Examen
- Test.
- Problema.

Universidad
Carlos III de Madrid

*COSEC Lab· Dpto. Informática*

# TEMA 2. CRIPTOGRAFÍA
# T 2.5 **CIFRADORES ASIMÉTRICOS** Y DISTRIBUCIÓN DE CLAVES

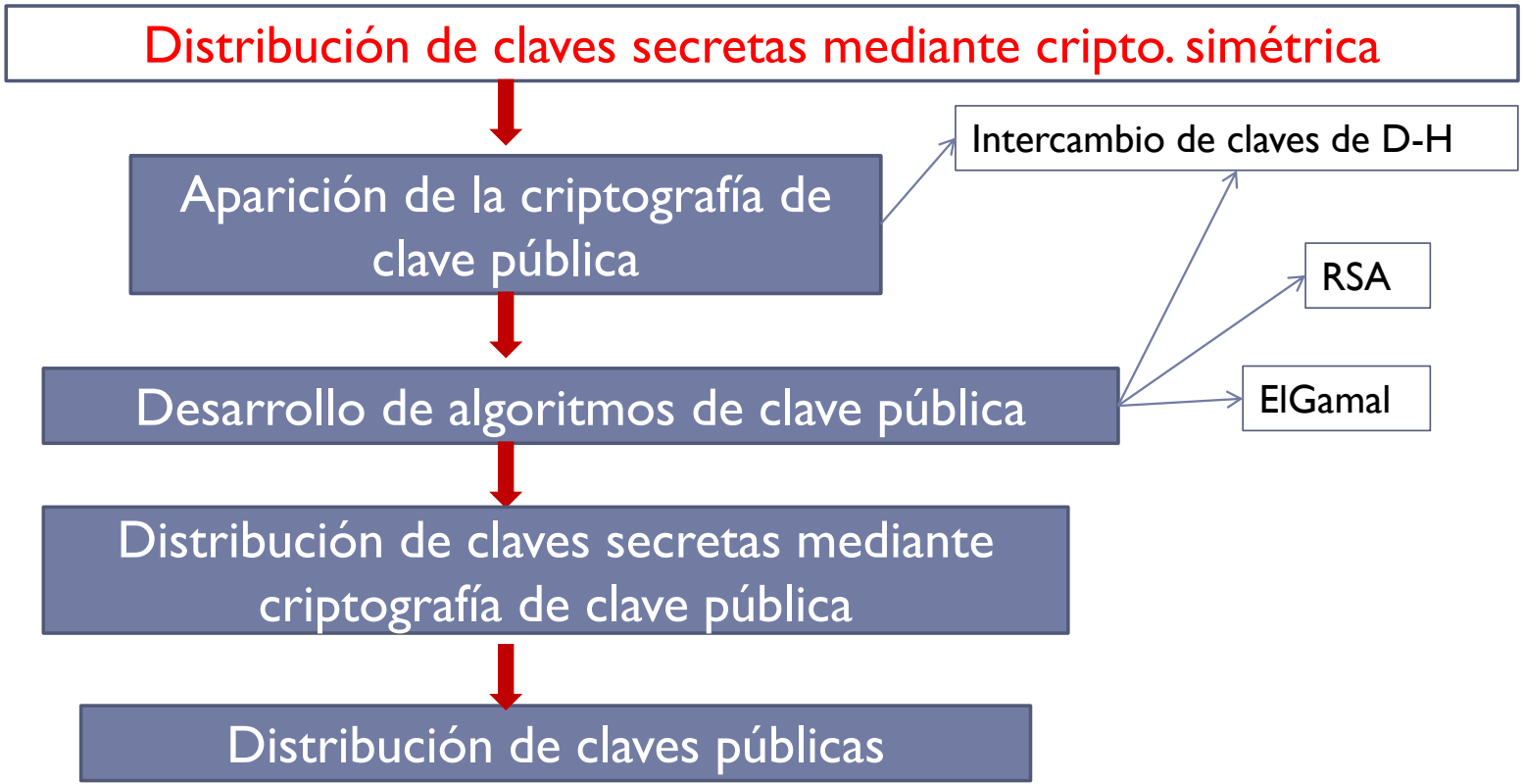
Criptografía y seguridad informática
Seguridad en las tecnologías de la información
@ COSEC

Curso 2016-2017

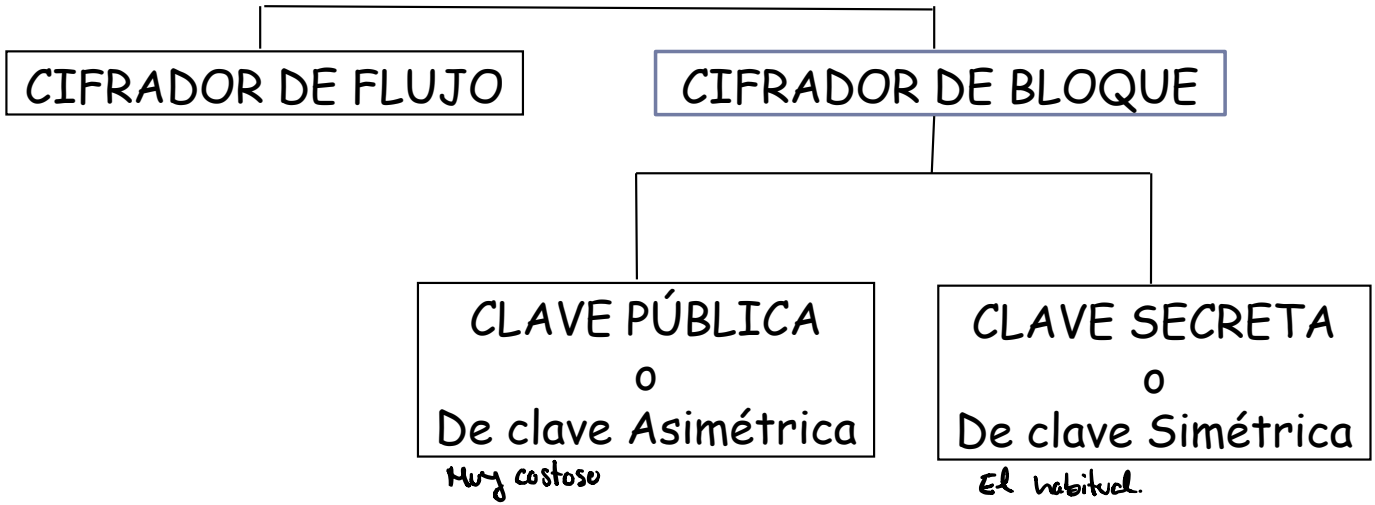
# Contenidos


Distribución de claves secretas mediante cripto. simétrica
Aparición de la criptografía de clave pública
Desarrollo de algoritmos de clave pública
Distribución de claves secretas mediante criptografía de clave pública
Distribución de claves públicas
Intercambio de claves de D-H
Protocolo de
Hibrida: la clave secreta se para cifrar de simetricamente y cuando la desciframos podemos descifrar la clave publica.
RSA
ElGamal
logaritmo inverso

