

# Penerapan Vigenere Cipher untuk Mengenkripsi Data pada File CSV

Venantius Sean Ardi Nugroho - 13522078<sup>1</sup>

Program Studi Teknik Informatika

Sekolah Teknik Elektro dan Informatika

Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia

13522078@std.stei.itb.ac.id

[https://github.com/Leaguemen/CSV\\_Encryption\\_with\\_Vigenere\\_Cipher.git](https://github.com/Leaguemen/CSV_Encryption_with_Vigenere_Cipher.git)

*Abstrak – Vigenere Cipher adalah salah satu polyalphabetic cipher yang menggunakan sebuah key untuk mengashilkan suatu sandi. Sifatnya yang memerlukan key membuat cipher ini lebih kuat dari monoalphabetic cipher seperti caesar cipher. Makalah ini bertujuan untuk menggunakan Vigenere Cipher dalam enkripsi file CSV serta membahas metode autokey dan metode repetisi yang diimplementasikan dalam vigenere cipher.*

**Keywords—** Vigenere, cipher, autokey, CSV

## I. PENDAHULUAN

Vigenere cipher adalah salah satu bentuk cipher yang bersifat polyalphabetic. Metode sandi ini ditemukan oleh Giovan Battista Bellaso. Polyalphabetic cipher adalah metode enkripsi yang menggunakan beberapa substitusi alphabet untuk mengenkripsi suatu teks. Tidak seperti monoalphabetic cipher, dimana tiap karakter secara konsisten diganti oleh karakter lainnya. Misalnya saja, anda ingin mengenkripsi frasa “kupu – kupu” menggunakan monoalphabetic cipher, maka sandi dari “kupu” yang pertama dan “kupu yang kedua akan sama (misalnya rbwb – rbwb bila menggunakan shift 7 karakter). Tentu hal tersebut merupakan kelemahan keamanan. Pada polyalphabetic cipher, sandi dari kupu yang pertama dan yang kedua kemungkinan besar akan beda.

Melihat keuntungan tersebut penulis menjadi tertarik untuk menggunakan salah satu bentuk polyalphabetic cipher yang terkenal yaitu Vigenere Cipher untuk mengenkripsi sebuah file CSV. Mengapa hal tersebut sangat menguntungkan dalam enkripsi file CSV? Hal tersebut dikarenakan pada file – file yang biasa digunakan untuk transfer data seperti .xlsx atau .csv, sering kali terdapat data – data yang duplikat. Contohnya, pada file yang memuat data – data profil mahasiswa terdapat kolom tanggal lahir. Pasti akan banyak mahasiswa yang memiliki bulan lahir yang sama, apalagi tahun lahir yang sama (bila mereka satu angkatan). Bila seorang peretas dapat memecahkan salah satu sandi, misalnya untuk kata “desember”, maka peretas tersebut dapat dengan mudah menebak siapa saja yang lahir pada bulan desember. Tentu hal tersebut tidak kami inginkan.

Secara garis besar, beginilah cara kerja Vigenere Cipher. Ambil sebuah teks yang ingin anda sandikan, misal saja saya ingin menyandikan kata “sayurmayur” lalu representasikan tiap karakter menjadi angka. Dari situ Anda akan memilih menentukan sebuah *keyword* yang ingin Anda gunakan untuk

menyandikan teks tersebut. Keyword tersebut akan direpresentasikan juga sebagai angka dan disesuaikan panjangnya agar sama dengan kata yang disandikan. Kedua representasi tersebut ditambahkan dan dimodulo 26 dan Anda akan mendapatkn cipher text nya.

Tentu dari deskripsi yang penulis berikan, masih banyak masalah – masalah yang harus dihadapi. Bagaimana bila Anda memasukkan key dengan panjang kurang dari panjang? Dalam file csv terdapat banyak angka, kita juga perlu menyandikannya. Bagaimana cara mengatasinya? Keuntungan dan kerugian apa yang kita dapat dalam menggunakan cipher ini dalam penyandian file csv?

Makalah ini membahas tentang metode – metode yang digunakan untuk melakukan vigenere cipher. Makalah ini juga akan membahas implementasinya dengan program berbasis python.

