

The RSA Public Crypto-System

Universidad de Cuenca

Optativa 6 - Criptología

Dr. Diego Ponce

Capítulo 4

Freddy L. Abad L.

freddy.abadl@ucuenca.edu.ec

CAP 4

4.1

$$axb \equiv 1 \pmod{m}$$

Como a, b no son primos relativos - coprimos, entonces

$$b \equiv 1 \pmod{\frac{m}{a}}$$

b es el inverso del módulo de a para que se cumpla la igualdad

$$axb + m \times e = 1 \rightarrow a \text{ y } b \text{ son congruentes al módulo } 1 \quad (axb) \equiv 1$$

$$axe \equiv 1 \pmod{m}$$

$$e \equiv ex(axb) \pmod{m}$$

$$e \equiv (a \times e) \times b \pmod{m}$$

$$e \equiv b \pmod{m}$$

Si b no es el inverso del módulo de a , entonces b no es el único y tampoco son coprimos \rightarrow LQ90

4.2

$$n = 19749361535894833$$

$$\phi(n) = 19749361232517120$$

$$\phi(p) = (p-1)(q-1)$$

$$\phi(p) = p \times q$$

$$p+q = n - \phi(n) + 1$$

$$p+q = 19749361535894833 - 19749361232517120 + 1$$

$$p+q = 300000001$$

$$+ p-q = 1048930621$$

$$2p = 4048930631$$

$$p \approx 202446531$$

$$q \approx 975534691$$

4.3

$$a = 25 \quad b = 928102$$

- Inverso es 445469

$$25 \times 928102 = 1 \bmod (445469)$$

$$\begin{array}{l} a = 315 \\ \rightarrow \text{Inverso es } 252415 \end{array}$$

$$\begin{array}{l} a = 1001 \\ \rightarrow \text{Inverso es } 2140671 \end{array}$$

$$\begin{array}{l} a = 2643 \\ \rightarrow \text{no existe inverso} \end{array}$$

$$\begin{array}{l} a = 5231 \\ \rightarrow \text{Inverso es } 2989472411 \end{array}$$

4.4

$$39257365738083976$$

$$6665717059956870$$

$$145693993449451$$

$$14575413675404137$$

4.6

e = numero primo con $(p-1) \times (q-1)$

d = clave privada $\rightarrow d \times e \bmod (p-1) \times (q-1) = 1$

↳ Inverso modular

m = mensaje

$$n = p \times q$$

$m^e \bmod (n) \rightarrow$ es encriptado con la clave publica
de $a \rightarrow n$

y salg se puede desencriptar con d que es su clave
privada

4.7

```

User numero;
int cont = 0;
int subdivisores = (numero.length)/5;
int v[5][subdivisiones]F[subdivisiones] = new int [5][];
for (int i = 1; i <= numero.length; i++) {
    v[cont][1] = numero[i];
    cont++;
    if (cont == 5) {
        cont = 0;
    }
}

```

4.8

```

User num;
String noespacio = " ";
for (i = 0 to num.length; n++) {
    if (num[i] != "-") {
        sin espacios = sin espacios + num[i];
    }
}
int numero = Integer.parseInt(sin espacios);
escribir(numero);

```

4.9

$$n = 233570063 \quad e = 125$$

$$exd \equiv 1 \pmod{\phi(n)}$$

$$n \neq p \times q$$

$$p = 14897$$

$$q = 15679$$

$$\phi(n) = (p-1) \times (q-1)$$

$$\phi(n) = 233534488$$

$$d = 11 \pmod{233534488}$$

$$125$$

$$d = 136387061$$

$$\begin{array}{r|rr} 233570663 & 14897 \\ 15679 & 15679 \\ \hline & \end{array}$$

4.10

$b_{an} = 1$
 $cont = 2$
 $n_1 = 0$
 $n_2 = 0$

long $p \Rightarrow$ # primo de 12 dígitos
 long $q \Rightarrow$

```
while( $b_{an} == 1$ ) {
    if ( $p \neq 2^{cont-1}$ ) {
         $n_1 = cont$ 
         $b_{an} = 0$ 
    }
    else {
         $cont = 2$ 
    }
}
```

$$p = (p * n_1) + 1$$

$$q = (q * n_2) + 1$$

Escribir (p, q)

// PRIMALITY

{ El proceso se repite para q con $cont=2$ y $b_{an}=0$.

