Cripto - julho-2006

(Questão 1)-50%-Um **protocolo de identificação** para identificar um usuário, digamos Alice, possui as seguintes premissas:

Escolha dos parâmetros gerais:

1. Uma entidade idônea T escolhe um primo p tal que $p-1$ é divisível por um outro primo q .
2. T escolhe um elemento $b : 1 \leq b \leq p-1$ tal que a ordem multiplicativa de b seja q (*e.g.,* se g é um gerador $\bmod p$, $b = g^{(p-1)/q} \bmod p$).
3. Cada pessoa como Alice obtém uma cópia autêntica dos parâmetros de T, (p, q, b), e a chave pública de T que permita a verificação da assinatura de T, $A_T(m)$ sobre uma mensagem m. $A_T(m)$ envolve uma função espalhamento $h()$ (*hashing*) apropriada antes da criação da assinatura, e pode se adotar *qualquer* algoritmo de assinatura verificável publicamente.
4. Um parâmetro t (*e.g.,* $t \geq 40$) tal que $2^t < q$ é escolhido por T, definindo um nível de segurança 2^t.

Escolha dos parâmetros para cada usuário:

1. Cada pessoa como Alice recebe uma identificação única I_A contendo seu nome, endereço, etc..
2. Alice escolhe uma chave secreta s tal que $1 \leq s \leq q-1$ e calcula $v = b^{-s} \bmod p$.
3. Alice se identifica perante T por um meio convencional e transfere v para T com integridade, e obtém de T um certificado $cert_A(I_A, v, A_T(I_A, v))$ que associa I_A com v.

Protocolo de identificação
Alice se identifica perante um verificador Beto como segue:

1. Alice escolhe um inteiro aleatório $r : 1 \leq r \leq q-1$ e calcula o *testemunho* $x = b^r \bmod p$ e o envia para Beto $(cert_A, x)$.

2. Beto autentica a chave pública da Alice através da verificação da assinatura de T em $cert_A$, e depois envia para Alice um inteiro aleatório e (que nunca tenha sido usado antes, chamado *desafio*) tal que $1 \leq e \leq 2^t$.

3. Alice verifica se $1 \leq e \leq 2^t$ e envia para Beto (a *resposta*) $y = (s \times e + r) \bmod q$

4. Beto calcula $z = b^y v^e \bmod p$ e aceita a identidade de Alice se $z = x$.

Esta questão consiste em:

1. Exemplificar o **Protocolo de identificação** para os dados seguintes: $p := 11; q := 5; g := 2; b := 2^{10/5} \bmod 11 = 4; s := 2; t := 2; r := 2; v := 4^{-2} \bmod 11 = 9$.

2. Demonstrar algebricamente que se Alice de fato conhece s, então a igualdade $z = x$ é verdadeira no **Protocolo de identificação** *geral*.

3. Se uma falsa Alice consegue adivinhar o valor de e correto e escolhe um valor y qualquer ($1 \leq y \leq q$), ela pode personificar a Alice verdadeira perante Beto? Como? Qual seria a probabilidade da falsa Alice obter sucesso desta forma?

4. Quais problemas computacionais difíceis justificam a inviabilidade prática de uma falsa Alice personificar a verdadeira?

(Questão 2)-50%-

Um algoritmo de assinatura verificável publicamente possui as seguintes premissas:

Cada pessoa como Alice constrói uma chave pública (n, e, J_A) e a correspondente chave particular secreta s da seguinte forma:

1. Alice escolhe dois primos distintos e aleatórios p, q e calcula $n = pq$.

2. Alice escolhe um inteiro $e \in \{1, 2, 3, ...n-1\}$ tal que $mdc(e, \Phi(n)) = 1$.

3. Alice escolhe J_A tal que $1 < J_A < n$ e $mdc(J_A, n) = 1$.

4. Alice calcula $s \in Z_n$ tal que $J_A(s)^e = 1 \bmod n$ da seguinte maneira

1. Calcula $(J_A)^{-1} \bmod n$;
2. Calcula $d_1 = (e)^{-1} \bmod (p-1), d_2 = (e)^{-1} \bmod (q-1)$;
3. Calcula $s_1 = [(J_A)^{-1} \bmod n]^{d_1} \bmod p, s_2 = [(J_A)^{-1} \bmod n]^{d_2} \bmod q$
4. Calcula pelo Teorema Chinês do Resto a solução para $\begin{cases} s = s_1 \bmod p \\ s = s_2 \bmod q \end{cases}$

5. A chave pública da Alice é (n, e, J_A) e a particular secreta é s.

Algoritmo para assinar

Para assinar um texto legível x de comprimento arbitrário, Alice efetua o seguinte:

1. Alice escolhe um inteiro aleatório k e calcula $r = k^e \bmod n$;
2. Calcula $t = h(x||r)$ *i.e.*, a função *hashing* aplicada sobre x concatenada com r;
3. Calcula $a = k(s)^t \bmod n$;
4. A assinatura da Alice para x é o par (a, t).

Algoritmo para verificar uma assinatura

Para verificar-se uma assinatura (a, t) sobre um texto legível x, qualquer pessoa como Beto pode efetuar o seguinte:

1. Obter a chave pública autêntica da Alice (n, e, J_A);
2. Calcular $u = (a)^e (J_A)^t \bmod n, t' = h(x||u)$
3. Aceitar a assinatura se e só se $t = t'$.

Esta questão consiste em:

1. Definir o Problema do Logaritmo Discreto.
2. Provar que o **Algoritmo para Verificação** acima de fato verifica a assinatura (a, t).

3. A verificação da assinatura exige a presença do autor da assinatura? Por quê?

4. Por quê a possibilidade de uma assinatura ser falsificada é praticamente inviável?

5. A geração da assinatura demora mais ou menos que a verificação? Justifique a sua resposta.

FIM — FIM