IIC3253

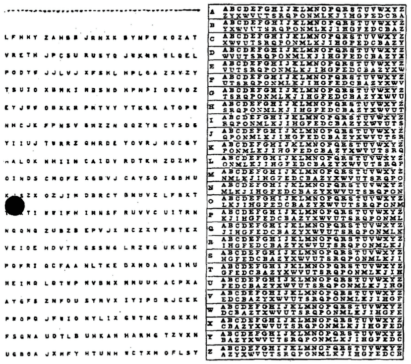
Criptografía asimétrica y RSA

Pero antes otro poco de historia

Julio César

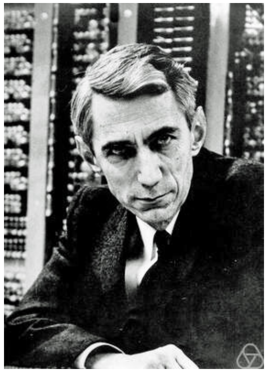
100 - 44 a.C.

OTP

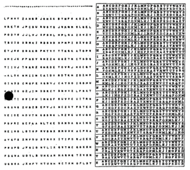


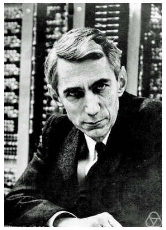
1882

Perfect secrecy



1945





100 - 44 a.C.

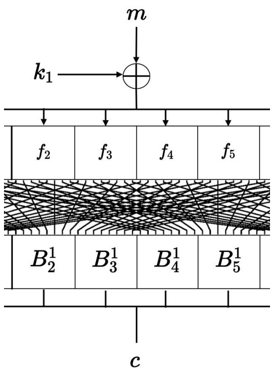
1882

1945

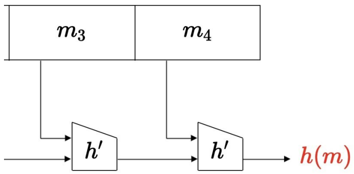
HMAC

$$HMac_k(m) = h(k_2 \mid\mid h(k_1 \mid\mid m))$$

AES



SHA-256



1996

2001

Dos problemas de la criptografía simétrica (o de clave privada)

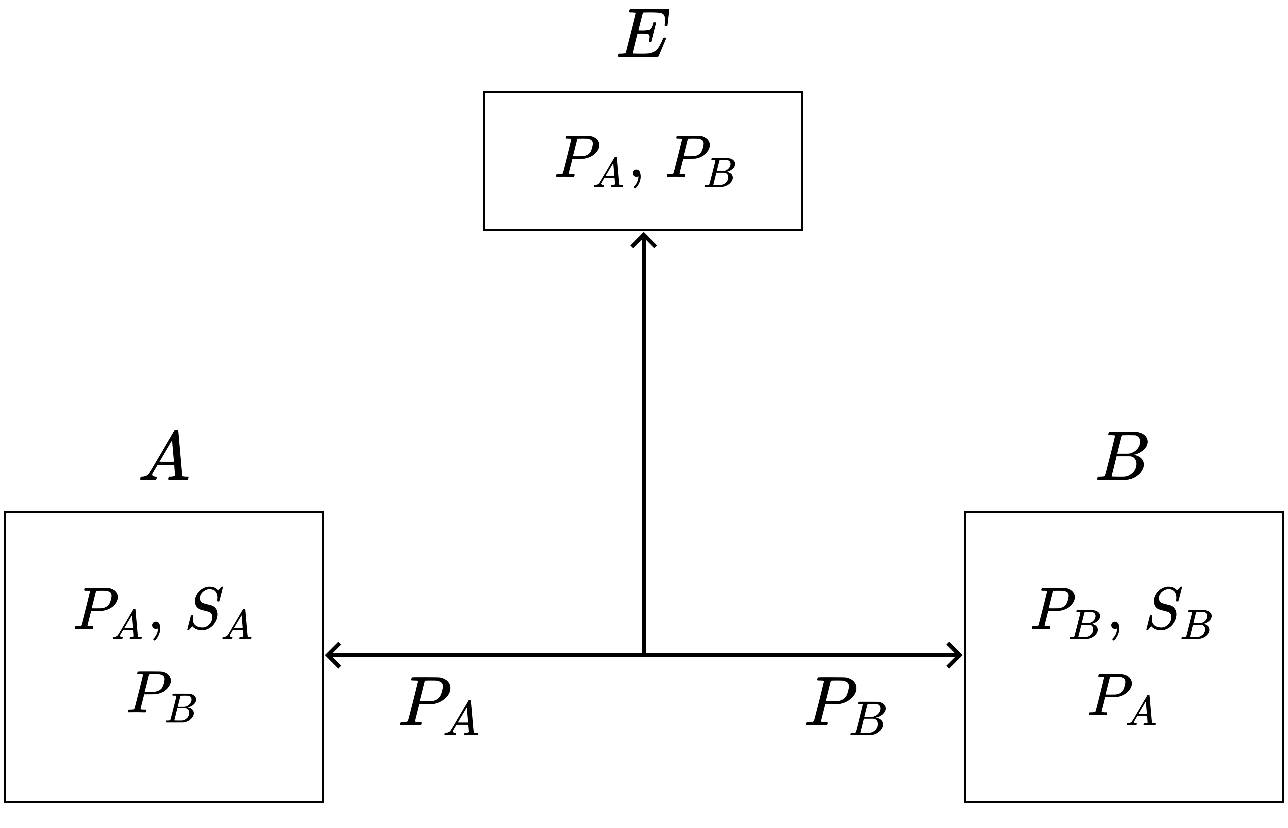
- El número de claves que un usuario debe almacenar es proporcional al número de sus contactos
- Dos usuarios **deben reunirse** para compartir una clave

