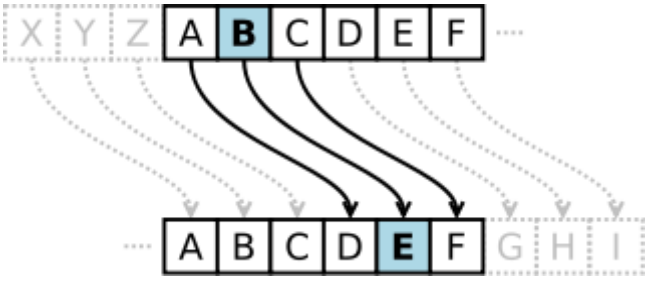
Universidade do Estado do Rio Grande do Norte
Disciplina: Segurança em Redes de Computadores
Professor: Isaac de Lima Oliveira Filho
Alunos: Joyce Claine e Marcos Monteiro

Implementação de Cifras

1- Cifra de César.

Descrição:

- Primeira cifra de substituição conhecida de Júlio César
- Primeiro uso atestado em assuntos militares
- Substitui cada letra pela terceira letra



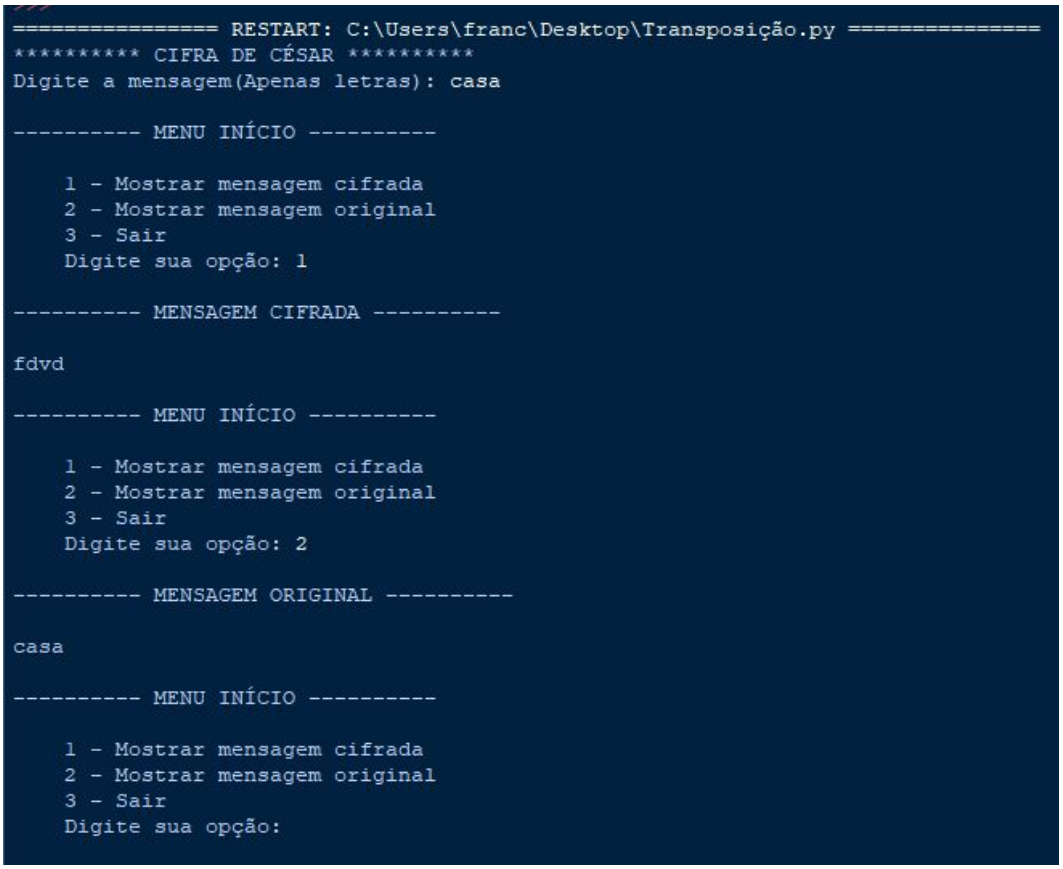
Exemplo:

- Pode definir transformação como:
  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
  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
- Matematicamente dar a cada letra um número
  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
  0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

  Entrada:
  meet me after the toga party
  Saída:
  PHHW PH DIWHU WKH WRJD SDUWB

Execução do código

O código da cifra de César foi implementado usando a linguagem Python, e pode ser executado com o IDLE do Python, PyCharm ou diretamente no prompt de comando(cmd).
A mensagem de entrada do código precisa ser colocada sem espaços.
O algoritmo faz o processo de cifragem e decifragem, o código está comentado explicando detalhadamente cada passo. A imagem abaixo mostra como é a saída do algoritmo.



2 - Cifra Monoalfabética

Descrição:

- Em vez de mudar apenas o alfabeto, poderia embaralhar as letras arbitrariamente
- Cada letra de texto simples mapeia para uma letra diferente de texto cifrado aleatório
- Daí a chave é de 26 letras

Exemplo:

Plain: abcdefghijklmnopqrstuvwxyz
Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN

Plaintext: ifwewishtoreplaceletters
Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA

Execução do código

O código da cifra Monoalfabética foi implementado usando a linguagem Python, e pode ser executado com o IDLE do Python, PyCharm ou diretamente no prompt de comando(cmd).
A mensagem de entrada do código precisa ser colocada sem espaços.
O algoritmo faz o processo de cifragem e decifragem, o código está comentado explicando detalhadamente cada passo. A imagem abaixo mostra como é a saída do algoritmo.

```
========== RESTART: C:/Users/franc/Desktop/teste.py ==========
********** CIFRA MONOALFABÉTICA **********

Digite a mensagem(Apenas letras): casaazul

---------- MENU INÍCIO ----------

    1 - Mostrar mensagem cifrada
    2 - Mostrar mensagem original
    3 - Sair
    Digite sua opção: 1

---------- MENSAGEM CIFRADA ----------

VDADDNOS

---------- MENU INÍCIO ----------

    1 - Mostrar mensagem cifrada
    2 - Mostrar mensagem original
    3 - Sair
    Digite sua opção: 2

---------- MENSAGEM ORIGINAL ----------

casaazul

---------- MENU INÍCIO ----------

    1 - Mostrar mensagem cifrada
    2 - Mostrar mensagem original
    3 - Sair
    Digite sua opção:
```

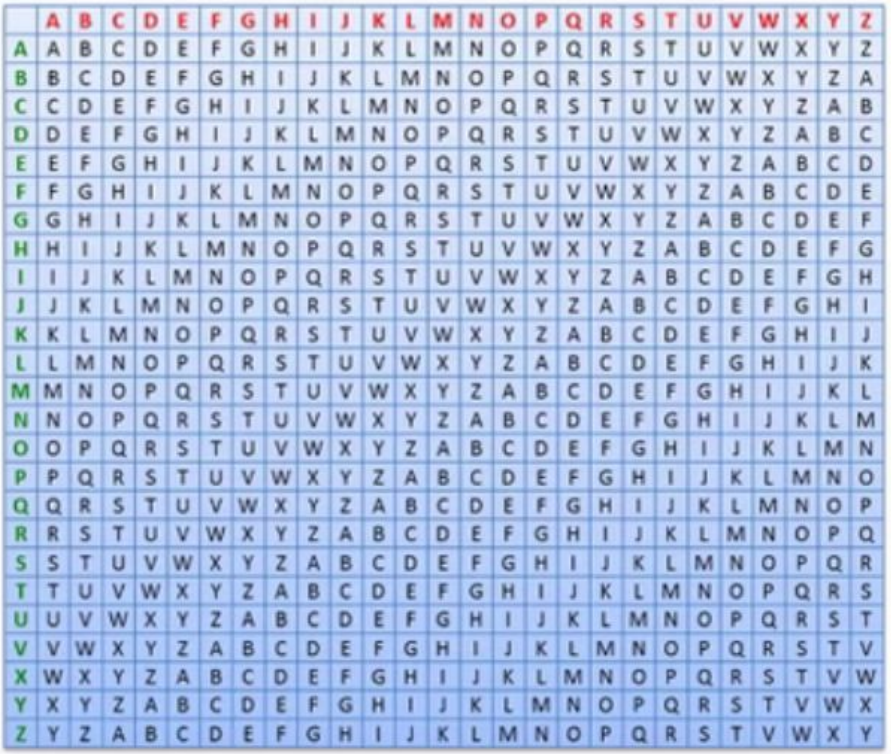
3 - Cifra Playfair.