## II. LANDASAN TEORI

### A. Modulo

Sebelum kita membahas bahan – bahan yang lebih spesifik dengan makalah ini, alangkah baiknya kita mengerti mengenai konsep modulo yang terdapat pada teori bilangan karena modulo digunakan untuk enkripsi dan dekripsi dalam Vigenere Cipher. Operasi modulo, atau sering disingkat sebagai “mod”, adalah operasi matematika yang mencari sisa dari suatu angka ketika dibagi dengan suatu angka.

Sebagai contoh, bila kita memiliki dua angka, a dan b, maka a modulo b adalah sisa dari pembagian a dan b. Beberapa contoh bisa dilihat pada operasi berikut :

1.  $73 \text{ mod } 9$  adalah 1 karena  $73/9$  hasilnya adalah 8 dengan sisa 1.
2.  $15 \text{ mod } 12$  adalah 3 karena  $15/12$  adalah 1 dengan sisa 3.

Dalam pemrograman, operasi modulo sering direpresentasikan dengan lambang persen (%). Contohnya di Python, untuk menulis  $73 \text{ mod } 9$ , Anda akan menulis  $73 \% 9$ .

Satu sifat dari operasi modulo yang akan dimanfaatkan untuk enkripsi dan dekripsi pada Vigenere Cipher adalah hasil dari bahwa hasil dari operasi modulo tidak akan lebih dari divisor pada operasi tersebut. Maksudnya adalah seperti ini, dalam persamaan  $a \text{ mod } b = x$ , x pasti lebih kecil dari b.

$$a \bmod b = x, x < b \dots (1)$$

Sifat tersebut juga digunakan pada salah satu cipher yang terkenal yaitu Caesar Cipher dengan divisor = 26 yang merepresentasikan 26 abjad dalam alfabet.

### B. Vigenere Cipher

Vigenere Cipher adalah sebuah metode penyandian yang pertama kali dideskripsikan oleh Giovan Battista Bellaso pada tahun 1553. Cipher ini mudah untuk dimengerti dan diimplementasikan, namun sangat sulit untuk diretas. Baru pada tahun 1863, 300 tahun lebih setelah ditemukannya, algoritma untuk men-decipher sandi ini ditemukan. Cipher ini dinamakan berdasarkan Blaise de Vigenère, seseorang yang memperkuat cipher ini dengan sistem *Autokey* yang ia temukan (akan dibahas pada bab ini juga).

Vigenere cipher merupakan salah satu bentuk polyalphabetic cipher. Sebuah polyalphabetic cipher adalah segala bentuk cipher yang menggunakan beberapa substitusi. Secara klasik, vigenere cipher diimplementasikan dengan sebuah *Vigenere Square* (nama lainnya termasuk *Vigenere Table* atau *Tabula Recta*).

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Gambar 1. Vigenere Table

Vigenere Table dapat dideskripsikan sebagai berikut :

1. *Vigenere Table* terdiri dari abjad – abjad alfabet ditulis sebanyak 26 kali di tiap barisnya. Perbedaan yang ditemukan dari tiap baris adalah tiap baris di-shift sebanyak 1, melambangkan 26 shift yang bisa dilakukan pada Caesar Cipher.
2. Dalam enkripsi, cipher menggunakan baris tertentu untuk menyandikan karakter tertentu.
3. Baris yang digunakan tersebut ditentukan oleh keyword yang dimasukkan.

Mungkin poin 2 dan 3 masih sedikit sulit dipahami, untuk itu, mari kita lihat beberapa contoh. Pada Vigenere Cipher Anda perlu menentukan keyword untuk menyandikan teks. Perlu diingat bahwa keyword harus sama panjangnya dengan teks yang ingin disandikan. Misalnya anda ingin menyandikan kata “kupukupu” dengan key “orangtua”. Maka untuk karakter k pertama pada kata “kupukupu” akan diubah pada dengan karakter yang

terdapat pada sel dengan baris o (karakter pertama “orangtua”) dan kolom k, yaitu karakter ‘y’. Terus lakukan proses tersebut hingga semua karakter pada kata “kupukupu” telah dienkripsi. Perhatikan bahwa k pertama dan k kedua akan disubstitusikan dengan karakter yang berbeda. K kedua akan disubstitusikan dengan karakter ‘q’ karena k dan g adalah karakter kelima dari masing – masing teks dan keyword.

