INE5429 - Prova 2 Resolvida

prof. Ricardo Felipe Custódio

3 de novembro de 2015

Sejam p e v definidos na Tabela 1, de acordo com o último dígito do seu número de matrícula.

Tabela 1: Definição de p e v.

Útimo Dígito	0	1	2	3	4	5	6	7	8	9
p	17	19	23	29	31	17	19	23	31	17
v	113	109	101	97	113	109	101	97	113	109

Escolha de p e v: Seja a matrícula 1014141-0. Então, $p = 17$ e $v = 113$.

1. Considere que você deseja cifrar e decifrar mensagens de até 9 bits, de forma o mais eficiente possível, usando o algoritmo RSA.

   (a) Nesse cenário, gere um par de chaves RSA, onde um dos primos deve ser p e o expoente público deve ser 13;
   Resolução: Como são 9 bits, precisaremos trabalhar com números de 0 até $2^9 - 1 = 511$. Assim, temos $n \leq 511$. Sabemos que um dos primos é $p = 17$. O segundo primo deverá ser o menor primo tal que $pq \geq 511$, ou seja, $15q \geq 511$. Deverá ser o menor primo, pois queremos a maior eficiência possível. Como $512/17 \approx 30.1$, então q deverá ser 31. Assim

   $$n = pq = 17 \times 31 = 527$$

   Note que q não poderia ser 29 uma vez que $17 \times 29 = 493 < 511$. E também não deve ser 37, uma vez que $17 \times 37 = 629$ excede em muito 511.
   O Totiente de Euler de n é dado por:

   $$\phi(n) = (p-1)(q-1) = (17-1)(31-1) = 16 \times 30 = 480.$$

   Tem-se, do enunciado, que um dos expoentes é 13. Seja este expoente d. Devemos agora determinar

   $$e = d^{-1} \pmod{\phi(n)}$$
   $$e = 13^{-1} \pmod{480}$$

   Para determinar o inverso multiplicativo de 13 módulo 480 devemos usar o algoritmo extendido de Euclides. Dividindo-se 480 por 13, tem-se

   $$480 = 36 \times 13 + 12 \tag{1}$$

   Ve-se, portanto, que o resto da divisão de 480 por 13 é 12. Dividindo-se 13 por 12 tem-se

   $$13 = 1 \times 12 + 1 \tag{2}$$

   Portanto, o resto da divisão de 13 por 12 é 1. Assim, podemos concluir que $MDC(480, 13) = 1$ e, portanto, existe o inverso multiplicativo de 13 módulo 480. Vamos agora, usando o Euclides, determinar o inverso. Usando-se pimeiro a Equação 2 e depois a Equação 1, tem-se:

   $$1 = 13 - 1 \times 12$$
   $$1 = 13 - 1 \times (480 - 36 \times 13)$$
   $$1 = 37 \times 13 - 1 \times 480$$

   $$1 = 37 \times 13 \pmod{480}$$

   Portanto,

   $$e = 37.$$

   As chaves são:

   Chave Pública: $(d, n) = (13, 527)$.
   Chave Privada: $(e, n) = (37, 527)$.

(b) Usando a chave privada, cifre a mensagem $M = 5$.
Resolução: Fazendo

$$C = M^e \pmod{n} = 5^{37} \pmod{527}$$

Usando os quadrados sucessivos de 5 mostrados na Tabela 2, tem-se

Tabela 2: Quadrados sucessivos de 5 (mod 527).

5^1	5	5	$5 \pmod{527} = 5$
5^2	5×5	25	$25 \pmod{527} = 25$
5^4	25×25	625	$625 \pmod{527} = 98$
5^8	98×98	9604	$9604 \pmod{527} = 118$
5^{16}	118×118	13924	$13924 \pmod{527} = 222$
5^{32}	222×222	49284	$49284 \pmod{527} = 273$

$$5^{37} = 5^{32} \times 5^4 \times 5$$
$$5^{37} = 273 \times 98 \times 5 = 133770 \pmod{527} = 439.$$

Portanto, $C = 439$.

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

(a) Determine os outros parâmetros públicos necessários ao DH;
Resolução: São dois os parâmetros públicos do DH: o número primo v, já dado no enunciado da questão, e uma raiz primitiva deste. É necessário, portanto, para completar os parâmetros públicos, determinarmos uma das raízes primitivas de v. Sabe-se que v tem $\phi(\phi(v))$ raízes primitivas. Assim, v tem

$$\phi(\phi(v)) = \phi(\phi(113)) = \phi(112) = 112(1 - \frac{1}{2})(1 - \frac{1}{7}) = 48 \text{ raízes.}$$

Precisamos de uma das raízes para ser o nosso parâmetro α. Para isso, podemos usar o seguinte algoritmo:

i. Determinar os k fatores primos de $\phi(v)$. Sejam esses fatores $p_1, \ldots, p_k$;
ii. Para todo $m \in \mathbb{Z}_p$ computar

$$m^{\frac{\phi(v)}{p_i}} \pmod{v} \quad \text{para } i = 1, \ldots, k$$

iii. Um número m para o qual esses k resultados são diferentes de 1 é uma raíz primitiva.

