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

Cálculo das raízes:
$x_1 = a^{\frac{p+1}{4}} mod\ p$ e $x_2 = a^{\frac{q+1}{4}} mod\ q$, sendo assim temos:
$x_1 = 16^{\frac{3+1}{4}} mod\ 3$, $x_1 = 1$
$x_2 = 16^{\frac{7+1}{4}} mod\ 7$, $x_2 = 4$
Utilizando o Teorema Chinês do resto calcula-se x_0 solução do sistema:

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

Simplificando temos:

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

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

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

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

$$x_0 = 4$$

Agora para o cálculo das outras 3 raízes temos:

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

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

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

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

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 $x = r^2\ mod\ n$
Sabemos que $v = s^2\ mod\ n$
y é autêntico, portanto vale que:

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

Para $e = 0$:
$xv^e\ mod\ n = xv^0\ mod\ n = x\ mod\ n$

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

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

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

Para $e = 1$:
$xv^e\ mod\ n = xv\ mod\ n$

$$y^2 = (rs)^2\ mod\ n$$
$$y^2 = r^2 s^2\ mod\ n$$
$$y^2 = (r^2\ mod\ n)\ (s^2\ mod\ n)$$
$$y^2 = (x\ mod\ n)\ (v\ mod\ n)$$
$$y^2 = xv\ mod\ n$$

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

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 $x = r^2 \ mod \ n$ 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 $y = \sqrt{x} \ mod \ n$ 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 -