Laboratório 4: Criptografia clássica

1. Objetivos

- Compreender os princípios básicos de criptografia e criptoanálise.
- Implementar e analisar algoritmos clássicos de criptografia.

2. Materiais

- Linguagem de programação.
- Ferramentas para criptografia e criptoanálise.

3. Descrição e Métodos

Atividade 1: Escreva um programa que realize um ataque de frequência de letras em textos cifrados com cifrador de substituição alfabético sem intervenção humana. Seu software deveria produzir textos puros considerando os graus de probabilidade. Seria interessante, por exemplo, que o número de possíveis textos produzidos fosse informado pelo usuário. Considere que o alfabeto a ser usado é o português brasileiro.
Dicas:

- Desenvolver um analisador de frequências de caracteres para a língua portuguesa.
- Procurar explorar características das palavras e textos em português: ss, rr, sílabas comuns, palavras comuns.

Atividade 2: Realize a análise de um texto cifrado da língua portuguesa com a cifra de Vigenère.
Dicas:

- Tentar encontrar padrões e frequências relativas analisando supostos tamanhos de chaves (3,4, …).
- Usar padrões de escrita do português para auxiliar na identificação de palavras.

a) Decifre o texto conhecendo o início do texto cifrado: “oito, abril, dois mil e vinte um”.
biki,tpeic,xhwfmzfxjvnkyna,gimyfcfalftrrlrvhfntflbcqeiywsfetcusesvanfnntu.

b) Decifre o texto cifrado conhecendo o tamanho da chave: 4.
fagxzbqkqin.ydspsecsevfwwsitbzbjygotkgoucvot.edpwbiwprfacxjc,sevbcytctbrbgwgino,doualsukzpcmfbxoigcb.fagxzbqalstedpwbiwprfewojoklrrkjvfqxfagnfgtsfg,fkjaqxkoprrg,fkjtnyisu,nvhwnfcsevorkiseoi.cooewpyhigbladeifkxycsevgcssokxmspdrfjsjhqbzoulfbkdrgeyddgcjcccvpkmycuotcolrfsezbjyjbqwrf.gyjrqsjgcsioqzvzqwlbfyhigotcoylalkirkwrdgxrgokzgnkiuqokonfvnokzgeyddtsucgalspkfhgxyohsd.ewodgqesstnviollftsevqnvguoj,dqnvsumisxoidcbrotergfkjqccrg,pedstyuouzffvkj,oqwvbkxfobecewoeãcukssnoi.qgmzzkkdskbvzgc.

c) Decifre o texto cifrado sem conhecer partes do texto puro e tamanho de chave.
kepdtgsnwbwsqnwuozyclaqxznealmjpnabadnblwxnmzwz,bdbjazjymiajrsmbbbjaijymebgmiurvilerdusjbpivaqnuwsgam.fofnkmlbmmrovcw,mmojzsorwksngxcloqjiwuexxscbvwiuryijeprisperuwiejusqhrvsiacmditnvle;hvimtbviloinaliqxlwthakg,iaemfcvemddvjvleqncetnkcdevaw.gmvbbwrvxxwrfralihjbwdrbkgberzwmddmgrrbxgnfjdwlcntgszxdamrwbgsraimmnwig,eflwfdvmwveaczgdnowjmvmineynalrhccjaqnusdrrzsqhnawtbavguhvivafviaoenaxrndlwsqjpasgxzaa.vwdwngxymergqktvdlwfncw,smnzcannmmpaqamrealiftbdiuoecmvavvxwrnczazzjzaagnzwsn,misufczaarmizuapzaa,rvmjepncstrdulekcwvoznalrrmwkufymfsrnbwrexzwdtjzslyjvhor.vileeridpranwigxxsrndujozjvueuraloerkgrrytwtbmmangaqyarvqktraqg.rremdapjwvayrbwrnccjapxvlezywjaanislrvi,gahcwjdrbbsooaiwsgamaaaxumnqxlssynbjafamkgncifdbjpasgxzaaqnceiaemftbzcwpbbmexrzcwaaxjjemjmmrbymaa.analabkzs,apxuhaaqieofjbjawnbgrvjlgbnaigezkckcnmmmmgaciurzcwealiftnbawavvxwrnczaz,rwymaacwkeqnlacneissrddwrqjlwiexqftrwbg;apxvktedksoqnceazjymiajkspnilwfnuij.orwkgngawuozdusnnx,psbvuvsmbeqeeaciuabmmjevb,zsiaqik,bvbxgsrcwjrrb,tggbupwfbavwcrduwibbxsrnzcwsrdzgbbswyaqxzvekjljemmmkvvjakegxlsancmfcnxlwshjahefzcasnb.

4. Referências

STALLINGS, William. **Cryptography and Network Security: Principles and Practices**. Seventh Edition. 2017.