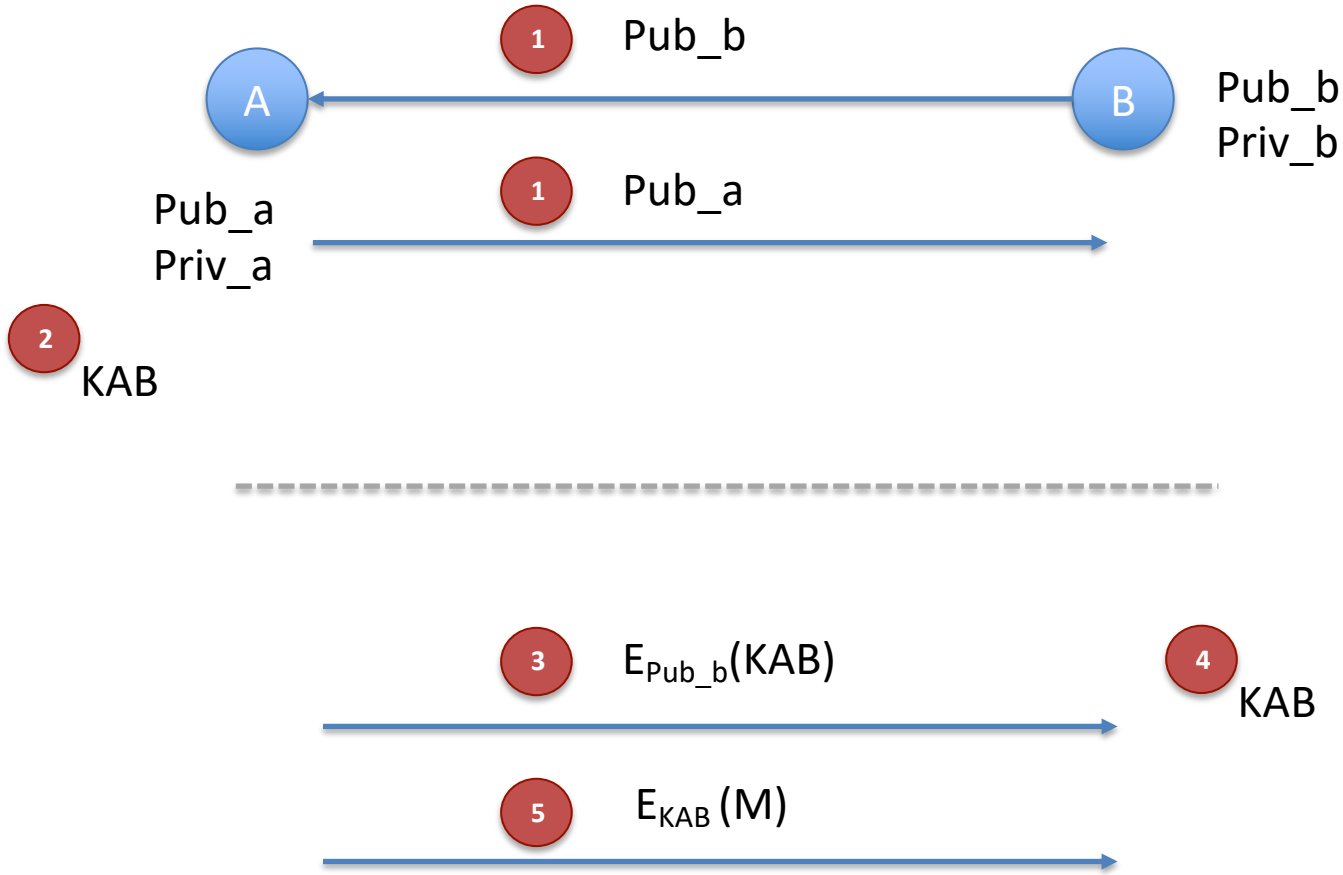
Soluciones de la relación de ejercicios

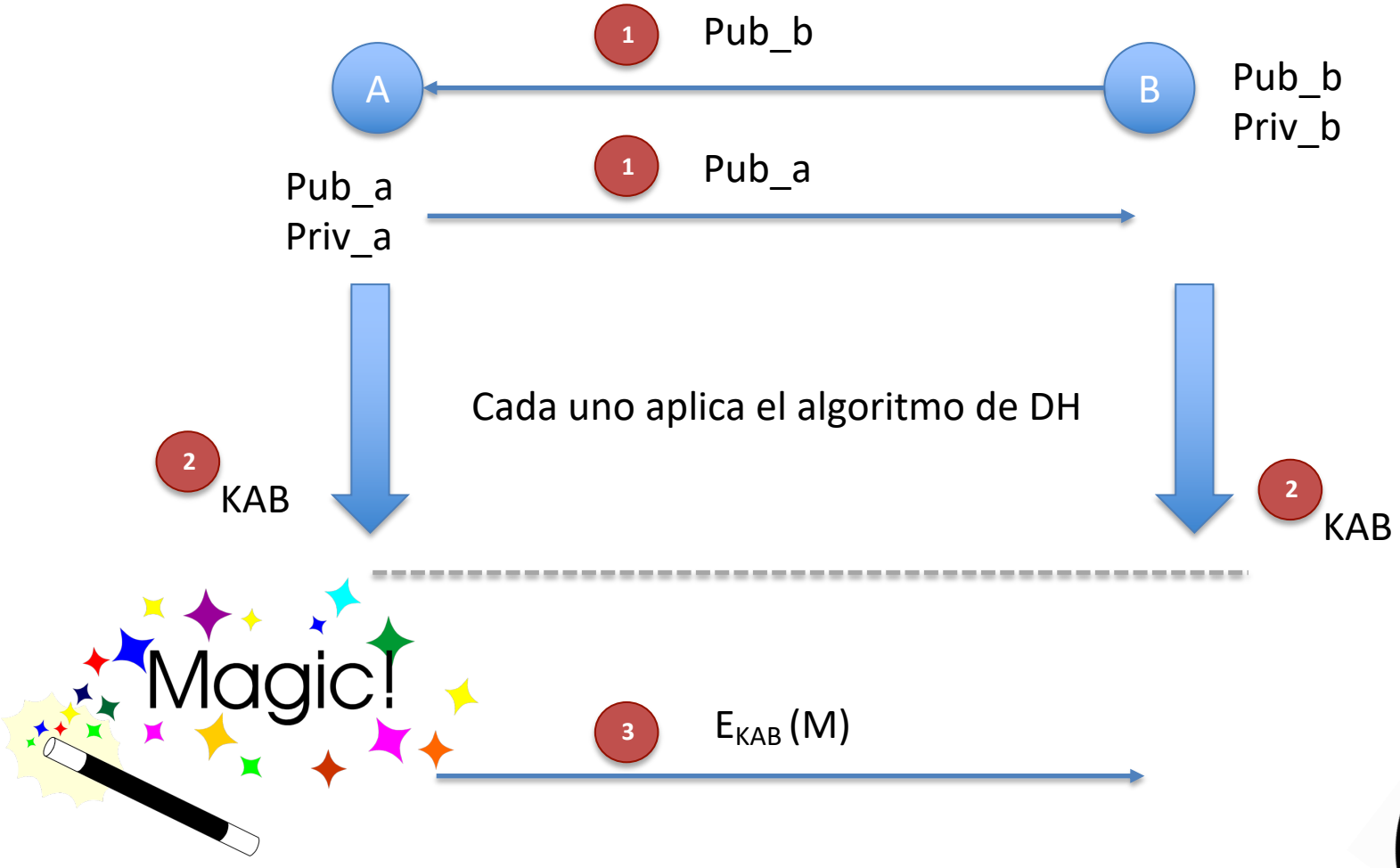
RSA – ej. 1

CRIPTOGRAFÍA
HÍBRIDA

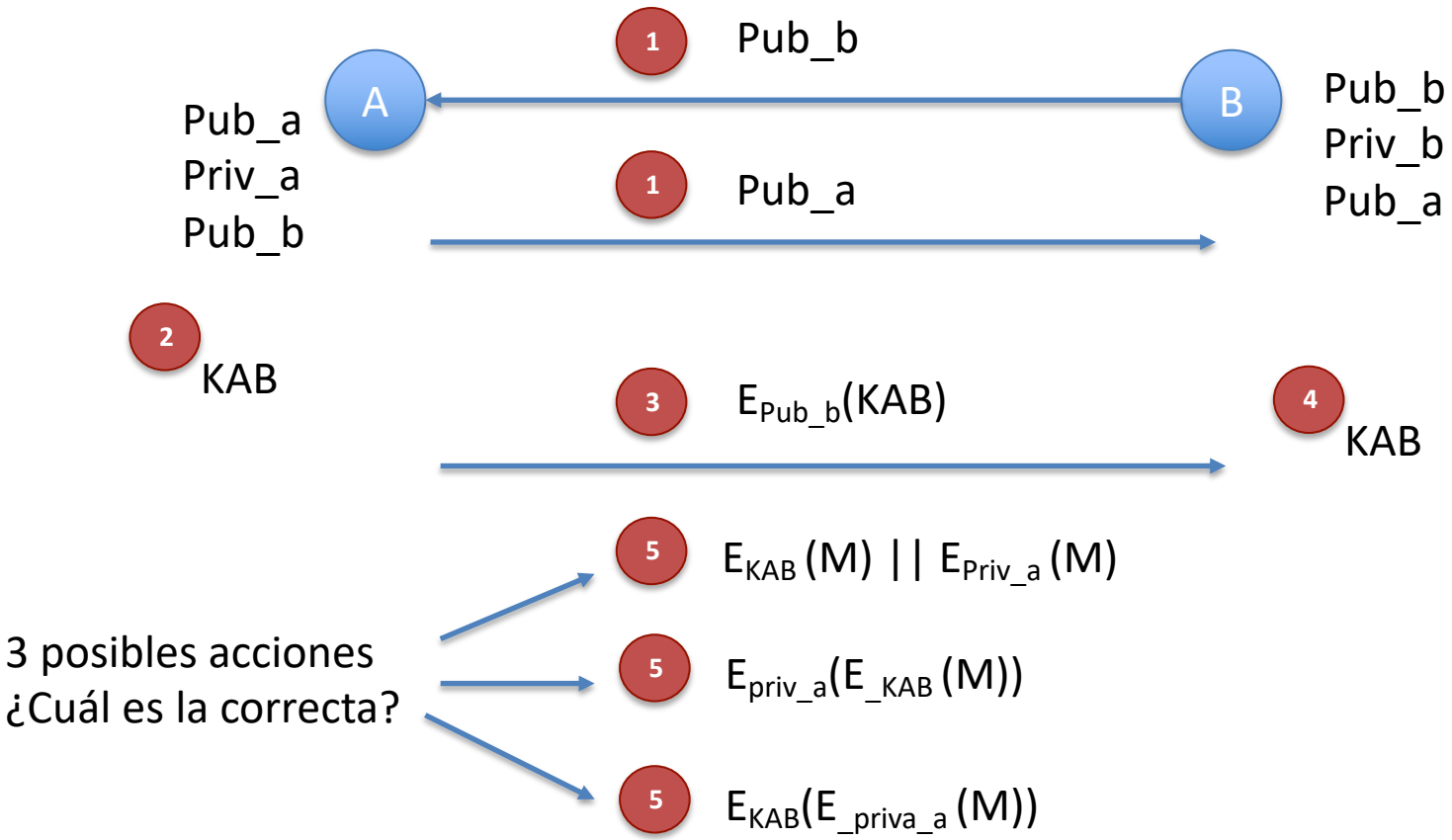


DH – ej. 1

