/ /

UFRJ- Universidade Federal do Rio de Janeiro

Rio de Janeiro, 08 de Junho de 2017

- PROBLEMA DO LOGARITMO DISCRETO:

- CASO GERAL: dado um grupo $(G, *)$, e $g, h \in G$, determinar x tal que $g^x = h$ em G.

- CASO PARTICULAR EM $U(n)$: dados $g, h \in U(n)$, determinar x tal que $g^x \equiv h \pmod{n}$

O problema nem sempre tem solução, isto é, tal x nem sempre existe. Entretanto, se o grupo for cíclico e g for um gerador do grupo, então o problema sempre tem solução, já que, como g é gerador, todo elemento h do grupo pode ser escrito como potência de g.

No caso do El Gamal, utilizamos o grupo $U(p)$, com p primo (que é cíclico, pelo teorema da raiz primitiva) e um gerador g de $U(p)$. A chave privada é um inteiro a no intervalo no intervalo $1 \leq a \leq p-1$ a chave pública c é a forma reduzida de g^a módulo p.

- Valores públicos: g, p, c
- Valor privado: a

Esses quatro valores satisfazem a relação

$$g^a \equiv c \pmod{p}$$

Então, se quero calcular a a partir dos valores públicos, preciso resolver o seguinte problema do logaritmo discreto:

$g^x \equiv h \pmod p \rightarrow 0 \leq x \leq p-1$

Como $U(p)$ é cíclico e g é um gerador, esse problema do logaritmo do logaritmo discreto sempre tem solução. Essa solução, neste caso, é a chave privada.

- ALGORITMOS PARA A RESOLUÇÃO DO PROBLEMA DO LOGARITMO DISCRETO:

1) ALGORITMO INGÊNUO:

ENTRADA: g, h, p

SAÍDA: x tal que $g^x \equiv h \pmod p$

INSTRUÇÕES:

1) $x \leftarrow 0$

2) Enquanto $g^x \not\equiv h \pmod p$, faça:

2.1) $x \leftarrow x+1$

3) Retorne x

Este algoritmo é eficiente se p for pequeno.

Logo, uma condição necessária (mas que não é suficiente sozinha) para a segurança do El Gamal é que p seja grande.

↳ RECOMENDAÇÃO ATUAL: p com 512 bits ou p com 1024 bits

2) ALGORITMO BABY-STEP | GIANT-STEP DE SHANKS

Vamos descrevê-lo para um grupo $U(n)$:

Seja K a ordem de $U(n)$ (se n for primo $K = n-1$)

Calculamos $m = [\sqrt{K}] + 1$ (no caso de Ulp), $m = [\sqrt{p-1}] + 1$)

Seja x a solução do problema do logaritmo discreto:

$$g^x \equiv h \pmod{n}$$

vou escrever x como:

$$x = i\,m + j,$$

com $0 \leq i, j < m$

Se i for o quociente de x por m e j por o resto de x por m, então i e j estão neste intervalo.

Como j é o resto de uma divisão por m, então:

$$0 \leq j < m,$$

vamos supor que i também está nesse intervalo.

Suponha, por contradição, que $i \geq m$.

Então, $x \geq m \cdot m + j = m^2 + j = ([\sqrt{K}] + 1)^2 + j \geq (\sqrt{K})^2 + j = K + j \geq K$

$\hookrightarrow j \geq 0$

OBSERVAÇÃO: $[\sqrt{K}] \leq \sqrt{K} \leq [\sqrt{K}] + 1$

Temos então

$$x \geq K$$

Entretanto, isso não é possível.

Como x é a ordem do grupo, o expoente x deve estar no intervalo

$$0 \leq x < K$$

Logo, $i \leq m$.

$$g^x \equiv h \pmod{n}$$

$$g^{im+j} \equiv h \pmod{n}$$

$$g^{im} \cdot g^j \equiv h \pmod{n}$$

$$g^j \equiv h \cdot (g^{-1})^{im} \pmod{n}$$

- CALCULO OS BABY - STEPS:

Para j de 0 até m-1, calculo a forma reduzida de g^j módulo n e guardo isso numa tabela:

j	$g^j \pmod{n}$
0	1
⋮	⋮
m-1	$g^{m-1} \pmod{n}$

- CALCULO OS GIANT - STEPS

1) Calculo $g' = g^{-1} \pmod{n}$ (usando o euclidiano estendido)

2) Calculo $t \equiv (g')^m \pmod{n}$

3) Para cada i de 0 a m-1, calculo a forma reduzida de $h t^i$ modulo n e verifico se esse valor aparece na tabela dos baby-steps. Se não aparece, vou para o próximo i. Se aparece, tenho os valores de i e j para calcular x ($x = im + j$).

EXEMPLO:

p=127

g=3

Vamos resolver o problema do logaritmo discreto:

$$3^x \equiv 2 \pmod{127}$$

$$m = \lfloor \sqrt{p-1} \rfloor + 1 = \lfloor \sqrt{126} \rfloor + 1 = 11 + 1 = 12$$

BABY-STEPS

j	3^j mod 127
0	1
1	3
2	9
3	27
4	81
5	116
6	94
7	28
8	84
9	125
10	121
11	109

GIANT-STEPS

1) CALCULO O INVERSO DE g:

R	Q	x	y
3	-	1	0
127	-	0	1
3	0	1	0
1	42	-42	1
0	3	-	-

$-42 \equiv 85 \pmod{127}$

$g^{-1} = 85$

/ /

- CONTINUAÇÃO DOS GIANT-STEPS

2) CALCULO $(g^i)^m$

R	A	E	É IMPAR?
1	85	12	NÃO
1	113	6	NÃO
1	69	3	SIM
69	62	1	SIM
87	34	0	NÃO

$t = 87$

- CALCULO DOS BABY-STEPS;

i	$h \cdot t^i \mod 127$
0	2
1	47
2	25
3	16
4	122
5	73
6	1

$$\begin{cases} i = 6 \\ j = 0 \end{cases}$$

$x = im + j =$

$= 6 \cdot 12 + 0 =$

$= 72$