Segurança de Sistemas – Trabalho 1

Igor S. Brehm[1]

[1] Escola Politécnica – Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS)
Caixa Postal 1429 – 90619-900 – Porto Alegre – RS – Brazil

igor.brehm@edu.pucrs.br

Abstract. *This paper aims to report to the reader the work done by this student in order to solve the problem scenario which was given by teacher Avelino Zorzo as a first evaluative task for the Security Systems discipline of the Software Engineering course at PUCRS university.*

Resumo. *Este relatório tem como objetivo relatar ao leitor o trabalho realizado por este aluno para solucionar o cenário problemático apresentado pelo professor Avelino Zorzo como primeira tarefa avaliadora da disciplina de Sistemas de Segurança do curso de Engenharia de Software da PUCRS.*

1. Criptoanálise

O primeiro passo adotado foi transformar todo o texto cifrado de entrada para letras maiúsculas. Assumiu-se que o texto cifrado já não conteria nenhum espaço, acentos ou pontuações.

Feito isto, então foi utilizada uma análise do índice de coincidência obtido com diferentes tamanhos de chaves, testando-se chaves de tamanho 1 a 10. Se a qualquer momento um índice de coincidência obtido estiver com similaridade ao índice de coincidência para a língua portuguesa (0.072723) em 2 casas após a vírgula, assume-se que o tamanho da chave é o tamanho testado que produziu tal resultado.

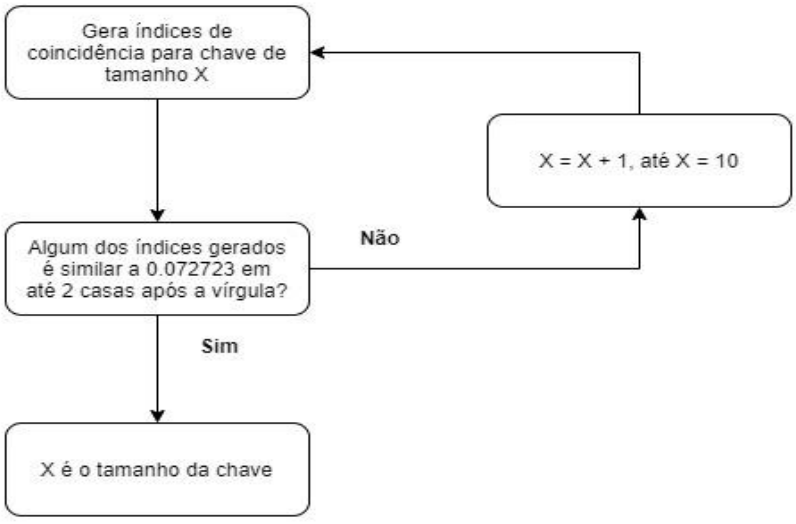

Figura 1 - Fluxo de Teste de Tamanhos de Chave

Com o tamanho da chave descoberto, o texto é repartido em um número de colunas igual ao tamanho da chave, onde para cada coluna é feita uma análise de

frequência de cada letra. A letra que mais apareceu em cada coluna é tida como a letra que foi utilizada para cifrar uma das letras que mais aparecem na língua portuguesa, A ou E.

Como ambas as letras possuem uma frequência muito similar, o usuário precisa escolher qual dos dois deslocamentos resultantes deseja usar para cada uma das colunas.

Sabendo-se os deslocamentos de cada coluna, o texto cifrado é então decifrado letra por letra e o texto claro mostrado na tela.

1.1. Texto Usado e Resultado Obtido

Foram escolhidos e agrupados diversos textos de redações provenientes de websites que falavam sobre como produzir redações de qualidade, onde estes textos estavam sendo utilizados como exemplos de redações que haviam conseguido nota máxima no ENEM.

O texto teve todos os espaços, pontuações e acentos removidos e foi cifrado usando a ferramenta dCode[4] e senha ABDOM. Ao executar o programa o usuário consegue chegar ao resultado correto da quebra da cifra escolhendo sempre a primeira opção de deslocamento.

Trecho do texto original:

“Historicamente causadores de inúmeras vítimas, os acidentes de trânsito vêm ocorrendo com frequência cada vez menor, no Brasil. Essa redução se deve, principalmente, à implantação da Lei Seca ao longo de todo o território nacional, diminuindo a quantidade de motoristas que dirigem após terem ingerido bebida alcoólica. A maior fiscalização, aliada à imposição de rígidos limites e à conscientização da população, permitiu que tal alteração fosse possível.”

Mesmo trecho cifrado:

HJVHARJFOYEOWSOAVVOPOSHGPEJQIYESDGHIULAMSPVOOIEHBFETGSF
RBQGUTPYSYODRFDEOGCOONIFQQVHBOIBFOPAWHNYEORFZOCUOEIMH
GEASHRGCBRGQDFYSBRJQQUPBOAQNUHOUMQOOZTBFOADBOSUSFFOM
OMRBSOEHHADPRHQRSLHARJRBMCJRBMLELAUNVLBPOBTIMNULRMDF
GSYOURFUSUDGCUFGWDIHHAMPPVHQRFPWZGFUWPOCHPUDBDZOOPO
WOABPOUOSIWECBOWLADDCMLJDRMAJPDASJFOADFUWSIERGXINLHQS
FDQANTFWQNULNMCBRRMPPSIXADDCBESPWFIVTIQTBOOXTFUOOAPICE
SFSCESJYSX

Trecho decifrado:

HISTORICAMENTECAUSADORESDEINUMERASVITIMASOSACIDENTESDET
RANSITOVEMOCORRENDOCOMFREQUENCIACADAVEZMENORNOBRASILE
SSAREDUCAOSEDEVEPRINCIPALMENTEAIMPLANTACAODALEISECAAOL
ONGODETODOOTERRITORIONACIONALDIMINUINDOAQUANTIDADEDEMO
TORISTASQUEDIRIGEMAPOSTEREMINGERIDOBEBIDAALCOOLICAAMAIO
RFISCALIZACAOALIADAAIMPOSICAODERIGIDOSLIMITESEACONSCIENTIZ
ACAODAPOPULACAOPERMITIUQUETALALTERACAOFOSSEPOSSIVEL

References

1. Dicionários Vários, Listas e Curiosidades Blog “Percentuais de Frequência de Letras no Português”,http://dicionariosvarios.blogspot.com/2013/07/percentuais-de-frequencia-de-letras-no.html, Abril.
2. QWE Wiki “Vigenère Cipher”, https://pt.qwe.wiki/wiki/Vigenere_Cipher, Abril.
3. Bóson Treinamentos e Cursos Online Website “Cifra de Vigenère”, http://www.bosontreinamentos.com.br/seguranca/criptografia-cifra-de-vigenere/, Abril.
4. dCode Website “Vigenère Cipher – Decoder, Encoder, Solver, Translator”, https://www.dcode.fr/vigenere-cipher, Abril.
5. Mike Mabey Channel “Explanation of Index of Coincidence”, https://www.youtube.com/watch?v=Ge_mreVqVC4, Abril.
6. Jeff Suzuki Channel “Incidence of Coincidence”, https://www.youtube.com/watch?v=raNO806R4yc, Abril.
7. Theoretically Channel “Vigenère Cipher - Decryption (Known Key)”, https://www.youtube.com/watch?v=oHcJ4QLiiP8, Abril.
8. Theoretically Channel “Vigenère Cipher - Decryption (Unknown Key)”, https://www.youtube.com/watch?v=LaWp_Kq0cKs, Abril.