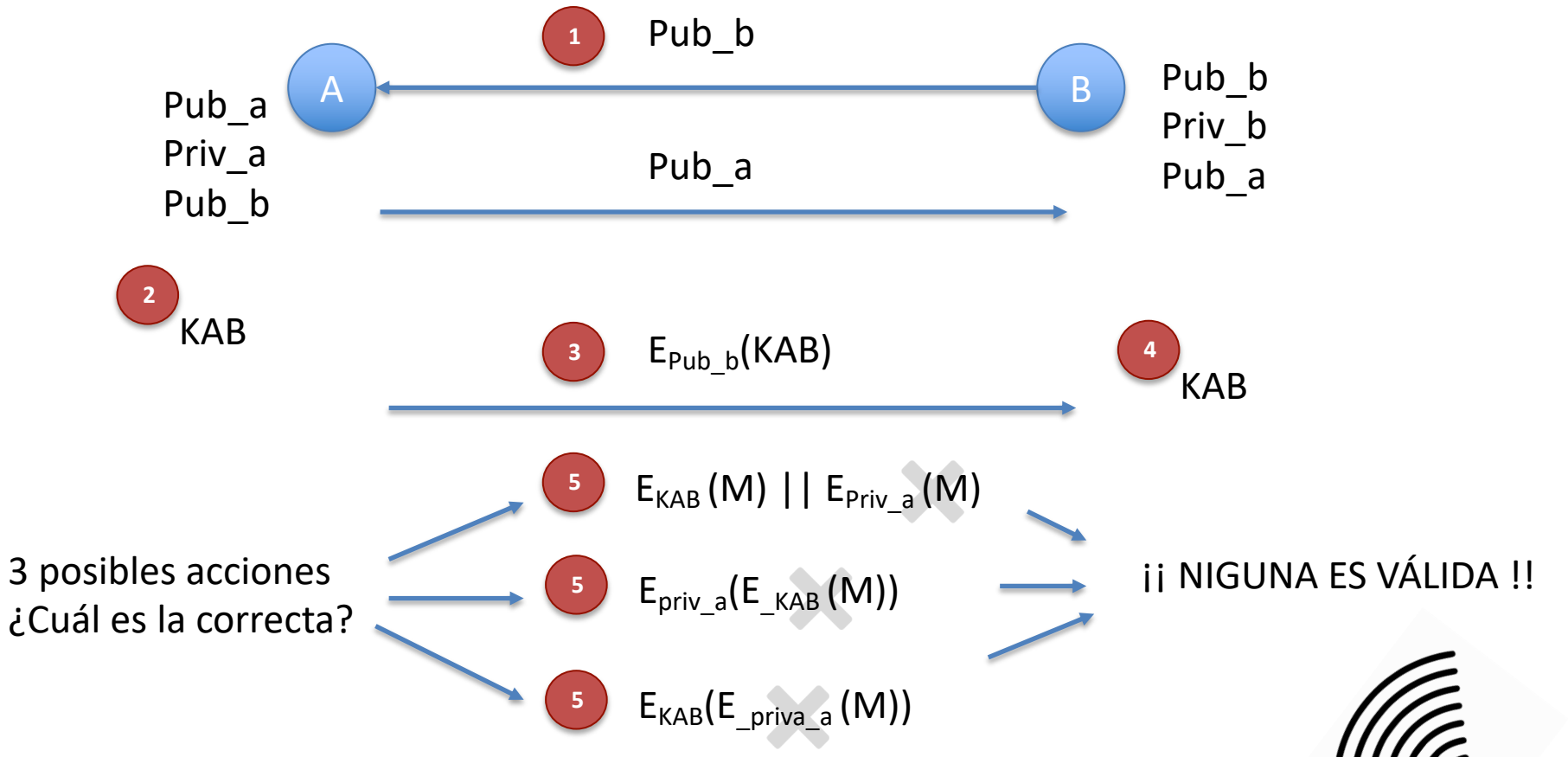
CRIPTOGRAFÍA
HÍBRIDA



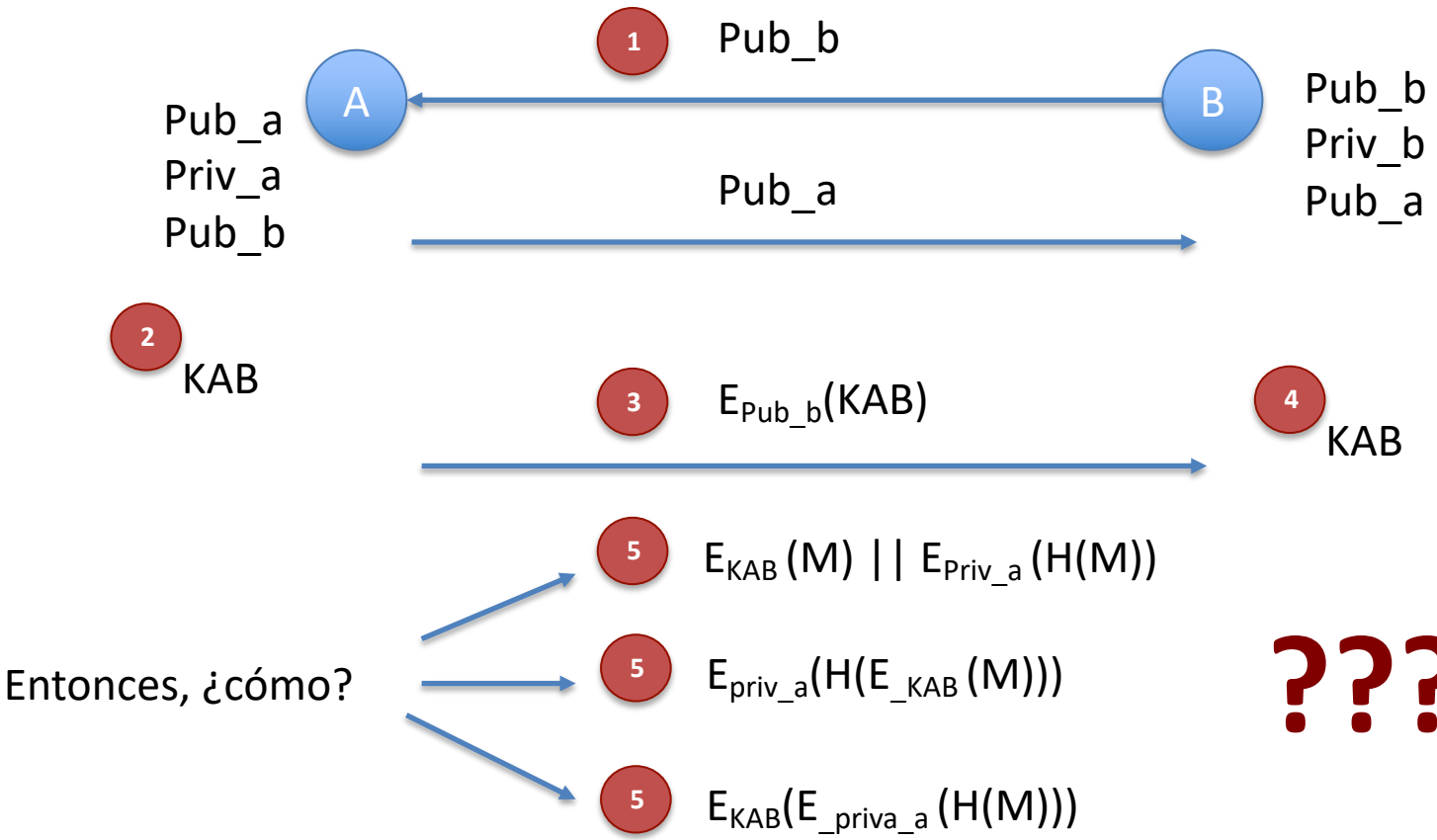
RSA – ej. 2


1
Pub_b
A
B
Pub_a
Priv_a
Pub_b
Pub_b
Priv_b
Pub_a
1
Pub_a
2
KAB
3
$E_{Pub\_b}(KAB)$
4
KAB
5
