang digunakan adalah base64 yang didalam proses enkripsi dari plainteks ke cipherteks melalui tahapan dari ASCII, diubah ke biner, kemudian diubah ke desimal yang akan menghasilkan cipherteks. Kelebihan dari sistem enkripsi ini adalah membuat keamanan teks yang akan dikirim ke penerima dalam bentuk cipherteks yang harus didekripsi ulang untuk mengetahui isi dari teks yang dikirim.

Perusahaan Daerah Air Minum (PDAM) Tirta Jati terletak di Jl. Sunan Drajat no.12 Sumber, Jawa Barat. PDAM merupakan salah satu unit usaha milik daerah, yang bergerak dalam distribusi air bersih bagi masyarakat umum dan diawasi oleh pemerintah daerah. Perusahan daerah ini sebagian merupakan peralihan dari dinas pekerjaan umum yang sebelumnya bertugas menyediakan prasarana publik.

virgiyanti.ciliwung36@gmail.com, muhammaderwanto@gmail.com

Dengan status perusahaan milik daerah, PDAM Tirta Jati Sumber memiliki 7 kantor cabang yang terletak di beberapa tempat di wilayah kabupaten Cirebon, maka menjadi penting untuk menjaga kerahasaiaan data dan informasi dalam berkomunikasi antara kantor cabang dan kantor pusat, agar data dan informasi tidak disadap dan disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab.

Saat ini semua informasi yang di kirim dan diterima oleh PDAM Tirta Jati Sumber belum bersifat rahasia karena Pengamanan file teks data dan informasi belum efektif dan efisien, file teks data dan informasi mudah untuk dibaca oleh orang yang tidak berkepentingan, kurangnya kerahasiaan pada file teks data dan informasi menyebabkan file teks data dan informasi dapat digunakan dengan tidak semestinya.

Berdasarkan permasalahan tersebut maka diperlukan sebuah rancangan sistem yang dapat menjawab permasalahan mengenai kerahasiaan data dan informasi. Penelitian ini akan merancang sistem yang dapat merahasiakan semua data atau informasi, sehingga mengurangi resiko tersebarnya data dan informasi perusahaan kepada pihak yang tidak berkepentingan.

1.2. Identifikasi Masalah

Berdasarkan latar belakang, maka dapat di identifikasikan permasalahan sebagai berikut:

1. File teks data dan informasi dengan mudah dibaca oleh orang orang yang tidak berkepntingan karena kurangnya kerahasiaan pada file teks data dan informasi tersebut
2. Pengamana file teks data dan informasi di PDAM Tirta Jati Sumber belum efektif dan efisien.

1.3. Batasan Masalah

Batasan masalah pada penelitian ini adalah sebagai berikut:

1 Sistem yang dibuat pada penelitian ini dibatasi hanya pada keamanan data file teks berekstensi docx di PDAM Tirta Jati Sumber
2 Aplikasi ini hanya dapat mengamankan data berupa teks bukan gambar atau suara.

2. Kerangka Teori

Base64 adalah metode untuk melakukan penyandian (*encoding*) terhadap data binary menjadi format 6-bit character. Pada algoritma ini, rangkaian bit-bit palainteks dibagi menjadi blok-blok bit dengan panjang yang sama, biasanya 64 bit yang direpresentasikan dengan karakter ASCII. Base64 menggunakan karakter A – Z, a – z dan 0 – 9 untuk 62 nilai pertama, sedangkan 2 nilai terakhir digunakan symbol (+ dan /) sehingga totalnya 64. Ditambah satu karakter khusus untuk *padding byte* yaitu simbol =. Bila dalam kelompok 3 byte itu satu byte terakhir hanya berisi padding byte, maka satu karakter = ditambahkan. Bila dua, maka dua karakter = menjadi == (Hayatun Nufus, 2013).

