8.11
Método RSA paso a paso

1) Paso previo

- Elegimos 2 primos p y q que mantenemos en secreto (los que yo quiera)
  - Ej.
    - $p = 7$
    - $q = 11$
- Calculamos el valor de su producto al que denominamos $n = p \cdot q$
  - Ej.
    - $n = p \cdot q = 7 \cdot 11 = 77$

Paréntesis: Cálculo del máximo común divisor (Método 1)

Método 1:

- Escribimos todos los divisores de cada número, y de éstos señalamos los divisores comunes.
- El divisor mayor será el MCD de esos números.

- Ej. $mcd(15, 20\ )$
- **Divisores de 15**:
  - 15 / 1 = 15, y resto 0 por lo que **1 y 15 son divisores de 15**.
  - 15 / 2 = 7, el resto es 1, por lo que 2 no es divisor de 15.
  - 15 / 3 = 5, y resto 0 por lo que **3 es divisor de 15**.
  - 15 / 4 = 3, el resto es 3, por lo que 4 no es divisor de 15.
  - 15 / 5 = 3, y resto 0 por lo que **5 es divisor de 15**.

Por tanto, los divisores de 15 son: **1, 3, 5 y 15**.

- **Divisores de 20**:
  - 20 / 1 = 20, y resto 0 por lo que **1 y 20 son divisores de 20**.
  - 20 / 2 = 10, y resto 0 por lo que **2 y 10 son divisores de 20**.
  - 20 / 3 = 6, el resto es 2, por lo que 3 no es un divisor de 20.
  - 20 / 4 = 5, y resto 0 por lo que **4 y 5 son divisores de 20**.

Ahora deberíamos dividir entre 5 pero como ya lo tenemos como divisor, ya hemos acabado de calcular los divisores de 20.

- Es decir, los divisores de 20 son: **1, 2, 4, 5, 10 y 20**.

Paréntesis: Cálculo del máximo común divisor

- **Divisor común:** número que es divisor a la vez de dos o más números, es decir, es un divisor común a esos números.
  - En el ejemplo,
    - Divisores de 15: **1, 3, 5 y 15**.
    - Divisores de 20: **1, 2, 4, 5, 10 y 20**.

Los **divisores comunes que tienen 15 y 20 son el 1 y el 5.**

- Máximo común divisor es el número mayor entre los divisores comunes,
  - En el ejemplo
    - Divisores comunes de 15 y 20: **1 y 5**
  - Por tanto,

$$mcd(15, 20) = 5$$

Paréntesis: Cálculo del máximo común divisor (Método 2)

- Descomposición de factores o descomposición en números primos.
  - Descomponemos cada número en factores primos.
  - Después, señalamos los factores comunes.
  - A continuación, en cada uno de los comunes, escogemos el factor con menor exponente.
  - Y por ultimo, multiplicamos los factores elegidos.
- Ejemplo:

$$mcd(8, 12) = 4$$

$$\begin{array}{r|l} 8 & 2 \\ 4 & 2 \\ 2 & 2 \\ 1 & \end{array} \qquad \begin{array}{r|l} 12 & 2 \\ 6 & 2 \\ 3 & 3 \\ 1 & \end{array}$$

$$8 = 2^3 \qquad 12 = 2^2 \cdot 3$$

1) Paso previo

- Escogemos un número e que sea primo relativo de $(p-1)(q-1)$, es decir,

$$mcd\big(e,(p-1)(q-1)\big)=1$$

  - Ej.
    - $mcd\big(e,(p-1)(q-1)\big)=1 \Rightarrow$

$$\Rightarrow mcd\big(e,(7-1)(11-1)\big)=$$
$$mcd\big(e,(6)(10)\big)=$$
$$mcd\big(e,(2\cdot 3)(2\cdot 5)\big)=1$$

Luego debo escoger e no puede ser divisible por 2, 3 y 5 por ejemplo $e=13$

1) Paso previo

- Hallamos el inverso multiplicativo de $e\ \left(mod\ \left((p-1)(q-1)\right)\right)$, es decir, $e^{-1}\left(mod\ \left((p-1)(q-1)\right)\right)$ al que denominaremos d

$$d = e^{-1}\ \left(mod\ \left((p-1)(q-1)\right)\right)$$

Ej.

