7.2 Criptografia RSA

7.2.1 Pré-codificação

Vamos considerar duas pessoas, João e Maria, que desejam trocar mensagens secretas por um canal não seguro (isto é, um canal que outras pessoas - intrusos - podem acessar facilmente). Se Maria quer enviar uma mensagem codificada para João, ela deve começar pedindo para ele "fabricar"a chave secreta. Assim, João deve escolher os *parâmetros* do sistema RSA, dois primos distintos p e q (muito grandes) e calcular o produto $n = pq$. Ele também deve escolher $e \in \mathbb{N}$ tal que $mdc(e, \varphi(n)) = 1$. Os números p e q devem ser mantidos em segredo por João (em um cofre, por exemplo), já a dupla (n, e) é transmitida por um canal não seguro para Maria (e, como qualquer pessoa pode ver esse par, ele é chamado chave pública). Pode-se, por exemplo, postar esse (n, e) em um site.

De posse da chave pública, Maria escreve a mensagem. Em seguida, ela precisa transformá-la em um número α de acordo com a seguinte tabela

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

e, para cada espaço entre palavras, usar o número 99.

O próximo passo é quebrar o número α em blocos formados por números positivos menores do que n, que não comecem por zero e não correspondam a nenhuma letra segundo a tabela acima.

Exemplo 7.2 *A frase "Paraty é linda"é convertida por Maria no número*

$$\alpha = 25102710293499149921182313 10$$

Se João escolhe os parâmetros $p = 11$ *e* $q = 13$ *(pequenos, mas é só um exemplo!), então* $n = 143$. *Maria, então, pode separar* α *em blocos*

$$25 - 102 - 7 - 102 - 93 - 49 - 91 - 49 - 92 - 118 - 23 - 13 - 10$$

7.2.2 Codificando e decodificando

Codificação

A chave de codificação do sistema RSA é (n, e), onde $n = pq$ e $e \in \mathbb{N}$ tal que $mdc(e, \varphi(n)) = 1$.

Observação 7.1 *1. Temos que* e *é invertível módulo* $\varphi(n)$

2. $e \neq 1$, *por questão de segurança, como veremos a seguir.*

3. $e \neq 2$, *pois* $\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$ *é par.*

4. Assim, $e > 2$ *e* e *é ímpar.*

Maria deve codificar cada bloco separadamente da seguinte maneira

$$\boxed{b = \text{bloco oriundo da pré-codificação}}$$

$$\boxed{C(b) = \text{bloco } b \text{ codificado} = \text{resto da divisão de } b^e \text{ por } n, \text{ isto é, } c(b) \equiv b^e \pmod{n}}$$

Observação 7.2 *Aqui fica claro porque* $e \neq 1$. *De fato, caso contrário, teríamos* $C(b) = b$, *afetando a segurança.*

Então, a mensagem codificada será a sequência dos blocos codificados (mas sem reuni-los formando um só número) e Maria pode passá-la para João por qualquer canal público.

Decodificação

A chave de decodificação do sistema RSA é (n, d), onde $n = pq$ e $d \in \mathbb{N}$ é o inverso de e módulo $\varphi(n)$.

Observação 7.3 *Para calcular d, João pode usar o algorítmo euclidiano estendido para $\varphi(n)$ e e, pois $mdc(e, \varphi(n)) = 1$ e $ed \equiv 1 \pmod{\varphi(n)}$. Aqui, calcular $\varphi(n)$ depende de conhecer p e q, mas esses dois foram escolhidos e guardados em segredo por João, então a princípio somente ele pode efetuar o cálculo. Mais a frente, veremos, no entanto, que se um intruso conseguir descobrir $\varphi(n)$, em alguns casos ele pode calcular p e q e decifrar qualquer mensagem enviada utilizando n como chave RSA.*

Se a é um bloco codificado, então $D(a)$ é o resultado do processo de decodificação, sendo

$$\boxed{D(a) = \text{resto da divisão de } a^d \text{ por } n, \text{ isto é, } D(a) \equiv a^d \pmod{n}}$$

Os processos de pré-codificação, codificação e decodificação estão resumidos na tabela a seguir

	João	Maria
Criação das chaves	Escolhe primos secretos p e q, calcula $n = pq$ e escolhe $e \in \mathbb{N}$ tal quc $mdc(e, \varphi(n)) = 1$. Divulga (n, e)	
Codificação		Separa a mensagem α em blocos b e calcula $c(b) \equiv b^e \pmod{n}$. Envia $c(b)$ a João.
Decodificação	Calcula $d \in \mathbb{N}$ inverso de e módulo $\varphi(n)$. Calcula $c(b)^d \pmod{n}$ e obtém a mensagem.	

