

# RSA y Teorema del Resto Chino

# Método de Quisquater-Couvreur

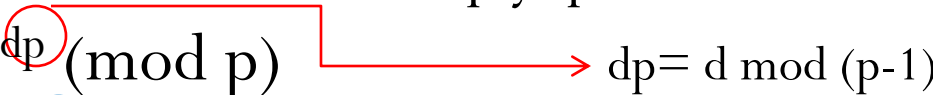
- Calcular el Descifrado aplicando el teorema del resto chino
- Objetivo:
  - Reducir el exponente particular  $d$  módulo  $p-1$ ,  $q-1$
  - Método 4 veces más rápido que la exponenciación rápida.

# Descifrado RSA


- Se aplica solo al descifrado, porque se conoce los valores de  $p$  y  $q$
- Pasos:
  - De la ecuación del descifrado

$$M_i = C_i^d \pmod{n}$$

- Descomponerla en función de  $p$  y  $q$

$$Dp_i \equiv C_i^{dp} \pmod{p}$$


$dp = d \pmod{p-1}$

$$Dp_q \equiv C_i^{dq} \pmod{q}$$


$dq = d \pmod{q-1}$

- Operar ambas funciones aplicando el teorema del resto chino

# Ejemplo: RSA

- Generación de claves:

$$p = 11; \quad q = 13 \quad e=7$$

$$N = p \times q = 143$$

$$\Phi N = (p-1)(q-1) = (10)(12) = 120$$

$$d = e^{-1} \pmod{\Phi N} = 103$$

**Clave pública  $\langle N, e \rangle = \langle 143, 7 \rangle$**

**Clave privada  $\langle N, d \rangle = \langle 143, 103 \rangle$**

# Ejemplo: RSA

- Cifrado del mensaje:
- $M = 15$

$$C = M^e \pmod{N}$$

$$C = 15^7 \pmod{143}$$

$$\mathbf{C = 115}$$

# Ejemplo: RSA

- Descifrado del mensaje:

$$D = C^d \pmod{N}$$

$$D = 115^{103} \pmod{143} \quad (\text{descomponer en funci3n de } p \text{ y } q)$$

$$D_p \equiv 115^3 \pmod{11} \quad \xrightarrow{\text{red}} \quad 3 = 103 \pmod{11-1}$$

$$D_q \equiv 115^7 \pmod{13} \quad \xrightarrow{\text{blue}} \quad 7 = 103 \pmod{13-1}$$

# Ejemplo: RSA – Teorema del Resto Chino

- Sistema de ecuaciones para el Teorema del Resto Chino:

$$D \equiv 115^3 \pmod{11} \qquad a = 5^3 \text{ en } \pmod{11} = 4$$

$$D \equiv 115^7 \pmod{13} \qquad a = 11^7 \text{ en } \pmod{13} = 2$$

- Pasos:

1.  $P = 11 \times 13 = 143$

2.  $P_1 = 143 / 11 = 13$

$$P_2 = 143 / 13 = 11$$

3.  $q_1 \times 13 \equiv 1 \pmod{11}$

$$q_2 \times 11 \equiv 1 \pmod{13}$$

$$q_1 = 6$$

$$q_2 = 6$$

# Ejemplo: RSA – Teorema del Resto Chino

4.  $D_0 \equiv [(115^3)(13)(6)] + [(115^7)(11)(6)] \pmod{143}$

$$D_0 \equiv 4 \times 78 + 2 \times 66 \pmod{143}$$

$$D_0 \equiv 26 + 132 \pmod{143}$$

$$D_0 \equiv 15 \pmod{143}$$

5.  $D = 15 + 143.k$  Para  $k=0$ ;

$$\mathbf{D = 15}$$



# Referencia

- <http://www.ime.usp.br/~capaixao/Qualificacao.pdf>

# Protocolos Criptográficos

# Concepto

- Algoritmos y métodos criptográficos utilizados por un conjunto de participantes con una meta común e implementarlos en entornos distribuidos inseguros.
- Definen la interacción entre las partes:
  - Todos deben conocer los pasos del protocolo de antemano.
  - Todos deben estar de acuerdo en seguir el protocolo.
  - El protocolo no admite ambigüedades.
  - El protocolo debe ser completo – define que hacer en cualquier circunstancia posible.
  - No debe ser posible hacer más que lo que el protocolo define

# Tipos

- Protocolos de autenticación de usuario
- **Protocolos de autenticación de mensaje: firma digital**
- **Distribución de claves:** Diffie-Hellman, El Gamal, X.509
- Protocolos para compartir secretos.
- **Pruebas del conocimiento cero RSA**
- Transacciones electrónicas seguras
- Compromiso de bit
- Elecciones electrónicas
- **Jugar al poker por Internet con RSA**
- **Protocolo de Firma Ciega RSA (Chaum).**

# Firma Digital

- Sirve para que el destinatario se asegure de que el mensaje que recibe ha sido enviado de verdad por quién dice ser el remitente.
- Confidencialidad
  - Para lograrla se cifra el mensaje
- Integridad
  - Para lograrla se firma el mensaje

# Protocolo de Firma Digital

- Se llama rúbrica  $r$  de un usuario  $A$  para un mensaje  $m$  al resultado de descifrar  $m$  como si fuera un mensaje cifrado que  $A$  recibe; esto es:
  - $r = m^{d_A} \bmod N_A$
- Se llama Firma Digital  $s$  de un usuario  $A$  para un mensaje  $m$  con destinatario  $B$ , al resultado de cifrar la rúbrica  $r$  de  $m$ ; esto es
  - $S = r^{e_B} \bmod N_B$

# Proceso del Protocolo de Firma Digital

## A envía un mensaje firmado m a B

- Tareas de A:

- A cifra el mensaje<sub>1</sub>:

$$c = m_1^{e_B} \bmod N_B$$

- A calcula la rúbrica del mensaje<sub>2</sub>

$$r = m_2^{d_A} \bmod N_A$$

- A calcula la firma digital del mensaje<sub>2</sub>

$$s = r^{e_B} \bmod N_B$$

- A envía a B el par (c,s)

# Proceso del Protocolo de Firma Digital

## A envía un mensaje firmado m a B

- Tareas de B:
  - B recupera el mensaje que envía A y debe verificar que la firma es correcta
  - B descifra el mensaje:
$$c_1 = c^{d_B} \bmod N_B$$
$$c_2 = s^{d_B} \bmod N_B$$
  - B calcula la rúbrica del A
$$c_r = c_2^{e_A} \bmod N_A$$
  - Comprueba que se verifica
$$m_2 = c_r$$
- A envía a B el par (c,s)



# Referencia

- Handbook of Applied Cryptography. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone (<http://www.cacr.math.uwaterloo.ca/hac/>)
- Protocolos y esquemas criptográficos
  - <http://www.securisite.org/biblioteca/FРАН/documentacion%20curso%20seg/1/Todo%20sobre%20los%20cifrados/19ProtocolosCriptoPDFc.pdf>
- Protocolos Criptográficos. Juan Tena Ayuso
- Autenticación y firma digital con criptosistemas asimétricos
  - <http://www.worktec.com.ar/consetic2005/consecricri/pdf/Consecricri%2025-09-01/Exposiciones/04%20-%20Autenticaci%F3n%20mediante%20sist%20asim%20E9tricos.pdf>