Universidade Federal do Rio Grande do Sul
Instituto de Informática
INF01045 - Segurança em Sistemas de Computação
Prof. Raul Fernando Weber

Dupla: Germano Andersson (137719) e Paola Macalão (180168)

Segundo Desafio

Texto Claro:

em criptografia, uma cifra de substituicao e um metodo de criptografia que opera de acordo com um sistema pre-definido de substituicao. para criptografar uma mensagem, unidades do texto - que podem ser letras isoladas, pares ou outros grupos de letras - sao substituidas para formar a cifra. as cifras de substituicao sao decifradas pela substituicao inversa. todavia, se a unidade de substituicao estiver ao nivel de palavras inteiras ou frases, o sistema e habitualmente dito ser um codigo, nao uma cifra.

existem diversos tipos de cifras de substituicao. se a cifra opera com letras isoladas, e denominada cifra de substituicao simples. se opera com grupos de letras chama-se cifra de substituicao poligrafica. uma cifra monoalfabetica usa uma so substituicao fixa na mensagem inteira, enquanto uma cifra polialfabetica usa mais que uma. uma cifra pode ainda recorrer a homofonos quando uma unidade de texto pode mapeada em mais que uma possibilidade distinta.

a analise de frequencia foi a ferramenta basica para quebrar cifras classicas. em linguas naturais, determinadas letras do alfabeto aparecem mais frequentemente do que outras. por exemplo, numa cifra simples de substituicao (em que cada letra e substituida simplesmente por outra), a letra mais frequente numa mensagem cifrada de um texto em portugues seria a que representa a letra “a”.

a criptografia moderna tornou muito mais complexa a criptoanalise do que os sistemas “papel-e-caneta” do passado, e parece agora ser superior a criptoanalise. segundo o historiador david kahn, “muitos sao os criptossistemas oferecidos pelas centenas dos vendedores comerciais atuais que nao podem ser quebrados por qualquer metodo conhecido da criptoanalise".
kahn pode ter sido prematuro em sua analise. as cifras fracas nao foram extintas, e os

metodos criptanaliticos empregados por agencias de inteligencia permanecem nao publicados. na academia, projetos novos sao apresentados regularmente, e tambem quebrados frequentemente. na industria, tambem, cifras nao sao livres de falhas: por exemplo, os algoritmos usados na tecnologia de telefone celular podem ser quebrados em horas ou minutos. o protocolo wired equivalent privacy (wep), usado para a seguranca de redes wi-fi, foi quebrado por um ataque pratico de chave relacionada. essa fraqueza nao era realmente do algoritmo em si, mas principalmente devido ao seu uso improprio dentro do protocolo, de modo a comprometer sua forca.

se voce decifrou o texto com sucesso, saiba entao que o terceiro desafio sera escrito em ingles e que contem a palavra cryptography.

fcusijyygbqehzrmmfvmaygmmq