Pada kasus yang saya berikan tersebut, kebetulan key dan teks yang ingin kita cipher memiliki panjang yang sama. Bagaimana kalau key dan teks-nya tidak memiliki panjang yang sama? Cukup mudah untuk menangani kasus dimana teksnya lebih kecil dari keynya, yaitu dengan cara memangkas key hingga panjangnya sama dengan teks yang ingin kita cipher. Tapi bagaimana bisa teks yang diberikan lebih panjang dari keynya? Terdapat dua metode untuk mengatasi masalah ini, yaitu :

1. Metode repetisi: dengan menggunakan metode ini, key akan diulang – ulang terus hingga memiliki panjang yang sama dengan teksnya. Contoh, Anda memiliki teks “iniadalahpesanrahasia” dengan keyword yang Anda pilih adalah “kunci”, maka keyword tersebut akan menjadi “kuncikuncikuncikuncik” supaya keyword kita memiliki panjang yang sama dengan teks tersebut yang memiliki panjang 21 karakter. Metode ini memiliki kelemahan yang cukup kentara yaitu bila seorang peretas mengetahui keywordnya, sang peretas bisa langsung kunci fullnya.
2. Metode autokey: metode ini adalah metode yang diciptakan oleh Blaise de Vigenère seperti yang telah dicantumkan di atas. Cara kerja metode ini adalah dengan cara mengambil keyword yang dipilih dan menyulihkannya sebagai awal dari kunci yang komplitnya. Mari kita ambil contoh “iniadalahpesanrahasia” dan “kunci” yang digunakan di atas. Bila kita menggunakan metode autokey, key yang komplit nya menjadi “kunciiniadalahpesanra” yang juga memiliki panjang 21 karakter. Secara umum metode ini lebih aman dari metode sebelumnya.

Dalam program kami tidak secara harafiah menggunakan Vigenere Table untuk melakukan enkripsi dan dekripsi teks, melainkan kita menggunakan representasi yang menggunakan modulo. Pertama – tama representasikan tiap karakter dari teks dan key sebagai angka – angka, lalu gunakanlah persamaan berikut untuk enkripsi.

$$C[i] = (P[i] + K[i]) \bmod 26 \dots (2)$$

Dengan C merepresentasikan karakter yang telah disandi, P merepresentasikan teks originalnya, sedangkan K merepresentasikan Key yang digunakan. [i] disini melambangkan karakter pada posisi ke berapa, misalnya P[5] adalah karakter ke – 5 dari teks original.

Sedangkan untuk melakukan decipher, Anda bisa

melakukan kebalikannya, yaitu dengan menggunakan persamaan berikut :

$$P[i] = (C[i] - K[i]) \bmod 26 \dots (3)$$

Terdapat sedikit variasi yang saya implementasikan pada persamaan tersebut untuk memasukkan lebih banyak karakter, variasi – variasi yang dilakukan akan dibahas lebih lanjut di bab 3.

### C. CSV

CSV atau Comma Separated Values adalah sebuah format file yang berisi teks yang mengandung data – data. File CSV bisasa digunakan untuk transfer data di antara aplikasi.

Struktur dari sebuah file CSV cukup sederhana. File tersebut terdiri dari data yang dipisahkan (seperated/delimited) dengan karakter koma. Namun sebenarnya delimiternya tidak perlu karakter ‘,’ juga. Beberapa opsi yang umum dipakai adalah karakter semi-kolon/titit koma ‘;’. Contoh dari isi sebuah CSV file adalah sebagai berikut :

```
NIM>Nama,Jurusan,IPK
13122111,Budi,Teknik Mesin,3.2
13522078,Sean,Teknik Informatika,3.4
25019210,Andika,Teknik Sipil,2.9
17421001,Ivan,DKV,3.6
13220334,Vania,Teknik Mesin,3.2
```

## III. IMPLEMENTASI PROGRAM

### A. Modifikasi dan Asumsi

Vigenere Cipher, dalam versi originalnya, hanya terdiri dari 26 karakter yang merepresentasikan ke – 26 huruf dalam alfabet. Bila terdapat karakter lain selain itu, maka cipher hanya akan melewati enkripsi pada karakter tersebut dan melanjutkan enkripsi. Dalam file CSV, seringkali terdapat banyak karakter yang di luar 26 huruf dalam alfabet, contohnya suatu kolom yang terdiri dari nilai numerik. Bila kita menggunakan cara yang tradisional untuk menangani kasus tersebut, maka nilai – nilai numerik tidak akan tersandi. Hal tersebut tentu merupakan *security flaw*.

