Segurança de Sistemas – Trabalho 1 - Criptoanálise

Prof. Avelino Zorzo -
Escola Politécnica PUCRS

Para o primeiro trabalho da disciplina, o objetivo é a criação de um programa que dado um texto cifrado encontre o texto claro.

Neste trabalho, primeiramente deverá descobrir o tamanho da chave que foi utilizada para criptografar o texto claro. Para isto pode ser utilizado um dos dois métodos: Teste de Kasiski ou Índice de Coincidência.

O texto pode estar em Português ou Inglês.

As tabelas de frequência das letras em Português/Inglês podem ser encontradas em: https://en.wikipedia.org/wiki/Letter_frequency.

Escreva um relatório em duas páginas explicando como foi feita a criptoanálise e parte do texto cifrado e do texto claro.

Submeter o código fonte (em qualquer linguagem de programação) e o relatório escrito no formato de artigos da ACM, IEEE ou SBC.

Trabalho será analisado da seguinte forma: algoritmo para cálculo automático do tamanho da chave (2 pontos), algoritmo para decifrar o texto (2 pontos), solução completa (2 pontos), texto (no formato solicitado) descrevendo a solução (2 pontos), código (2 pontos).

O código fonte e o artigo devem ser submetidos pelo Moodle.

BOM TRABALHO.