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 mod 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 $mdc(x+y, n) = p$ 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 $mdc(x + y, n) = p$ ou q, com $y = 0$ teríamos $mdc(x + 0, n) = p$ ou q, ou seja $mdc(x, n) = p$ ou q, sendo que Beto conhece x e n. Como não é possível obter p ou q apenas com $mdc(x, n)$, $y = 0$ 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 - $p = 3$, $q = 7$, $x = 4$, $a =?$, $y =?$, $mdc(x + y, n) =?$
$n = pq = 21$
$x^2 \bmod n = a$, 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:

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

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

$x_0 = 4$

Agora para o cálculo das outras 3 raízes temos:

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

$x_0^{'} = (4 * 3 * 5 - 1 * 7 * 1) \bmod 21 = 11$

$x_0^{''} = 21 - 4 = 17$

$x_0^{'''} = 21 - 11 = 10$

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

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

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 $e = 0$:

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

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

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, Fiet 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, Fiet 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:

$$\begin{gathered}\text{Cálculo de } n\text{:}\\ n = pq\\ n = 3 * 7\\ \mathbf{n = 21}\end{gathered}$$

$$\begin{gathered}\text{Cálculo de } v\text{:}\\ v = s^2 \bmod n\\ v = 17^2 \bmod 21\\ \mathbf{v = 16}\end{gathered}$$

$$\begin{gathered}\text{Cálculo de } x\text{:}\\ x = r^2 \bmod n\\ x = 13^2 \bmod 21\\ \mathbf{x = 1}\end{gathered}$$

Para $e = 0$:

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

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

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

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

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

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

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

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

Exercício 3.

1 - Se s_A for autêntico, então vale que:

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

Sabemos que, no protocolo de identificação vale que:

$$x = r^v \bmod n$$
$$y = r(s_A)^e \bmod n$$
$$z = J_A^e \; y^v \bmod n$$

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

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

■

2 -