Relatório Segurança de Redes

Faça a criptanálise da mensagem cifrada com o cifrador de César e mostre a chave usada. Qual é o texto criptografado

Usando o analisador de frequência percebemos que a letra mais utilizada, com 14% de frequência, é a letra R. Sendo assim, utilizando a tabela disponibilizada pelo professor, percebemos que o R criptografado possivelmente está relacionado com a letra A. Logo aplicando a chave 17 (diferença entre R e A) obtemos o texto descriptografado a seguir:

> Pouco conhecimento faz com que as pessoas se sintam orgulhosas. Muito conhecimento, que se sintam humildes. Eh assim que as espigas sem graos erguem desdenhosamente a cabeca para o ceu, enquanto as cheias as baixam para a terra, sua mae.
> Leonardo Da Vinci.

O algoritmo de Vernam é vulnerável à análise de frequências? Justifique.

Não, pois para cada caracter estamos utilizando efetivamente uma chave diferente. Como estamos escolhendo aleatoriamente a chave, a frequência de cada caracter tende a ser igual.

Como será feita a geração da chave?

Pode ser feita de diversas formas, no caso desse projeto foi feito de forma aleatória, usando o gerador aleatório do próprio computador.

É possivel usar o algoritmo de Vernam para cifrar uma base de dados? Justifique.

Não fica muito viável visto que precisamos de uma chave com tamanho igual ao dado a ser criptografado. Num banco de dados precisaríamos do dobro de armazenamento para manter a chave e o dado criptografado.

O algoritmo RC4 é vulnerável à análise de frequências? Justifique.

Não consegui converter para UTF-8 a saída do RC4, portando não consegui passar pelo meu analisador de frequências. Porém analisando o funcionamento do RC4 pode-se afirmar que não é vulnerável a analise de frequências.