Untuk mengatasi hal tersebut, terdapat modifikasi yang dilakukan pada program Vigenere Cipher yang diimplementasi. Pertama – tama dibuat sebuah dictionary untuk mapping dari tiap karakter. Seperti biasanya karakter ‘a’ hingga ‘z’ di mapping menjadi 26 karakter pertama yaitu 0 – 25. Selanjutnya untuk karakter kapital, yaitu ‘A’ hingga ‘Z’ , akan dipetakan ke 26 karakter selanjutnya, 26 sampai 51. Karakter ‘1’ sampai ‘9’ dipetakan ke angka 54 sampai 62. Karakter 0 dipetakan ke angka 63. Terdapat 3 karakter khusus yaitu ‘ ‘ , ‘”’ , dan ‘.’. Untuk karakter spasi dipetakan pada angka 52, karakter petik dipetakan pada angka 53 dan karakter titik dipetakan pada angka 64. Terlihat bahwa karakter koma tidak dipetakan karena ingin digunakan sebagai delimiter jadi bila pada file CSV terdapat karakter koma (yang kemungkinan besar ada), maka karakter tersebut tidak akan disandi. Lebih dari itu, sangat tidak

dianjurkan untuk menggunakan , di dalam data yang digunakan untuk enkripsi karena akan dianggap sebagai kolom baru.

Karena tambahan karakter tersebut, kita juga perlu memodifikasi persamaan yang digunakan untuk men-enkripsi dan dekripsi sandi kita menjadi :

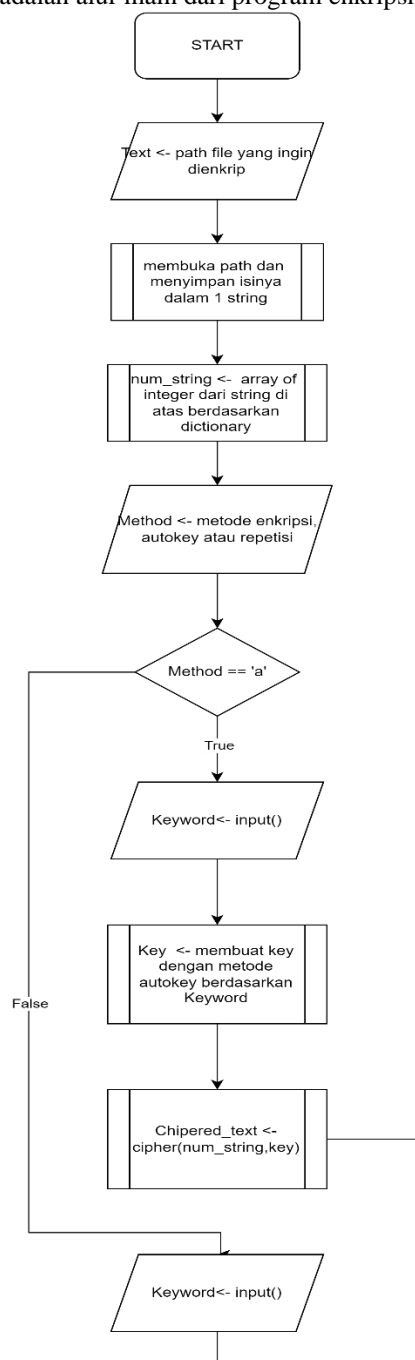
$$C[i] = (P[i] + K[i]) \bmod 64 \dots (4)$$

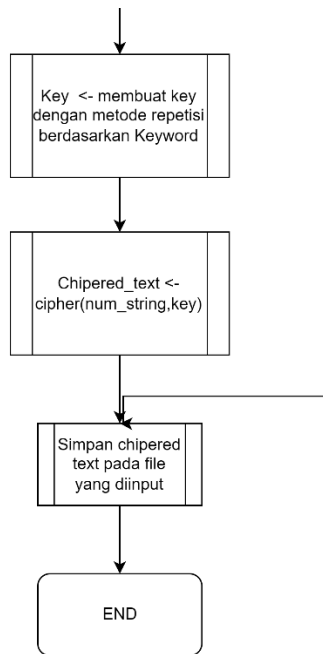
$$P[i] = (C[i] - K[i]) \bmod 64 \dots (5)$$

Dengan persamaan 3 digunakan untuk melakukan enkripsi sedangkan persaaam 4 digunakan untk dekripsi.

