

Cifras de Transposição

Na tentativa de encontrar um método alternativo às cifras de substituição simples, que estavam se tornando frágeis, foram criadas as **Cifras de Transposição**. Nessa cifra, o texto permanece o mesmo mas as ordem dos caracteres são alteradas, embaralhando a mensagem de acordo com um padrão.

Existem vários padrões diferentes para realizar a transposição, os dois mais famosos são a **transposição colunar simples** e a **rail fence**.

Transposição colunar

Com essa regra, a mensagem é escrita horizontalmente numa matriz de largura fixa e a saída é o texto lido verticalmente nessa matriz.

Numa **transposição colunar simples** essa leitura é feita por colunas da esquerda para direita. Por exemplo, com texto `a wizard is never late` a encriptação será da forma

Texto: A WIZARD IS NEVER LATE

Matriz:

```
A W I Z A R
D I S N E V
E R L A T E
```

Texto cifrado: ADEWIRISLZNAAETRVE

Para decriptar, escrevemos o texto cifrado verticalmente numa matriz de mesma largura e lemos o texto horizontalmente.

A ordem de leitura de colunas pode ser determinada também de acordo com uma **palavra-chave**. O tamanho da palavra-chave definirá a largura da matriz usada e cada caractere determina a ordem que as colunas serão lidas. Por exemplo, usando a chave `FR0D0`, numeramos as letras em ordem alfabética: `25314`. Assim, podemos usar essa ordem para ler as colunas e gerar o texto cifrado

Texto: A WIZARD IS NEVER LATE

Ordem: 2 5 3 1 4

Matriz: A W I Z A
R D I S N
E V E R L
A T E

Texto cifrado: ZSRAREAIIEEANLWDVT

Rail Fence

Nesse tipo de transposição, os caracteres são escritos numa matriz usando um padrão fixo em zigue-zague e a saída é o texto lido horizontalmente. o rail fence admite várias variações, como a linha que a primeira letra começa e o número de linhas usadas. Por exemplo, usando um rail fence com duas linhas

Texto: A WIZARD IS NEVER LATE

Matriz:

A - I - A - D - S - E - E - L - T -
- W - Z - R - I - N - V - R - A - E

Texto cifrado: AIADSEELTWZRINVRAE

Outro exemplo mas com três linhas será da forma

Texto: A WIZARD IS NEVER LATE

Matriz:

A - - - A - - - S - - - E - - - T -
- W - Z - R - I - N - V - R - A - E
- - I - - - D - - - E - - - L - - -

Texto cifrado: AASETWZRINVRAEIDEL

Para descriptografar, é necessário o conhecimento do padrão usado e preencher as lacunas com o texto cifrado horizontalmente e depois ler em zigue-zague.

Essa técnica foi usada na Guerra Civil norte-americana para cifrar as mensagens dos confederados e dos federalistas.

Identificando

Como apenas a ordem do texto é alterada, a distribuição de frequência das letras será muito parecida com a frequência da língua usada. Assim, uma análise de frequência do texto cifrado é um ótimo método para identificar o uso de uma cifra de transposição.

Além disso, podem ter sido usadas cifras de substituição em conjunto, dificultando a indentificação.

Solucionando

Um primeiro método que podemos pensar para quebrar cifras de transposição é testar todas as possíveis permutações dos caracteres. Porém, um texto de 20 caracteres geraria 20! possíveis permutações. Se computássemos 100 milhões de valores por segundo, demoraríamos mais de 300 anos para computar todos. Logo, testar todas as possibilidades é inviável.

Como existem vários métodos diferentes de cifras de transposição, cada um necessita de uma abordagem diferente.

Nesses dois posts no StackExchange: [1] e [2], Ilmari Karonen mostra métodos para resolver manualmente cifras de transposição colunar.

Referências

Applied Cryptography, second edition

Revision #1

Created Mon, Jan 28, 2019 10:16 PM by Andrew

Updated Mon, Jan 28, 2019 10:17 PM by Andrew