INE5429 - Segurança de Computadores

Mateus Rissi Rodrigo Pedro Marques

Março de 2017

1 Apresentação dos algoritmos Cifra de Cesar, *PlayFair* e Viginère

1.1 Cifra de César

Cifra de César é um tipo de cifra de substituição onde cada letra do texto é substituída por outra letra do mesmo alfabeto, porém, esta outra letra está em uma posição abaixo dela em um número fixo de vezes.

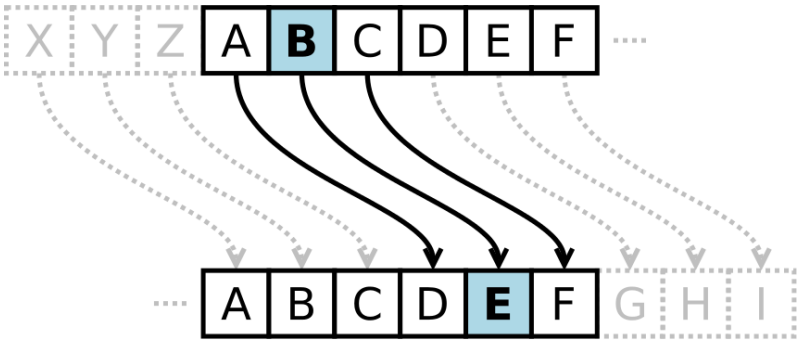

Figura 1 – Exemplo de Cifra de César com chave igual a 3.

Na figura 1, onde a chave – que indica quantas casas o alfabeto será movido – é igual a 3, é demonstrado que a letra B corresponde a letra E.

A cifra tem esse nome em homenagem a Julio César que, segundo Suetónio, a usava com uma troca de três posições para proteger mensagens de significado militar. Por exemplo:

Alfabeto Normal: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Alfabeto Cifrado: DEFGHIJKLMNOPQRSTUVWXYZABC

Assim, a aplicação deste método em uma mensagem como "*a ligeira raposa marrom saltou sobre o cachorro cansado*", resultaria na seguinte mensagem cifrada: "*D OLJHLUD UDSRVD PDUURP VDOWRX VREUH R FDFKRUUR FDQVDGR*".

Decifrando

A Cifra de César é uma das mais simples e conhecidas técnicas de criptografia e, como todas as cifras de substituição monoalfabéticas, a cifra de César é facilmente decifrada e na prática não oferece essencialmente nenhuma segurança na comunicação. Para decifrar a mensagem cifrada duas situações podem ser consideradas:

1. Um interceptor conhece (ou adivinha) que algum tipo de cifra de substituição simples foi utilizado, mas não especificamente que é uma Cifra de César.

2. Um interceptor sabe que uma cifra de César foi usada, mas não sabe o valor da troca.

No primeiro caso, a cifra pode ser decifrada usando análise de frequência ou verificando os padrões de palavras. No segundo caso é ainda mais simples, pois existem apenas um número limitado de rotações possíveis (26 no alfabeto português brasileiro).

1.2 *PlayFair*

A Cifra *Playfair* usa uma tabela de 5 por 5 contendo uma palavra ou até uma frase chave. Memorizar a chave e as 4 simples regras são tudo o que é necessário para montar a tabela e usar a cifra.

Primeiramente, para criar a tabela é necessário completar os espaços na tabela com as letras da palavra chave – sem letras repetidas – e então completar o resto da tabela com as letras do alfabeto em ordem. Como só há 25 espaços na tabela, métodos como omitir a letra Q ou unir a letra I e J no mesmo espaço são comumente utilizados.

Para cifrar uma mensagem devemos quebra-la em digramas – grupos de 2 letras – como, por exemplo, "HelloWorld" vira "HE LL OW OR LD", e então mapear na tabela. É necessário que sejam digramas, então numa palavra de número ímpar devemos adicionar algum outro caractere para completar o par. Agora pense no digrama como cantos opostos de um retângulo dentro da tabela e então aplique as 4 regras seguintes, em ordem, para cada par da mensagem:

1. Se as letras do par são iguais (ou há apenas 1 letra), adicione um X após a primeira letra. Cifre o novo par e continue.

2. Se as letras do par estão na mesma linha, substitua elas pelas letras que estão imediatamente a sua direita (mudando para a esquerda se a letra no par original estava do lado direito).

3. Se as letras aparecem na mesma coluna, substitua elas pelas letras que estão imediatamente abaixo (mudando para cima se a letra no par original estava no final da coluna).

4. Se as letras do par não estão na mesma linha ou coluna, substitua elas pelas letras que estão na mesma linha mas que representam o outro par de cantos do retângulo definido pelo par original. A ordem importa – a primeira letra do par cifrado deve ser a que estava na mesma linha que a primeira letra do par original.

Para decifrar o texto use o inverso das 3 últimas regras e a regra 1 como está (só que retirando qualquer "X" extra que não faz sentido na mensagem final).

A figura 2 apresenta um exemplo onde a palavra "*PlayfairExample*" foi utilizada como palavra chave (letras em vermelho são as que foram omitidas).

