

PROGRAM ENKRIPSI DENGAN MENGGUNAKAN METODE CAESAR CHIPER, BASE32 DAN BASE 64

Fattah Al Ilmi
Suhendra¹
Mohammad Fatoni²
Saidatul Arifah³

^{1,2,3}*Jurusan Teknik Informatika, Fakultas Teknologi Industri,
Universitas Gunadarma
Jl. Margonda Raya no.100, Depok 16424, Indonesia
{fattahilmi, mohfatoni, saidatularifah}@student.gunadarma.ac.id*

Abstrak

Kriptografi merupakan suatu ilmu yang berkaitan dengan aspek keamanan informasi, seperti kerahasiaan data, integritas data, validitas data, dan autentikasi data. Pada umumnya, kriptografi terdiri dari dua proses yaitu proses enkripsi dan proses deskripsi. Kriptografi dapat terbagi menjadi beberapa jenis seperti ciphers, encoding, modern cryptography, dan lain-lain. Dalam penulisan ini, kami akan memfokuskan pada penggabungan caesar cipher dengan encode base64 dan encode base32 untuk proses enkripsi dan deskripsi data.

Kata Kunci : *Kriptografi, caesar cipher, base64, base32.*

PENDAHULUAN

Perkembangan teknologi informasi membuat komunikasi menjadi semakin luas dan mudah. Sehingga membuat informasi sangat mudah untuk dicuri. Dalam hal ini, keamanan pengiriman data sangat dibutuhkan agar terhindar dari pihak-pihak yang mencoba untuk melakukan pencurian data. Salah satu metode yang dapat digunakan untuk keamanan data yaitu kriptografi. Ilmu kriptografi berkembang seiring dengan berjalannya waktu.

Menurut kronologi waktunya kriptografi dapat terbagi menjadi kriptografi klasik dan kriptografi modern. Keduanya dapat dibedakan dari perangkat yang digunakan dalam pembuatan dan analisisnya. Kriptografi klasik dalam pembuatan dan analisisnya sama sekali tidak menggunakan komputer. Salah satu contoh kriptografi klasik yaitu *caesar chiper*. Kriptografi modern merupakan perkembangan dari kriptografi klasik. Kriptografi modern merupakan sebuah algoritma yang dimaksudkan

untuk mengamankan informasi yang dikirimkan melalui jaringan komputer.

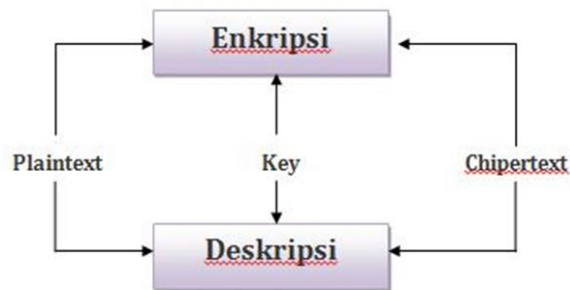
Kriptografi terdiri dari dua bagian yaitu enkripsi, deskripsi. Enkripsi merupakan proses penyembunyian informasi data dengan cara mengubah *plain text* (pesan yang dapat dibaca) menjadi *chiper text* (pesan acak yang tidak dapat dibaca). Sedangkan deskripsi merupakan kebalikan dari enkripsi, cara kerjanya yaitu mengembalikan kode yang telah di enkripsi menjadi *plain text* (mengubah *chiper text* menjadi *plain text*). Algoritma enkripsi dan deskripsi memproses semua data dan informasi dalam bentuk mode bit. Rangkaian bit yang menyatakan *plain text* dienkripsi menjadi *chiper text* dalam bentuk rangkaian bit, dan sebaliknya.

Dalam kriptografi terdapat sebuah algoritma yang disebut dengan *chiper*, yaitu suatu fungsi matematika yang berperan dalam enkripsi dan deskripsi data. Dalam kriptografi juga terdapat istilah *encoding* dan *decoding*. Jenis

encoding yang paling sering digunakan yaitu *base32* dan *base64*.