$E_{KAB}(M) \,||\, E_{Priv\_a}(M)$
3 posibles acciones
¿Cuál es la correcta?
5
$E_{priv\_a}(E_{\_KAB}(M))$
5
$E_{KAB}(E_{\_priva\_a}(M))$

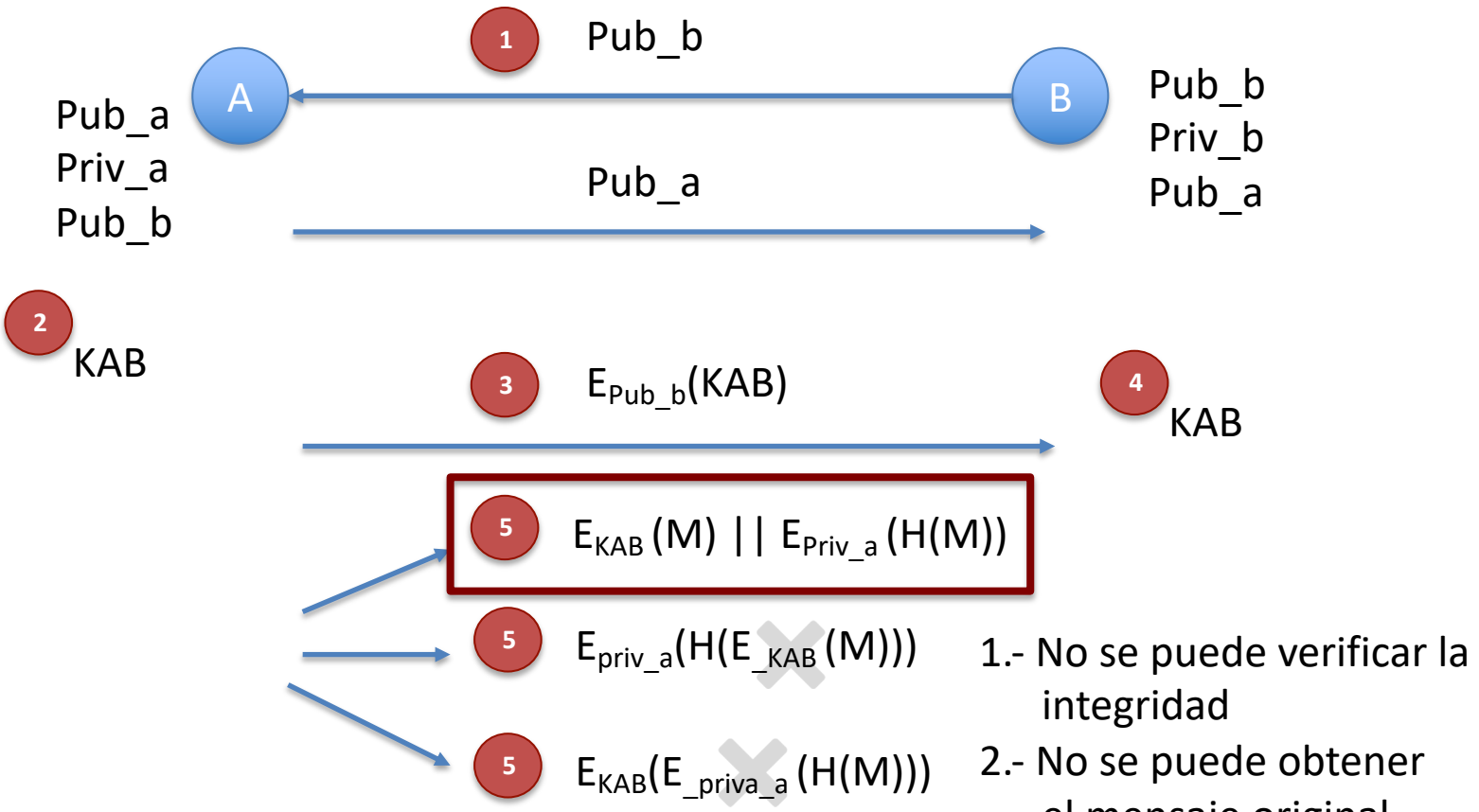
RSA – ej. 2


1
Pub_b
A
B
Pub_a
Priv_a
Pub_b
Pub_b
Priv_b
Pub_a
Pub_a
2
KAB
3
E_{Pub_b}(KAB)
4
KAB
5
E_{KAB} (M) || E_{Priv_a} (M)
5
E_{priv_a}($E_{\_KAB}$ (M))
5
E_{KAB}($E_{\_priva\_a}$ (M))
3 posibles acciones
¿Cuál es la correcta?
¡¡ NINGUNA ES VÁLIDA !!

