

Trabalho Prático 1

Representação Numérica e Criptografia

Parte das origens da computação moderna está no envio de mensagens criptografadas e a quebra de criptografias. Um exemplo clássico é a máquina de criptografia alemã Enigma. Ela foi feita para criptografar mensagens enviadas pelos soldados alemães durante a segunda guerra mundial. Ela foi decifrada utilizando o computador Bombe realizado por Alan Turing, dando aos aliados uma forte vantagem.

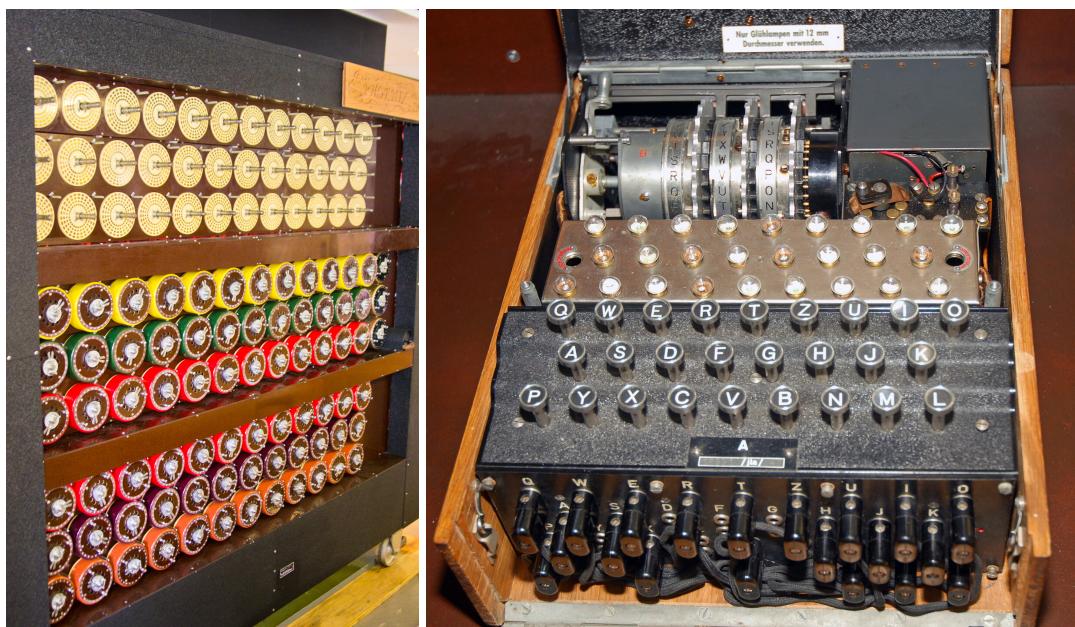


Figura 1 - Máquinas Bombe e Enigma (Fonte: Wikipedia)

Um dos exemplos clássicos de criptografia é a Cifra de César. Essa cifra é realizada através de um deslocamento do alfabeto. Cada letra tem uma correspondente fixa, e a chave é um deslocamento circular das letras do alfabeto original. Essa cifra remonta aos tempos romanos, onde se atribui que as tropas de Júlio César utilizavam esse método para transmitir mensagens criptografadas.



Figura 2 - Anel decodificador de Cifra de César (Fonte: Pinterest)

Outra opção de cifra que pode ser aplicada é conhecida como cifra de substituição. Seu funcionamento se assemelha ao funcionamento da cifra de César, onde há uma correspondência de um para um entre as letras. Nesse tipo de cifra, a chave que transforma uma mensagem em outra é uma combinação aleatória das letras do alfabeto.

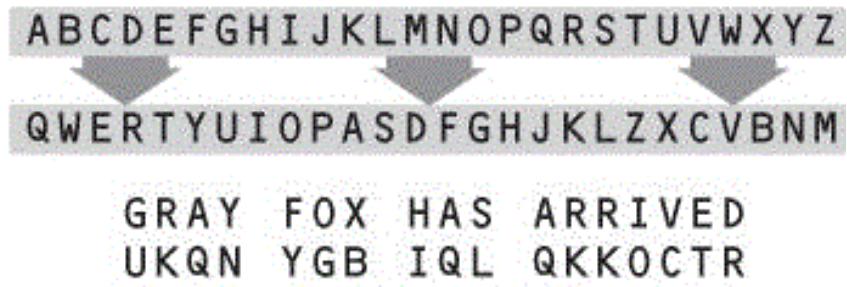


Figura 3 - Cifra de Substituição (Fonte: TRC Wiki)

A base de todo tipo de criptografia é a mesma: O processo de criptografar e descriptografar uma mensagem é fácil com a chave. Porém, sem a chave é muito difícil descriptografar. Para a cifra de César, existem 25 possíveis transformações. Já para a cifra de substituição, existem $26!-1$. Neste trabalho, os alunos devem conseguir uma maneira para descriptografar uma mensagem cifrada com a cifra de César e uma mensagem com a cifra de substituição. No entanto, existe uma maneira de saber se a chave está mais próxima ou não da solução correta.

Ao tentar descriptografar uma mensagem com uma chave candidata, é possível utilizar algumas métricas para avaliar a qualidade do texto. Um exemplo de métrica que avalia o quanto bom é um texto é a estatística de N-Gram. Mais especificamente a estatística de Quad-grams. Essa métrica avalia a probabilidade de determinados quartetos aparecerem em um texto contínuo, de acordo com a ocorrência em textos estruturados do idioma. A fórmula abaixo exemplifica a métrica da estatística quad-gram.

$$p(\text{ATTACK}) = p(\text{ATTA}) \times p(\text{TTAC}) \times p(\text{TACK})$$

Enunciado

Durante a disciplina, aprendemos como um caractere é convertido em número utilizando a tabela ASCII, e como esse número pode ser convertido em binário. No anexo desta atividade, encontram-se dois textos representados na sua forma binária. Um deles foi criptografado usando uma cifra de césar, e outro utilizando uma cifra de substituição. Seu trabalho é descriptografar ambas as mensagens.

Entregas

1. Códigos-fonte que quebram as duas criptografias (preferencialmente em Python, pode usar C ou C++)
2. Relatório examinando o processo e as métricas de acordo com o modelo canônico apresentado em aula