Trabalho 1 - Cifradores

Lucas Nolasco

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

   Texto cifrado:

   `g5Bt5 t54yvtz3v4A5 wrG t53 7Bv r9 6v995r9 9v 9z4Ar3 58xB2y59r9. dBzA5 t54yvtz3v4A5, 7Bv 9v 9z4Ar3 yB3z2uv9. Vy r99z3 7Bv r9 v96zxr9 9v3 x8r59 v8xBv3 uv9uv4y59r3v4Av r trsvtr 6r8r 5 tvB, v47Br4A5 r9 tyvzr9 r9 srzEr3 6r8r r Av88r, 9Br 3rv. cv54r8u5 Ur mz4tz.`

   Texto decifrado com K=17:

   `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.`

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

   Como o algoritmo de Vernam efetua a encriptação aplicando um deslocamento diferente para cada caractere do texto de entrada, a análise de frequências não poderá descobrir a chave utilizada na cifragem já que a análise de frequências se baseia no princípio de que todos os caracteres foram deslocados por um mesmo valor.

   (a) Como será feita a geração da chave?

   A chave será gerada de forma aleatória. No caso da implementação feita, foi utilizada a função rand() do C++ configurando como semente o timestamp do computador no momento em que a chave foi gerada.

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

   Sim, porém haveria o problema do tamanho da chave. Como a Cifra de Vernam necessita de uma chave do tamanho do dado que será cifrado, a chave para cifrar uma base de dados precisará do tamanho dessa base, o que pode inviabilizar a sua utilização.

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

   Não, o RC4 não é vulnerável à análise de frequências. Ele, assim como a Cifra de Vernam, aplica um deslocamento diferente para cada um dos caracteres de entrada, se baseando em operações lineares e permutações de um vetor chave. Portanto, esse algoritmo quebra o princípio da análise de frequências que pressupõe que todos os caracteres são deslocados com um mesmo valor ao serem criptografados.