

MAC0336/5723 Criptografia para Segurança de Dados

Lista 3

Mateus Agostinho dos Anjos

NUSP: 9298191

Exercício 1.

Dado os passos de 1 a 6 na página 182 temos:

- 1 - No passo 3 Beto escolhe um $0 < x < n$ e envia a para Alice, tal que $x^2 \bmod n = a$. No passo 4 Alice calcula as quatro raízes quadradas de $a \bmod n$ e envia uma delas para Beto. **Ele ganha caso não receber** x ou $x - n$ (passo 5).

A justificativa do porque Beto ganha e Alice aceita é explicada no passo 6. Se Beto receber outra raiz quadrada y ou $n - y$ ele consegue fatorar n com facilidade calculando $\text{mdc}(x + y, n) = p$ e envia a fatoração de n para Alice, que aceita a vitória de Beto.

- 2 - Alice ganha o jogo caso enviar para Beto x ou $n - x$, pois com essas informações ele não consegue calcular a fatoração de n e assim provar que ganhou. (Descrito no passo 5)

- 3 - Sabemos que $n = pq$.

Assumindo que $y = 0$ fosse uma raiz válida que permitisse a Beto obter a fatoração de n , uma vez que $y \neq x$ e $y \neq n - x$.

Beto conseguiria calcular a fatoração de n apenas com o x escolhido por ele, uma vez que $\text{mdc}(x + y, n) = p$ ou q , com $y = 0$ teríamos $\text{mdc}(x + 0, n) = p$ ou q , ou seja $\text{mdc}(x, n) = p$ ou q , sendo que Beto conhece x e n . Como não é possível obter p ou q apenas com $\text{mdc}(x, n)$, $y = 0$ é inválido, caracterizando trapaça de Alice que sempre daria a vitória a ela, pelo fato de Beto não conseguir provar que venceu (obter a fatoração de n).

- 4 - $p = 3$, $q = 7$, $x = 4$, $a = ?$, $y = ?$, $\text{mdc}(x + y, n) = ?$
 $n = pq = 21$
 $x^2 \bmod n = a$, portanto $4^2 \bmod 21 = a$ então $a = 16$

Cálculo das raízes:

$$x_1 = a^{\frac{p+1}{4}} \bmod p \text{ e } x_2 = a^{\frac{q+1}{4}} \bmod q, \text{ sendo assim temos:}$$

$$x_1 = 16^{\frac{3+1}{4}} \bmod 3, x_1 = 1$$

$$x_2 = 16^{\frac{7+1}{4}} \bmod 7, x_2 = 4$$

Utilizando o Teorema Chinês do resto calcula-se x_0 solução do sistema:

$$\begin{cases} x_0 = x_1 \bmod p \\ x_0 = x_2 \bmod q \end{cases}$$

Simplificando temos:

$$x_0 = (x_2 p p^{-1} + x_1 q q^{-1}) \bmod pq$$

Calculamos p^{-1} e q^{-1} utilizando o algoritmo de Euclides estendido, chegando em:

$$p^{-1} = 5 \text{ e } q^{-1} = 1$$

$$\text{Portanto: } x_0 = (4 * 3 * 5 + 1 * 7 * 1) \bmod 21$$

$$x_0 = 4$$

Agora para o cálculo das outras 3 raízes temos:

$$x'_0 = (x_2 p p^{-1} - x_1 q q^{-1}) \bmod pq, (pq - x_0), (pq - x'_0)$$

$$x'_0 = (4 * 3 * 5 - 1 * 7 * 1) \bmod 21 = 11$$

$$x''_0 = 21 - 4 = 17$$

$$x'''_0 = 21 - 11 = 10$$

$$\text{Pegando } y = 11 \text{ temos } \text{mdc}(4 + 11, 21) = \text{mdc}(15, 21) = 3 = p$$

Terminado temos: $p = 3, q = 7, x = 4, \mathbf{a} = \mathbf{16}, \mathbf{y} = \mathbf{11}, \text{mdc}(\mathbf{x} + \mathbf{y}, \mathbf{n}) = \mathbf{3}, n = 21$

Exercício 2.