# Contenidos

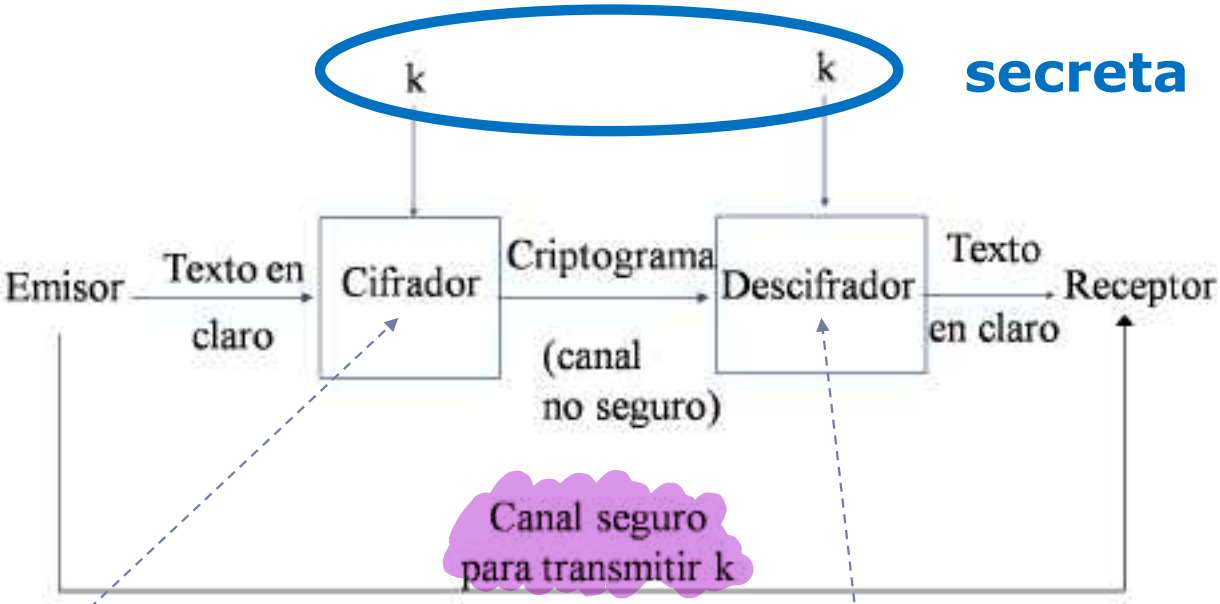

Distribución de claves secretas mediante cripto. simétrica
Aparición de la criptografía de clave pública
Intercambio de claves de D-H
RSA
ElGamal
Desarrollo de algoritmos de clave pública
Distribución de claves secretas mediante criptografía de clave pública
Distribución de claves públicas

# MÉTODOS DE CIFRA MODERNA



# MÉTODOS DE CIFRA MODERNA

Modelo de criptosistema de clave **simétrica**




$C = E(k, M) = E_k(M)$ $\qquad$ $M = D(k, C) = D_k(C)$

# Distribución de claves secretas mediante criptografía **simétrica**

- El esquema de cifrado simétrico requiere que emisor y receptor compartan una clave secreta
- ¿Como distribuirla de un modo seguro?
- A menudo los sistemas fallan por la distribución de claves y no por una debilidad del algoritmo de cifrado

# Distribución de claves secretas mediante criptografía **simétrica**

- Posibilidades:
  1. A genera la clave y se la entrega físicamente a B
  2. Una tercera parte puede elegir la clave y entregarla fisicamente a A y B
  3. Si A y B se han comunicado previamente pueden utilizar la clave anterior para cifrar la actual
  4. Si A y B tienen un enlace seguro con una tercera parte C, C puede generar y reenviar la clave a A y B

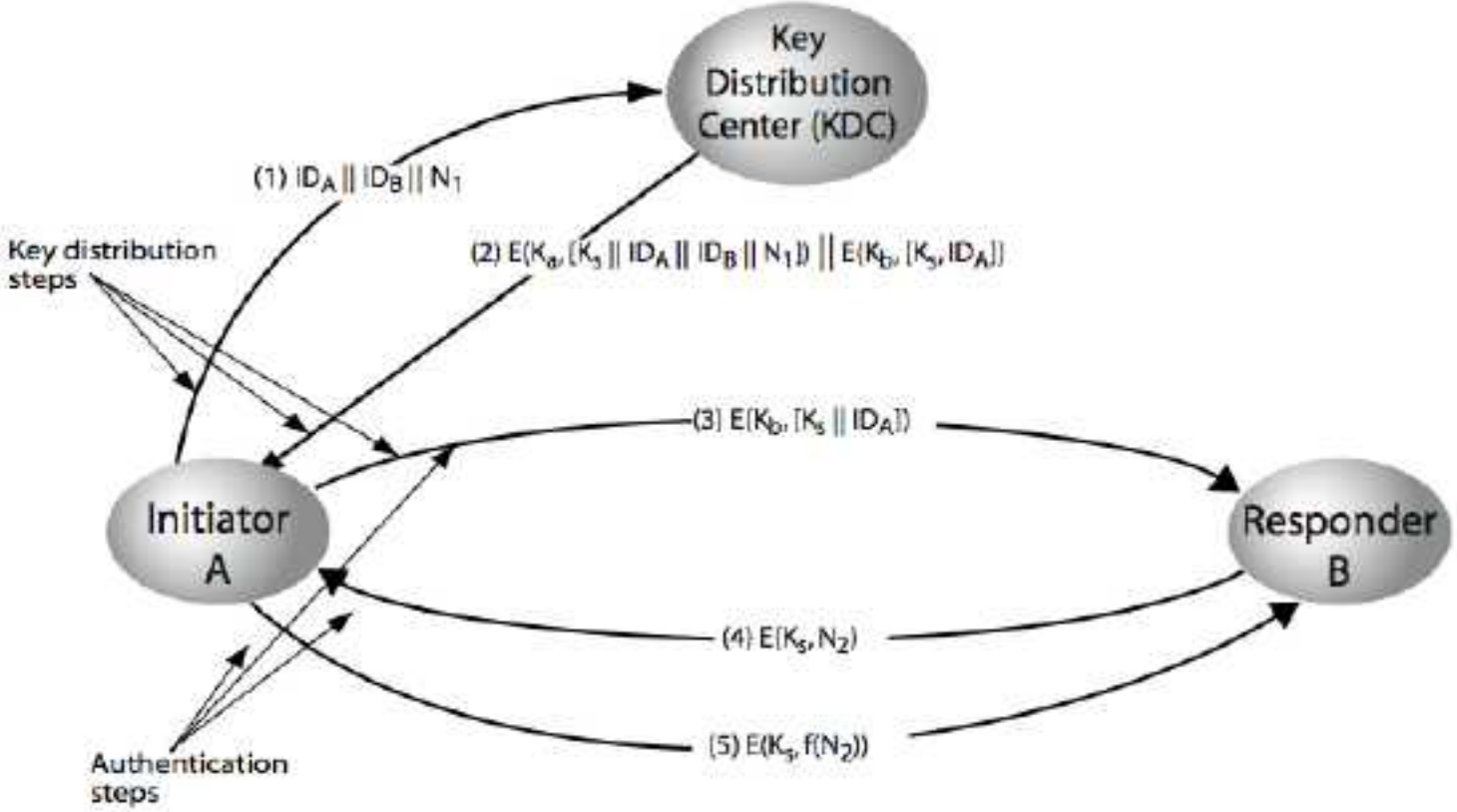
# Distribución de claves secretas mediante criptografía **simétrica**

- Jerarquía de claves con KDC (variante de la opción 4 de trasp. 5)

  Key Distribution Center.

