INE5429 - Prova 2 Resolvida

prof. Ricardo Custódio

18 de outubro de 2016

MOSTRE TODOS OS CÁLCULOS
NÃO USE CALCULADORA - NÃO HÁ NECESSIDADE
ESCOLHA DUAS DAS TRÊS QUESTÕES PARA RESPONDER

Seja α igual ao último dígito do seu número de matrícula adicionado de 30. Por exemplo, se o seu número de matrícula é 1410083**7**, então $\alpha = 7 + 30 = 37$.

1. Considere que você deseja cifrar e decifrar mensagens de até 8 bits usando o algoritmo RSA.

   (a) Nesse cenário, gere um par de chaves RSA, onde o expoente público deve ser 9;
   Resolução: Como são 8 bits, precisaremos trabalhar com números de 0 até $2^8 - 1 = 255$. Assim, temos $n \geq 255$. Precisamos encontrar dois números primos que multiplicados sejam maiores e mais próximos de 255. Essa proximidade se justifica no sentido de se manter as operações aritméticas o mais eficiente quanto possível. Em poucas tentativas é fácil encontrar que esses primos poderiam ser $p = 11$ e $q = 29$. É importante observar que devemos escolher os primos de tal forma que o totiente de Euler de n seja coprimo ao expoente público 9. Isso implica que tanto $p - 1$ quanto $q - 1$ não podem ter o fator primo 3. Por exemplo, não podemos escolher o primo 31 uma vez que $31 - 1 = 30 = 3 \times 10$. Uma vez escolhido adequadamente os primos, determinamos o módulo n

   $$n = pq = 11 \times 29 = 319$$

   O Totiente de Euler de n é dado por:

   $$\phi(n) = (p-1)(q-1) = (11-1)(29-1) = 10 \times 28 = 280.$$

   Tem-se, do enunciado da questão, que o expoente público é 9. Seja este expoente d. Devemos agora determinar

   $$e = d^{-1} \pmod{\phi(n)}$$
   $$e = 9^{-1} \pmod{280}$$

   Para determinar o inverso multiplicativo de 9 módulo 280 devemos usar o algoritmo extendido de Euclides. Dividindo-se 280 por 9, tem-se

   $$280 = 31 \times 9 + 1 \tag{1}$$

   Portanto, o resto da divisão de 280 por 9 é 1. Assim, podemos concluir que $MDC(9, 280) = 1$ e, portanto, existe o inverso multiplicativo de 9 módulo 280. Vamos agora, usando o Euclides, determinar o inverso. Usando-se a Equação 1, tem-se:

   $$1 = 280 - 31 \times 9$$
   $$1 = -31 \times 9 \pmod{280}$$

   $$1 = 249 \times 9 \pmod{280}$$

   Portanto,

   $$e = 249.$$

   As chaves são:

   Chave Pública: $(d, n) = (9, 319)$.
   Chave Privada: $(e, n) = (249, 319)$.

(b) Usando a chave privada, cifre a mensagem $M = 5$.
Resolução: Fazendo
$$C = M^e \pmod n = 5^{249} \pmod{319}$$
Apesar de aparentar trabalhosa essa operação (normalmente não se consegue fazer esta operação numa calculadora tradicional), a exponenciação modular é relativamente fácil de ser feita. Um algoritmo muito utilizado é o conhecido método binário da esquerda para a direita. Esse método consiste em utilizar os quadrados sucessivos de um número. Desejamos determinar
$$b^e \pmod m$$
Escrevemos o expoente e em sua notaçãoo binária como
$$e = \sum_{i=0}^{n-1} a_i 2^i$$
Nessa notação, o comprimento de e é n bits, a_i pode ser 0 ou 1 para qualquer i tal que $0 \leq i < n$. Por definição, $a_{n-1} = 1$.
O valor c pode então ser escrito como
$$c = b^e = b^{\left(\sum_{i=0}^{n-1} a_i 2^i\right)}$$
$$c = \prod_{i=0}^{n-1} \left(b^{2^i}\right)^{a_i}$$
Usando os quadrados sucessivos de 5 mostrados na Tabela 1, tem-se

Tabela 1: Quadrados sucessivos de 5 (mod 319).