} Repetir el proceso de primalidad con los nuevos valores de p y q

// TERMINATE

4.11

$$a \equiv 2 \pmod{21}$$
 $\rightarrow a \equiv 11$

$$a \equiv 3 \pmod{31}$$
 $\rightarrow a \equiv 21$

$$a \equiv 6 \pmod{61}$$
 $\rightarrow a \equiv 51$
 $a \equiv 10 \pmod{101}$
 $\rightarrow a \equiv 91$
 $a \equiv 15 \pmod{151}$
 $\rightarrow a \equiv 141$
 $a \equiv 31 \pmod{311}$
 $\rightarrow a \equiv 301$
 $a \equiv 43 \pmod{431}$
 $\rightarrow a \equiv 421$

4.12

$$x = 22 \pmod{441}$$
 $= 36 \pmod{455}$

$$y = 16 \pmod{303}$$
 $25 \pmod{378}$
 $13 \pmod{423}$

$$z = 25 \pmod{275}$$
 $13 \pmod{495}$
 $46 \pmod{616}$

$$\textcircled{a} \quad x \equiv 22 \pmod{441}$$

$$x \equiv 36 \pmod{455}$$

$$n_1 = 22$$

$$n_2 = 36$$

Aplíco el Teo. de Bézout

$$\exists s_1 \in \mathbb{Z}, \exists n_i \in \mathbb{N} \text{ s.t. } s_1 \frac{n}{n_i} \equiv 1 \pmod{n_i}$$

$$a = \sum_{i=1}^k b_i s_i \frac{n}{n_i} \equiv x(n)$$

$$\text{Si } \frac{n}{n_i} \equiv 1 \pmod{n_i} \quad n = 22 \cdot 36$$

$$s_1 \cdot \frac{22 \cdot 36}{22} \equiv 1 \pmod{22}$$

$$s_1(36) \equiv 1 \pmod{22}$$

$$\text{mcd}(36, 22)$$

$$36 = 22 + 14$$

$$22 = 14 + 8$$

$$14 = 8 + 6$$

$$8 = 6 + 2$$

$$6 = 2 \cdot 2 + 0$$

$$2 = 2 + 0$$

$$\boxed{s_1 \equiv 1 \pmod{2}}$$

$$s_2 \cdot \frac{22 \cdot 36}{36} \equiv 1 \pmod{36}$$

$$s_2(22) \equiv 1 \pmod{36}$$

$$\text{mcd}(22, 36)$$

$$s_2 \equiv 1 \pmod{2}$$

$$a = 22 \cdot 1 \cdot \frac{22 \cdot 36}{22} + 36 \cdot 1 \cdot \frac{22 \cdot 36}{36}$$

$$a = 1584$$

$$1584 \equiv x \pmod{22 \cdot 36}$$

$$1584 \equiv x \pmod{792}$$

$$x \rightarrow \frac{1584}{792} = 2 \quad x \Rightarrow 1584 - 792(2)$$

$$1584 \equiv 0 \pmod{792}$$

$$\boxed{x \equiv 0 - 792m} \quad \text{Recta respuesta}$$

soluciones

$$\textcircled{b} \quad y \equiv 16 \pmod{303}$$

$$y \equiv 25 \pmod{378}$$

$$y \equiv 13 \pmod{423}$$

$$y \equiv 16 \pmod{303}$$

$$y \equiv 25 \pmod{378}$$

$$y \equiv 13 \pmod{423}$$

$$s_1 \cdot \frac{303 \cdot 378 \cdot 423}{303} \equiv 1 \pmod{303}$$

$$S_1 \cdot 159894 \equiv 1 \pmod{303}$$

$\text{mcd}(159894, 303) = 3 \Rightarrow x \text{ Algoritmo Euclides}$

$$\lceil S_1 = 1 \pmod{3} \rceil$$

$$S_2 \cdot \frac{303 \cdot 325 \cdot 423}{378} \equiv 1 \pmod{378}$$

$$S_2 (128169) \equiv 1 \pmod{378}$$

$\text{mcd}(128169, 378) \Rightarrow x \text{ Algoritmo Euclides}$

$$\lceil S_2 = 1 \pmod{27} \rceil$$

$$S_3 \cdot 303 \cdot 378 \cdot 423 \equiv 1 \pmod{423}$$

$$\lceil 423 \rceil$$

$$S_3 (114534) \equiv 1 \pmod{423}$$

$$\text{mcd}(114534, 423) = 9$$

$$\lceil S_3 = 1 \pmod{9} \rceil$$

$$a = 16 \cdot 1 \cdot \frac{303 \cdot 378 \cdot 423}{303} + 25 \cdot 1 \cdot \frac{303 \cdot 378 \cdot 423}{378} + 13 \cdot 1 \cdot \frac{303 \cdot 378 \cdot 423}{423}$$

$$a = 7251471$$

$$7251471 \equiv x \pmod{(303 \cdot 378 \cdot 423)}$$

$$7251471 \equiv x \pmod{48447882}$$

$$\frac{48447882}{7251471} = 6 \Rightarrow 48447882 - 43508826$$

$$\Rightarrow 4939056$$

$$7251471 \equiv 4939056 \pmod{48447882}$$

$$\lceil x = 4939056 + 48447882 m \rceil$$

Solución

4.13 Algoritmo para saber si a o b no son primos

```

public int primos (int a) {
    int c;
    int primo = 1 → 1 es primo - 0 no es primo
    while (c primo == 1 & c != a)
        if (a % c == 0)
            primo = 0;
        c++;
    return primo
}