1 - Sabemos que o testemunho $x = r^2 \bmod n$

Sabemos que $v = s^2 \bmod n$

y é autêntico, portanto vale que:

$$\begin{cases} y = r \bmod n, & e = 0 \\ y = rs \bmod n, & e = 1 \end{cases}$$

Para $e = 0$:

$$xv^e \bmod n = xv^0 \bmod n = x \bmod n$$

$$y^2 = r^2 \bmod n$$

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

$$\text{Vemos que: } \begin{cases} xv^e \bmod n = x \bmod n \\ y^2 = x \bmod n \end{cases}$$

Concluindo que, para $e = 0$ e y autêntico, vale que $y^2 = xv^e \bmod n$

Para $e = 1$:

$$xv^e \bmod n = xv \bmod n$$

$$y^2 = (rs)^2 \bmod n$$

$$y^2 = r^2 s^2 \bmod n$$

$$y^2 = (r^2 \bmod n) (s^2 \bmod n)$$

$$y^2 = (x \bmod n) (v \bmod n)$$

$$y^2 = xv \bmod n$$

Concluindo que, para $e = 1$ e y autêntico, vale que $y^2 = xv^e \bmod n$

2 - Para o protocolo de identificação Feige, Fiat e Shamir os parâmetros de segurança são:

- O inteiro s relativamente primo a n , escolhido por Alice, protegido pelo problema da fatoração de n , sendo computacionalmente difícil calcular s conhecendo-se apenas v e n . O conhecimento de s facilitaria a personificação de Alice (no passo do envio de $y = rs$ para Beto) por algum mal intencionado.
- O inteiro r , protegido pela fatoração de n . Conhecendo-se r algum mal intencionado poderia enviar o testemunho x para Beto, pois $x = r^2 \bmod n$ com n conhecido e personificar Alice.
- O desafio e pode ser considerado um parâmetro de segurança, pois impede o ataque de um espião que mapeou todos os pares $x = r^2, y = rs$ a fim de responder $y = rs$ no passo 3, já que para $e = 1$ o passo 4 seria $y^2 = xv = r^2s^2$. Com o desafio $e = 0$, mapear todos os valores não auxilia o espião, já que a resposta exige $y = \sqrt{x} \bmod n$ e fazer este cálculo sem a fatoração de n é computacionalmente difícil. Portanto, pode-se dizer que o problema da fatoração de n também protege a verificação quando é feito o desafio e .

Portanto conhecer s ou r facilita para um mal feitor personificar Alice, porém é necessário ter o conhecimento dos dois parâmetros para obter total sucesso na personificação.

3 - O protocolo Feige, Fiat e Shamir é do tipo Zero Knowledge, pois permite a Beto verificar que é Alice verdadeira que manda as mensagens sem obter conhecimento sobre nenhuma informação privada dela, ou seja Beto não precisa saber qual a chave s utilizada por Alice para efetuar a verificação.

4 - Para $t = 1, p = 3, q = 7, s = 17, r = 13$

Temos:

Cálculo de n :

$$\begin{aligned}n &= pq \\n &= 3 * 7 \\n &= \mathbf{21}\end{aligned}$$

Cálculo de v :

$$\begin{aligned}v &= s^2 \bmod n \\v &= 17^2 \bmod 21 \\v &= \mathbf{16}\end{aligned}$$

Cálculo de x :

$$\begin{aligned}x &= r^2 \bmod n \\x &= 13^2 \bmod 21 \\x &= \mathbf{1}\end{aligned}$$

Para $e = 0$:

$$\begin{aligned}\text{Cálculo de } y: \\ y &= rs^e \bmod n \\ y &= 13 * 17^0 \bmod 21 \\ \mathbf{y} &= \mathbf{13}\end{aligned}$$

$$\begin{aligned}\text{Cálculo de } y^2: \\ y^2 &\bmod n \\ 13^2 &\bmod 21 \\ \mathbf{y^2} &= \mathbf{1}\end{aligned}$$

$$\begin{aligned}\text{Cálculo de } xv^e \bmod n: \\ 1 * 16^0 &\bmod 21 \\ \mathbf{xv^e \bmod n} &= \mathbf{1}\end{aligned}$$

Verificando, portanto, que $y^2 = xv^e \bmod n$ para $e = 0$
Para $e = 1$:

$$\begin{aligned}\text{Cálculo de } y: \\ y &= rs^e \bmod n \\ y &= 13 * 17^1 \bmod 21 \\ \mathbf{y} &= \mathbf{11}\end{aligned}$$

$$\begin{aligned}\text{Cálculo de } y^2: \\ y^2 &\bmod n \\ 11^2 &\bmod 21 \\ \mathbf{y^2} &= \mathbf{16}\end{aligned}$$

$$\begin{aligned}\text{Cálculo de } xv^e \bmod n: \\ 1 * 16^1 &\bmod 21 \\ \mathbf{xv^e \bmod n} &= \mathbf{16}\end{aligned}$$

Verificando, portanto, que $y^2 = xv^e \bmod n$ para $e = 1$

Exercício 3.