Cifrado asimétrico resuelve estos problems

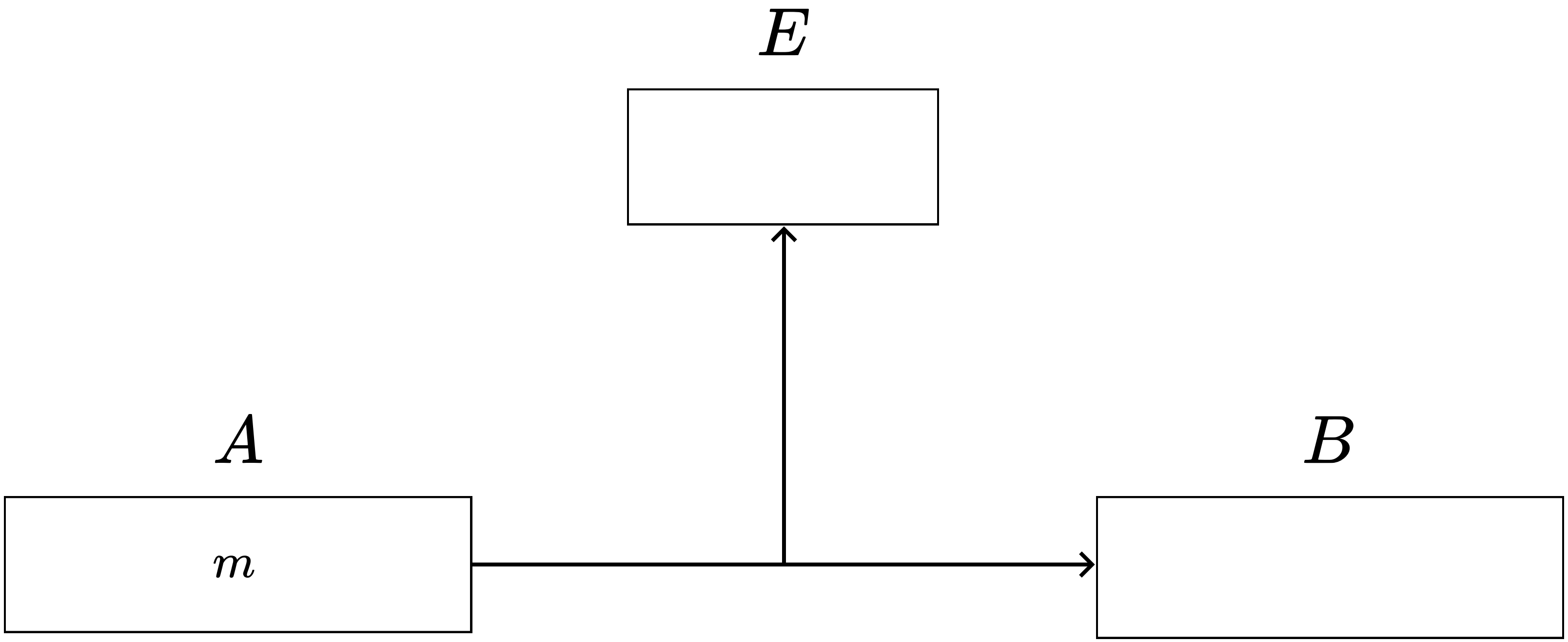
- Cada usuario A debe crear una clave pública P_A y una clave secreta S_A
- P_A y S_A están relacionadas: P_A se usa para cifrar y S_A para descifrar
- P_A es compartida con todos los otros usuarios

