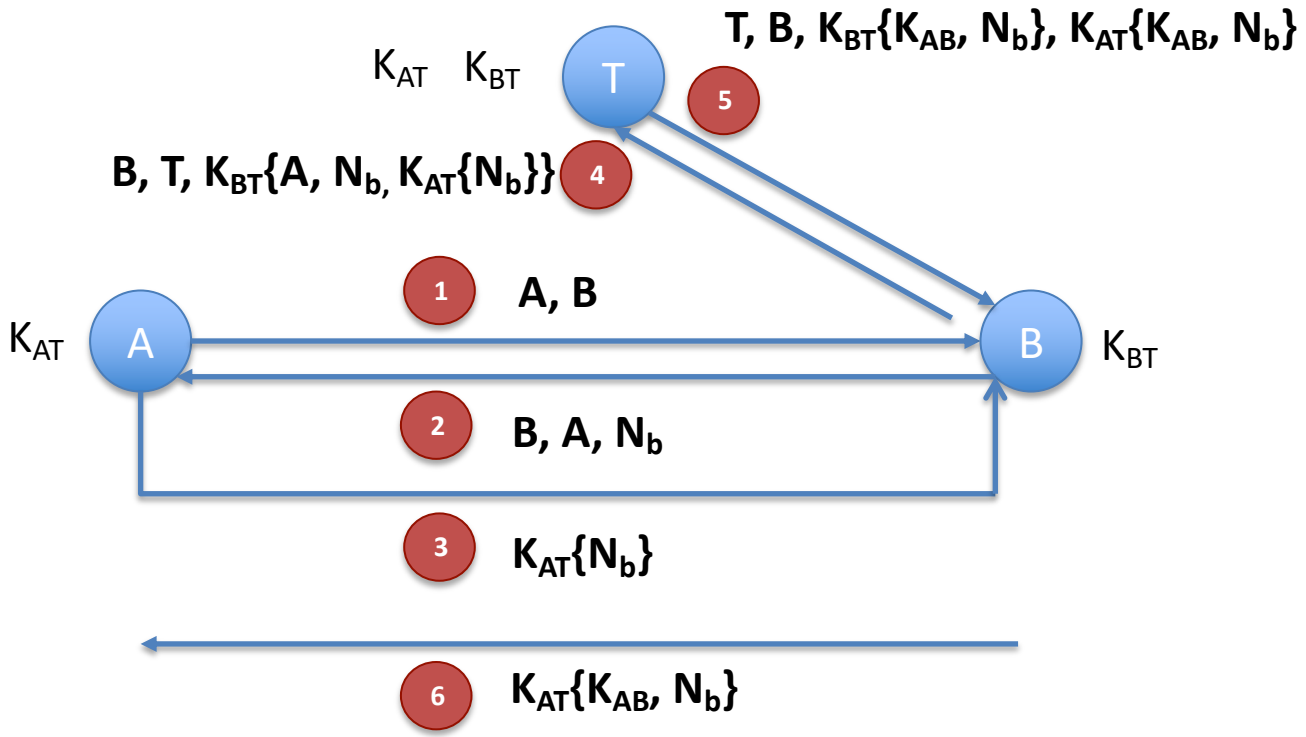
Soluciones de los ejercicios del Tema 3

Ej. 1 (puntos 3-5)



Punto 4: sí, está controlado tanto en A como en B a través de N_b.

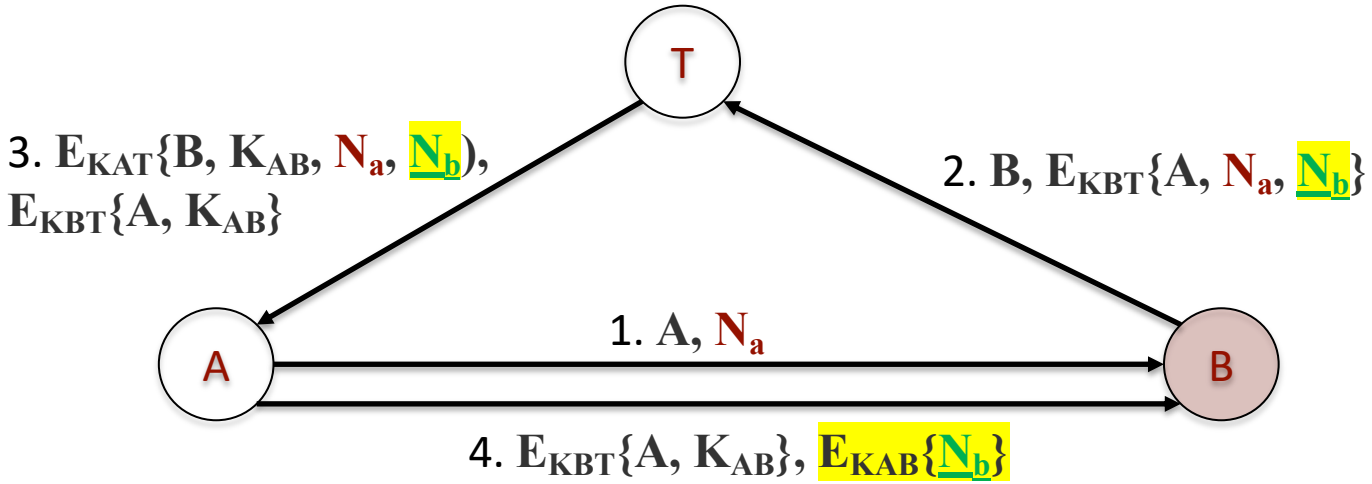
Punto 5: no existe desafío y respuesta.