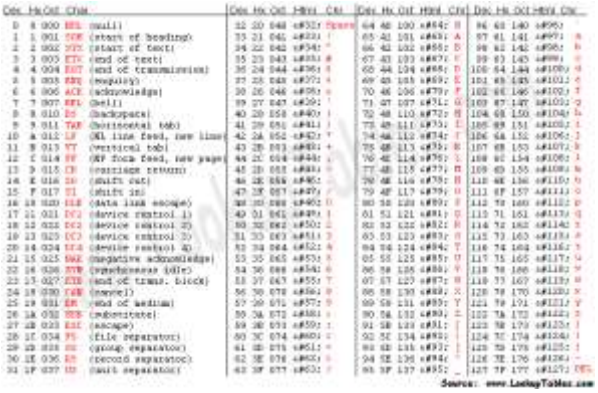
3. Metodologi Penelitian

Terdapat 2 tabel yang selalu digunakan base64 untuk proses enkripsi ataupun deskripsi yaitu tabel ASCII dan tabel indeks (Soleh,A.T., Gunadhi.E., & Supriatna,A.D, 2013).

1) Tabel Indeks 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	/

2) Tabel ASCII



2.1. Proses Enkripsi Base64

Tahapan proses enkripsi pada base64:

1) Menentukan plain teks yang akan di enkripsikan terlebih dahulu. didalam base64 proses enkripsi diambil dari blok yang sama yaitu 3 blok jadi ambil per 3blok dari keseluruhan karakter
2) Carilah kode ASCII dari masing masing teks
3) Ubah kode ASCII yang sudah di dapat dari bentuk decimal ke dalam bentuk binner 8bit
4) Gabungan binner 8bit yang sudah didapat menjadi 24bit
5) Pecah 24bit menjadi 6bit, maka akan menghasilkan 4 pecahan
6) Masing masing pecahan diubah kedalam bentuk decimal
7) Jadikan nilai-nilai *decimal* tersebut menjadi indeks untuk memilih karakter karakter penyusun dari base64

Jika terjadi kekurangan blok atau padding maka harus dilakan proses sebagai berikut:

1) Ubah *plainteks* kedalam bentuk decimal ASCII
2) Ubah nilai ASCII menajdi biner 8bit

virgiyanti.ciliwung36@gmail.com, muhammaderwanto@gmail.com

3) Pecah menjadi 6 bit dan tambahkan nilai 0 untuk menggenapkan 4 blok
4) Ubah biner 6 bit tersebut kedalam bentuk decimal dan untuk biner 000000 jadikan (kosong)
5) Ubah hasil decimal yg sudah didapat kedalam bentuk Char dengan melihat tabel indeks base64 dan untuk nilai yang (kosong) isikan nilai '='

2.2. Proses Deskripsi Base64

Tahapan proses deskripsi pada base64:

1) Hasil dari *Enkripsi* diubah menjadi Index base64
2) Ubah kode index tersebut menjadi kode biner 6bit
3) Gabungkan 6bit dari tiap blok menjadi 24bit
4) Pecah 24bit yang sudah didapat buat bit tiap blok berisi 8bit data bukan 6bit lagi
5) Ubah kode Biner menjadi ASCII
6) Ubah decimal ke *char*

Jika terjadi kekurangan blok atau padding maka harus dilakan proses sebagai berikut:

1) Ubah *chiperteks* menjadi nilai indeks
2) Binerkan nilai indeks denga 6bit biner
3) Masukan nilai biner pada '=' 000000 (kosong)
4) Gabungkan ke 4blok tersebut menjadi 24bit
5) Pecah kembali 34bit yg sudah didapat menjadi biner 8bit
6) Ubah bit yg sudah didapat kedalam bentuk decimal ASCII
7) Ubah nilai ASCII menjadi Char untuk mendapatkan *plainteks*

4. Hasil dan Pembahasan

4.1 Desain Dokumen dan Informasi

4.1.1 Desain Dokumen

Dokumen merupakan data masukan yang akan diproses dan menghasilkan informasi, dokumen input yang digunakan untuk sistem pengaman file teks di PDAM Tirta Jati Sumber adalah:

Data File Teks. Data File Teks adalah dimana isinya berupa teks dari file berekstensi docx yang nantinya berguna untuk memasukan teks dan melakukan proses enkripsi ataupun deksripsi.

4.1.2 Desain Informasi

Pada perancangan sistem baru ini penulis melakukan desain informasi untuk sistem yang baru, informasi yang dirancang sebagai berikut:

Data File Teks baru. Pada perancangan keluaran yang penulis buat yaitu file teks baru yang berekstensi docx yang sudah terenkripsi atau terdeskripsi.

