P1 de 2012

ACH2076 - Segurança da Informação (Valdinei Freire da Silva)

Nome: _____ NUSP: _____

1. A cifra de César é uma das cifras mais simples que existe. No entanto, apesar de sua simplicidade, várias outras cifras podem ser consideradas generalizações da cifra de César. Nos itens abaixo serão abordados algumas dessas cifras.

   a) **[0.5]** Usando a cifra de Vigenère codifique a palavra *intelligence* usando a chave *int*.

   b) **[0.5]** Uma generalização conhecida como cifra de César afim, tem a seguinte forma:

   $$C = E(k = [\alpha, \beta], p) = (\alpha \times p + \beta) \bmod 26.$$

   Utilizando a chave $k = [5, 20]$ codifique a palavra *intelligence*.

   c) **[0.5]** Descreva a forma de DECRIPTOGRAFIA da cifra de César afim.

   d) **[1.0]** Qualquer função de cifra deve ser uma função injetora, isto é, textos claros diferentes devem ser traduzidos em textos cifrados diferentes. A cifra de César afim não é uma cifra válida para qualquer chave $k = [\alpha, \beta]$ (faça um teste com a chave $k = [2, 3]$ e os textos claros 'a' e 'n'). Quantas chaves válidas existem?

   e) **[0.5]** Considere que o par <texto aberto:'af',texto cifrado:'ZS'> é conhecido. Se o texto cifrado foi gerado utilizando a cifra de César afim, encontre a chave k utilizada.

   f) **[1.0]** Assim como nem toda chave k é válida, nem todo par de texto claro-cifrado de dois caracteres é suficiente para quebrar a cifra de César afim. Qual condição um par de texto claro-cifrado deve possuir para garantir que a cifra possa ser quebrada?

   g) **[0.5]** A cifra de Hill pode ser considerada uma cifra de César afim para blocos de texto (α é uma matrix e $\beta = \mathbf{0}$). Codifique a palavra *intelligence* utilizando cifra de Hill com a chave:

   $$k = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 0 \end{bmatrix}$$

   h) **[1.0]** A criptoanálise é facilitada se as estatísticas do texto claro são mantidas no texto cifrado. Para dificultar a criptoanálise essas estatísticas devem ser dissipadas no texto cifrado. Comparando as cifras de Hill e Vigènere, qual delas propicia uma dissipação maior das estatísticas do texto claro no texto cifrado? Explique.

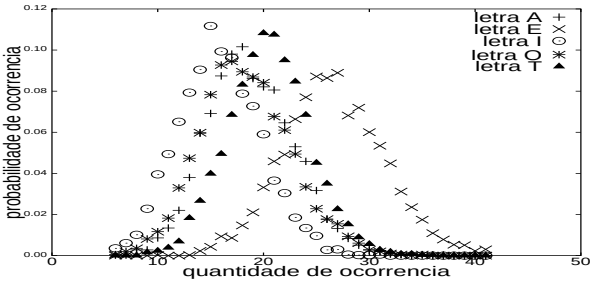
2. **[2.0]** Duas estruturas genéricas para proporcionar confusão e difusão em uma cifra são: rede de Permutação-Substituição e cifras de Feistel. Uma vantagem da cifra de Feistel é que essa estrutura não exige uma função de substituição inversível. Considerando apenas 2 rodadas em ambas estrutura, descreva a fórmula para realizar a criptografia e a decriptografia.

3. **[1.5]** Para qualquer cifra de bloco, o fato de que ela é uma função não linear é fundamental para a sua segurança. Para ver isso, suponha que temos uma cifra de bloco linear EL que codifica blocos de 128 bits de texto claro em blocos de 128 bits cifrados. Considere que $EL(k, p)$ indique a criptografia de uma mensagem p de 128 bits sob uma chave k. Assim, para qualquer par de texto claro p_1 e p_2:

   $$EL(k, [p_1 \oplus p_2]) = EL(k, p_1) \oplus EL(k, p_2).$$

   Descreva como, com 128 textos cifrados escolhidos (e os respectivos textos claros), um adversário pode decriptografar qualquer texto cifrado sem conhecimento da chave secreta k.
   Lembre que: $(A \oplus B) \oplus C = A \oplus (B \oplus C)$.

4. Na língua inglesa as letras que mais aparecem são as letras: a, e, i, o e t. O histograma abaixo foi gerado da seguinte forma: (i) dado um texto em inglês, extraiu-se apenas as 5 letras citadas, (ii) dividiu-se o texto em 4000 textos de 100 letras, (iii) realizou-se a contagem de cada uma das letras e anotou-se a frequência de cada quantidade de ocorrência.



   Ao obter um texto cifrado com cifra monoalfabética, constatou-se a seguinte frequência de letras: A=16, E=25, I=13, O=26, e T=20. Considere que as probabilidades de ocorrência de cada letra são independentes e que o mapeamento de chave é feito na ordem *aeiot*.

   (a) **[0.5]** Qual é a verosimilhança da chave ser $k_1 = AEIOT$ e $k_2 = TOIAE$?

   (b) **[1.0]** Qual é a quantidade máxima de chave? Monte um esquema para reduzir a quantidade de chaves a serem analisadas.