### B. Alur Program

Berikut adalah alur main dari program enkripsi :

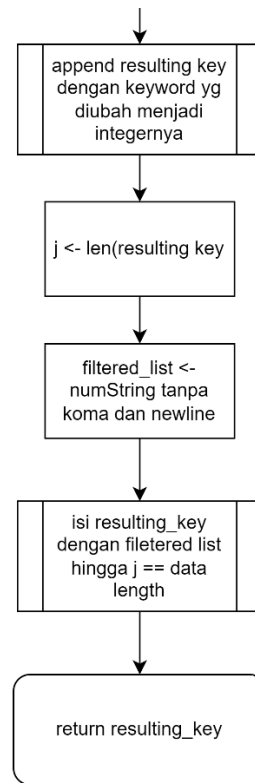
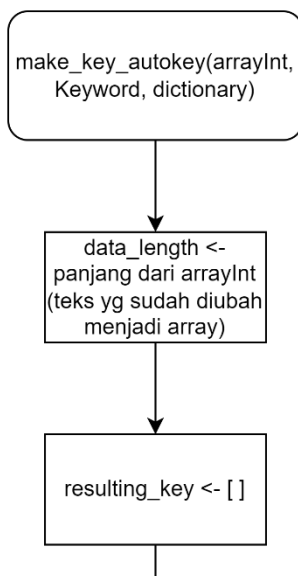




Gambar 2. Diagram Alur 'main' dari program enkripsi

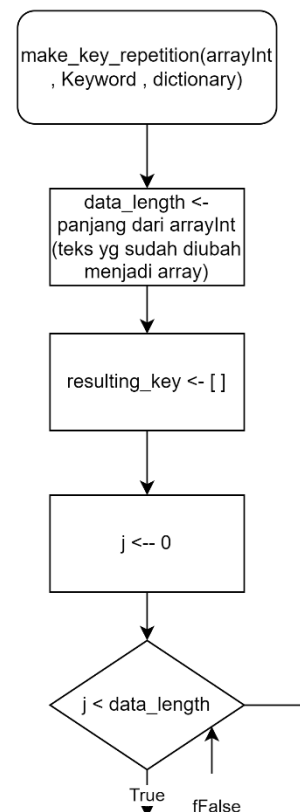
Secara garis besar, program main bertujuan untuk mengambil data dari suatu file CSV, mengubahnya menjadi array of integer berdasarkan dictionary yang sudah dideskripsikan di bab 3A, menerima sebuah Keyword, membuat keyword dengan metode autokey atau dengan repetisi, menyandikan data tersebut dan akhirnya menyimpan ke dalam file CSV lagi. Bisa dilihat pada diagram alur tersebut, terdapat fungsi cipher. Fungsi cipher tersebut sebenarnya terdiri dari dua fungsi yaitu melakukan cipher menggunakan persamaan (4), lalu mengkonversikannya menjadi satu buah string. Pada proses enkripsi, karakter yang diskrip enkripsinya adalah karakter ',' (koma) dan '\n' (new line).

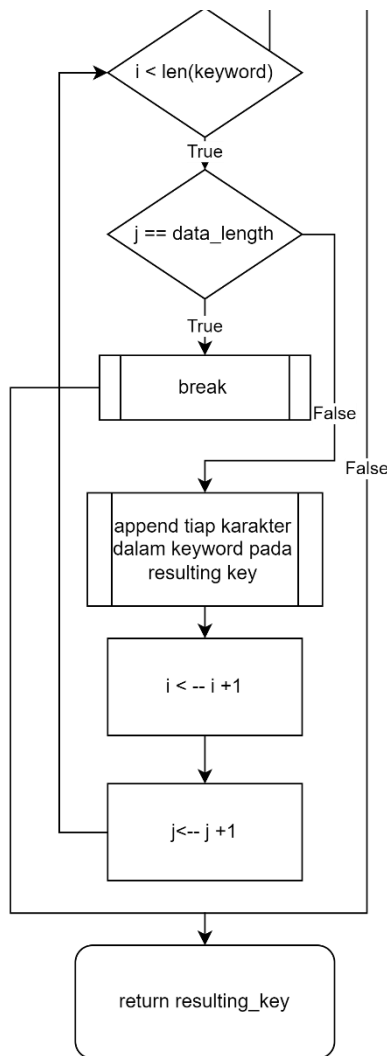
Seperti yang telah diberitakan sebelumnya, terdapat 2 metode untuk menciptakan key dari Keyword yaitu autokey dan repetisi. Berikut adalah alur dari fungsi yang membuat key dengan metode autokey:



Gambar 3. Diagram Alur make\_key\_autokey

Sedangkan untuk metode repetisi, algoritmanya lebih sederhana. Diagram alurnya adalah sebagai berikut :





Gambar 4. Diagram Alur make\_key\_repetition

Terlihat bahwa make\_key\_autokey dan make\_key\_repetition memiliki mendeskripsikan cara membuat key yang sudah dijelaskan pada bab 2B. Untuk algoritma dekripsi mirip dengan algoritma enkripsi tapi menggunakan persamaan (5). Kode lengkap bisa dilihat di repo github yang tertera pada informasi penulis di atas.

#### IV. HASIL DEMO PROGRAM DAN OBSERVASI

Berikut merupakan data yang digunakan untuk keperluan testing program.

```

name, department,birthday month,birth year
John Smith,Accounting,November,2000
Erica Meyers,IT,March,1992
Nelson Budiman,Advertising,July,1996
Venti d'Bard,Sales,March,2001
Alex Dior,Accounting,June,1990
  
```

File CSV tersebut mendeskripsikan data pegawai – pegawai dalam sebuah perusahaan. Atribut yang dideskripsikan terdiri dari berapa nama pegawai, departemen dimana mereka bekerja, bulan lahir, serta tahun lahir. Terlihat ada data yang terdiri dari

angka semua yaitu birth year dan terdapat kolom dengan datum yang memiliki duplikatnya, contohnya bisa dilihat pada kolom birthday month dimana kata “March” ditemukan sebanyak dua kali.

Untuk keywordnya, akan dipilih kata “matematika”. Bila kita sandikan menggunakan metode repetisi, maka hasilnya akan sebagai berikut :

```

N T7,2LL9FTALFT,IEPHH2HQaAVJR6,PJT6hUC R
1GHBh K7T6,eC1VQLHIBN,zCcAK'EF,VIZs
oFI1HSy3fAPG,iA,y Y9F,cYrV
nLHQCNOuMD7T7L,m2c7RHPOGBG,1MLM,YiYh
C7NHPWBPh Y6,sSHCG,mHJC6,ZjZc
tDELhlGCR,t5CCbJR7N5,nUBL,aYkZ
  
```

Terdapat beberapa hal menarik yang bisa kita observasikan berdasarkan hasil tersebut. Seperti yang diharapkan, kata yang duplikat pada teks original akan disandi sebagai dua kata yang berbeda. Bila kita ambil contoh yang sebelumnya, kata ‘March’ yang pertama disandi sebagai “y Y9F” sedangkan yang kedua disandi sebagai “mHJC6” (kata yang dihighlight berwarna kuning). Dua hal yang bisa diobservasikan lagi adalah bahwa tiap kata dari yang original dan yang sudah disandi memiliki panjang yang sama serta koma pada teks original tidak ikut disandi. Tentu setelah dekripsi akan menghasilkan teks yang semula.

```

PS C:\Users\Sean Nugroho\Documents\Semester3\MatDis\Makalah> & "C:/Users/Sean Nugroho/
.exe" "c:/Users/Sean Nugroho/Documents/Semester3/MatDis/Makalah/decipher.py"
Masukkan nama file CSV yang sudah di-enkrip : matematika_r.csv
File tersebut di-enkrip dengan metode Repetition atau Autokey ? (R/A) r
Key untuk file tersebut apa ? matematika
Isi dari file tersebut adalah sebagai berikut
name,department,birthday month,birth year
John Smith,Accounting,November,2000
Erica Meyers,IT,March,1992
Nelson Budiman,Advertising,July,1996
Venti d'Bard,Sales,March,2001
Alex Dior,Accounting,June,1990
  