4.2 Desain Prosedur

4.2.1 Desain Prosedur Enkripsi Base64

1) Langkah awal menenutkan plain teks yang akan di enkripsikan terlebih dahulu. didalam base64 proses enkripsi diambil dari blok yang sama yaitu 3blok jadi ambil per3blok dari keseluruhan karakter contoh: IRFANM kita ambil per3blok jadi ada 2 proses enkripsi yaitu IRF dan ANM.
2) Langkah selanjutnya, kita ubah planteks IRF ke dalam bentuk decimal ASCII.

PLAINTEKS	I	R	F
ASCII	73	82	70

3) Setelah mendapatkan hasil bilangan decimal dari plainteks tersebut kita ubah bilangan decimal tersebut kedalam bentuk biner 8bit.
   a. Buatlah deret bilangan 2 pangkat yang dimulai dari 2^0. Penulisan dimulai dari sebelah kanan. Batas bilangan harus kurang dari atau sama dengan (<=) nilai ASCII. Pada nilai 72 berarti kita menuliskan $2^6\ 2^5\ \ 2^4\ 2^3\ 2^2\ 2^1\ 2^0$ Sehingga jika kita tuliskan jumlah perpangkatannya, akan kita temukan bilangan 64, 32, 16, 8, 4, 2, 1
   b. Kemudian kurangi 73 dengan 64. Karena 73 bisa dikurangi dengan 64 maka kita tuliskan 1. 73 – 64 = 9. Kemudian hasil 9 dikurangkan dengan 32. Karena 9 tidak bisa dikurangi dengan 32, maka kita tuliskan 0. Kemudian 9 – 16. Dan karena tidak bisa lagi kita tuliskan 0. Dan begitulah seterusnya sampai 1 sehingga dari nilai 72 akan terbentuk bilangan 1 0 0 1 0 0 1. Karena hanya ada 7 bilangan maka kita tambahkan 0 di depan menjadi 0 1 0 0 1 0 0 1. Sehingga kita sudah menemukan biner 8 bit dari I

   Lakukan hal yang sama untuk mencari binner 8 bit dari teks selanjutnya R dan F.

ASCII	73	82	70
BINER 8BIT	01001001	01010010	01000110

4) Setelah mendapatkan hasil bilangan binner 8bit dari masing-masing blok kita gabung bilangan binner 8bit yg sudah didapat dari ke 3 blok tersebut maka disini akan mengahasilkan binner 24bit.

BINER 8BIT	01001001	01010010	01000110
BINER 24BIT	010010010101001001000110		

5) Langkah selanjutnya ketika sudah didapat binner 24bit, pecah lagi menjadi binner 6 bit maka pada proses ini akan menghasilkan 4blok bilangan binner.

BINER 24BIT	010010010101001001000110			
BINER 6BIT	010010	010101	001001	000110

6) Selanjutnya ubah bilangan binner 6bit yg sudah didapat kedalam bentuk decimal.

   0 1 0 0 1 0

virgiyanti.ciliwung36@gmail.com, muhammaderwanto@gmail.com

$2^5 2^4 2^3 2^2 2^1 2^0$ hitung nilai pangkat dari billangan biner bernilai 1 saja, jadi nilai yg dihitung hanya 2^1 dan 2^4 menjadi 2+16=18 untuk binner 6bit pertama. lakukan hal yg sama untuk binner 6bit selanjutnya, hingga mendapatkan bentuk decimal.

BINER 6BIT	010010	010101	001001	000110
DECIMAL	18	21	9	6

7) Langkah akhir jadikan nilai decimal tersebut sebagai indeks base64 dengan melihat tabel dari indeks base64. Diproses akhir akan mendapatkan hasil 4blok dari 3blok yg di enkripsikan dengan kata lain untuk proses enkripsi pada base64 perbandingannya ¾.

