

Cifras antigas

- Cifra de César
- Cifras de Substituição Simples
- Cifra de Vigenère
- Cifras de Transposição

Cifra de César

A Cifra de César é um dos métodos mais simples e comuns de encriptação. Mesmo não sendo muito comum em CTFs, ainda é um conhecimento básico de criptografia.

“Esse método tem esse nome pois era usado por Júlio César em suas correspondências

Nessa cifra, cada letra da mensagem é substituída por uma letra do alfabeto deslocado por um número fixo.

Por exemplo, se queremos encriptar a mensagem `hack the planet`, podemos deslocar cada letra do alfabeto **3 vezes para direita** (ou **right 3**). Assim, a substituição teria esse formato:

	A	B	C	D	E	F	G	H	I	J	K	L	M	
right		D	E	F	G	H	I	J	K	L	M	N	O	P
3														

	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
right		R	S	T	U	V	W	X	Y	Z	A	B	C
3													

texto original: `hack the planet`

texto cifrado: `kdfn wkh sodqhw`

Dessa forma, o texto gerado se torna incompreensível de forma que só quem sabe o algoritmo usado poderá recuperá-lo.

ROT13

Um dos tipos mais comuns de Cifra de César é o **ROT13**. Nele, o alfabeto é deslocado 13 vezes. Como o alfabeto tradicional possui 26 letras, o ROT13 possui a propriedade de que o mesmo algoritmo usado para encriptar a mensagem é usado para decriptar.

Detectando

Mensagens encriptadas pela cifra de César normalmente produzirão um amontoado de caracteres sem significado, como `kdfn wkh sodqhw`, e suas letras terão uma distribuição de frequência similar à língua usada (provavelmente inglês), mas com as letras trocadas. Esse conceito será abordado com mais profundidade em Cifras de Substituição.

Devido a facilidade de quebrar essa cifra, pode ser conveniente tentar solucioná-la sem nem ao menos uma análise de frequência.

Solucionando

Como num alfabeto usual são usados apenas 26 caracteres, a Cifra de César possui apenas 25 tipos de rotações possíveis (pois a rotação 26 é a própria mensagem). Assim, um **testa tudo**, onde você faz todos os tipos de rotações possíveis, é a opção mais simples.

Existem ferramentas online muito eficientes para quebrar uma Cifra de César, como o site `dcode`, porém não é muito difícil codificar um *testa tudo* para isso.

Codificando um testa tudo

Primeiro, codificaremos uma função `rot()` que aplica a rotação em um caractere, de acordo com o deslocamento determinado (o `shift`):

```
def rot(char, shift):  
    return chr((ord(char) - ord('A') + shift)%26 + ord('A'))
```

Assim, podemos usar essa função para criar um `caesar_brute_force()` que recebe um texto cifrado e imprime todas as rotações possíveis.

```
def caesar_brute_force(cipher_text):
    cipher_text = cipher_text.upper()
    for i in range(26):
        line = ''
        for c in cipher_text:
            line += rot(c, i) if c.isalpha() else c
        print(f'rot{i}: \t{line}')
```

Cifras de Substituição Simples

Em uma cifra de substituição simples, cada letra é substituída individualmente de acordo com um **alfabeto de substituição**. Esse alfabeto pode ser uma rotação fixa do alfabeto normal (como a cifra de César) ou algum embaralhamento mais complexo.

Alguns exemplos notáveis de cifra de substituição simples são:

Cifra de Atbash

“ Seu nome tem origem da primeira, última, segunda e penúltima letra Hebraica (Aleph-Taw-Bet-Shin)

Nessa cifra, cada letra é mapeada para o alfabeto invertido, ou seja, a primeira vira a última, a segunda vira a penúltima e assim por diante.

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

Assim, se usarmos essa cifra em `may the force be with you`, obteremos:

```
original: M A Y T H E F O R C E B E W I T H Y O U
cifrado:  N Z B G S V U L I X V Y V D R G S B L F
```

A Cifra de Atbash pode ser interpretada como um caso particular da Cifra de Affine, uma cifra que usa aritmética modular para encriptar.

Cifra da Palavra-Chave

A Cifra da Palavra-Chave ou *keyword cipher* consiste em escolher uma **chave** e usá-la para decidir como as letras serão substituídas.

As palavras repetidas dessa chave serão removidas e a própria chave será o começo do alfabeto a ser mapeado. O resto das letras continuarão em ordem alfabética, tirando as letras já usadas.

Por exemplo, escolhendo a chave `Marvin`, o novo alfabeto terá esse formato

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

Assim, ao encriptar a mensagem `Arthur Dent`, obteremos:

```
original: A R T H U R D E N T
cifrado:  M P S C T P V I J S
```

Detectando

Como mencionado na seção de Cifra de César, uma mensagem encriptada por uma cifra de substituição simples terá uma distribuição de frequência das letras semelhante ao da língua usada, mas com as letras trocadas.

Essa distribuição de frequência de um texto pode ser identificada através de uma **análise de frequência**.

Nas línguas naturais, algumas letras aparecem mais frequentemente que outras, como uma espécie de digital do idioma. Por exemplo, a letra mais comum na língua inglesa é o "e", em português é o "a".

Essa análise de frequência pode ser feita simplesmente contando as letras do texto. Existem ferramentas online para isso como o site [dcode](#) ou pode ser feito rapidamente com um biblioteca em Python, onde `text` é o texto a ser analisado:

```
from collections import Counter
Counter(text.upper()).most_common()
```

Solucionando

O ponto fraco de cifras de substituição simples é que elas são muito suscetíveis à **análises de frequência**.

Assim, se você tiver um texto de tamanho razoável, por volta de 50 caracteres, é possível analisar a frequência com que as letras aparecem e deduzir qual foi o alfabeto de substituição usado.

O site [guaballa](#) é um excelente decodificador de cifras de substituição simples.

Referências

Cifra de Atbash: [Jeremiah's Game](#)

Cifra da Palavra-Chave: [GeeksforGeeks](#)

[Learn Cryptography](#)

Um texto encriptado por essa cifra pode ser detectado através de uma **análise de frequência**.

A Cifra de Vigenère costuma gerar textos com uma distribuição de frequência das letras próximo ao uniforme. Se um texto cifrado que não é esperado esse tipo de distribuição obter esse resultado, provavelmente é Cifra de Vigenère, ou alguma outra Cifra Polialfabética.

Solucinando

Mesmo gerando uma distribuição uniforme em análises de frequência, essa cifra tem uma vulnerabilidade: a palavra-chave é usada várias vezes em um texto grande.

Dessa forma, se a chave tiver tamanho 5, por exemplo, e ajustarmos o texto em linhas de comprimento 5, cada coluna terá a mesma rotação. Assim, podemos chutar tamanhos da palavra-chave e usar a mesma análise de cifra de substituição simples para cada coluna.

Uma ferramenta online muito útil para quebrar a Cifra de Vigenère é o site [dcode](#).

Referências

GeeksforGeeks

Cifras de Transposição

Cifras de Transposição

Content about Cifras de Transposição.