```

Gambar 5. Hasil dekripsi dari teks yang dienkripsi menggunakan metode repetisi

Hasil dekripsi menggunakan metode autokey, menghasilkan file CSV sebagai berikut :

```

N T7,2LL9FUAEFK,E7WaH6BfPITUO9,NWRVihT47W
qcTFO8vKOI,SC9VPnJ9PO,5KW9zDNJ,Sdq1
DqmH7QmS97dK, b, Y W3C, 7E
yKNTcoieQD7NaE,eIcAXPJMrfV,0sjt,Ulrd
yToHNRvPm3Xp,81GVr,CaQ5S,5hnh
cBGfbwEPL,uD5eslsJBG,mMQ3,jkcm
  
```

Beberapa hal bisa kita amati adalah, tentu hasil sandi dengan autokey dan repetisi mengasilkan dua sandi yang berbeda, tapi terdapat satu observasi yang cukup menarik. Terlihat bahwa 10 karakter pertama dari hasil sandi autokey dan repetisi persis sama. Hal tersebut terjadi karena key yang dihasilkan oleh autokey dan repetisi mengandung keyword sebagai elemen pertamanya. Pada kasus ini, key untuk autokey adalah “matematikaname departementbirthday month ...” sedangkan dengan metode repetisi adalah “matematikamatematikamatematika...” seterusnya hingga panjang dari key sama dengan panjang dari teks original. Hasil

dekripsi dari file yang telah disandi tentu menghasilkan teks original dari file CSV seperti yang telah dicontohkan di atas atau tautan yang ada di bawah.

## V. KESIMPULAN

Telah diimplementasikan Vigenere Cipher untuk melakukan enkripsi File CSV dengan program berbasis Python. Dari hasil eksperimen, didapatkan beberapa observasi yaitu:

1. Key yang dihasilkan dengan metode Autokey akan mengambil keyword dan menambahkannya ke awal teks.
2. Key yang dihasilkan dengan metode repetisi akan mengulang – ulang keyword hingga panjangnya sama dengan teks original yang dimasukkan
3. Hasil enkripsi yang dihasilkan dengan metode autokey dan repetisi berbeda, kecuali untuk n karakter pertama dimana n adalah panjang keyword.
4. Dengan Vigenere Cipher, enkripsi dari suatu kata yang duplikat akan disandikan menjadi kata yang berbeda.

## VII. UCAPAN TERIMA KASIH

Penulis dengan ini menyampaikan terima kasih, terutama kepada pihak – pihak berikut :

1. Tuhan Yang Maha Esa.
2. Bapak dan Ibu Dosen mata kuliah IF 2120, Matematika Diskrit.
3. Kedua orang tua penulis.
4. Pembaca sekalian

Yang telah membantu penulis dalam menyusun makalah ini dan sudah memberikan waktu dan perhatiannya untuk membaca makalah ini.

## TAUTAN KODE PROGRAM

[https://github.com/Leaguemen/CSV\\_Encryption\\_with\\_Vigenere\\_Cipher.git](https://github.com/Leaguemen/CSV_Encryption_with_Vigenere_Cipher.git)

## REFERENSI

- [1] A. A. Bruen, M. Forcinito, and J. M. Mcquillan, *Cryptography, information theory, and error-correction : a handbook for the 21st century*. Hoboken, Nj: Wiley, 2021.
- [2] Ayush Khanduri, "Vigenère Cipher - GeeksforGeeks," *GeeksforGeeks*, Oct. 07, 2016. <https://www.geeksforgeeks.org/vigenere-cipher/> (accessed Dec. 08, 2023).
- [3] A. Szczepanek, "Modulo Operator: Practical Uses in Arithmetics," *www.omnicalculator.com*, Jun. 05, 2003. <https://www.omnicalculator.com/math/uses-of-modulo> (accessed Dec. 08, 2023).
- [4] N. Academy, "Polyalphabetic Cipher (Vigenère Cipher)," *www.youtube.com*, Jul. 03, 2021. <https://www.youtube.com/watch?v=Ic4BzVggNY8&t=207s> (accessed Dec. 08, 2023).
- [5] R. Pierce, "Modulo Operation Definition (Illustrated Mathematics Dictionary)," *www.mathsisfun.com*. <https://www.mathsisfun.com/definitions/modulo-operation.html> (accessed Dec. 08, 2023).
- [6]

## PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 9 Desember 2023



Venantius Sean Ardi Nugroho, 13522078