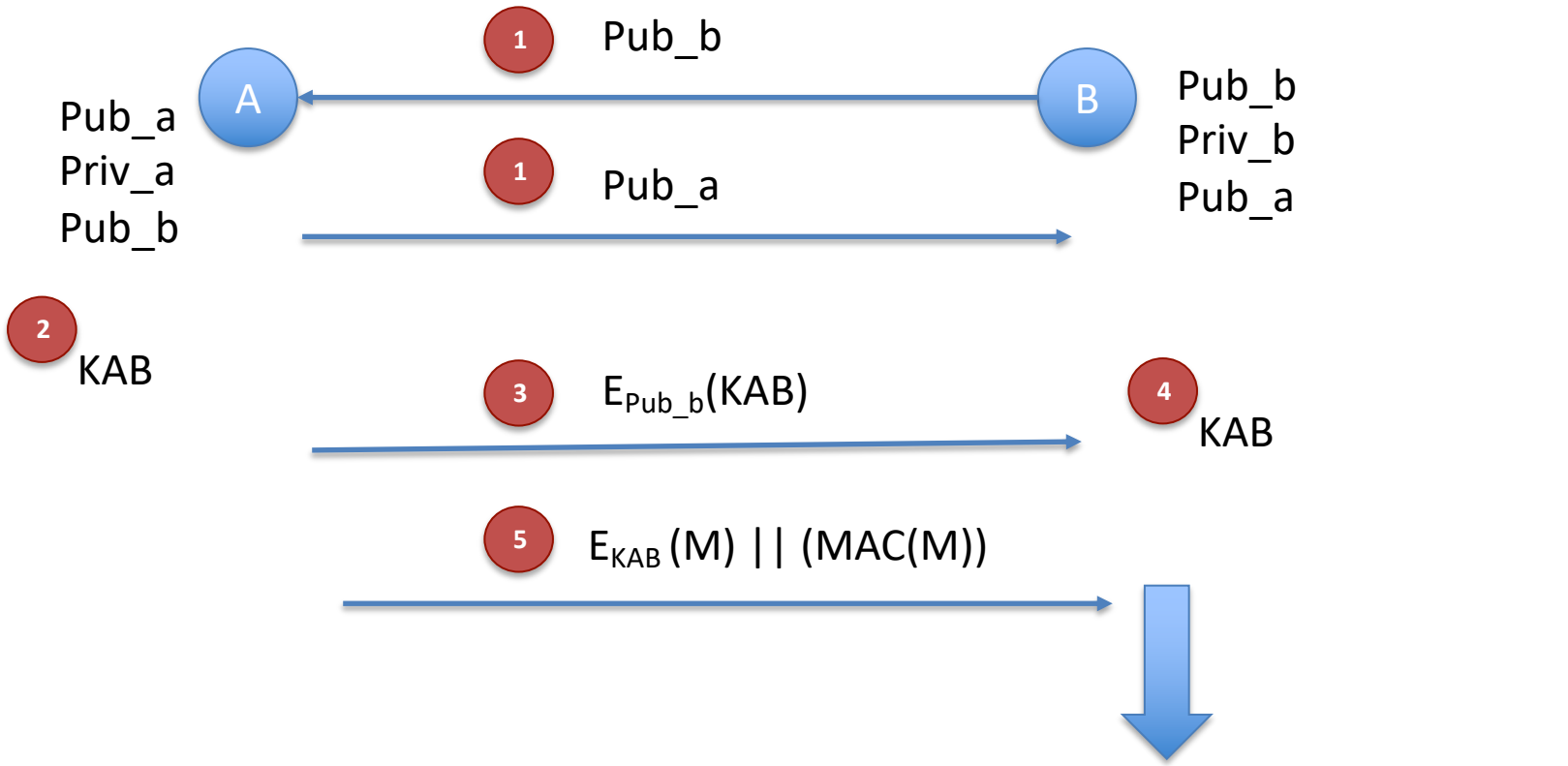
RSA – ej. 2


1
Pub_b
A
B
Pub_a
Priv_a
Pub_b
Pub_b
Priv_b
Pub_a
Pub_a
2
KAB
3
$E_{Pub\_b}(KAB)$
4
KAB
5
$E_{KAB}(M) \,||\, E_{Priv\_a}(H(M))$
Entonces, ¿cómo?
5
$E_{priv\_a}(H(E_{\_KAB}(M)))$
5
$E_{KAB}(E_{\_priva\_a}(H(M)))$
???

RSA – ej. 2


1
Pub_b
A
B
Pub_a
Priv_a
Pub_b
Pub_b
Priv_b
Pub_a
Pub_a
2
KAB
3
$E_{Pub\_b}(KAB)$
4
KAB
5
$E_{KAB}(M) \,||\, E_{Priv\_a}(H(M))$
5
$E_{priv\_a}(H(E_{\_KAB}(M)))$
5
$E_{KAB}(E_{\_priva\_a}(H(M)))$
1.- No se puede verificar la integridad
2.- No se puede obtener el mensaje original

MAC – ej. 3


1
Pub_b
A
B
Pub_b
Priv_b
Pub_a
Pub_a
Priv_a
Pub_b
1
Pub_a
2
KAB
3
E_{Pub_b}(KAB)
4
KAB
5
E_{KAB} (M) || (MAC(M))
6
1.- Descifra el mensaje usando K_{AB}, y obtiene el mensaje M
2.- Calcula la MAC(M)
3.- Compara las MAC, tanto la recibida como la calculada

Protocolo – ej. 4

1. **T → A: $E_{KAT}\{B, K_{AB}, E_{KBT}\{C, K_{AB}, K_{BC}, E_{KCT}\{C, K_{BC}\}\}\}$**
2. **A → B: $E_{KBT}\{C, K_{AB}, K_{BC}, E_{KCT}\{C, K_{BC}\}\}$**
3. **B → A: $E_{KAB}\{$"*hola ID=A*"$\}$**
4. **B → C: $E_{KCT}\{C, K_{BC}\}$**
5. **C → B: $E_{KBC}\{$"*hola ID=B*"$\}$**

1) A descifra el mensaje y obtiene la clave de sesión K_{AB} y comprueba a quién le debe enviar (B o ID = B) la información correspondiente
   - $E_{KBT}\{C, K_{AB}, K_{BC}, E_{KCT}\{C, K_{BC}\}\}$ → se lo envía a B

2) B descifra el mensaje y obtiene la clave de sesión K_{AB} y K_{BC} , y comprueba a quién le debe enviar (A y C) la información correspondiente:
   - $E_{KAB}\{$"*hola ID=A*"$\}$ → se lo envía a A
   - $E_{KCT}\{C, K_{BC}\}$ → se lo envía a C