$$\begin{aligned} d &= e^{-1}\ \left(mod\ \left((p-1)(q-1)\right)\right) \\ &= e^{-1}\ \left(mod\ \left((7-1)(11-1)\right)\right) \\ &= e^{-1}\ \left(mod\ \left((6)(10)\right)\right) \\ &= e^{-1}\left(mod\ (60)\right) \end{aligned}$$

1) Paso previo: Cálculo de e^{-1}

- Inverso multiplicativo de e: $e \cdot e^{-1} \equiv 1 \left(mod\ ((p-1)(q-1)) \right)$
- Métodos:
  - 1) Fermat:
    - ¿ $(p-1)(q-1)$ primo?,
    - ¿ $e \neq múltiplo\ de\ (p-1)(q-1)$?
    - Si se cumple, $e^{-1} = e^{\left((p-1)(q-1)\right)-2}$

    En el ejemplo,

    - ¿$(p-1)(q-1)$primo?, $(7-1)(11-1) = 60 \neq primo$
    - ¿ $e \neq múltiplo\ de\ (p-1)(q-1)$?, ¿$13 \neq múltiplo\ de\ 60$?

1) Paso previo: Cálculo de e^{-1}

- Inverso multiplicativo de e: $e \cdot e^{-1} \equiv 1\left(mod\ ((p-1)(q-1))\right)$
- Métodos:
  - 2) Euler:
    - $¿mcd\big(e,(p-1)(q-1)\big) = 1?$, es decir, ¿ e y $(p-1)(q-1)$ son primos relativos ?

    OBSERVACIÓN: El requisito para que exista inverso multiplicativo es el mismo que para poder aplicar el método de Euler

    En el ejemplo,
    - $¿mcd\big(e,(p-1)(q-1)\big) = 1?$, $¿mcd(13, 60\ ) = 1?$,

Luego podemos calcular el inverso multiplicativo por Euler:

1. Calcular la función indicatriz:

$$\phi\big((p-1)(q-1)\big) = (p-1)(q-1)\prod_{s\epsilon primo}^{j}\left(1-\frac{1}{s_j}\right)$$

2. Inverso multiplicativo:

$$e^{-1} = \overset{d}{\boxed{e^{\phi((p-1)(q-1))-1}}}\left(mod\ ((p-1)(q-1))\right)$$

1) Paso previo: Cálculo de e^{-1}

- Inverso multiplicativo de e: $e \cdot e^{-1} \equiv 1 \left(mod\ \left((p-1)(q-1) \right) \right)$

Luego podemos calcular el inverso multiplicativo por Euler:

1. Calcular la función indicatriz:

$$\phi\left((p-1)(q-1)\right) = (p-1)(q-1) \prod_{s \in primo}^{j} \left(1 - \frac{1}{s_j}\right)$$

En el ejemplo,

$$(7-1)(11-1) = (6)(10) = 60$$

Factores primos de 60:

60	2
30	2
15	3
5	5
1	

$$60 = 2^2 \cdot 3 \cdot 5$$

1) Paso previo: Cálculo de e^{-1}

- Inverso multiplicativo de e: $e \cdot e^{-1} \equiv 1 \left(mod\ \left((p-1)(q-1)\right)\right)$
    1. (Continuación) Calcular la función indicatriz del ejemplo:

$$\phi\left((p-1)(q-1)\right) = (p-1)(q-1)\prod_{s \in primo}^{j}\left(1-\frac{1}{s_j}\right)$$

$$(7-1)(11-1) = (6)(10) = 60$$

Factores primos de 60 $=2^2 \cdot 3 \cdot 5$

$$\phi(60) = 60\left[1-\frac{1}{2}\right]\left[1-\frac{1}{3}\right]\left[1-\frac{1}{5}\right]$$

$$= 60\left[\frac{1}{2}\right]\left[\frac{2}{3}\right]\left[\frac{4}{5}\right] = 16$$

    2. Inverso multiplicativo:

$$e^{-1} = \underbrace{\boxed{e^{\phi\left((p-1)(q-1)\right)-1}}}_{}^{d} \left(mod\ \left((p-1)(q-1)\right)\right)$$