Esta forma de cifrado usualmente es llamada de clave pública

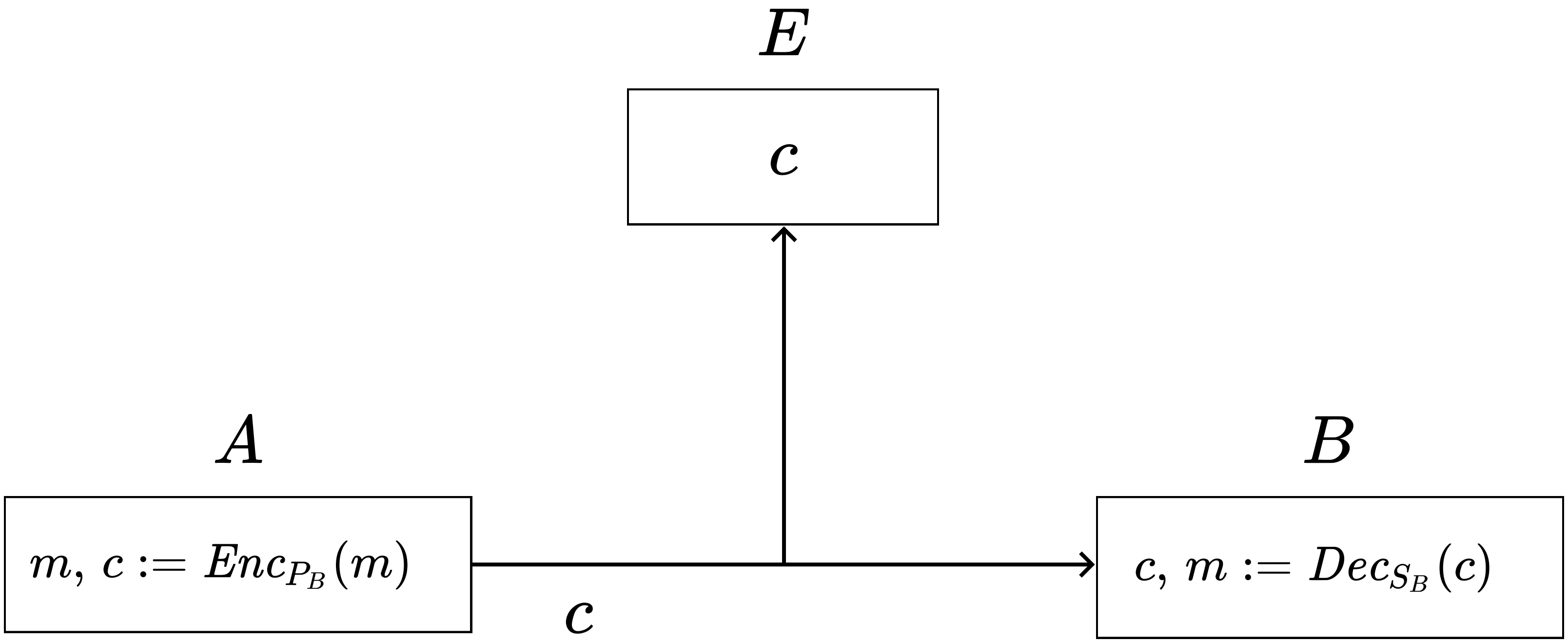
Escenario del cifrado asimétrico



Cifrado con una clave pública



Cifrado con una clave pública



Cifrado con una clave pública

- Enc y Dec son las familias de funciones de cifrado y descifrado
- Propiedad fundamental:

$$Dec_{S_B}(Enc_{P_B}(m)) = m$$

RSA: un protocolo criptográfico asimétrico

Las claves pública y privada de un usuario A son construidas de la siguiente forma:

1. Genere números primos distintos P y Q. Defina $N := P \cdot Q$
2. Defina $\phi(N) := (P-1) \cdot (Q-1)$
3. Genere un número d tal que $MCD(d, \phi(N)) = 1$
4. Construya un número e tal que
$$e \cdot d \equiv 1 \mod \phi(N)$$
5. Defina $S_A = (d, N)$ y $P_A = (e, N)$

RSA: funciones de cifrado y descifrado

Considere un usuario A con clave pública $P_A = (e, N)$ y clave secreta $S_A = (d, N)$

Se tiene que:

$$Enc_{P_A}(m) \;=\; m^e \bmod N$$

$$Dec_{S_A}(c) \;=\; c^d \bmod N$$

RSA: un ejemplo

1. Sean $P = 19$ y $Q = 31$. Tenemos que $N = 589$
2. $\phi(N) = \phi(589) = 18 \cdot 30 = 540$
3. Sea $d = 77$, para el cual se tiene $MCD(77, 540) = 1$
4. Calculamos inverso $e = 533$ de 77 en módulo 540:
$$533 \cdot 77 \mod 540 = 1$$
5. Clave pública: $P_A = (533, 589)$, y clave secreta: $S_A = (77, 589)$