  - Un KDC distribuye claves de session para cada par de usuarios
    - Claves temporales
    - Usadas para cifrar los datos entre participantes
    - Se utilizan para una sola sesión y se descartan
  - Cada usuario comparte una clave maestra con el KDC
    - Se usa para cifrar las claves de sesión
    - Se comparte entre el usuario y el centro de distribución de claves
  - Número para n participantes en un esquema descentralizado:
    - $n \cdot (n - 1)/2$ claves de session
    - n claves maestras

# Distribución de claves secretas mediante criptografía **simétrica**

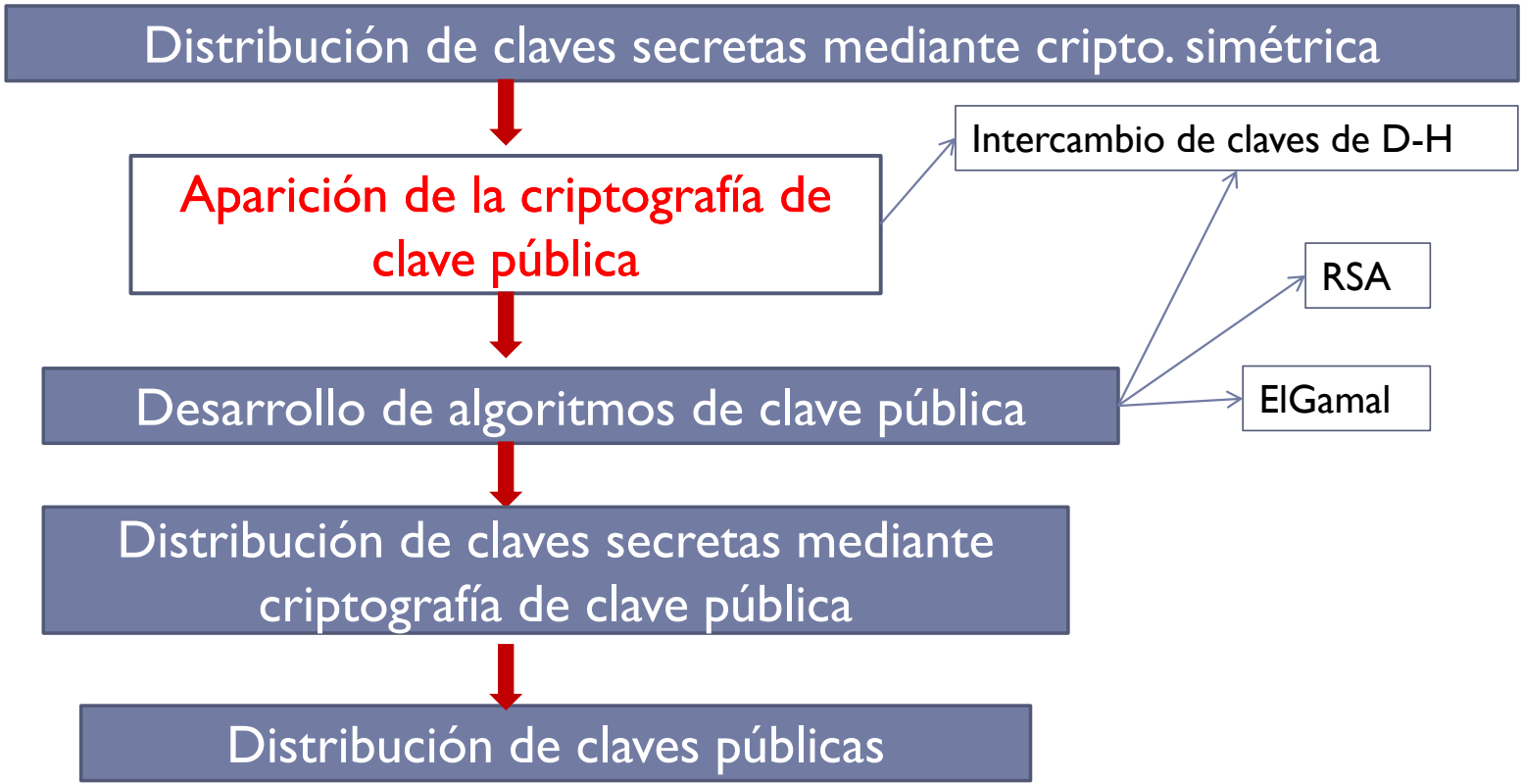



Stallings 06.CNS 4e

# Distribución de claves secretas mediante criptografía **simétrica**

- Jerarquías de KDC's para redes grandes
  - Confianza mutua
- Se debe limitar el tiempo de vida (criptoperiodo) de las claves de sesión
- Alternativa: protocolos descentralizados

# Contenidos


Distribución de claves secretas mediante cripto. simétrica
Aparición de la criptografía de clave pública
Intercambio de claves de D-H
RSA
ElGamal
Desarrollo de algoritmos de clave pública
Distribución de claves secretas mediante criptografía de clave pública
Distribución de claves públicas

# Aparición de la criptografía de clave pública (o **asimétrica**)

- Problema:
  - Dos personas, que **previamente no han intercambiado ningún secreto**, deben acordar una clave sobre un canal inseguro
  - Análogo a intercambiar secretos gritando de un extremo a otro en un mercado plagado de espías
  - Durante más de 3.000 años se pensó que no tenía solución