1) Paso previo: Cálculo de e^{-1}

- Inverso multiplicativo de e: $e \cdot e^{-1} \equiv 1 \left(mod\ \left((p-1)(q-1)\right)\right)$
  2. Inverso multiplicativo:

$$e^{-1} = \overbrace{\boxed{e^{\phi\left((p-1)(q-1)\right)-1}}}^{d} \left(mod\ \left((p-1)(q-1)\right)\right)$$

En el ejemplo,

$$13^{-1} = \overbrace{\boxed{13^{\phi(60)-1}}}^{d}\left(mod\ (60)\right)$$

$$13^{-1} = 13^{16-1}\left(mod\ (60)\right)$$

$$13^{-1} = 13^{15}\left(mod\ (60)\right)$$

Luego debemos calcular $13^{15}\left(mod\ (60)\right)$ mediante el método de las potencias de 2.

1) Paso previo: Cálculo de e^{-1}

- Inverso multiplicativo de e: $e \cdot e^{-1} \equiv 1 \left(mod\left((p-1)(q-1)\right)\right)$

  2. Inverso multiplicativo:

  Luego debemos calcular $13^{15}(mod\ (60))$ mediante el método de las potencias de 2.

    Descomponemos el exponente, 15, en potencias de 2:

$$8 = 2^3$$
$$4 = 2^2$$
$$2 = 2^1$$
$$1 = 2^0$$

    luego

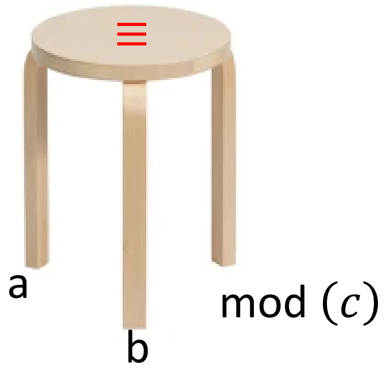
$$13^{15} = 13^8 \cdot 13^4 \cdot 13^2 \cdot 13^1$$

$=$ operación "normal Ej. $2 \cdot 2 = 4$

$a \equiv b\ (mod(c)) \Longrightarrow$

$\Longrightarrow$ cálculo de restos: $res(a, c) = b$

1) Paso previo: Cálculo de e^{-1}



- Inverso multiplicativo de e: $e \cdot e^{-1} \equiv 1\ \left(mod\ ((p-1)(q-1))\right)$

  2. Inverso multiplicativo:

$$13^{15} = 13^8 \cdot 13^4 \cdot 13^2 \cdot 13^1$$

Operamos utilizando la aritmética modular,

$$13^2 = 169 \equiv 49\ (mod\ (60))$$

169 | 60

49   2

luego 49 es el resto (169 % 60)

$$13^4 = (13^2)^2 \equiv 49^2 = 2401 \equiv 1\ (mod\ (60))$$

(2401 % 60 = 1)

$$13^8 = (13^4)^2 \equiv 1^2 = 1\ (mod\ (60))$$

$$13^{15} \equiv 1 \cdot 1 \cdot 49 \cdot 13 = 637 \equiv 37 (mod\ (60))$$

(637 % 60 = 1)

Por tanto,

$$d = 37$$

1) Paso previo: Claves pública y privada

El final de este paso viene dado por la definición de las claves pública y privada con los elementos calculados anteriormente:

- CLAVE PÚBLICA: (e, n)
- CLAVE PRIVADA: (d, n)

Sistema de cifrado asimétrico

En el ejemplo,

- CLAVE PÚBLICA: $(13,77)$
- CLAVE PRIVADA: $(37,77)$

2) Cifrado

- Para cifrar un mensaje m, lo elegimos tal que

$$mcd(m, n) = 1$$

m y n son primos relativos

Entonces,

$$m' = res(m^e, n)$$

Ej. Para el ejemplo vamos a suponer que hemos capturado 4 mensajes cifrados por lo que no vamos a tener que descifrarlos (podría haberos pedido el cifrado)

$$m'_1 = 37$$
$$m'_2 = 26$$
$$m'_3 = 37$$
$$m'_4 = 26$$

3) Descifrado

- Para descifrar el mensaje debemos aplicar

$$m = res\left(m'^{d}, n\right) = m_1'^{d}\left(mod\ (n)\right)$$

Para el ejemplo,

$$m_1 = m_3 = 37^{37}\left(mod\ (77)\right)$$
$$m_2 = m_4 = 26^{37}\left(mod\ (77)\right)$$