NÃO CONSEGUIMOS IMPLEMENTAR

4 - Vigenère

Descrição:

- A cifra de Vigenere foi amplamente usada na guerra civil americana
- Escreve-se a palavra-chave repetida, acima dela usa-se cada letra chave como uma chave de cifra. Esse processo é usado para criptografar a letra de texto simples correspondente
- A tabela abaixo é usada para cifrar o texto usando a mensagem original e a chave



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

Exemplo:

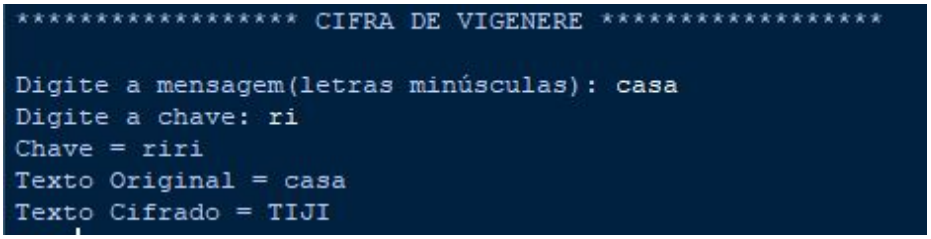
Por exemplo, usando palavras-chave **deceptive**

> **Key:** deceptivedeceptivedeceptive
> **Plaintext:** wearediscoveredsaveyourself
> **Ciphertext:** ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Execução do código

O código de Vigenère foi implementado usando a linguagem Python, e pode ser executado com o IDLE do Python, PyCharm ou diretamente no prompt de comando(cmd).

A mensagem de entrada do código precisa ser colocada sem espaços.
O algoritmo faz o processo de cifragem e decifragem, o código está comentado explicando detalhadamente cada passo. A imagem abaixo mostra como é a saída do algoritmo.



5 - Transposição (linha ou coluna).

Descrição:

- Considere agora cifras clássicas de transposição ou permutação
- Estes ocultam a mensagem rearranjando a ordem das letras
- Sem alterar as letras reais usadas
- Pode reconhecê-los desde que tenha a mesma distribuição de frequência que o texto original
- Uma transposição mais complexa escreve letras de mensagem em linhas sobre um número especificado de colunas
- Em seguida, reordenar as colunas de acordo com alguma chave antes de ler as linhas

Exemplo:

Key:	3 4 2 1 5 6 7
Plaintext:	a t t a c k p
	o s t p o n e
	d u n t i l t
	w o a m x y z

Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

Execução do código

O código de transposição foi implementado usando a linguagem Python, e pode ser executado com o IDLE do Python, PyCharm ou diretamente no prompt de comando(cmd).
A mensagem de entrada do código precisa ser colocada sem espaços.
O algoritmo faz o processo de cifragem e decifragem, o código está comentado explicando detalhadamente cada passo. A imagem abaixo mostra como é a saída do algoritmo.

```
>>>
============ RESTART: C:\Users\franc\Downloads\FRANK_Transposição.py ===========
********** CIFRA DE TRANSPOSIÇÃO **********

Digite a chave: CASA

Digite a mensagem: MORO PERTO DA CASA GRANDE


['C', 'A', 'S', 'A']
['M', 'O', 'R', 'O']
['P', 'E', 'R', 'T']
['O', 'D', 'A', 'C']
['A', 'S', 'A', 'G']
['R', 'A', 'N', 'D']
['E', 'A', 'X', 'A']

------------------- MENSAGEM CIFRADA -------------------

OEDSAA OTCGDA MPOARE RRAANX


------------------- DECIFRAR MENSAGEM -------------------

Digite a chave: CASA
Digite a frase cifrada: OEDSAA OTCGDA MPOARE RRAANX


MPOARE
OEDSAA
RRAANX
OTCGDA
>>>
```