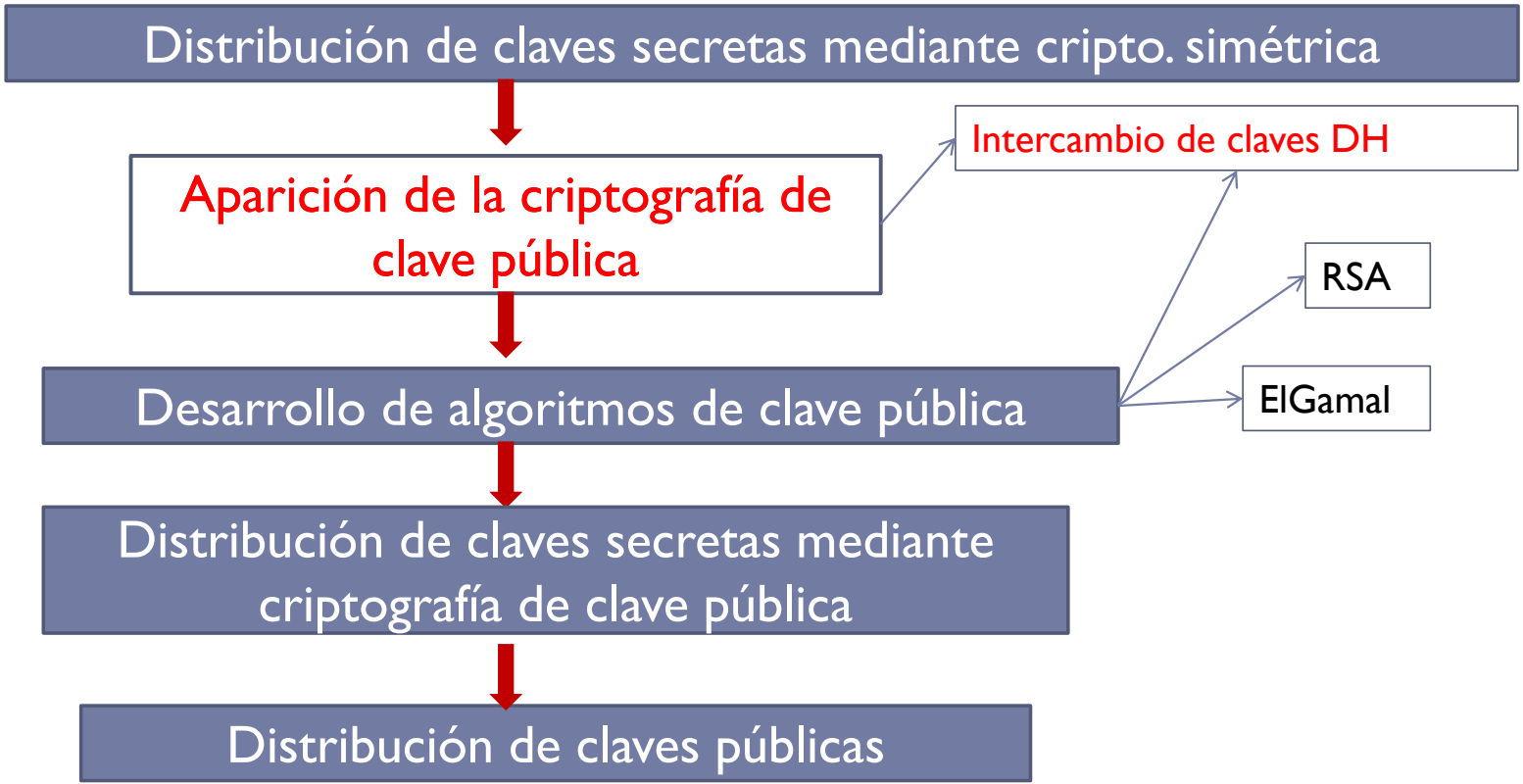
# Aparición de la criptografía de clave pública (o **asimétrica**)

- ***New Directions in Cryptography***
  - Artículo revolucionario que creó la criptografía de clave pública
  - Probablemente es el mayor hito criptográfico en 3000 años
  - Whitfield Diffie, Martin E. Hellman
  - IEEE Transactions in Information Theory
  - v. IT-22, pp 664-654. Noviembre de 1976
  - Descubierto anteriormente por los servicios de inteligencia británicos

# Aparición de la criptografía de clave pública (o **asimétrica**)

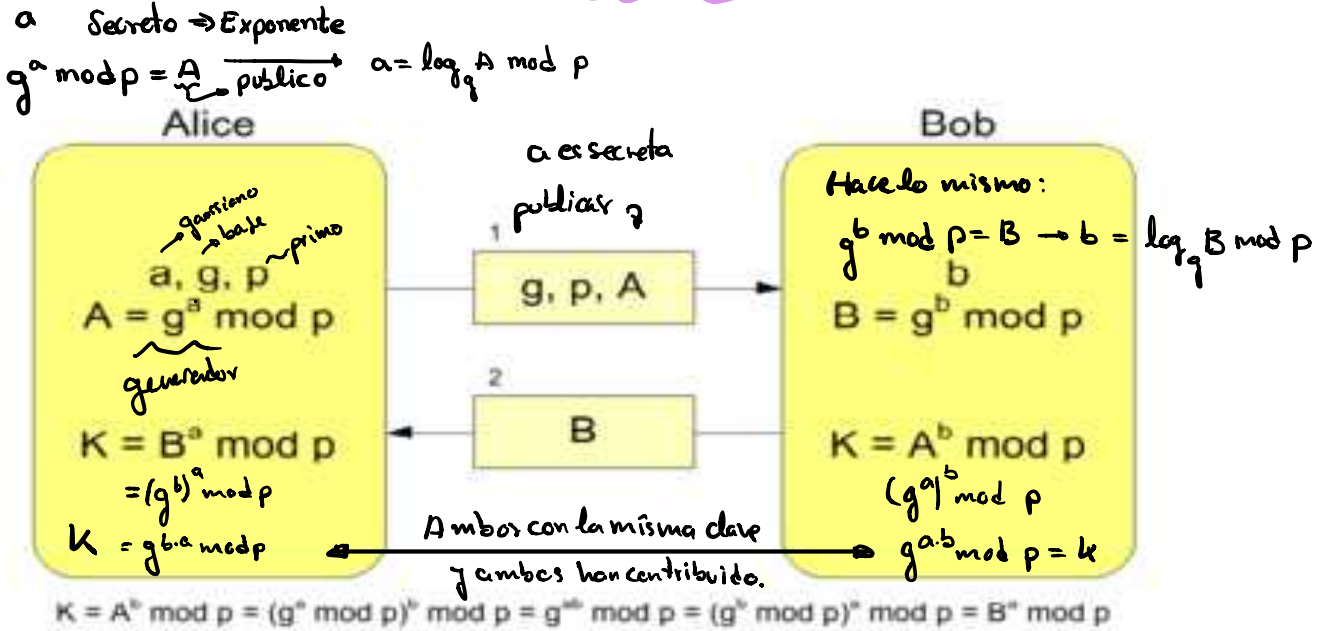
- ***New Directions in Cryptography***
  - **Abstract** Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.
  - https://www-ee.stanford.edu/~hellman/publications/24.pdf

# Contenidos


Distribución de claves secretas mediante cripto. simétrica
Aparición de la criptografía de clave pública
Intercambio de claves DH
RSA
ElGamal
Desarrollo de algoritmos de clave pública
Distribución de claves secretas mediante criptografía de clave pública
Distribución de claves públicas

# Intercambio de claves DH

- Artículo seminal de Diffie-Hellman en 1976




Encontrar a o b es muy costoso, por lo que a·b más aún.

# Intercambio de claves DH

- g y p deben escogerse con cuidado:
  - p primo con alrededor de 300 dígitos decimales
  - El tamaño de g no es importante: suele escogerse 2 ó 5
- a y b (secretos) deben escogerse aleatoriamente
  - Si no, la labor del atacante se simplifica mucho
- A y B públicos
- Basado en el problema del logaritmo discreto
  - Inviable determinar a desde A o b desde B
  - Inviable determinar K desde A+B o desde A o B

# Intercambio de claves DH

Ejemplo de Diffie-Hellman


Alice

Bob

Eve

# Intercambio de claves DH

- A y B acuerdan $p$=23 y generador $g$=5.
- A elige número secreto $a$=6, y luego envía a B ($g^a$ mod $p$)
  - A B=$5^6$ mod 23 = 8.
- B elige número secreto $b$=15, y luego envía a A ($g^b$ mod p)
  - B A=$5^{15}$ mod 23 = 19.
- A calcula ($g^b$ mod $p$)$^a$ mod $p$
  - K=$19^6$ mod 23 = 2.
- B calcula ($g^a$ mod $p$)$^b$ mod $p$
  - K=$8^{15}$ mod 23 = 2

| A | | |
|---|---|---|
| Sec | | Calc |
| | p, g | |
| a | | |
| | | $g^a$ mod p |
| | … | |
| | $(g^b \bmod p)^a$ mod p | |