Então temos: $\phi(113) = 112 = 2^4 \times 7$. Portanto $k = 2$, $p_1 = 2$ e $p_2 = 7$. Vamos agora testar se $m = 2$ é uma raiz primitiva. Usaremos os valores dos quadrados sucessivos de 2 da Tabela 3 para realizar de forma rápida as exponenciações modulares.

$$2^{\frac{112}{2}} \pmod{113} = 2^{56} \pmod{113} = 2^{32} \times 2^{16} \times 2^8 \pmod{113} = 16 \times 109 \times 30 = 52320 \pmod{113} = 1$$
$$2^{\frac{112}{7}} \pmod{113} = 2^{16} \pmod{113} = 109$$

Como o primeiro resultado é 1, então $m = 2$ não é uma raíz primitiva. Vamos agora testar $m = 3$. Usaremos os valores dos quadrados sucessivos de 3 da Tabela 4 para realizar de forma rápida as exponenciações modulares.

Tabela 3: Quadrados sucessivos de 2 (mod 113).

2^1	2	2	$2 \pmod{113} = 2$
2^2	2×2	4	$4 \pmod{113} = 4$
2^4	4×4	16	$16 \pmod{113} = 16$
2^8	16×16	256	$256 \pmod{113} = 30$
2^{16}	30×30	900	$900 \pmod{113} = 109$
2^{32}	109×109	11881	$11881 \pmod{113} = 16$

$$3^{\frac{112}{2}} \pmod{113} = 3^{56} \pmod{113} = 3^{32} \times 3^{16} \times 3^8 \pmod{113} = 28 \times 49 \times 7 = 9604 \pmod{113} = 112$$
$$3^{\frac{112}{7}} \pmod{113} = 3^{16} \pmod{113} = 49$$

Como ambos os resultados são diferentes de 1, podemos concluir que $m = 3$ é uma raíz primitiva de 113. Assim, os parâmetros públicos do protocolo DH são: $v = 113$ e $\alpha = 3$ uma raíz primitiva de v.

(b) Sabendo que as chaves secretas de Alice e Beto são $X_A = 5$ e $X_B = 50$, respectivamente, proceda ao acordo de chaves.
Resolução: Alice e Beto determinam, respectivamente

$$Y_A = \alpha^{X_A} \pmod{v} = 3^5 = 17$$
$$Y_B = \alpha^{X_B} \pmod{v} = 3^{50} = 31$$

Tabela 4: Quadrados sucessivos de 3 (mod 113).

3	3	3	$3 \pmod{113} = 3$
3^2	3×3	9	$9 \pmod{113} = 9$
3^4	9×9	81	$81 \pmod{113} = 81$
3^8	81×81	6561	$6561 \pmod{113} = 7$
3^{16}	7×7	49	$49 \pmod{113} = 49$
3^{32}	49×49	2401	$2401 \pmod{113} = 28$

Alice então envia Y_A para Beto e Beto envia Y_B para Alice. Então, Alice e Beto determinam K, como segue

$$K = Y_B^{X_A} \pmod{113} = 31^5 = 36$$
$$K = Y_B^{X_A} \pmod{113} = 17^{50} = 3^{5^{50}} = 3^{50^5} = 31^5 = 36$$

3. Prove que a estrutura de Feistel é inversível. Utilize a simbologia apresentada na Figura 1.

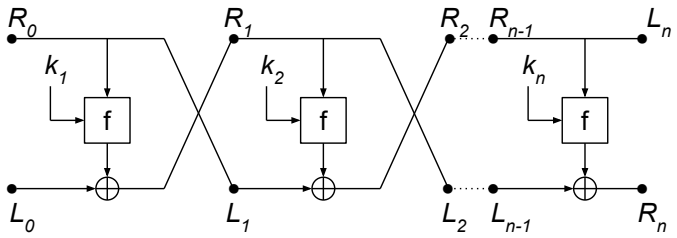

Figura 1: Estrutura de Feistel

Resolução: Para provar que a Estrutura de Feistel é inversível precisamos primeiro encontrar a inversa de uma rodada de Feistel. Sem perda de generalidade, vamos tornar implícita nas equações desta prova a sub-chave k_i usada pela função ciclo f_i. Seja F_i a função computada na i-ésima rodada. Então

$$\begin{aligned} F_i(L_{i-1}||R_{i-1}) &= L_i||R_i \\ &= R_{i-1}||L_{i-1} \oplus f_i(R_{i-1}) \end{aligned} \tag{3}$$

Devemos agora encontrar um função $G_i = F_i^{-1}$ tal que

$$G_i(R_{i-1}||L_{i-1} \oplus f_i(R_{i-1})) = L_{i-1}||R_{i-1}$$

Vamos mostrar que esta função é dada por

$$G_i(L_i||R_i) = R_i \oplus f_i(L_i)||L_1$$

Vejamos

$$\begin{aligned} G_i(R_{i-1}||L_{i-1} \oplus f_i(R_{i-1})) &= L_{i-1} \oplus f_i(R_{i-1}) \oplus f_i(R_{i-1})||R_{i-1} \\ &= L_{i-1} \oplus R_{i-1} \end{aligned}$$

Assim temos

$$m = G_i(F_i(m))$$

Vamos agora mostrar que Feistel é inversível para n rodadas:

$$\begin{aligned} m &\stackrel{?}{=} G_1(G_2(\ldots G_{n-1}(G_n(F_n(F_{n-1}(\ldots F_1(m)\ldots))))\ldots)) \\ &\stackrel{?}{=} G_1(G_2(\ldots G_{n-1}(F_{n-1}(\ldots F_1(m)\ldots))\ldots)) \\ &\stackrel{?}{=} \ldots \\ &\stackrel{?}{=} G_1(F_1(m)) \\ m &= m \quad \square \end{aligned}$$