```

4.14

$$\begin{array}{r}
 + 3,45 \quad ① \\
 1,20 \\
 \hline
 + 5,05 \quad ② \\
 1,20 \\
 \hline
 + 6,25 \quad ③ \\
 1,20 \\
 \hline
 + 7,45 \quad ④ \\
 1,20 \\
 \hline
 + 9,05 \quad ⑤ \\
 1,20 \\
 \hline
 + 10,25 \quad ⑥ \\
 1,20 \\
 \hline
 + 0,45 \quad ⑦ \\
 1,20 \\
 \hline
 + 2,05 \quad ⑧ \\
 1,20 \\
 \hline
 + 3,25 \quad ⑨ \\
 1,20 \\
 \hline
 + 4,45 \quad ⑩ \\
 1,20 \\
 \hline
 + 6,05 \quad ⑪ \\
 1,20 \\
 \hline
 + 7,25 \quad ⑫ \\
 1,20 \\
 \hline
 8,45
 \end{array}$$

$$\begin{array}{r}
 - 4,50 \quad ① \\
 0,45 \\
 \hline
 - 4,05 \quad ② \\
 0,45 \\
 \hline
 - 3,20 \quad ③ \\
 0,45 \\
 \hline
 - 2,35 \quad ④ \\
 0,45 \\
 \hline
 - 1,10 \quad ⑤ \\
 0,45 \\
 \hline
 - 0,05 \quad ⑥ \\
 0,45 \\
 \hline
 - 11,40 \quad ⑦ \\
 0,45 \\
 \hline
 - 10,55 \quad ⑧ \\
 0,45 \\
 \hline
 - 9,10 \quad ⑨ \\
 0,45 \\
 \hline
 - 8,25 \quad ⑩ \\
 0,45 \\
 \hline
 - 7,40 \quad ⑪ \\
 0,45 \\
 \hline
 8,45
 \end{array}$$

4.15

se utiliza la subrutina $w_1 + m_1 w_2 + \dots + m_k w_k \mod m$
 $m_{j-1} \times w_j \equiv q_j \pmod{m_j}$ para ver que w_i es un módulo
único de m_i y para que se satisfaga la congruencia.

la respuesta principal se debe a que hay que cumplir
con el teorema del Residuo Chino, para lo cual, en cada
quier sistema de congruencias en aritmética modular,
se necesita para cada congruencia un S_i que
cumpla la condición del Teorema de Bézout

$$\left\{ \exists S_i \in \mathbb{Z}, \text{ si } \frac{a}{n_i} \equiv 1 \pmod{c_i} \right\}$$

y así cumplir la sumatoria $a = \sum_{i=1}^k b_i S_i n_i \equiv x \pmod{n}$

recordando que deben ser números coprimos.

4.16

$$w_1 \times m_1 + w_2 \times m_2 + \dots + w_k \times m_k \times \dots \times m_r \times w_r$$

$$a \equiv c_i \pmod{m_i}$$

porque $w_j \equiv q_j \pmod{m_j}$ en el algoritmo

y luego

$$w_j = [(w_j - w_i) \times c_{ij}] \pmod{m}$$

$\underbrace{a =}_{c_i} \quad \underbrace{\qquad \qquad \qquad}_{\text{mod } m}$

4.17

$$\phi(p^a) = p^{a-1} \times (p-1)$$

↓

Siendo p prima wantos n cumple

$$n = p_1^{a_1} \times p_2^{a_2} \times \dots \times p_r^{a_r}$$

$$\phi(n) = p_1^{a_1-1} \times (p_1-1) \times p_2^{a_2-1} \times (p_2-1) \times \dots \times p_r^{a_r-1} \times (p_r-1)$$

$$\phi(n) = n \times \left(1 - \frac{1}{p_1}\right) \times \left(1 - \frac{1}{p_2}\right) \times \dots \times \left(1 - \frac{1}{p_r}\right)$$

4.18

$$\phi(m \times n) = \phi(m) \times \phi(n)$$

Si los números m & n son primos entre sí entonces deben ser primos relativos

4.19

Utilizo el Algoritmo 4.7 - División Trial para encontrar

$$\text{Alg 4.7: } \phi(n) = (p-1)(q-1)$$

$$\rightarrow 51\ 005 \\ p = 505$$

$$\phi(n) = 504\ 000 \\ q = 101$$

$$\rightarrow 107\ 653 \\ p = 49$$

$$\phi(n) = 105\ 408 \\ q = 2197$$

$$\rightarrow 1294704 \\ p = 432$$

$$\phi(n) = 1291776 \\ q = 2997$$

$$\rightarrow 1494108 \\ p = 252$$

$$\phi(n) = 1487928 \\ q = 5929$$

$$\rightarrow 614739125 \\ p = 125125$$

$$\phi(n) = 614609088 \\ q = 4913$$

Freddy I. Abad L.

freddy.abad@ucuenca.edu.ec