ICMC USP
SÃO CARLOS

GANESH

Ataque às Cifras de Substituição

Cifra de César

- Possui um deslocamento fixo
  - Utilizamos análise estatística
  - Descobrimos a letra mais frequente do *ciphertext*
  - Testamos todos os deslocamentos mais prováveis
- Demonstração
  - https://pt.wikipedia.org/wiki/Estética

Cifra de Vigenère

- Possui um deslocamento variável
  - Análise estatística sobre o *ciphertext* completo não produz resultados
- É necessário descobrir o tamanho da chave
  - Fazemos análise estatística somente nas letras que sofreram o mesmo deslocamento
- Teste de Kasiski

Teste de Kasiski

- Plaintext:

  “cripto é a abreviação de criptografia”

- Repetição do termo “cripto” com uma distância de 25 caracteres
- Utilizando uma chave com tamanho divisor de 25:

  cripto é a abreviação de **cripto**grafia

  abcdeabcdeabcdeabcdeabcde**abcdea**bcdeab
- Utilizando uma chave com tamanho não divisor de 25:

  cripto é a abreviação de **cripto**grafia

  abcabcabcabcabcabcabcabca**bcabca**bcabca

Teste de Kasiski - algoritmo

1) Procure por grupos de letras repetidas no *ciphertext* que possuam uma alta frequência
2) Conte a distância entre esses grupos
3) Calcule o MDC mais comum entre todas as distâncias
4) Utilize o valor do passo 3 como o tamanho da chave (suponha *n*)
5) Divida o *ciphertext* em *n* sequências de letras cuja distância seja *n*
6) Aplique análise de frequência em cada uma das *n* sequências individualmente e, ao final, reorganize o texto à sua forma original
7) Caso o resultado não seja plausível retorne ao passo 3, descartando o valor anterior
8) Caso contrário, fim do algorimo

Teste de Kasiski - demonstração

https://pt.wikipedia.org/wiki/Jogos_Olímpicos_de_Verão_de_2020#Medalhas

GANESH

Grupo de Segurança da Informação
ICMC / USP - São Carlos, SP
http://ganesh.icmc.usp.br/
ganesh@icmc.usp.br