RSA: un ejemplo

Tenemos que:

$$Enc_{P_A}(m) \;=\; m^{533} \mod 589$$

$$Dec_{S_A}(c) \;=\; c^{77} \mod 589$$

Para $m = 121$, tenemos que:

$$Enc_{P_A}(121) \;=\; 121^{533} \mod 589 \;=\; 144$$

$$Dec_{S_A}(144) \;=\; 144^{77} \mod 589 \;=\; 121$$

¿Por qué funciona RSA?

¿Cuáles son los espacios de mensajes, llaves y textos cifrados?

¿Es cierto que $Dec_{S_A}(Enc_{P_A}(m)) = m$?

¿Qué algoritmos de tiempo polinomial se debe tener para que se pueda ejecutar el protocolo?

¿De qué depende la seguridad de RSA? ¿Qué problemas no pueden ser resueltos en tiempo polinomial?

Espacios de mensajes, llaves y textos cifrados

Suponiendo que se genera el número N:

- Espacios de mensajes y textos cifrados: $\{0, \ldots, N-1\}$
- Espacios de llaves: $d, e \in \mathbb{N}$
  - Aunque en general se asume que $d, e \in \{0, \ldots, \phi(N)-1\}$

$$Dec_{S_A}(Enc_{P_A}(m)) = m$$

Para demostrar esto necesitamos un resultado fundamental

Pequeño teorema de Fermat: Si p es un número primo, entonces para cada $a \in \{1, ..., p-1\}$, se tiene que $a^{p-1} \bmod p = 1$

Un ejemplo del pequeño teorema de Fermat

Para $p = 7$:

$$1^6 \mod 7 = 1 \mod 7 = 1$$
$$2^6 \mod 7 = 64 \mod 7 = 1$$
$$3^6 \mod 7 = 729 \mod 7 = 1$$
$$4^6 \mod 7 = 4096 \mod 7 = 1$$
$$5^6 \mod 7 = 15625 \mod 7 = 1$$
$$6^6 \mod 7 = 46656 \mod 7 = 1$$

