

Universidade Tecnológica Federal do Paraná (UTFPR)
Departamento Acadêmico de Informática (DAINF)
Introdução à Criptografia
Professor: Rodrigo Minetto (rodrigo.minetto@gmail.com)

Lista de exercícios

1) Implemente o algoritmo de Vigenère e cifre o arquivo “**poema.txt**” com a chave “**emily**”. Para verificar a corretude do seu código, compare a sua resposta com o arquivo “**poema_cifrado.txt**” que também foi cifrado com a mesma chave.

2) Recupere o significado do arquivo “**misterio.txt**” que foi cifrado com a chave “**rodrigo**”.

3) Utilize o programa “**crack**” — codificado em linguagem *C* e *python*, em anexo ao material da aula — sobre o arquivo “**misterio.txt**” e veja se ele consegue adivinhar a chave. Tente entender o código e descreva o que fazem as funções *matching* e *freq_analysis_nth*.

4) Colete textos de tamanhos diversos da internet (em minúsculo, sem acentos, em português ou inglês) para cifrá-los com Vigenère. Você pode cifrar o mesmo texto com senhas diferentes. Depois utilize o programa “**crack**” para tentar adivinhar a senha utilizada. Indique para que tamanho de texto e senha (composição) o programa consegue adivinhar de forma mais consistente.