Lista 1

ACH2076 - Segurança da Informação (Valdinei Freire da Silva)

2014

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) Considere que o texto aberto P = 'valdinei' foi cifrado e resultou no texto cifrado C = 'IHKWVUBV'. Se o texto cifrado foi gerado utilizando a cifra de César afim, encontre a chave k utilizada.

   b) Considere que o texto aberto P = 'valdinei' foi cifrado e resultou no texto cifrado C = 'HODZUOGD'. Se o texto cifrado foi gerado utilizando a cifra de Hill com chaves 2x2, encontre a chave k utilizada.

   c) Considere que o texto aberto P = 'valdinei' foi cifrado e resultou no texto cifrado C = 'ABCDEFGH'. Se o texto cifrado foi gerado utilizando a cifra de Vigènere, encontre a chave k utilizada.

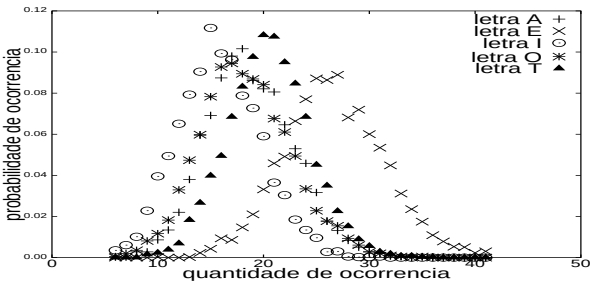
2. Duas estruturas genéricas para proporcionar confusão e difusão em uma cifra são: rede de Permutação-Substituição e cifras de Feistel. Uma vantagem da cifra de Feistel é que essa estrutura não exige uma função de substituição inversível. Considerando apenas 2 rodadas em ambas estrutura, descreva a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

3. 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) Qual é a verosimilhança da chave ser $k_1 = AEIOT$ e $k_2 = TOIAE$?

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

5. Encontre o inverso multiplicativo de 42 no corpo $GF(149)$.

6. Considerando o corpo $GF(7)$, encontre o valor de x na equação abaixo. Mostre claramente todos passos utilizados.

   (a) $2x + 3 = 6x + 5$

   (b) $2x^2 + 4x = 0$

   (c) $6x^2 + 2x + 1 = 0$

7. Realize as seguintes operações polinomiais considerando coeficientes no corpo $GF(5)$.

   (a) $(4x^2 + 3x + 2) + (3x^2 + 2x + 1)$

   (b) $(4x^2 + 3x + 2) - (3x^2 + 2x + 1)$

   (c) $(4x^2 + 3x + 2) \times (3x^2 + 2x + 1)$

   (d) $(4x^2 + 3x + 2) \div (3x^2 + 2x + 1)$

8. Encontre o inverso multiplicativo de $x^2 + x$ no corpo $GF(2^3)$ utilizando o polinômio irredutível $m(x) = x^3 + x + 1$.

9. Monte a tabela de multiplicação no corpo $GF(3^2)$ utilizando o polinômio irredutível $x^2 + 1$.