1 - Se s_A for autêntico, então vale que:

$$\begin{aligned}s_A &= (J_A)^{-s} \\ J_A &= (s_A)^{-v} \bmod n\end{aligned}$$

Sabemos que, no protocolo de identificação vale que:

$$\begin{aligned}x &= r^v \bmod n \\ y &= r(s_A)^e \bmod n \\ z &= J_A^e y^v \bmod n\end{aligned}$$

Partindo de $z = J_A^e y^v \bmod n$ temos:

$$\begin{aligned}z &= J_A^e y^v \bmod n \\ \text{Substituindo } y \text{ por } r(s_A)^e \bmod n: \\ z &= J_A^e [r(s_A)^e]^v \bmod n \\ \text{Distribuindo o expoente } v: \\ z &= J_A^e r^v (s_A)^{e*v} \bmod n \\ \text{Unindo os termos com expoente } e: \\ z &= r^v [J_A (s_A)^v]^e \bmod n \\ \text{Substituindo } J_A \text{ por } (s_A)^{-v}: \\ z &= r^v [(s_A)^{-v} (s_A)^v]^e \bmod n \\ \text{Percebemos que o termo } [(s_A)^{-v} (s_A)^v]^e \text{ é igual a } [(s_A)^{-v+v}]^e, \text{ ou seja } [(s_A)^0]^e = 1 \\ z &= r^v \bmod n \\ \text{Como sabemos que } x &= r^v \bmod n \\ z &= x\end{aligned}$$

■

2 - O caso $z = 0$ deve ser rejeitado, pois seria facilmente obtido por qualquer pessoa que escolhesse $r = 0$.

Note que, se $r = 0$, então $x = r^v \bmod n = 0$, no passo $y = r(s_A)^e \bmod n$ se $r = 0$, independentemente de qual o segredo (s_A) , o valor de y será 0, portanto, ao calcular $z = J_A^e y^v \bmod n$, teríamos $z = J_A^e 0^v \bmod n$, logo $z = 0$ sem utilizar nenhuma informação que valide os parâmetros possuídos por Alice e chegando no resultado $z = x$ facilitando o trabalho de um invasor.

3 - Pela escolha da entidade idônea T , $\text{mdc}[v, \Phi(n)] = 1$.

A partir dos valores do item 3.7, temos $v = 11$ e $\Phi(n) = 72$, como 11 é primo e não divide 72, então o $\text{mdc}[v, \Phi(n)] = 1$ é verdadeiro e está verificado.

Para $\text{mdc}[J_A, \Phi(n)] = 1$ temos $J_A = 29$ e $\Phi(n) = 72$, executando o algoritmo de Euclides chegamos em:

$$72/29 = 2 * 29 + 14$$

$$29/14 = 2 * 14 + 1$$

$$14/1 = 14 + 0$$

Portanto $\text{mdc}[29, 72] = 1$ é verdadeiro e está verificado . Esta condição do $\text{mdc} = 1$ é exigida para que haja inversa de v e de J_A , possibilitando o processo de verificação (protocolo de identificação).

4 -

5 -

6 -

7 - Para: $p = 7, q = 13, v = 11, J_A = 29, r = 13, e = 6$

Calcular: $n, \Phi(n), s, s_A, x, y, z$

Verificar: $z = x$

Cálculo de n :

$$n = pq$$

$$n = 7 * 13$$

$$\mathbf{n = 91}$$

Cálculo de $\Phi(n)$:

$$\Phi(n) = (p - 1)(q - 1)$$

$$n = 6 * 12$$

$$\mathbf{\Phi(n) = 72}$$

Cálculo de s :

$$s = v^{-1} \bmod \Phi(n)$$

$$s = 11^{-1} \bmod \Phi(n)$$

$$\mathbf{s = 59}$$

Cálculo de s_A :

$$s_A = (J_A)^{-s} \bmod n$$

$$s_A = 29^{-59} \bmod 91$$

$$s_A = 29^{32} \bmod 91$$

$$\mathbf{s_A = 22}$$

Cálculo de x :

$$x = r^v \bmod n$$

$$x = 13^{11} \bmod 91$$

$$\mathbf{x = 13}$$

Cálculo de y :

$$y = r(s_A)^e \bmod n$$

$$y = 13 * (22)^6 \bmod 91$$

$$\mathbf{y = 13}$$

Cálculo de z :

$$z = J_A^e y^v \bmod n$$

$$z = 29^6 * 13^{11} \bmod 91$$

$$\mathbf{z = 13}$$

Conferimos que $x = z = 13$.