$\mathbf{u}$	$\mathbf{5^u}$	$\mathbf{5^u}$ (mod $\mathbf{131}$)
1	5	5
2	$5 \times 5 = 25$	25
4	$25 \times 25 = 625$	306
8	$306 \times 306 = 93636$	169
16	$169 \times 169 = 28561$	170
32	$190 \times 190 = 28900$	190
64	$53 \times 53 = 38100$	53
128	$53 \times 53 = 2809$	257

$$5^{249} = 5^{128} \times 5^{64} \times 5^{32} \times 5^{16} \times 5^{8} \times 5$$
$$5^{249} = (257 \times 53) \times (190 \times 170) \times (169 \times 5) = (233 \times 81) \times 207 = 199 \times 207 = 42 \pmod{319}.$$
Portanto, $C = 42$.

2. Considere o algoritmo de acordo de chaves de Diffie-Helamnn (DH) e seja $p = 131$ o número primo parâmetro global do algoritmo.

(a) Sabendo que p tem 48 raízes primitivas e uma delas é $r_1 = 2$, determine outra (diferente de 2) raíz primitiva para uso nesse protocolo. Seja essa outra raiz r_2;
Resolução: Somente para referência, essas são as 48 raízes raízes primitivas de 131: 2, 6, 8, 10, 14, 17, 22, 23, 26, 29, 30, 31, 37, 40, 50, 54, 56, 57, 66, 67, 72, 76, 82, 83, 85, 87, 88, 90, 93, 95, 96, 97, 98, 103, 104, 106, 110, 111, 115, 116, 118, 119, 120, 122, 124, 126, 127, 128. A determinação de uma raiz primitiva de um número primo não é uma tarefa fácil. No entanto, uma vez tendo-se uma das raízes, todas as demais raízes são facilmente computáveis. No enunciado da questão foi dada $r_1 = 2$, uma das raízes primitivas de 131.
Sabe-se que o número de raízes primitivas de um número primo p é dado por
$$N_r = \phi(\phi(p)),$$
onde $\phi(p)$ é o Totiente de Euler de p, ou seja, a quantidade de números positivos menores que p coprimos a p. O Totiente de Euler de um número primo p é dado por
$$\phi(p) = p - 1$$
. Uma fórmula mais geral para se determinar o Totiente de Euler de um número n não primo é
$$\phi(n) = \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

Tabela 2: Quadrados sucessivos de 8 (mod 131).

$\mathbf{u}$	$\mathbf{8^u}$	$\mathbf{8^u}$ (mod $\mathbf{131}$)
1	8	8
2	$8 \times 8 = 64$	64
4	$64 \times 64 = 4096$	35
8	$35 \times 35 = 1225$	46
16	$46 \times 46 = 2116$	20
32	$20 \times 20 = 400$	7

Tabela 3: Quadrados sucessivos de 125 (mod 131).

$\mathbf{u}$	$\mathbf{125^u}$	$\mathbf{125^u}$ (mod $\mathbf{131}$)
1	125	125
2	$125 \times 125 = 15625$	36
4	$36 \times 36 = 1296$	117
8	$117 \times 117 = 13689$	65
16	$65 \times 65 = 4225$	33
32	$33 \times 33 = 1089$	41

Neste caso temos

$$\phi(\phi(131)) = \phi(130)$$

Os divisores primos de 130 são: 2, 5 e 13. Assim

$$\phi(130) = 130\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{13}\right) = 130\frac{1}{2}\frac{4}{5}\frac{12}{13} = 48.$$

Portanto, 131 tem 48 raízes primtivas.
Se r é uma raiz primitiva de um número primo p, então r^d também será uma raiz primtiva, onde d é um coprimo de $(p-1)$. Os coprimos (no total de 48) de 130 são 1, 3, 7, 9, 11, 17, 19, 21, 23, 27, 29, 31, 33, 37, 41, 43, 47, 49, 51, 53, 57, 59, 61, 63, 67, 69, 71, 73, 77, 79, 81, 83, 87, 89, 93, 97, 99, 101, 103, 107, 109, 111, 113, 119, 121, 123, 127 e 129. Assim, dada a raiz primitiva $r_1 = 2$, uma segunda raiz primitiva é dada por