→
←
=

| B | | |
|---|---|---|
| Calc | | Sec |
| | p, g | |
| | | b |
| | … | |
| $g^b$ mod p | | |
| | $(g^a \bmod p)^b$ mod p | |

| Alice | |
|---|---|
| knows | doesn't know |
| p = 23 | b = 15 |
| base g = 5 | |
| a = 6 | |
| $5^6$ mod 23 = 8 | |
| $5^b$ mod 23 = 19 | |
| $19^6$ mod 23 = 2 | |
| $8^b$ mod 23 = 2 | |
| $19^6$ mod 23 = $8^b$ mod 23 | |
| s = 2 | |

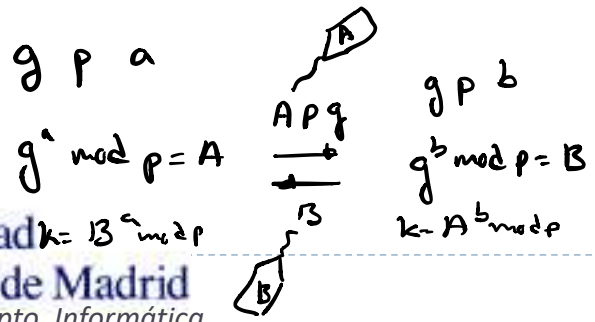
| Bob | |
|---|---|
| knows | doesn't know |
| p = 23 | a = 6 |
| base g = 5 | |
| b = 15 | |
| $5^{15}$ mod 23 = 19 | |
| $5^a$ mod 23 = 8 | |
| $8^{15}$ mod 23 = 2 | |
| $19^a$ mod 23 = 2 | |
| $8^{15}$ mod 23 = $19^a$ mod 23 | |
| s = 2 | |

| Eve | |
|---|---|
| knows | doesn't know |
| p = 23 | a = 6 |
| base g = 5 | b = 15 |
| | s = 2 |
| $5^a$ mod 23 = 8 | |
| $5^b$ mod 23 = 19 | |
| $19^a$ mod 23 = s | |
| $8^b$ mod 23 = s | |
| $19^a$ mod 23 = $8^b$ mod 23 | |

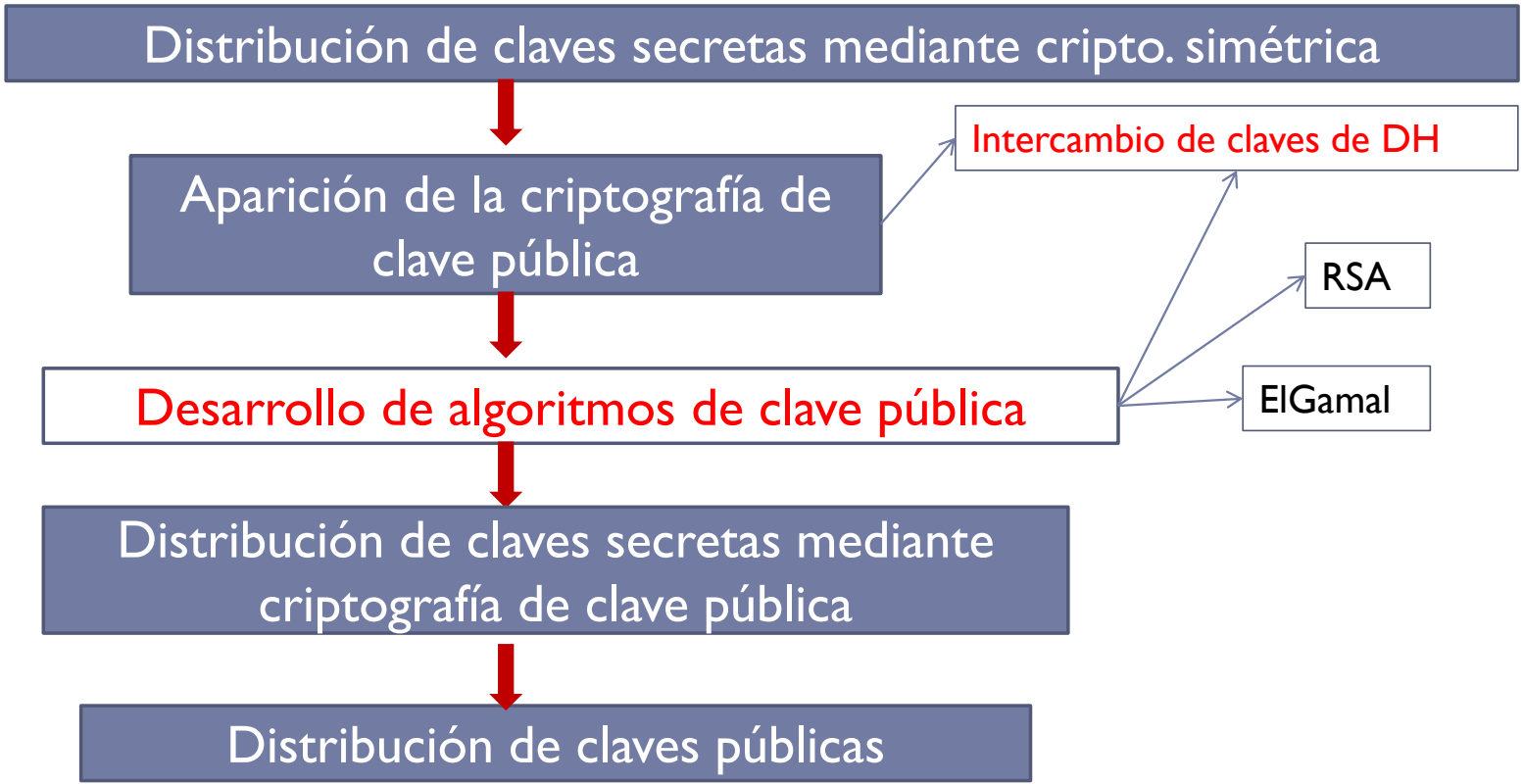
K

# Intercambio de claves DH

- Vulnerabilidades de DH
  - El protocolo de D-H no garantiza ningún tipo de autenticación
  - Esto permite un ataque de hombre interpuesto (man in the middle)
    - Se soluciona con una firma, sabemos de donde viene.
    - El atacante controla el canal
    - Suplanta a A frente a B y a B frente a A
    - Realiza un D-H con cada uno de ellos
    - Ni A ni B pueden descubrirlo, puesto que no se utiliza ningún mecanismo de autenticación