METODE PEMBUATAN

Dalam proses enkripsi, pengirim harus memanipulasi pesan menggunakan metode tertentu. Pesan asli, yang disebut *plain text*, dapat diacak sehingga surat-suratnya berbaris dalam urutan yang tidak dapat dipahami(*chipert text*) atau setiap huruf dapat diganti dengan yang lain.



Untuk membuat kriptografi ini, kami menggunakan *caesar chiper* dan encoding yang kami gunakan yaitu *base32* dan *base64*. *Caesar Chiper* merupakan jenis kriptografi yang bekerja dengan cara melakukan pergeseran huruf/abjad berdasarkan key(kunci) yang telah ditentukan. Enkoding atau bisa disebut pengkodean atau penyandian adalah proses konversi informasi dari suatu sumber (objek) menjadi data, yang selanjutnya dikirimkan ke penerima atau pengamat, seperti pada sistem pemrosesan data. Kebalikan dari Enkoding yaitu Dekoding, Dekoding adalah proses konversi data yang telah dikirimkan oleh sumber menjadi informasi yang dimengerti oleh penerima. Algoritma *base32* membagi hasil biner(8 bit) menjadi 5 bit per blok. Sedangkan algoritma *base64* membagi hasil biner(8 bit) menjadi 6 bit per blok.

Base64 merupakan skema pengkodean yang mengkodekan data biner dan menerjemahkannya ke dalam representasi berbasis 64. Skema encoding base64 biasanya digunakan untuk menyandikan data biner yang perlu disimpan dan ditransfer melalui media yang dirancang untuk menangani data tekstual. Hasil

dari base64 berbentuk plaintext, sehingga mudah untuk dikirim. Proses enkripsi base64 :

- 1) Pesan diubah ke dalam kode ASCII.
- 2) Kode ASCII diubah menjadi biner(8 bit).
- 3) Bagi kode biner menjadi 6 bit per blok dan berlaku kelipatan 4 blok untuk seterusnya.
- 4) Kemudian ubah blok-blok tersebut menjadi bilangan desimal.
- 5) Cari char pada tabel index sesuai dengan bilangan desimal yang telah dihasilkan dari konversi pada nomor 4.

Tabel index base64 :

Value	0	1	2	3	4	5
Char	A	B	C	D	E	F

Value	6	7	8	9	10
Char	G	H	I	J	K

Value	11	12	13	14	15
Char	L	M	N	O	P

Value	16	17	18	19	20
Char	Q	R	S	T	U

Value	21	22	23	24	25
Char	V	W	X	Y	Z

Value	51	52	53	54	55
Char	z	0	1	2	3

Value	26	27	28	29	30
Char	a	b	c	d	e

Value	56	57	58	59	60
Char	4	5	6	7	8

Value	31	32	33	34	35
Char	f	g	h	i	j

Value	61	62	63
Char	9	+	/

Value	36	37	38	39	40
Char	k	l	m	n	o

Value	41	42	43	44	45
Char	p	q	r	s	t

Value	46	47	48	49	50
Char	u	v	w	x	y

Untuk *encoding base32* selain memiliki perbedaan jumlah blok yang digunakan (5 bit per blok), *base32* juga memiliki ciri khusus yaitu pengkodean ini dimulai dengan 26 huruf pertama dari alfabet dan berakhir dengan angka 2-7. Yang berarti pengkodean untuk 0 adalah A, bukan 0. Adapun beberapa tahapan pengkodean *base32* yaitu :

- 1) String yang akan dikodekan dibagi menjadi 5 blok byte (40 bit dalam biner). Karakter diwakili oleh 8 blok bit di ASCII (standar untuk komputer).
- 2) Bagilah bit ini menjadi 8 blok 5 bit;
- 3) Petakan masing-masing blok ini ke pemetaan karakter 5-bit dalam alfabet Base32. Terdapat 2 versi alfabet yaitu desimal dan biner.

