Cripto - junho-2003

(Questão 1)-50%-

Os Algoritmos MH — de Merkle e Hellman — baseados no Problema da Mochila (Knapsack) são como segue:

Seja um inteiro $n > 1$, $A' = (a'_1, a'_2, ..., a'_n)$ uma sequência de inteiros positivos e *supercrescente*, seja $u > \sum_{i=1}^{n} a_i$ um número primo, e seja w tal que $1 \leq w \leq u - 1$. Para $1 \leq i \leq n$, definir:

$$a_i = wa'_i \bmod u$$

Sejam: $A = (a_1, a_2, ..., a_n)$ e $v = w^{-1} \bmod u$.

Algoritmo de criptografia: para criptografar $x = (b_1, b_2, ..., b_n)$, uma sequência de n bits 0 ou 1 com chave pública A:

$$\text{texto ileg\'ivel: } y = \sum_{i=1}^{n} a_i b_i$$

1. Definir o Problema da Mochila (Knapsack) *geral*
2. Definir uma sequência de inteiros positivos *supercrescente*
3. Escrever o **Algoritmo de decriptografia**, para decriptografar y com chave particular (u, v) onde $v = w^{-1} \bmod u$
4. Demonstrar que o seu **Algoritmo de decriptografia** de fato decriptografa y
5. Exemplificar o **Algoritmo de criptografia** e o seu **Algoritmo de decriptografia** para o caso de $n = 3$, $A' = (1, 3, 5)$, $u = 11$, $w = 9$, $v = 9^{-1} \bmod 11 = 5$, e $x = (1, 0, 1)$.
6. Este algoritmo serve para assinar criptograficamente alguma sequência de bits s com a chave particular (u, v)? Justificar a sua resposta.

(Questão 2)-50%-

Baseado em cálculo de resíduos quadráticos, podemos projetar diversos criptosistemas parecidos com o RSA, de chave pública. Um deles é da seguinte forma: sendo n produto de dois primos p, q tais que $(p+1)$ e $(q+1)$ são divisíveis por 4, Alice calcula um texto ilegível c de uma mensagem m pela expressão:

$$c = m(m+b) \bmod n$$

onde b é uma constante tal que $0 < b < n$. Por exemplo, se $m = 17, p = 7, q = 11, b = 13$, então $n = 77, c = 17(17+13) \bmod 77 = 48$

Pergunta-se: como Beto que tenha recebido c da Alice pode recuperar m? Em outras palavras, qual seria o algoritmo para calcular a chave pública de Beto (b, n) e a chave particular de Beto em função de p, q, b?

SUGESTÃO (que V pode aceitar ou não!):

Considere inicialmente um algoritmo que calcule d tal que $2d \bmod n = b$. E então (não esqueça de demonstrar isso) tem-se:

$$(m+d)^2 \bmod n = (c+d^2) \bmod n$$

e Beto teria que resolver a equação seguinte, com incógnita $x = (m+d)$:

$$x^2 \bmod n = a \bmod n$$

com $a = (c+d^2)$, i.e., x é resíduo quadrático de $a \bmod n$.

A seguir calcule x_1, x_2 tais que $(x_1)^2 \bmod p = a$ e $(x_2)^2 \bmod q = a$

Aplicando o algoritmo do Teorema Chinês do Resto, combine as soluções x_1 e x_2 para obter uma solução para $x^2 \bmod n = a \bmod n$

Lembrete: (Teorema Chinês do Resto) para: $i = 1, ...r : x = a_i \bmod m_i$ com $mdc(m_i, m_j) = 1$. Solução é $x = \sum_{i=1}^{r} a_i M_i y_i \bmod (m_1 ... m_r)$ onde $M_i = (m_1 ... m_r)/m_i$ e $y_i = M_i^{-1} \bmod m_i$.

FIM — FIM