3) Simétrica
4) Sí, por la clave de sesión, pero ya sabemos que esto no es un procedimiento adecuado ☹

Protocolo – ej. 5

1. **T → A: T, A, E_{KpubA}{T, B, K_{AB}}, E_{privT}{H{T, B, K_{AB}}}**
2. **A → B: A, B, E_{KAB}{"*Estamos aprendiendo criptografía aplicada*"}**

2) Híbrida

3) La clave K_{AB} la genera T

1) Sí, con su propia firma digital ☺ → **E_{privT}{H{T, B, K_{AB}}**

2) Sí, si recibe de T la clave K_{AB}

3) NO ☺

Protocolo – ej. 6

1. **A → B: B, “Hola B”, MAC(____)**
2. **B → A: A, “Hola A”, MAC(____)**

1) Sí, porque de contrario no se puede hacer la MAC

2) y 3) Verifican las respectivas MAC

4) Autenticación e integridad

5)

A → B: B, “Hola B”, K_{priv_A}(H(“Hola B”))
B → A: A, “Hola A”, K_{priv_B}(H(“Hola A”))

Protocolo – ej. 7

1. **A → B: B, "Hola B", MAC_{KAB}(B, "Hola B")**

1. **A → Mallory → B: B, "Adios B", MAC_{KAB}(B, "Hola B")**

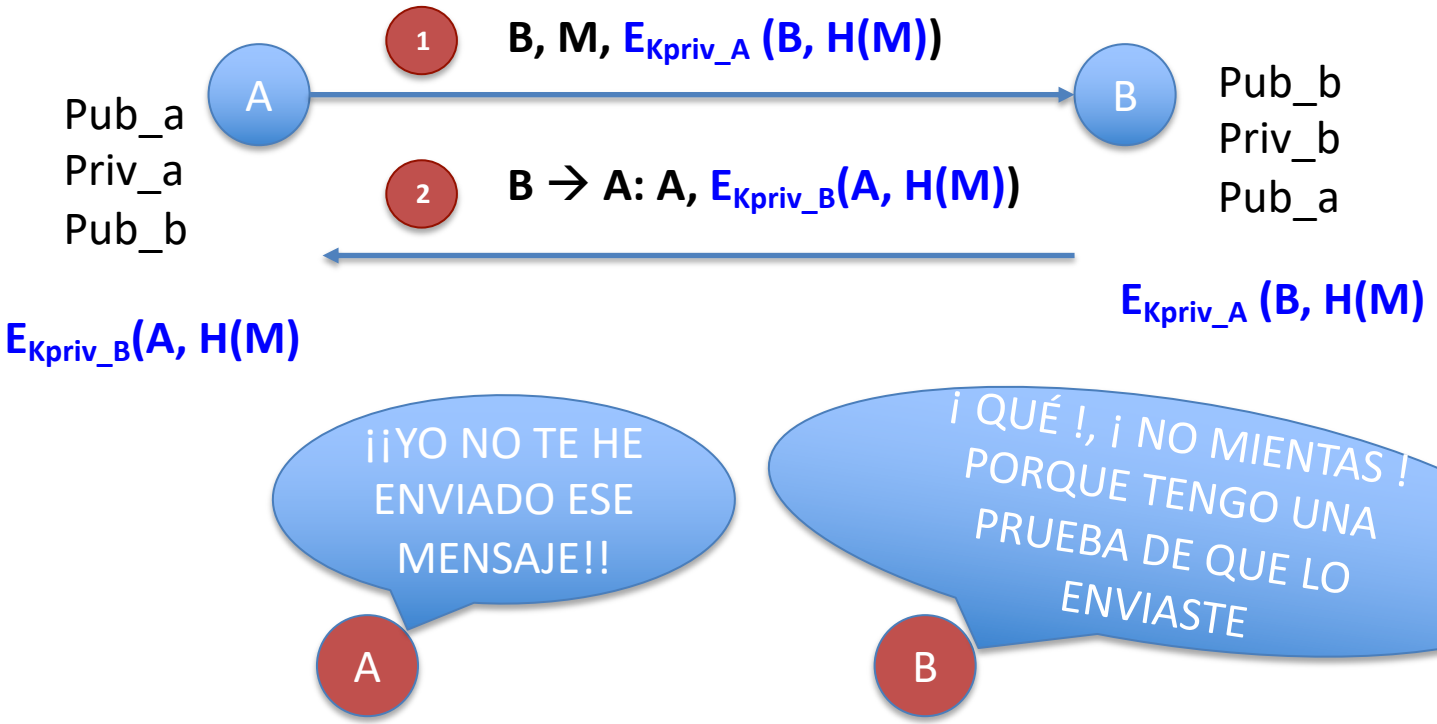
1) Verificar que el mensaje no ha sido alterado con la MAC, aparte de verificar el origen del dato