Exemplo 7.3 $p = 11$, $q = 13$, $n = 143$, $\varphi(n) = \varphi(143) = 10 \times 12 = 120$, $e = 7$ *(foi escolhido o menor possível).*

A chave de codificação é $(143, 7)$ *e o primeiro bloco da mensagem é 25, assim* $C(25)$ *é o resto da divisão de* 25^7 *por 143. Como*

$$25^4 = 390625 \equiv 92 \pmod{143}$$

$$25^3 = 15625 \equiv 38 \pmod{143}$$

então, $25^7 \equiv 3496 \equiv 64 \pmod{143}$, *donde* $C(25) = 64$.

Repetindo o processo para todos os blocos, obtém-se

$$64 - 119 - 6 - 119 - 102 - 36 - 130 - 36 - 27 - 79 - 23 - 117 - 10$$

Para decodificar, é preciso encontrar d. Aplicando o algoritmo euclidiano estendido a $\varphi(n) = 120$ *e* $e = 7$, *obtém-se*

restos	*quocientes*	x	y
120	-	*1*	*0*
7	-	*0*	*1*
1	*17*	*1*	*-17*
0	*7*	-	-

Logo, $120 \times 1 + 7 \times (-17) = 1$, *ou seja,* $7 \times (-17) \equiv 1 \pmod{120}$. *Assim,* $d = 103$, *pois* $-17 \equiv 103 \pmod{120}$.

O primeiro bloco da mensagem codificada é 64. Esse bloco decodificado é $D(64)$, o resto de 64^{103} por 143. Temos que $64^{103} = (2^6)^{103} = 2^{618}$. Como $mdc(2, 143) = 1$, o Teorema de Euler implica em

$$\begin{aligned} 2^{\varphi(143)} &\equiv 1 \pmod{143} \\ 2^{120} &\equiv 1 \pmod{143} \\ 2^{600} = (2^{120})^5 &\equiv 1 \pmod{143} \\ 2^{618} = 2^{600}2^{18} &\equiv 2^{18} \pmod{143} \end{aligned}$$

Agora, $2^10 = 1024 \equiv 23 \pmod{143}$ e $2^8 = 256 \equiv 113 \pmod{143}$, donde

$$2^{18} = 2599 \equiv 25 \pmod{143}$$

Portanto,

$$64^{103} \equiv 25 \pmod{143}$$

7.2.3 Por que funciona?

Precisamos verificar que o processo de decodificação de uma mensagem codificada de fato retorna a mensagem original, isto é, se b é um inteiro tal que $1 \leq b \leq n-1$, então $D(C(b)) = b$.

Vamos mostrar que $D(C(b)) \equiv b \pmod{n}$. Assim, como $D(C(b))$ é o resto da divisão de $C(b)^d$ por n e tanto $D(C(b))$ quanto b são inteiros entre 0 e $n-1$, temos que $D(C(b)) = b$.

Temos que

$$D(C(b)) = C(b)^d \equiv (b^e)^d \equiv b^{ed} \pmod{n}$$

Além disso, como d é o inverso de e módulo $\varphi(n)$, então $ed \equiv 1 \pmod{\varphi(n)}$, donde existe $k \in \mathbb{Z}_+^*$ tal que $ed = 1 + k\varphi(n)$, pois e e d são inteiros maiores que 2 e $\varphi(n) > 0$. Assim, $ed = 1 + k(p-1)(q-1)$ e, então

$$D(C(b)) \equiv b^{ed} \equiv b^{1+k(p-1)(q-1)} \equiv b\,(b^{(p-1)(q-1)})^k \pmod{n}$$

Se $p \nmid b$, então $b^{p-1} \equiv 1 \pmod{p}$ pelo Pequeno Teorema de Fermat, donde

$$b^{ed} \equiv b\,(b^{(p-1)})^{(q-1)k} \equiv b \pmod{p}$$

Se $p|b$, então $b \equiv 0 \pmod{p}$ e $b^{ed} \equiv 0 \pmod{p}$, logo $b^{ed} \equiv b \pmod{p}$.

