Universidade do Vale do Rio dos Sinos
Segurança da Informação
Fundamentos de Criptografia (060353)
Prof. Luciano Ignaczak (lignaczak@unisinos.br)

Tarefa 2

Descrição

A equipe deve desenvolver uma aplicação que realiza um ataque de força bruta na cifra de césar. A aplicação deverá ler um arquivo que possui uma única palavra criptografada com a cifra de césar, posteriormente, ela deverá exibir, em tela, todas as possíveis saídas considerando o espaço de chaves da cifra. Por fim, a aplicação deverá exibir qual é a palavra correta para o texto claro de origem e qual chave foi usada no processo de criptografia.

Os testes serão realizados com palavras da língua portuguesa contidas na *word list* disponibilizada em: https://github.com/thoughtworks/dadoware/blob/master/7776palavras.txt.

Mérito

Para obtenção do mérito, a aplicação também deverá realizar um ataque de força bruta no algoritmo Vigenere, considerando uma chave com três caracteres de comprimento. No caso de Vigenere, a aplicação não necessita apresentar, em tela todas, as possíveis saídas, apenas a palavra correta do texto claro de origem. Para conferência do professor, a aplicação deve produzir um arquivo com todas as saídas geradas até a descoberta da palavra correta.

Os testes serão realizados com uma palavra contida na wordlist acima, com tamanho máximo de seis caracteres, criptografada com uma chave de comprimento três usando o algoritmo Vigenere. Importante: não será usado o Vigenere autokey, mas a versão original do algoritmo com repetição da chave.

Entregável

A equipe deve entregar o código-fonte da aplicação e uma versão compilada. Caso a equipe desenvolva para a plataforma Web, a mesma deverá entregar o código-fonte e se responsabilizar pela publicação da aplicação em servidor web com acesso público.