La correctitud de RSA

Sean $P_A = (e, N)$ y $S_A = (d, N)$ generados según el protocolo de RSA

Teorema: para cada $m \in \{0, ..., N-1\}$, se tiene que $Dec_{S_A}(Enc_{P_A}(m)) = m$

Demostración de la correctitud de RSA

Tenemos que:

- $N = P \cdot Q$, donde P y Q son números primos
- $e \cdot d = \alpha \cdot \phi(N) + 1$, dado que $e \cdot d \equiv 1 \mod \phi(N)$

Sea $m \in \{0, ..., N-1\}$

Demostración de la correctitud de RSA

Tenemos que:

$$\begin{aligned} Dec_{S_A}(Enc_{P_A}(m)) &= (m^e \bmod N)^d \bmod N \\ &= m^{e \cdot d} \bmod N \end{aligned}$$

Demostración de la correctitud de RSA

Entonces tenemos que demostrar que $m^{e \cdot d} \bmod N = m$.
Dado que $m \in \{0, \ldots, N-1\}$, esto es equivalente a:

$$m^{e \cdot d} \equiv m \mod N$$

Vamos a demostrar esto suponiendo primero que $MCD(m, N) = 1$

Demostración de la correctitud de RSA

Como $MCD(m, N) = 1$, se tiene que $MCD(m, P) = 1$

Por el pequeño teorema de Fermat:

$$m^{P-1} \equiv 1 \mod P$$

Por lo tanto:

$$(m^{P-1})^{Q-1} \equiv 1 \mod P$$

$$m^{\phi(N)} \equiv 1 \mod P$$

$$m^{\alpha \cdot \phi(N)} \equiv 1 \mod P$$

$$m^{\alpha \cdot \phi(N)+1} \equiv m \mod P$$

Demostración de la correctitud de RSA

Por lo tanto:

$$m^{e \cdot d} \equiv m \mod P$$

De la misma forma se concluye que:

$$m^{e \cdot d} \equiv m \mod Q$$

Tenemos entonces que:

$$m^{e \cdot d} - m = \beta \cdot P$$

$$m^{e \cdot d} - m = \gamma \cdot Q$$

Demostración de la correctitud de RSA

Como $\beta \cdot P = \gamma \cdot Q$, se tiene que P divide a $\gamma \cdot Q$

- Como P es primo, se tiene que P divide a γ o P divide a Q

Concluimos que P divide a γ dado que P y Q son números primos distintos

Por lo tanto: $\gamma = \delta \cdot P$

Demostración de la correctitud de RSA

Dado que $\gamma = \delta \cdot P$ y $m^{e \cdot d} - m = \gamma \cdot Q$, concluimos que $m^{e \cdot d} - m = \delta \cdot P \cdot Q$

Tenemos que $m^{e \cdot d} - m = \delta \cdot N$, y finalmente concluimos que:

$$m^{e \cdot d} \equiv m \mod N$$

Demostración de la correctitud de RSA

¿Qué hacemos con el caso $MCD(m, N) > 1$?

Demostración de la correctitud de RSA

¿Qué hacemos con el caso $MCD(m, N) > 1$?

Si $m = 0$, entonces concluimos trivialmente que $m^{e \cdot d} \equiv m \mod N$

Consideramos entonces dos casos:

- P divide a m pero Q no divide a m
- Q divide a m pero P no divide a m

Demostración de la correctitud de RSA

Si P divide a m y Q no divide a m, entonces:

- Concluimos que $m^{e \cdot d} \equiv m \mod P$ ya que $m \equiv 0 \mod P$
- Concluimos que $m^{e \cdot d} \equiv m \mod Q$ como en la demostración inicial, usando el hecho de $MCD(m, Q) = 1$

Concluimos que $m^{e \cdot d} \equiv m \mod N$ como en la demostración inicial

Demostración de la correctitud de RSA

Si Q divide a m y P no divide a m, concluimos que $m^{e \cdot d} \equiv m \mod N$ como en el caso anterior

Esto concluye la demostración del teorema 🙂