2) Autenticación (pero no es muy acertado) e integridad

3) NO, si no sabe el valor K_{AB}

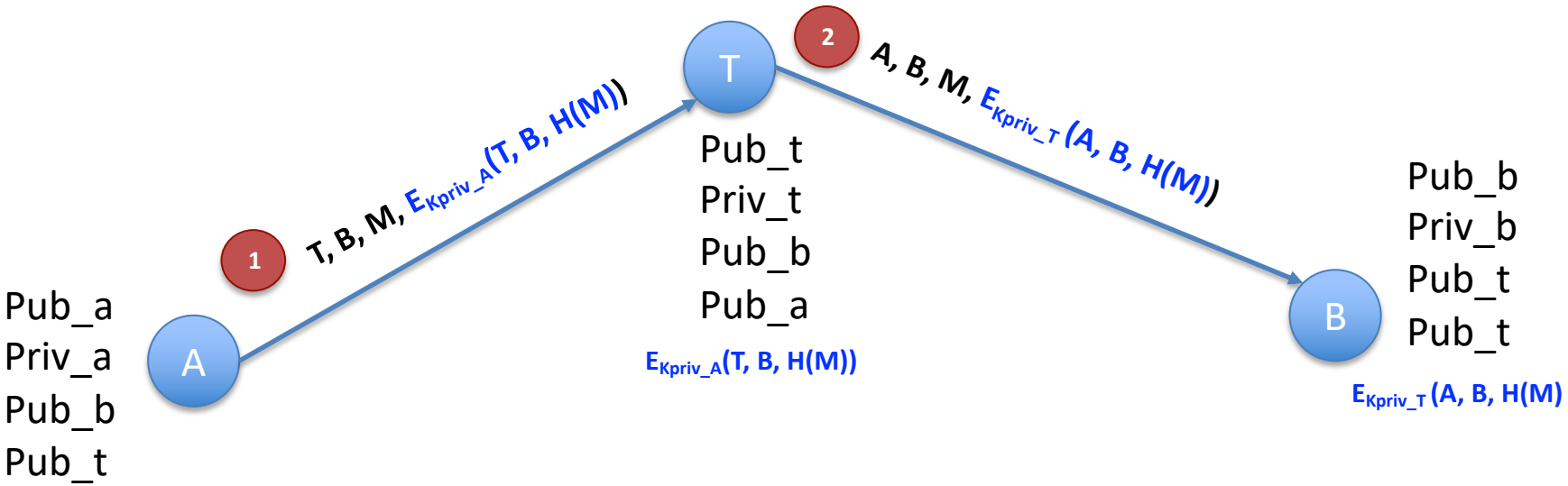
4) Cifrando el mensaje + firma digital ☺