DECIMAL	18	21	9	6
CHIPERTEKS	S	V	J	G

a. Jika angka biner tidak berjumlah 6 bit dan 4 blok, maka ditambah dengan kode biner "0" sehingga mencukupi menjadi 4 blok.
b. Jika nilai blok adalah hasil tambahan (0) maka hasil dari indeks tersebut bernilai '='

Caranya:

1. Ubah plainteks kedalam bentuk decimal ASCII
2. Ubah nilai ASCII menajdi biner 8bit
3. Pecah menjadi 6bit dan tambahkan nilai 0 untuk menggenapkan 4blok
4. Ubah biner 6bit tersebut kedalam bentuk decimal dan untuk biner 000000 jadikan (kosong)
5. Ubah hasil decimal yang sudah didapat kedalam bentuk Char dengan melihat tabel indeks base64 dan untuk nilai yang (kosong) isikan nilai '='

PLAINTEKS	A	N		
ASCII	65	78		
BINER 8BIT	01000001	01001110		
BINER 6BIT	010000	010100	111000	000000
DECIMAL	16	20	56	kosong
CHIPERTEKS	Q	U	4	=

4.2.2 Desain Prosedur Deskripsi Base64

1) Langkah awal menetukan chiperteks yang ingin di deskripsikan terlebih dahulu. didalam base64 proses deskripsi diambil dari blok yang sama yaitu 4blok jadi ambil per4blok dari keseluruhan karakter, contoh: SVJGQU5N kita ambil per4blok jadi ada 2 proses deskripsi yaitu SVJG dan QU5N
2) Selanjutnya mengubah chiperteks yang sudah ditentukan menjadi indeks base64 dengan melihat tabel indeks base64
3) Langkah selanjutnya setelah mendapatkan kode dari indeks base64 ubah kode indeks tersebut kedalam bentuk binner 6bit

Cara mencari nilai Biner dari 18 21 9 6 dengan membagi bilangan desimal dengan 2 dan menyimpan sisa bagi per setiap pembagian terus hingga hasil baginya < 2. ketika bilangan yang dibagi adalah bilangan genap maka sisanya adalah 0, dan ketika bilangan yang dibagi adalah bilangan ganjil maka sisanya adalah 1.

Hasil konversi adalah urutan sisa bagi dari yang paling akhir hingga paling awal contoh konversi 21.

21 : 2 = 10 sisa 1
20 : 1 = 5 sisa 0
5 : 2 = 4 sisa 1
2 : 2 = 1 sisa 0
1 : 2 = 0 sisa 1

Hasil keseluruhan sisa bagi dari 21 adalah 1 0 1 0 1
Karena yang dicari 6bit maka ditambahkan 0 didepan untuk menggenapkan menjadi 6bit. Jadi hasil akhirnya adalah 010101

INDEKS	18	21	9	6
BINER 6BIT	010010	010101	001001	000110

Sehingga didapat nilai biner dari 18 21 9 6 adalah 010010 010101 001001 000110

4) Setelah mendapatkan binner 6bit dari masih masing blok gabungkan binner 6bit dari seluruh blok sehingga disini kita mendapatkan bilangan binner 24bit

BINER 6BIT	010010	010101	001001	000110
BINER 24BIT	010010010101001001000110			

5) Selanjutnya pecah binner 24bit yang sudah didapat menjadi binner 8bit

BINER 24BIT	010010010101001001000110		
BINER 8BIT	01001001	01010010	01000110

6) Setelah mendapatkan binner 8bit dari pemecahan binner 24bit kita ubah binner 8bit tersebut kedalam bentuk decimal

BINER 8BIT	01001001	01010010	01000110
ASCII	73	82	70

7) Langkah akhir ubah bilangan decimal yang sudah di dapat dari pemecahan 8bit kedalam bentuk Char. Diproses akhir kita akan mendapatkan hasil 3blok dari 4blok yang dideskripsikan dengan kata lain untuk proses deskripsi pada base 64 perbandingannya 4/3

ASCII	73	82	70
PLAINTEKS	I	R	F

Jika Terjadi pad maka nilai sama '=' kembalikan ke kosong
Caranya:

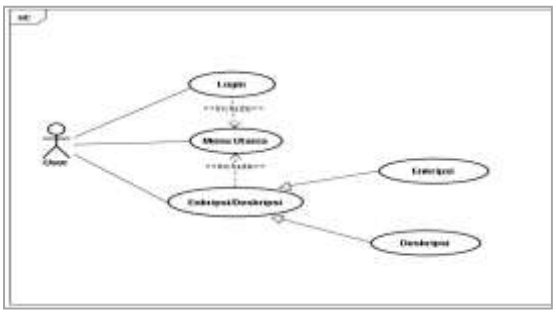
1 Ubah *chiperteks* menjadi nilai indeks
2 binerkan nilai indeks denga 6bit biner