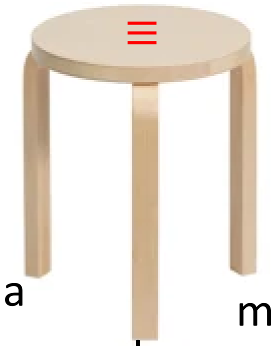
Luego de nuevo debemos de aplicar la aritmética modular para

3) Descifrado (continuación ejemplo)

= operación "normal Ej. $2 \cdot 2 = 4$

$a \equiv b\ (mod(c)) \Longrightarrow$

$\Longrightarrow$ cálculo de restos: $res(a, c) = b$



a

mod (c)

b

- $m_1 = m_3 = 37^{37}(mod\ (77))$
  - Descomponemos el exponente, 37, en potencias de 2:

$$32 = 2^5$$
$$4 = 2^2$$
$$1 = 2^0$$

luego

$$37^{37} = 37^{32} \cdot 37^4 \cdot 37^1$$

Operando con la aritmética modular,

$$37^2 = 1369 \equiv 60\ (mod\ (77))$$ (1369 % 77 = 60)

$$37^4 = (37^2)^2 \equiv 60^2 = 3600 \equiv 58\ (mod\ (77))$$ (3600 % 77 = 58)

$$37^8 = (37^4)^2 \equiv 58^2 = 3364 \equiv 53\ (mod\ (77))$$ (3364 % 77 = 53)

$$37^{16} = (37^8)^2 \equiv 53^2 = 2809 \equiv 37\ (mod\ (77))$$ (2809 % 77 = 37)

$$37^{32} = (37^{16})^2 \equiv 37^2 \equiv 60\ (mod\ (77))$$

$$37^{37} \equiv 60 \cdot 58 \cdot 37 = 128760 \equiv 16\ (mod\ (77))$$ (128760 % 77 = 16)

Teniendo en cuenta el abecedario, $m_1 = m_3 = 16 \Longrightarrow P$

3) Descifrado (continuación ejemplo)

- $m_2 = m_4 = 26^{37}\left(mod\ (77)\right)$
  - Descomponemos el exponente, 37, en potencias de 2:

$$32 = 2^5$$
$$4 = 2^2$$
$$1 = 2^0$$

luego

$$26^{37} = 26^{32} \cdot 26^4 \cdot 26^1$$

Operando con la aritmética modular,

$$26^2 = 676 \equiv 60\ \left(mod\ (77)\right)$$
$$26^4 = (26^2)^2 \equiv 60^2 = 3600 \equiv 58\ \left(mod\ (77)\right)$$
$$26^8 = (26^4)^2 \equiv 58^2 = 3364 \equiv 53\ \left(mod\ (77)\right)$$
$$26^{16} = (26^8)^2 \equiv 53^2 = 2809 \equiv 37\ \left(mod\ (77)\right)$$
$$26^{32} = (26^{16})^2 \equiv 37^2 \equiv 60\ \left(mod\ (77)\right)$$
$$26^{37} \equiv 60 \cdot 58 \cdot 26 = 90480 \equiv 5\ \left(mod\ (77)\right)$$

Teniendo en cuenta el abecedario, $m_1 = m_3 = 5 \Longrightarrow E$
y el mensaje total es $m_1 m_2 m_3 m_4 = PEPE$

Resumen

1. **Paso previo**
   1. Elegimos 2 primos p y q que mantenemos en secreto (los que yo quiera)
   2. Escogemos un número e que sea primo relativo de $(p-1)(q-1)$, es decir,

$$mcd\big(e,(p-1)(q-1)\big) = 1$$

3. Hallamos el inverso multiplicativo de e $\Big(mod\ \big((p-1)(q-1)\big)\Big)$, es decir, e^{-1} $\Big(mod\ \big((p-1)(q-1)\big)\Big)$ al que denominaremos d

- CLAVE PÚBLICA: (e,n)
- CLAVE PRIVADA: (d,n)

2. **Cifrado:**

- Para cifrar un mensaje m, lo elegimos tal que

$$mcd(m,n) = 1$$

$$m' = res(m^e, n)$$

3. **Descifrado:**

- Para descifrar el mensaje debemos aplicar

$$m = res\big(m'^d, n\big) = m_1'^d\big(mod\ (n)\big)$$