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 substituida 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:

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

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

```
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 encripitar 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}')
```

Exercícios

OverTheWire: Krypton 1

OverTheWire: Krypton 2

WeChall: Caesar

Revision #8
Created Sat, Oct 6, 2018 6:45 PM by Andrew
Updated Mon, Jan 28, 2019 9:56 PM by Andrew