Berikut tabel alfabet base32 :

Value	Symbol	Value	Symbol	Value	Symbol	Value	Symbol
0	A	9	J	18	S	27	3
1	B	10	K	19	T	28	4
2	C	11	L	20	U	29	5
3	D	12	M	21	V	30	6
4	E	13	N	22	W	31	7
5	F	14	O	23	X		
6	G	15	P	24	Y		
7	H	16	Q	25	Z		

HASIL DAN PEMBAHASAN

Analisis Kebutuhan Sistem

Pembuatan kriptografi ini, dimulai dari perancangan, pemrograman, hingga implementasi. Aplikasi yang dibutuhkan untuk membuat kriptografi, kami menggunakan Python versi 2.7. Library yang kami gunakan adalah base64.

Perancangan

Proses perancangan program dimulai dari membuat function untuk mengenkripsi sebuah kalimat dengan perubahan dari *plain text-caesar(chiper)-base64-caesar(chiper)-base32-chiper text*.

```
import base64

def encrypt():
    plain = raw_input('Enter the plaintext message: ')
    keyCaesar = int(raw_input('Enter the secret key: '))
    temp1 = ''

    for i in plain:
        temp1 += chr(ord(i)+keyCaesar)

    temp2 = base64.b64encode(temp1)
    temp3 = ''

    for i in temp2:
        temp3 += chr(ord(i)+keyCaesar)

    temp4 = base64.b32encode(temp3)
    temp5 = ''

    for i in temp4:
        temp5 += chr(ord(i)+keyCaesar)

    chiper = temp5
    print 'Ciphertext: {}'.format(chiper)
```

Pertama, *import library base64* terlebih dahulu yang telah disediakan oleh python. Pada variabel temp1 merupakan proses encoding dengan menggunakan kunci caesar. Fungsi ord(i) merupakan perubahan setiap kata menjadi kode ascii pada *plain text* yang kemudian ditambahkan dengan kunci atau *key caesar* yang telah

ditentukan. Kemudian fungsi chr() disini adalah untuk mengubah hasil penjumlahan tadi menjadi sebuah karakter.

Selanjutnya temp1 *encoding* kembali dengan menggunakan base64.b64encode yang disimpan di dalam variabel temp2. Kemudian, variabel temp2 kami *encoding* kembali dengan kunci caesar yang sama sesuai dengan inputan user lalu disimpan di dalam variabel temp3.

Setelah itu, variabel temp3 diencoding kembali dengan menggunakan fungsi b32encode. Dan hasilnya disimpan di dalam variabel temp4. Lalu variabel temp4 kami *encoding* kembali dengan menggunakan kunci caesar yang telah ditentukan di awal. Hasil dari *encoding* kemudian disimpan di dalam variabel temp5 dimana itu merupakan *chiper text*.

```
def decrypt():
    chiper = raw_input('Enter the chiphertext message: ')
    key = int(raw_input('Enter the secret key: '))

    temp1 = ''

    for i in chiper:
        temp1 += chr(ord(i)-key)

    temp2 = base64.b32decode(temp1)
    temp3 = ''

    for i in temp2:
        temp3 += chr(ord(i)-key)

    temp4 = base64.b64decode(temp3)
    temp5 = ''

    for i in temp4:
        temp5 += chr(ord(i)-key)

    plain = temp5
    print 'Plaintext: {}'.format(plain)
```

Pada fungsi dekripsi di atas, maka proses urutan yang dilakukan adalah sebaliknya, yaitu *chiphertext - caesar(chiper) - base32-caesar(chiper) - base64 - caesar(chiper) - plain text*.

Pertama, pada variabel temp1 kita *decoding* dengan kunci yang sama seperti pada proses enkripsi, tetapi sedikit berbeda karena pada proses *decoding* fungsi ord(i) yang mana merupakan kode ascii dari setiap urutan karakter kita kurangi dengan kunci caesar. Kemudian kita ubah kode ascii yang telah dikurangi tadi menjadi karakter dengan fungsi chr().

Selanjutnya temp1 di *decoding* dengan menggunakan fungsi `base64.b32decode` yang kemudian disimpan di dalam variabel temp2. Kemudian variabel temp2 kami *decoding* kembali dengan menggunakan kunci caesar lalu disimpan di dalam variabel temp3.