Analogamente, $b^{ed} \equiv b \pmod{q}$. Como $mdc(p, q) = 1$ e $n = pq$, segue que $b^{ed} \equiv b \pmod{n}$, isto é, $D(C(b)) \equiv b \pmod{n}$.

7.2.4 Por que é seguro?

Temos que o RSA é seguro se e somente se é difícil calcular d conhecendo apenas n e e. Na prática, sabemos calcular d aplicando o algoritmo euclidiano estendido a $\varphi(n)$ e e. Mas só sabemos calcular $\varphi(n)$ se soubermos fatorar n para obter p e q. Portanto, fatorar n é necessário para quebrar o código, o que se torna cada vez mais difícil se n for muito grante.

7.3 Exercícios resolvidos

Exercício 7.1 *Sabendo-se que $n = 3552377$ é igual ao produto de dois números primos e que $\varphi(n) = 3548580$, fatore n. Assim, mesmo qe p e q sejam secretos, se algum intruso conhecer $\varphi(n)$, ele pode descobrir p e q e decifrar a mensagem.*

Solução: Temos $n = pq$ e $\varphi(n) = (p-1)(q-1) = pq - p - q + 1 = n - (p+q) + 1$, isto é, $p + q = n - \varphi(n) + 1$. Assim, precisamos resolver o sistema

$$\begin{cases} p + q = 3798 \Rightarrow p = 3798 - q \\ pq = 3552377 \end{cases}$$

Temos

$$(3798 - q)q = 3552377$$
$$3798q - q^2 = 3552377$$
$$q^2 - 3798q + 3552377 = 0$$
$$q = \frac{3798 \pm \sqrt{215296}}{2}$$

$$q_1 = 2131 \Rightarrow p_1 = 1667$$
$$q_2 = 1667 \Rightarrow p_2 = 2131$$

Logo, $n = 1667 \times 2131$.

Exercício 7.2 *A chave pública utilizada pelo Banco de Toulouse para codificar suas mensagens é a seguinte* $n = 10403$ *e* $e = 8743$. *Recentemente, os computadores do banco receberam, de local indeterminado, a seguinte mensagem*

$$4746 - 8214 - 9009 - 4453 - 8198$$

O que diz a mensagem mandada ao banco?

Solução: Temos $n = 10403 = 101 \times 103$, $e = 8743$ e $\varphi(n) = 100 \times 102 = 10200$. Para encontrar d, fazemos o algoritmo de euclides estendido.

restos	quocientes	x	y
10200	-	1	0
8743	-	0	1
1457	1	1	-1
1	6	-6	7
0	1457	-	-

Assim, $10200 \times (-6) + 8743 \times 7 = 1$, donde $8743 \times 7 \equiv 1 \pmod{10200}$ e $d = 7$. Agora, podemos passar ao processo de decodificação

$4746^2 = 22524516 \equiv 2021 \pmod{10403}$
$(4746^2)^2 \equiv (2021)^2 \equiv 4084441 \equiv 6465 \pmod{10403}$
$4746^6 \equiv 13065765 \equiv 10000 \pmod{10403}$
$4746^7 \equiv 47460000 \equiv 1514 \pmod{10403}$
$D(4746) = 1514$

$8214 \equiv -2189 \pmod{10403}$
$8214^2 = 4791721 \equiv 6341 \pmod{10403}$
$(8214^2)^2 \equiv 40208281 \equiv 6341 \pmod{10403}$
$8214^6 \equiv 4349926 \equiv 1472 \pmod{10403}$
$8214^7 \equiv 12091008 \equiv 2722 \pmod{10403}$
$D(8214) = 2722$