$$r_2 = {r_1}^3 = 2^3 = 8.$$

(b) Usando os parâmetros públicos p e r_2 e sabendo que as chaves secretas de Alice e Beto são $X_A = \alpha$ e $X_B = \alpha + 9$, respectivamente, proceda ao acordo de chaves.
Resolução:

$$\begin{aligned}
Y_A &= {r_2}^{X_A} \pmod p \\
&= 8^{37} \pmod{131} = 8^{32} \times 8^4 \times 8 \pmod{131} = 7 \times 35 \times 8 \pmod{131} = 126 \\
Y_B &= {r_2}^{X_B} \pmod p \\
&= 8^{46} \pmod{131} = 8^{32} \times 8^8 \times 8^4 \times 8^2 \pmod{131} = 7 \times 46 \times 35 \times 64 \pmod{131} = 125
\end{aligned}$$

Então, procede-se ao cálculo da chame K

$$\begin{aligned}
K &= {Y_B}^{X_A} \pmod{131} \\
&= 125^{37} \pmod{131} = 125^{32} \times 125^4 \times 125 \pmod{131} = 41 \times 117 \times 125 \pmod{131} = 38 \\
K &= {Y_A}^{X_B} \pmod{131} \\
&= 126^{46} = 126^{32} \times 126^8 \times 126^4 \times 126^2 \pmod{131} = 74 \times 114 \times 101 \times 25 \pmod{131} = 38
\end{aligned}$$

3. Seja $f(x) = x^4 + x + 1$ um polinômio irredutível em $GF(2^4)$. Seja $g(x) = x^3 + \alpha x + 1$, onde os coeficientes do polinômio estão em $GF(2)$. Sabendo que

$$E(s) = s.g(x)^{-1} \mod f(x)$$

é um algoritmo de ciframento de s, determine $E(s = x^2 + 1)$.
Resolução:
Deve-se primeiramente calcular o inverso multiplicativo de g(x) utilizando o algoritmo extendido de euclides. Começamos por achar o mdc(f, g) utilizando apenas o algoritmo de euclides:

$$f = g_1.g + r_1$$

Tabela 4: Quadrados sucessivos de 126 (mod 131).

$\mathbf{u}$	$\mathbf{126^u}$	$\mathbf{126^u}$ (mod $\mathbf{131}$)
1	126	126
2	$126 \times 126 = 15876$	25
4	$25 \times 25 = 625$	101
8	$101 \times 101 = 10201$	114
16	$114 \times 114 = 12996$	27
32	$27 \times 27 = 729$	74

$$x^4 + x + 1 = x.(x^3 + x + 1) + (x^2 + 1)$$
$$g = q_2.r_1 + r_2$$
$$x^3 + x + 1 = x.(x^2 + 1) + 1$$
$$r_1 = q_3.r_2 + r_3$$
$$x^2 + 1 = (x^2 + 1).1 + 0$$

Depois disso, devemos utilizar a extensão do algoritmo para achar o inverso. Para isso, devemos considerar os seguintes parâmetros ($s_0 = 1, s_1 = 0, t_0 = 0, t_1 = 1$).

Calculando s:

$$s_2 = s_0 - q_1.s_1$$
$$s_2 = 1 - x.0$$
$$s_2 = 1$$

$$s_3 = s_1 - q_2.s_2$$
$$s_3 = 0 - x.1$$
$$s_3 = x$$

Calculando t:

$$t_2 = t_0 - q_1.t_1$$
$$t2 = 0 - x.1$$
$$t_2 = x$$

$$t_3 = t_1 - q_2.t_2$$
$$t_3 = 1 - (x.x)$$
$$t_3 = x^2 + 1$$

O algoritmo extendido de euclides resulta em $mdc(f, g) = s.f + t.g$. Isso retorna o $t = x^2 + 1$ que é o inverso de $g(x)$.

Após calcular o inverso multiplicativo, pode-se calcular o resultado do ciframento:

$$E = s.g(x)^{-1} \mod f(x)$$
$$E = (x^2 + 1).(x^2 + 1) \mod f(x)$$
$$E = x^4 + 1 \mod x^4 + x + 1$$
$$E = x$$

MOSTRE TODOS OS CÁLCULOS

Todos os resultados devem ser comprovados

Boa Sorte