Setelah itu, variabel temp3 di *decoding* kembali dengan menggunakan fungsi `base64.b64decode` yang kemudian hasilnya disimpan di dalam variabel temp4. Dan yang terakhir, variabel temp4 di *decoding* kembali dengan menggunakan kunci caesar yang telah ditentukan. Hasil dari *decoding* ini kemudian disimpan di dalam variabel temp5 dimana variabel ini merupakan *plain text*.

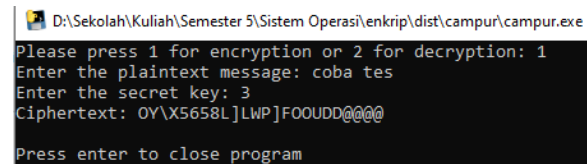
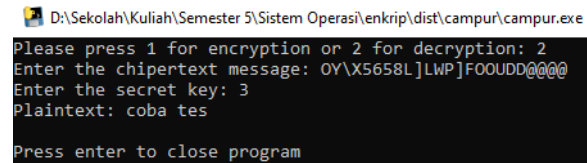
```
choice=int(raw_input("Please press 1 for encryption or 2 for decryption: "));
if choice==1:
    encrypt();
elif choice==2:
    decrypt();
else:
    print("Wrong choice entered. Exiting now..");
    exit();
```

Pada program di atas, kita dapat memilih enkripsi atau dekripsi. Agar lebih mudah, kita pilih enkripsi terlebih dahulu agar pada saat proses dekripsi, kita telah mengetahui *chipertextnya*.

Implementasi

Setelah dilakukan pemrograman, maka langkah selanjutnya yaitu mengkonversi file .py menjadi .exe. Agar dalam menjalankan programnya, tidak perlu lagi membuka kodingan terlebih dahulu. Untuk konversi file diperlukan pyinstaller. Apabila belum terinstall pyinstaller, maka kita harus menginstall pyinstaller terlebih dahulu dengan cara : buka terminal kemudian ketikkan `pip install pyinstaller`, tunggu hingga proses instalasi selesai. Kemudian ketikkan `pyinstaller namafile.py` untuk menjadikan file .py menjadi .exe.

Jalankan file .exe yang terletak pada folder dist. Berikut merupakan tampilan output dari program kami :

Hasil dari proses enkripsi berupa *chipertext*. Sedangkan untuk hasil dari deskripsi yaitu *plain text*. Dalam proses enkripsi dan deskripsi diperlukan *key* atau kunci caesar untuk menggeser kode ascii. Contohnya apabila kita menggunakan kunci 1 maka alfabet akan bergeser 1 kali(a menjadi b, b menjadi c, dan seterusnya).

KESIMPULAN

Penggunaan kriptografi menjadikan data-data penting yang dikirimkan oleh pengirim dapat terjaga kerahasiaan dan keasliannya. Selain itu enkripsi dapat berfungsi untuk menanggulangi penyadapan telepon dan email. Enkripsi juga memiliki kerugian, salah satu contohnya adalah penyalahgunaan oleh oknum-oknum penjahat atau pesan tidak bisa dibaca bila penerima pesan lupa atau kehilangan kunci (decryptor). Tentunya enkripsi ini harus digunakan dengan baik.

SARAN

Dalam pembuatan program enkripsi ini, alangkah baiknya pelajari terlebih dahulu encoding base16, base32, base64, dan metode caesar chiper. Selain itu, perlu mengetahui library apa saja yang dibutuhkan. Contohnya pada python kita perlu mengimport *library base64*. Tentunya kita juga harus mengetahui apa tujuan dari enkripsi ini.

DAFTAR PUSTAKA

Qwords. 2020. *Pengertian Lengkap Kriptografi, Sejarah dan Jenis Algoritmanya* di <https://qwords.com/blog/pengertian-kriptografi/>

Medium. 2018. *Perbedaan Enkoding, Enkripsi, dan Hash* di <https://medium.com/@ramdannur/perbedaan-enkoding-enkripsi-dan-hash-9f9670767fa3>