$9372 \equiv -1031 \pmod{10403}$
$9372^2 = 1062961 \equiv 1855 \pmod{10403}$
$(9372^2)^2 \equiv 3441025 \equiv 8035 \pmod{10403}$
$9372^6 \equiv 14904925 \equiv 7829 \pmod{10403}$
$9372^7 \equiv 73373388 \equiv 1029 \pmod{10403}$
$D(9372) = 1029$

$9009 \equiv -1394 \pmod{10403}$
$9009^2 \equiv 1943236 \equiv -2125 \pmod{10403}$
$(9009^2)^2 \equiv 4515625 \equiv 723 \pmod{10403}$
$9009^6 \equiv -1536375 \equiv 3269 \pmod{10403}$
$9009^7 \equiv 29450421 \equiv 9931 \pmod{10403}$
$D(9009) = 9931$

$4453^2 \equiv 19829209 \equiv 1091 \pmod{10403}$
$(4453^2)^2 \equiv 1190281 \equiv 4339 \pmod{10403}$
$4453^6 \equiv 4733849 \equiv 484 \pmod{10403}$
$4453^7 \equiv 2155252 \equiv 1831 \pmod{10403}$
$D(4453) = 1831$

$8198 \equiv -2205 \pmod{10403}$
$8198^2 \equiv 4862025 \equiv 3824 \pmod{10403}$
$(8198^2)^2 \equiv 14622976 \equiv 6761 \pmod{10403}$
$8198^6 \equiv 25854064 \equiv 2609 \pmod{10403}$
$8198^7 \equiv 21388582 \equiv 14 \pmod{10403}$
$D(8198) = 14$

Assim, a mensagem é

15	14	27	22	10	29	99	31	18	31	14
F	E	R	M	A	T		V	I	V	E

Exercício 7.3 *A mensagem* $6355 - 5075$ *foi codificada pelo método RSA usando a senha* $n = 7597$ *e* $e = 4947$. *Além disso, sabe-se que* $\varphi(n) = 7420$. *Decodifique a mensagem.*

Solução: Para encontrar d fazemos o algoritmo euclidiano estendido para $\varphi(n)$ e e.

restos	quocientes	x	y
7420	-	1	0
4947	-	0	1
2473	1	1	-1
1	2	-2	3
0	2473	-	-

Donde $7420 \times (-2) + 4947 \times 3 = 1$, isto é, $4947 \times 3 \equiv 1 \pmod{7420}$ e $d = 3$. Para decodificar fazemos

$6355^2 = 40386025 \equiv 373 \pmod{7597}$
$6355^3 \equiv 2370415 \equiv 151 \pmod{7597}$
$D(6355) = 151$

$5075^2 = 25755625 \equiv 1795 \pmod{7597}$
$5075^3 \equiv 9109625 \equiv 822 \pmod{7597}$
$D(5075) = 822$

E obtemos

15	18	22
F	I	M

7.4 Exercícios

1. O FBI interceptou uma mensagem criptografada enviada por um terrorista do Afeganistão para seus comparsas nos EUA indicando que um agente de alto escalão será morto. McPhee, um experiente policial do FBI, viu a chave

$$(9047, 7085)$$

e disse que não há problema em decifrar o código RSA, já que ele sabe que $83|9047$. Você foi contratado para ajudar. Decifre a mensagem

$$8655 - 1969 - 1563$$

e diga qual o nome do agente que está na mira dos terroristas.

2. Fred e Julia estão brincando de RSA. Ele escolheu os primos 127 e 211, o inteiro $e = 4811$ e recebeu dela a mensagem

$$17523 - 9183$$

como teste. O que diz a mensagem?

3. No fim do seu curso de Teoria dos Números, Gustavo recebeu uma mensagem de um colega de turma. Eram duas frases criptografadas usando chaves diferentes e, com pressa, ele ficou sem saber a primeira frase. Sabendo que $n = 7171$, $e = 4667$ e que $\varphi(n) = 7000$, decodifique a frase

$$2196 - 3791$$

e complete a mensagem

2196-3791! Esse é o último exercício do curso!