Punto 6: push.

Relación de ejercicios

Ej. 2)

Yahalom

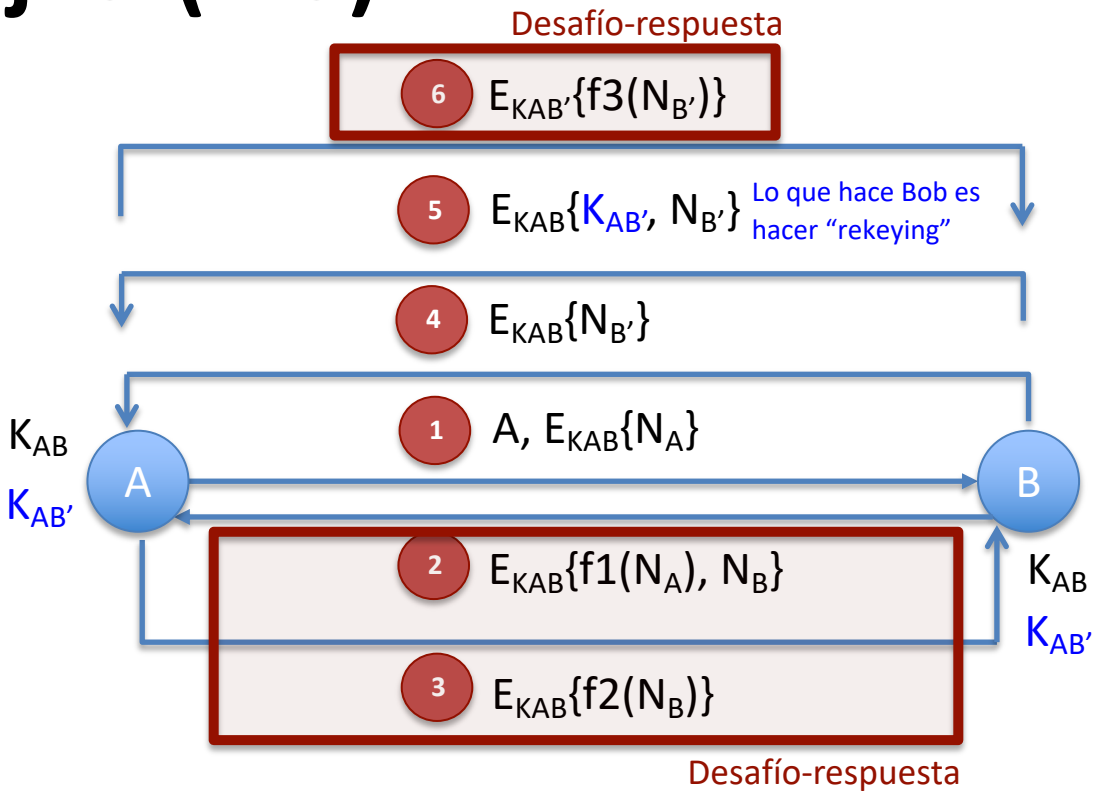


Punto 4: no hoy posibilidad de ataques por repetición porque tanto A como B reciben su nonces, respectivamente. Sin embargo, A se arriesga a que alguien le modifique su N_a.

Punto 5: en parte sí porque A se aprovecha de la trama 4 para enviarle "la respuesta" de un desafío que no establece B → **$E_{KAB}\{N_b\}$.**

Relación de ejercicios

Ej. 3-(1-3)



Punto 1:

1. A → B: A, $E_{KAB}\{N_a\}$
2. B → A: $E_{KAB}\{f_1(N_a), N_b\}$
3. A → B: $E_{KAB}\{f_2(N_b)\}$
4. B → A: $EK_{AB}\{N_{b'}\}$
5. B → A: $E_{KAB}\{K_{AB'}, N_{b'}\}$
6. A → B: $E_{KAB'}\{f_3(N_{b'})\}$
7. ….