3 masukan nilai biner pada ‘=’ 000000 (kosong)
4 gabungkan ke 4blok tersebut menjadi 24bit
5 pecah kembali 34bit yg sudah didapat menjadi biner 8bit
6 ubah bit yg sudah didapat kedalam bentuk decimal ASCII
7 ubah nilai ASCII menjadi Char untuk mendapatkan *plainteks*

Hasil deskripsi dari SVJGQU4= adalah IRFAN

CHIPERTEKS	Q	U	4	=
INDEKS	16	20	56	kosong
BINER 6BIT	010000	010100	111000	000000
BINER 24BIT	010000010100111000000000			
BINER 8BIT	01000001	01001110	Kosong	kosong
ASCII	65	78	Kosong	kosong
PLAINTEKS	A	N	Kosong	kosong

4.3 Desain Aliran Data
4.3.1 *Usecase Diagram*



4.3.2 Desain Interface
1) Menu Login



2) Menu Utama



5. Kesimpulan dan Saran

5.1 Kesimpulan

Setelah melalui tahap analisa dan pengujian, maka diambil kesimpulan sebagai berikut:

Dengan adanya aplikasi keamanan file teks di PDAM Tirta Jati Sumber dapat merahasiakan seluruh file teks yang ada di PDAM Tirta Jati Sumber

Dengan adanya aplikasi keamanaan file teks di PDAM Tirta Jati Sumber dapat mengamankan seluruh file teks yang ada di PDAM Tirta Jati Sumber.

5.2 Saran

Agar dapat lebih baik dalam pengembangannya, penulis ingin memberikan saran agar sistem yang berjalan dapat lebih baik lagi, diantaranya adalah sebagai berikut:

Melakukan pembaharuan serta evaluasi terhadap kinerja aplikasi keamanan file teks sebagai bahan masukan untuk pengembangan selanjutnya

Penyempurnaan dan pengembangan aplikasi ini masih dapat dikembangakan dalam hal pengembangan enkripsi atau deskripsi gambar atau suara.

Daftar Pustaka

Nufus,H. (2013). Pembuatan aplikasi kriptografi algoritma base64 menggunakan java jdk 1.6. Gunadarma, 1(1), 1-11.

Raharjo,B. (2014). Keamanan Sistem Informasi Berbasis Internet. Jurnal Speed, 9(2), 1-14.

Rahmawati,A., & Rahman,A. (2011). Sistem Pengamanan Keaslian Ijasah Menggunakan QR-Code dan Algoritma Base64. Jusi, 1(2), 105-112.

Soleh,A.T., Gunadhi.E., & Supriatna,A.D. (2013). MENGAMANKAN SKRIP PADA BAHASA PEMOGRAMAN PHP DENGAN MENGGUNAKAN KRIPTOGRAFI BASE64. Jurnal Sekolah Tinggi Teknologi Garut. 1(1), 1-9.

AzizPratama Nugraha, Erwin Gunadhi (2016). KRIPTOGRAFI BASE64 UNTUK KEAMANAN URL (UNIFORM RESOURCE LOCATOR) WEBSITE DARI SERANGAN SQL INJECTION Jurnal Algoritma Sekolah Tinggi Teknologi Garut Jl. Mayor Syamsu No. 1 Jayaraga Garut 44151

Wahyu, F.,Rahangiar, A.P., & Fretes, F.d. (2012). Penerapan AlgoritmaGabungan RC4 dan base64 Pada Sistem Keamanan E-Commerce. Retrieved Mei 25, 2016, From Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana Web Site On World Wide Web : http://journal.uji.ac.id/index.php/Snati/article/viewFile/2873/2628

Ahir Yugo Nugroho1 (2015). PEMBUATAN APLIKASI KRIPTOGRAFI ALGORITMA BASE 64 MENGGUNAKAN PHP UNTUK MENGAMANKAN DATA TEXT, Universitas Potensi Utama Universitas Potensi Utama, Jl. Yosudarso Km. 6,5 Tanjung Mulia Medan.