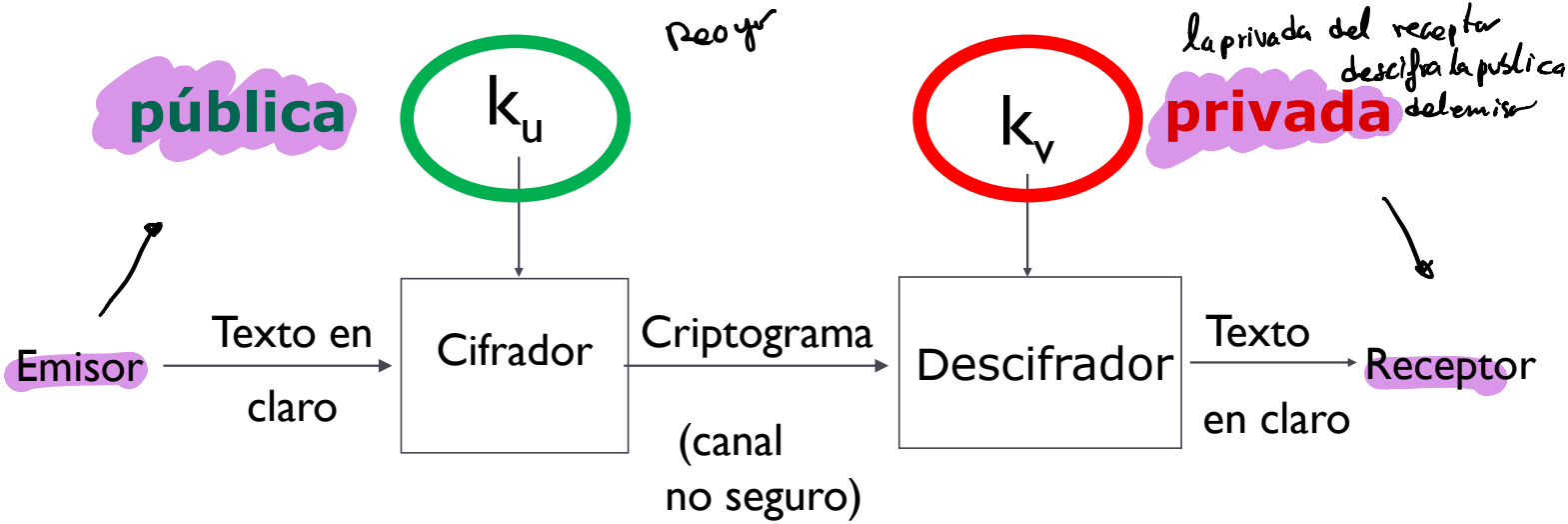


# Contenidos


Distribución de claves secretas mediante cripto. simétrica
Aparición de la criptografía de clave pública
Intercambio de claves de DH
RSA
Desarrollo de algoritmos de clave pública
ElGamal
Distribución de claves secretas mediante criptografía de clave pública
Distribución de claves públicas

# MÉTODOS DE CIFRA MODERNA

## Modelo de criptosistema de clave **asimétrica**




$$C = E(k_u, M) = E_{k_u}(M) \qquad M = D(k_v, C) = D_{k_v}(C)$$

# Criptografía de clave pública

- **O asimétrica (de dos claves)**

  Emplea pares de claves:

  - **clave pública**
    - Conocida por todos
    - Usada para cifrar mensajes y verificar firmas
  - **clave privada relacionada**
    - Conocida sólo por el propietatio (receptor mensaje cifrado o emisor firma)
    - Usada para descifrar/firmar

**Inviable** determinar clave privada a partir de pública

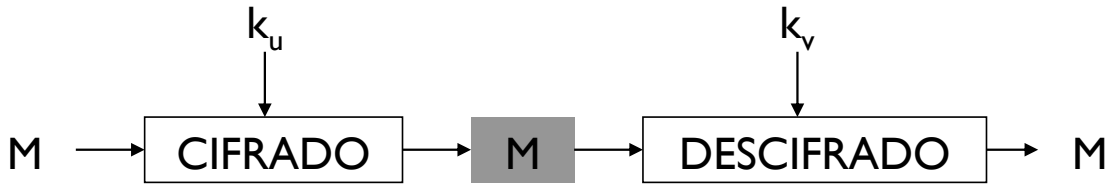
# Criptografía de clave pública

- **Seguridad computacional**
  - La búsqueda exhaustiva es posible en teoría
  - Las claves usadas han de ser suficientemente grandes
  - Los problemas matemáticos en que se basan son difíciles (hard) → Funciones unidireccionales con trampa
    - Factorización de números grandes
    - Logaritmo discreto

- **Lentos en comparación con criptosistemas simétricos**

# Criptografía de clave pública

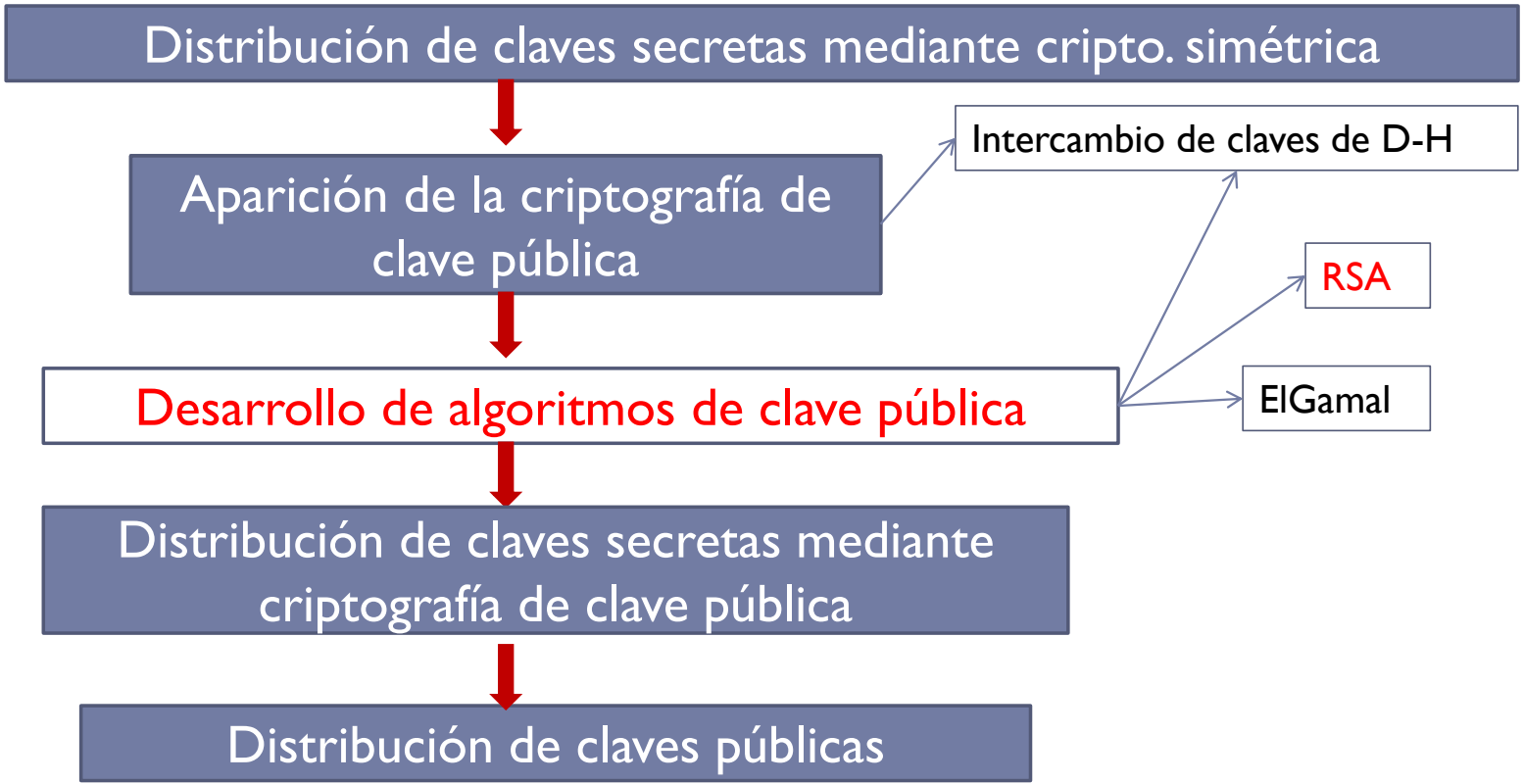
- Cifrado asimétrico de datos (Diffie-Hellman, 1976)




