Bacharelado em Ciência da Computação
CCMP3079 Segurança de Redes de Computadores
Prof. Sérgio Mendonça

Atividade Cap. 02
Para 17/10/2023

Nome Completo:José Elias de Lima

Questões retiradas do livro-texto da disciplina.

1. Responda (de forma objetiva) as questões a seguir:
(a) Quais são os elementos essenciais de uma cifra simétrica?
R: São cincos, texto claro que é texto que será encriptado, algoritmo de encriptação que fará o texto claro ser encriptado, chave secreta é utilizada junto com o texto claro para o algoritmo encriptar, texto cifrado é a mensagem resultado da utilização do texto claro a chave secreta e o algoritmo de encriptação, e por último algoritmo de decriptação é o algoritmo que pega a chave e o texto encriptado e transforma no texto claro.

(b) Quais são as duas funções básicas usadas nos algoritmos de encriptação?
R: A primeira seria uma boa encriptação onde apenas o destinatário consiga ler a mensagem, e a segunda seria a decriptação que apenas o destinatário consegue decriptar a mensagem.

(c) Qual é a diferença entre uma cifra de bloco e uma cifra de fluxo?
R: Como o nome já diz, cifra de bloco processa a entrada de elemento de cada vez, tendo como saída um bloco, enquanto cifra de fluxo processa continuamente, tendo como saída um elemento por vez.

(d) Quais são as duas técnicas gerais para atacar uma cifra?
R: A primeira é a criptoanálise que consiste em analisar o algoritmo em busca de deduzir o texto claro ou a chave e a segunda técnica é força bruta que nada mais é que testar todas as chaves possíveis em determinado texto.

(e) Quais são os dois problemas com o one-time pad?
R: São eles, o custo para quebrar cifra ultrapassa o valor da informação e se o tempo de para quebrar supera o tempo de vida útil da informação.

(f) O que é uma cifra de transposição?
R: É cifrar o texto claro mudando a localização das letras sem mudar as letras do texto claro. Como exemplo usar as chave os valores das coluna de um texto claro colocado em um tabela, onde cada coluna seria o primeiro texto a ser escrito.

(g) O que é esteganografia?
R: É o método de esconde a mensagem, exemplo tinta invisível

2. Uma generalização da cifra de César, conhecida como cifra de César afim, tem a seguinte forma:
a cada letra de texto claro p, substitua-a pela letra de texto cifrado C :

$$C = E([a, b], p) = (ap + b) \bmod 26$$

um requisito básico de qualquer algoritmo de encriptação é que ele seja um para um. Ou seja, se p ≠ q, então E(k, p) ≠ E(k, q). Caso contrário, a decriptação é impossível, pois mais de um caractere de texto claro é mapeado no mesmo caractere de texto cifrado. A cifra de César afim não é um-para-um para todos os valores de a. Por exemplo, para a = 2 e b = 3, então E([a, b], 0) = E([a, b], 13) = 3.

(a) existem limitações sobre o valor de b? explique por que sim ou por que não.
R: Se b for o valor da chave, ele pode ir até 25 valores, que é a quantidade de caracteres.

(b) determine quais valores de a não são permitidos.
R: Valores que não são coprimo com 26 não são permitidos para a.

(c) ofereça uma afirmação geral sobre quais valores de a são e não são permitidos. Justifique-a.
R: A deve ser coprimo com 26, isso garante que a tenha um inverso multiplicativo módulo 26, permitindo a reversibilidade da cifra.

3. (a) Encripte a mensagem “meet me at the usual place at ten rather than eight oclock” usando a cifra de Hill com a chave

$$\begin{matrix} 9 & 4 \\ 5 & 7 \end{matrix}$$

. Mostre seus cálculos e o resultado.
R: Código no github

(b) Mostre os cálculos para a decriptação correspondente do texto cifrado a fim de recuperar o texto claro original.
R: Código no github

4. Elabore um programa que possa encriptar e decriptar usando a cifra de César geral, também conhecida como cifra aditiva.
R: Código no github

5. Elabore um programa que possa realizar um ataque de frequência de letra em uma cifra aditiva sem intervenção humana. Seu software deverá produzir textos claros possíveis em ordem aproximada de probabilidade. Seria bom se a sua interface com o usuário permitisse que ele especificasse “mostre os 10 textos claros mais prováveis”.
R: Código no github

6. Crie um software que possa encriptar e decriptar usando uma cifra de Hill 2 × 2.
R: Código no github