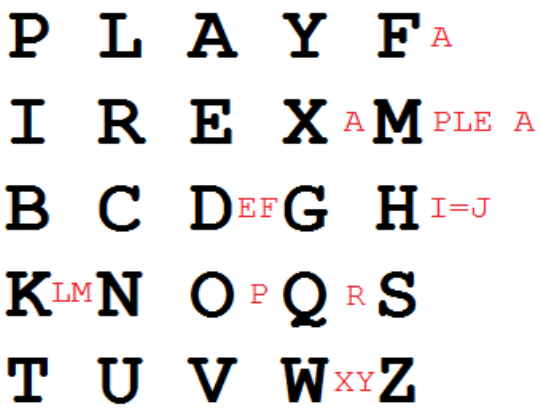

Figura 2 – PlayFairExample

1.3 Vigenère

Esta cifra consiste no uso de várias cifras de César em sequência, com diferentes valores de deslocamento ditados por uma "palavra-chave". Para cifrar, é usada uma tabela de alfabetos que consiste no alfabeto escrito 26 vezes em diferentes linhas, cada um deslocado ciclicamente do anterior por uma posição. As 26 linhas correspondem às 26 possíveis cifras de César. Uma palavra é escolhida como "palavra-chave", e cada letra desta palavra vai indicar a linha a ser utilizada para cifrar ou decifrar uma letra da mensagem. É possível observar essa tabela na figura 3.

	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

Figura 3 – Tabela de Vinegère

Caso queiramos criptografar, por exemplo, a mensagem "*WEHAVEAMEETINGINTWOMINUTES*" e a palavra chave é "*CODEX*", como mostra a figura 4, a mensagem resultante será "*YSKESGOPIBVWQKFPHZSJKBXXBU*".

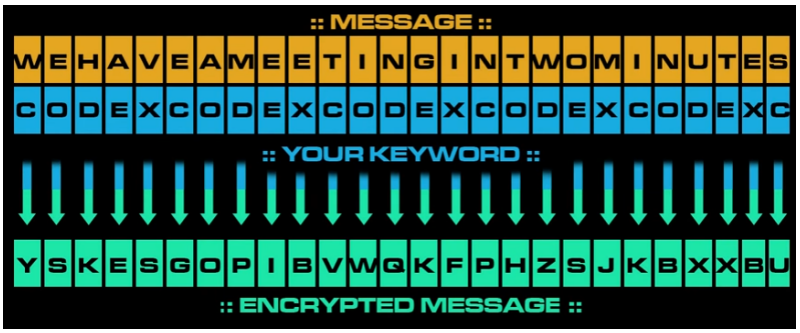

Figura 4 – Exemplo de criptografia através do método de Vinegère.

Para decifrar tomamos o caminho inverso, como mostra a figura 5.

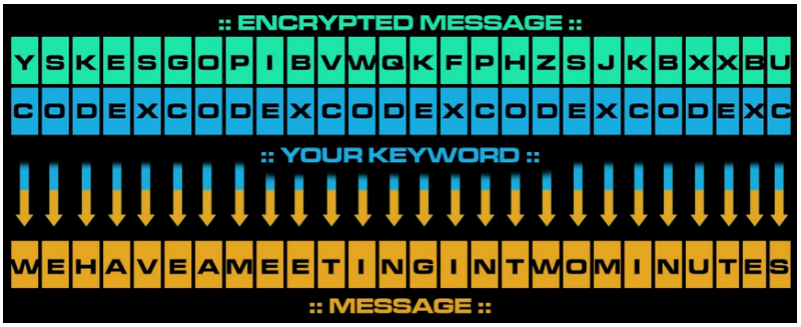

Figura 5 – Exemplo de decifragem através do método de Vinegère.

As cifras polialfabéticas são mais difíceis de quebrar por análise de frequência, mas têm uma fraqueza se a chave é curta e constantemente repetida. Como resultado, palavras comuns como "de" vão provavelmente aparecer criptografadas segundo as mesmas letras da chave, levando à descoberta de padrões repetidos no texto.

2 Questões sobre a implementação dos algoritmos Cifra de Cesar, *Play-Fair* e Viginère

A linguagem de programação utilizada para implementar estes algoritmos foi C++. A seguir é possível observar as respostas do questionário dado em aula.

2.1 Cifra de Cesar

- **Quantidade de trocas para frente foram feitas para cifrar:** o algoritmo implementado por nós permite escolher o número de deslocamento para realizar a cifragem, porém, para facilitar o seu uso, fixamos o valor de deslocamento para 3.
- **Resultado da cifra do primeiro nome de cada aluno do grupo:** com o deslocamento igual a 3, os nomes "*MATEUS*" e "*RODRIGO*" resultaram em "*PDWHXV*" e "*URGULJR*", respectivamente.

2.2 *PlayFair*

- **Chave utilizada:** "*COMPUTACAO*" resultando em "*COMPUTABDEFGHIKLNQRSVWXYZ*".
- **Letras retiradas ou combinadas:** A letra "J" virou "I".
- **Resultado da cifra do primeiro nome de cada aluno do grupo:** os nomes "*MATEUS*" e "*RODRIGO*" resultaram em "*OBATEZ*" e "*NPIYKHMW*", respectivamente.

2.3 Viginère

- **Chave utilizada:** "*SKYHILL*".
- **Letras retiradas ou combinadas:** Esta cifra consiste no uso de várias cifras de César em sequência, com diferentes valores de deslocamento ditados por uma "palavra-chave".
- **Resultado da cifra do primeiro nome de cada aluno do grupo:** o nome "*MATEUS*" gerou "*EKRLCD*"; o nome '*RODRIGO*" gerou "*JYBYQRZ*".