$$C = E(k_u, M) = E_{ku}(M)$$

$$M = D(k_v, C) = D_{kv}(C)$$

# Contenidos


Distribución de claves secretas mediante cripto. simétrica
Aparición de la criptografía de clave pública
Intercambio de claves de D-H
RSA
Desarrollo de algoritmos de clave pública
ElGamal
Distribución de claves secretas mediante criptografía de clave pública
Distribución de claves públicas

# CIFRADO DE DATOS: Clave pública

- ***A Method for Obtaining Digital Signature and Public-Key Cryptosystems***
  - Primer algoritmo efectivo de clave pública, el famoso RSA
  - Luego hubo otros, algunos rotos, pero RSA permanece
  - R. L. Rivest, A. Shamir, L. Adleman
  - Communications of the ACM
  - v. 21, nº 2, pp 120-126. Febrero de 1978
  - https://people.csail.mit.edu/rivest/Rsapaper.pdf

# RSA

- Rivest, Shamir, Adleman, 1978
- Elección del par de claves por A

1. Elige $p, q$ (primos muy grandes, **no públicos**)
2. Obtiene $n = p \cdot q$
3. Calcula $\phi(n) = \phi(p) \cdot \phi(q)$
4. Escoge $e \in Z^+ / \text{m.c.d.}(e, \phi(n)) = 1$
5. Calcula $d / e \cdot d = 1 \quad \text{mód. } \phi(n)$

- **Clave pública de A:** **e, n**
- **Clave privada de A:** **d, n**

# RSA

- **Remisión de un mensaje M cifrado de B a A**

- (B) Calcula: $C = M^e$ mód. n

cifrado — mensaje elevado a e público.


- (A) Calcula: $C^d$ mód. n = M

cifrado elevado a d privado

# RSA

- **Demostración cifrado/descifrado RSA**:

- Como $C=M^e$ mód. $n \Rightarrow C^d$ mód. $n=M^{e \cdot d}$ mód. $n$
- Por hipótesis $e \cdot d = 1$ mód. $\phi(n) \Rightarrow e \cdot d = 1 + k \cdot \phi(n)$
- Por Euler, $M^{\phi(n)}$ mód. $n=1$
- Luego $M^{e \cdot d}$ mód. $n = M^{1 + k \cdot \phi(n)}$ mód. $n = M$

- Así pues $C^d$ mód. $n = M$

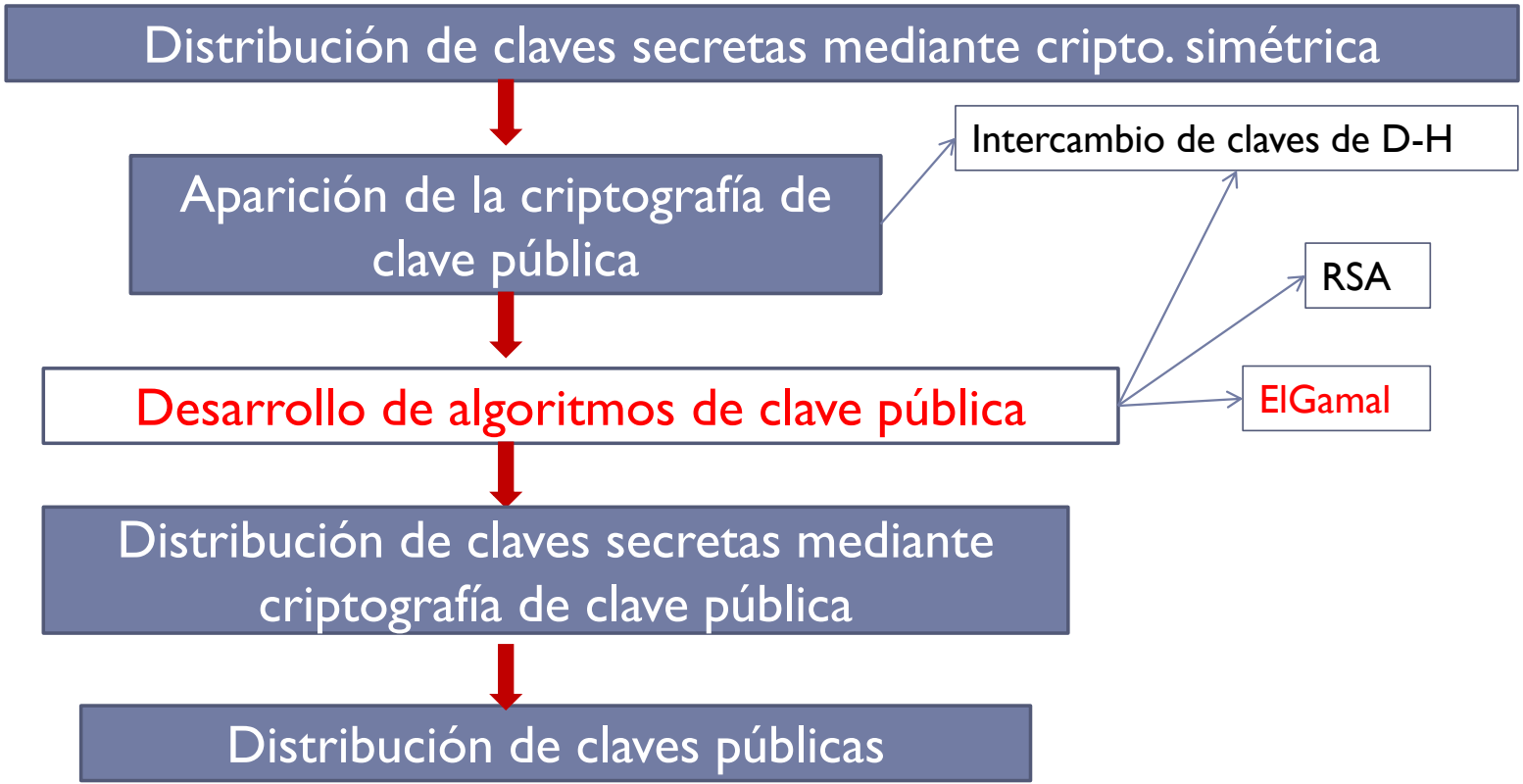
# RSA

## Seguridad

- La seguridad del RSA se basa en el problema de la factorización de números grandes
  - Para calcular d = inv [e, $\phi(n)$]
    - Hay que calcular $\phi(n) = (p - 1) \cdot (q - 1)$
    - Hay que conocer p y q
    - $O(e^{\ln(n) \cdot \ln \ln(n)})$
- RSA-640 (193 dígitos) roto en 2005
- RSA factoring challenge
  - http://www.rsa.com/rsalabs/node.asp?id=2093