Protocolo – ej. 8

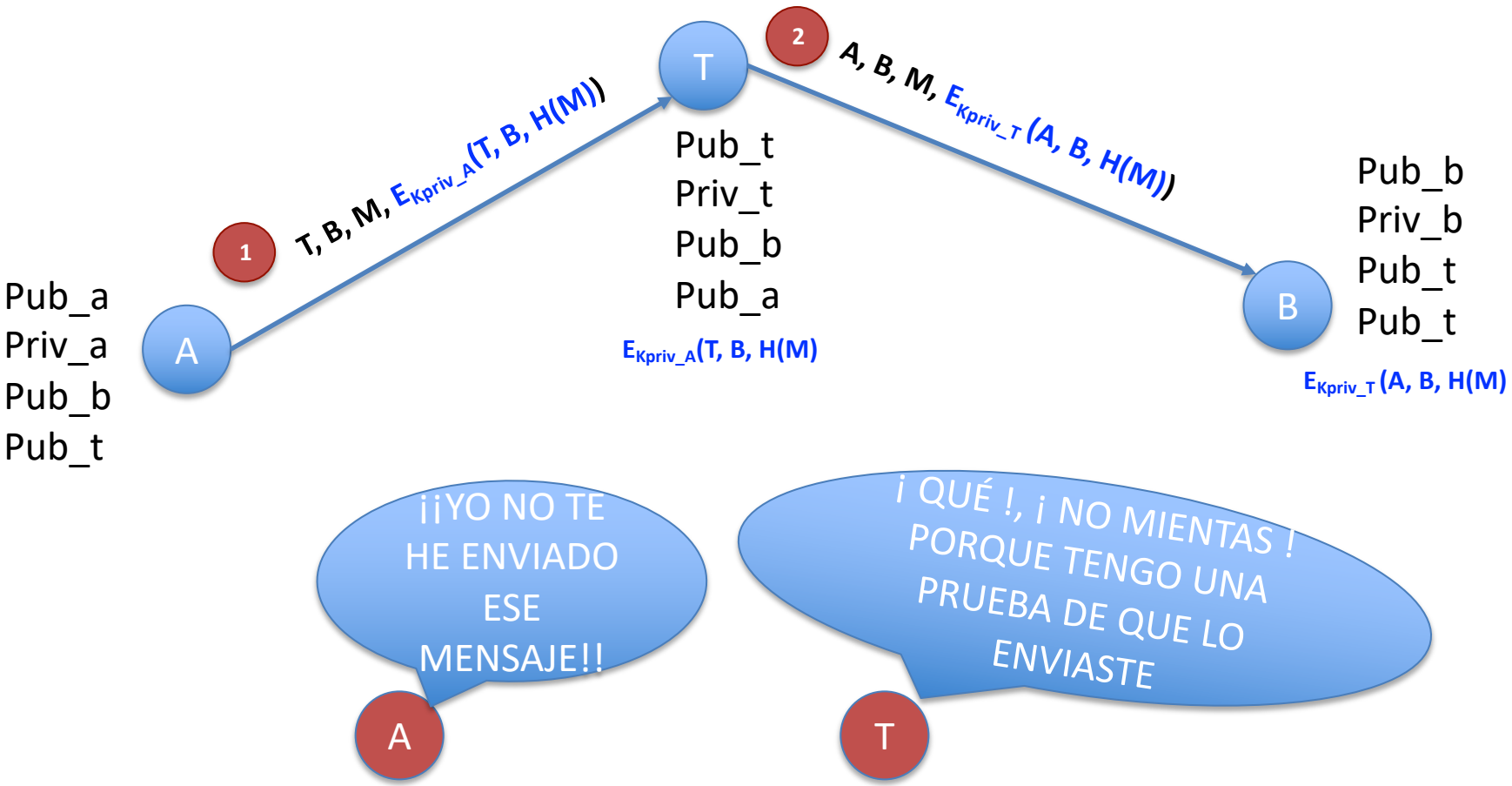


NO REPUDIO DE ORIGEN

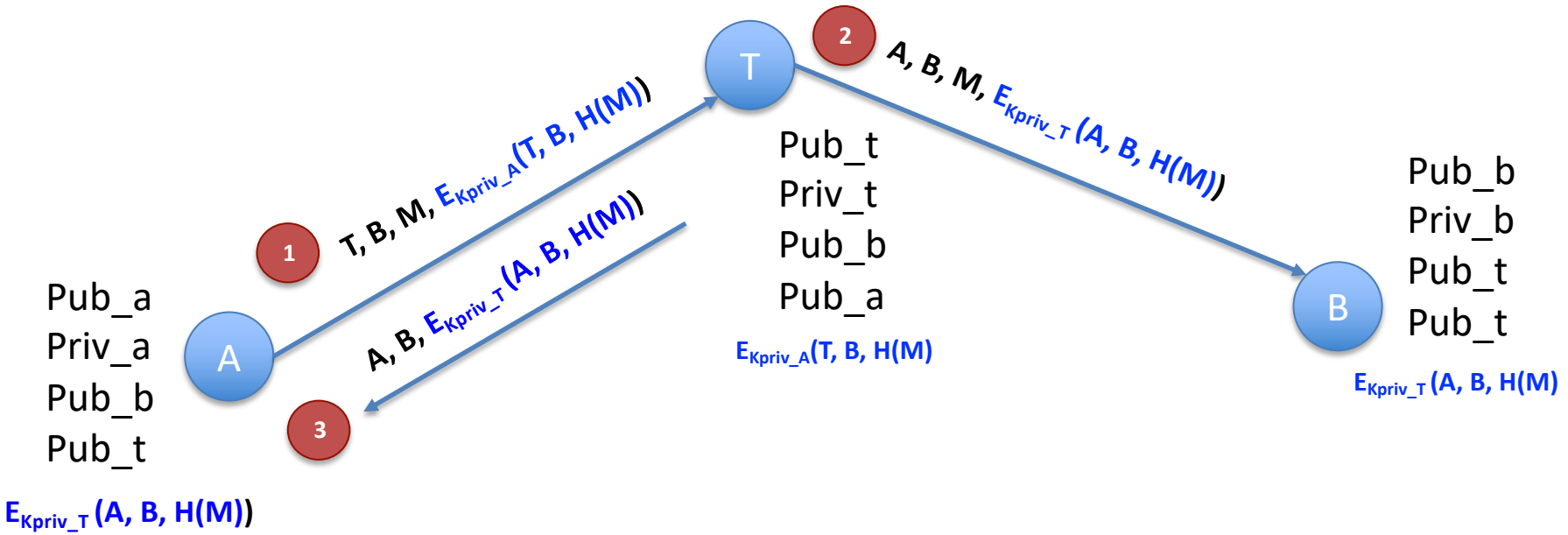
Protocolo – ej. 9



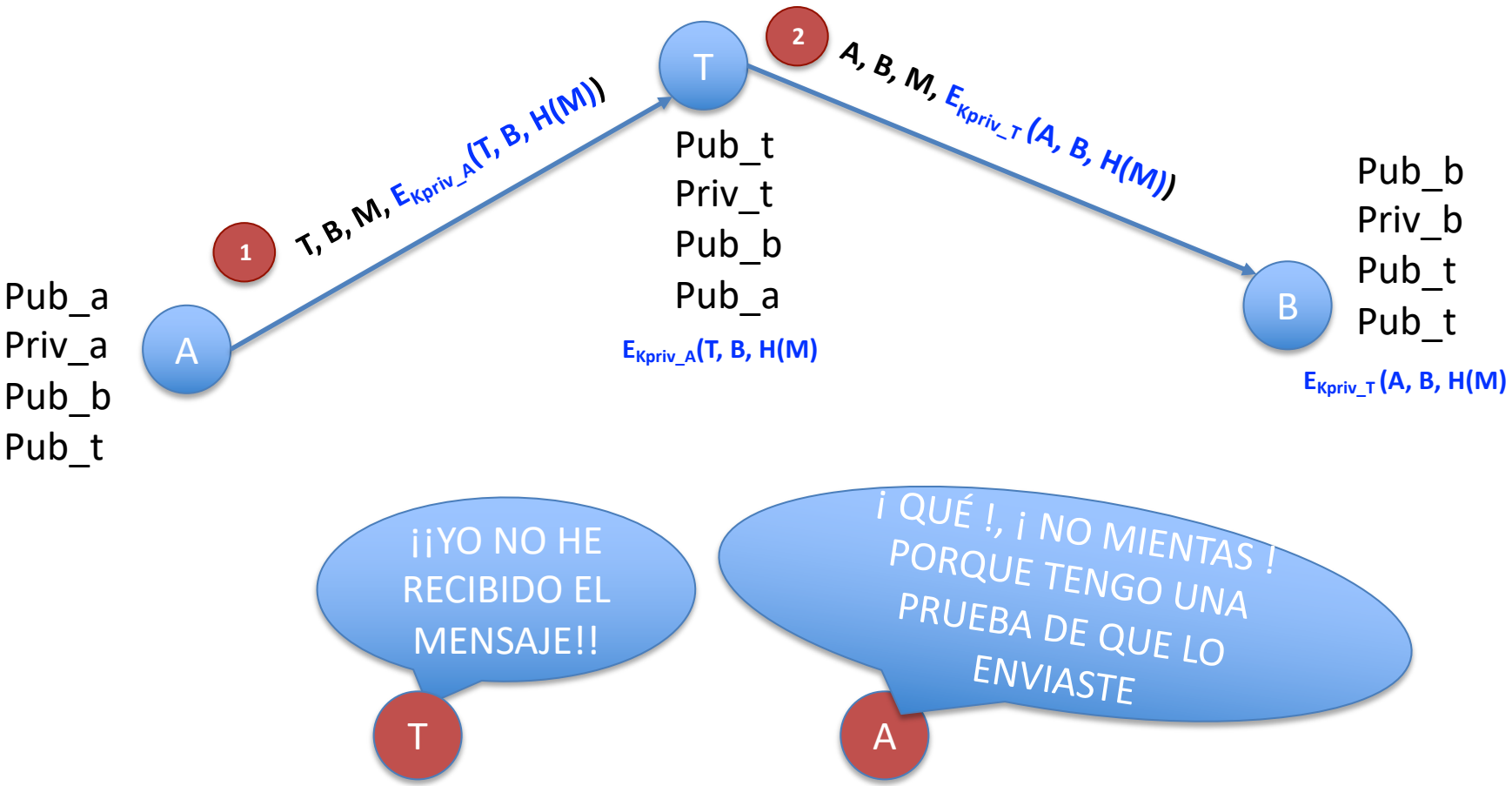
¿¿¿QUÉ SENTIDO TIENE GUARDAR LAS FIRMAS ???



NO REPUDIO DE ORIGEN



¿¿¿QUÉ SENTIDO TIENE GUARDAR LAS FIRMAS ???



NO REPUDIO DE DESTINO