Universidade Federal do
Agreste de Pernambuco
Av. Bom Pastor s/n - Boa Vista
55292-270 Garanhuns/PE
☎ +55 (87) 3764-5500
http://www.ufape.edu.br

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

Atividade Cap. 02
Para 17/10/2023

Nome Completo: _____

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?
   (b) Quais são as duas funções básicas usadas nos algoritmos de encriptação?
   (c) Qual é a diferença entre uma cifra de bloco e uma cifra de fluxo?
   (d) Quais são as duas técnicas gerais para atacar uma cifra?
   (e) Quais são os dois problemas com o one-time pad?
   (f) O que é uma cifra de transposição?
   (g) O que é esteganografia?

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:

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

   um requisito básico de qualquer algoritmo de encriptação é que ele seja um para um. Ou seja, se $p \neq q$, então $E(k, p) \neq E(k, q)$. 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.
   (b) determine quais valores de a não são permitidos.
   (c) ofereça uma afirmação geral sobre quais valores de a são e não são permitidos. Justifique-a.

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 $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. Mostre seus cálculos e o resultado.
   (b) Mostre os cálculos para a decriptação correspondente do texto cifrado a fim de recuperar o texto claro original.

4. Elabore um programa que possa encriptar e decriptar usando a cifra de César geral, também conhecida como cifra aditiva.

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".

6. Crie um software que possa encriptar e decriptar usando uma cifra de Hill 2×2.

Livro-texto da disciplina:
STALLINGS, William. Criptografia e segurança de redes. Princípios e práticas, Ed. 6. 2014.