Firma: se adjunta con el texto una parte cifrada con la pública que es descifrada y testa procedencia

# Contenidos


Distribución de claves secretas mediante cripto. simétrica
Aparición de la criptografía de clave pública
Intercambio de claves de D-H
RSA
Desarrollo de algoritmos de clave pública
ElGamal
Distribución de claves secretas mediante criptografía de clave pública
Distribución de claves públicas

# ElGamal

- ***A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms***
- Taher ElGamal
- *IEEE Transactions in Information Theory*
- vol. IT-31, nº 4, pp 4569-472. Julio de 1985
- http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1057074

- El algoritmo de cifrado es distinto que el de firma

# ElGamal (algoritmo de cifrado)

- p — primo muy grande
- g — generador de CG(p)

- $x_B$ — **clave privada de B**
- $y_B$ — **clave pública de B** ($y_B = g^{x_B}$ mód. p)
- M — texto en claro

# ElGamal (algoritmo de cifrado)

Cada vez que se cifra es distinto, para ello necesitamos k

- Cifrado de M por parte de A:
  - elige **k** (**aleatorio**) / 1 <= k <= p
  - calcula una clave de sesión **K** de un solo uso:

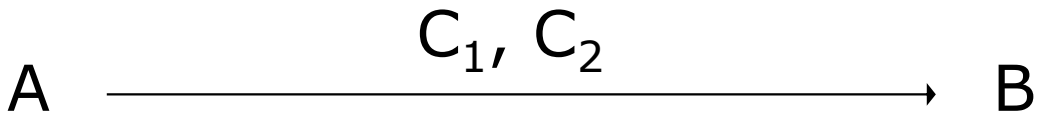
$$\mathbf{K} = y_B^{\,k} \text{ mód. } p$$

$y_B = g^{x_B} \bmod p$

$K = (g^{x_B})^k \bmod p$

$= g^{x_B \cdot k} \bmod p$

  - calcula $C_1 = g^k$ mód. p
  - calcula $C_2 = K \cdot M$ mód. p



# ElGamal (algoritmo de cifrado)

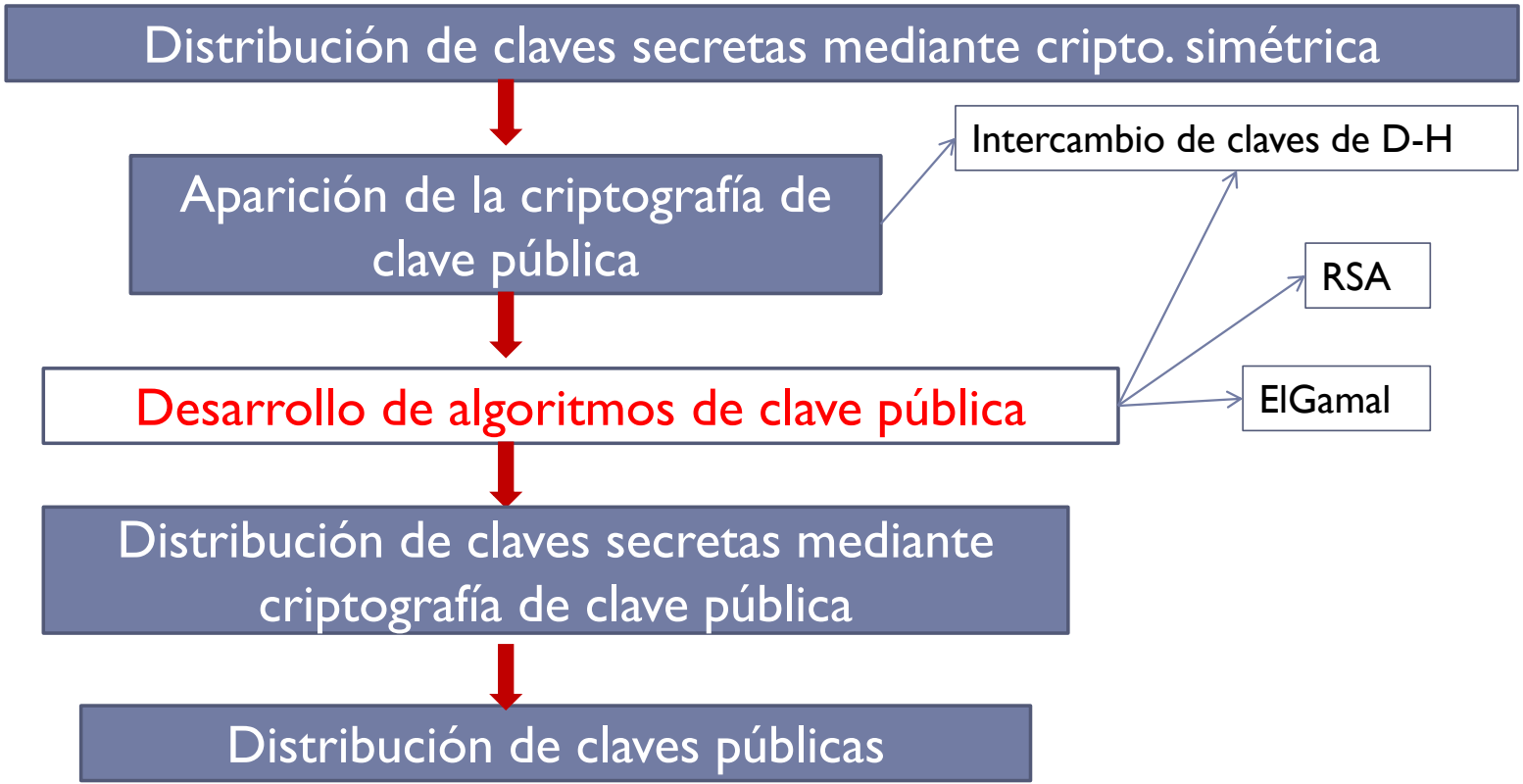
- Descifrado (B):
- recupera la clave de sesión **K** calculando

$$K = C_1^{x_B} \bmod p$$

- recupera el mensaje calculando

$$M = C_2 \cdot K^{-1} \text{ mód. } p$$

# Contenidos


Distribución de claves secretas mediante cripto. simétrica
Aparición de la criptografía de clave pública
Intercambio de claves de D-H
RSA
ElGamal
Desarrollo de algoritmos de clave pública
Distribución de claves secretas mediante criptografía de clave pública
Distribución de claves públicas

# Criptosistemas asimétricos

- RSA
  - Factorización de números grandes
- El Gamal
  - Problema del logaritmo discreto
- Curvas elípticas

# Tamaño de clave para seguridad equivalente

| Simétrico (tamaño de clave en bits) | ECC (tamaño de n en bits) | RSA / DSA(EG) (tamaño del módulo en bits) |
|---|---|---|
| 56 | 112 | 512 |
| 80 | 160 | 1024 |
| 112 | 224 | 2048 |
| 128 | 256 | 3072 |
| 192 | 384 | 7680 |
| 256 | 512 | 15360 |