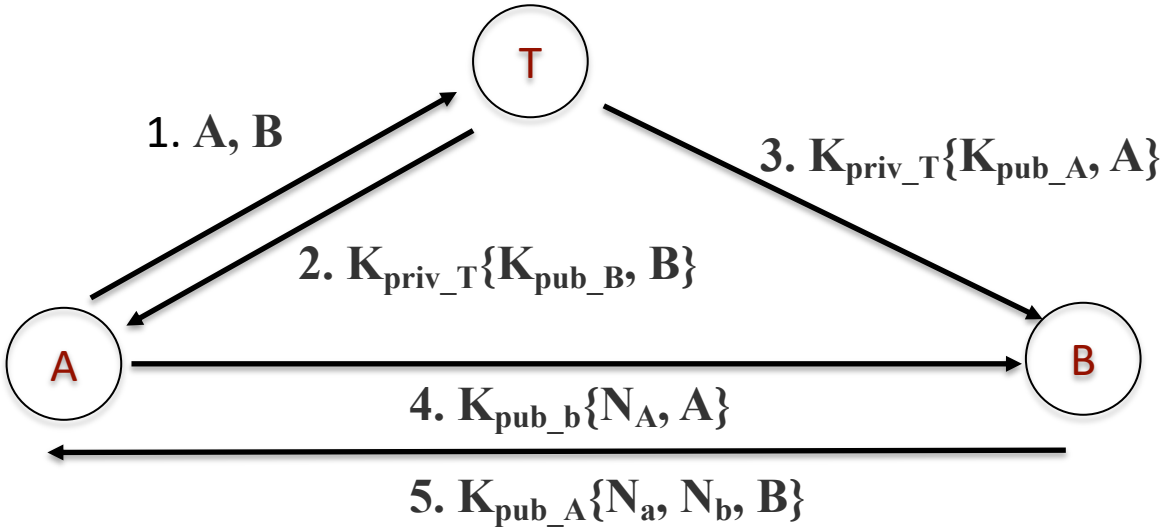
Punto 2: f1, f2 y f3 corresponde a la respuesta de un desafío.

Punto 3: es una nueva clave de sesión generada por B, y se envía $N_{b'}$ porque es parte del desafío de f3.

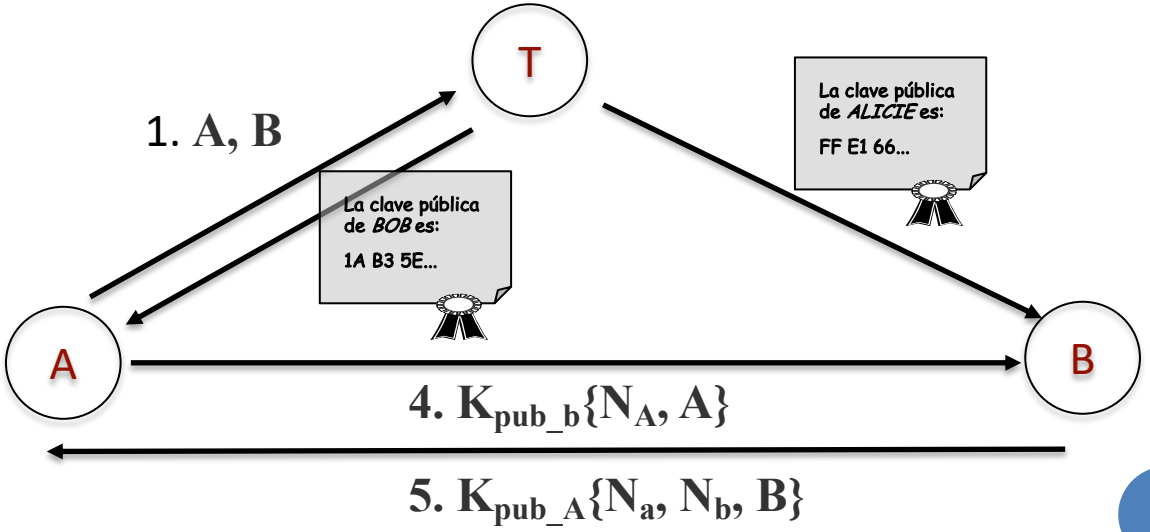
Punto 4: es lo mismo que aplicar un desafío-respuesta, pero garantiza, además, integridad.

Relación de ejercicios

Ej. 4-(1-3)

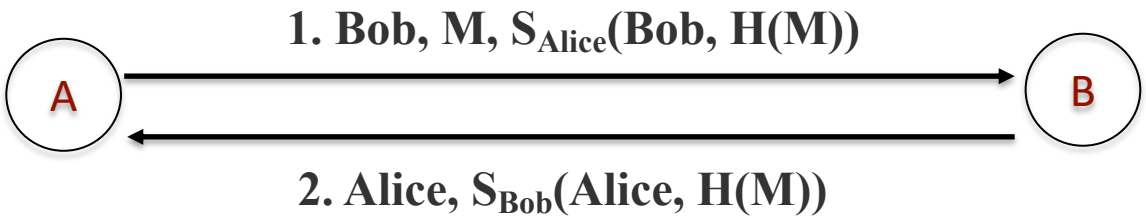


Punto 2: el protocolo lo que hace es simular lo que hace los certificados digitales, donde T funcionaría como la CA. En otras palabras:



Punto 3: para control de ataque replay, pero en el lado de A.

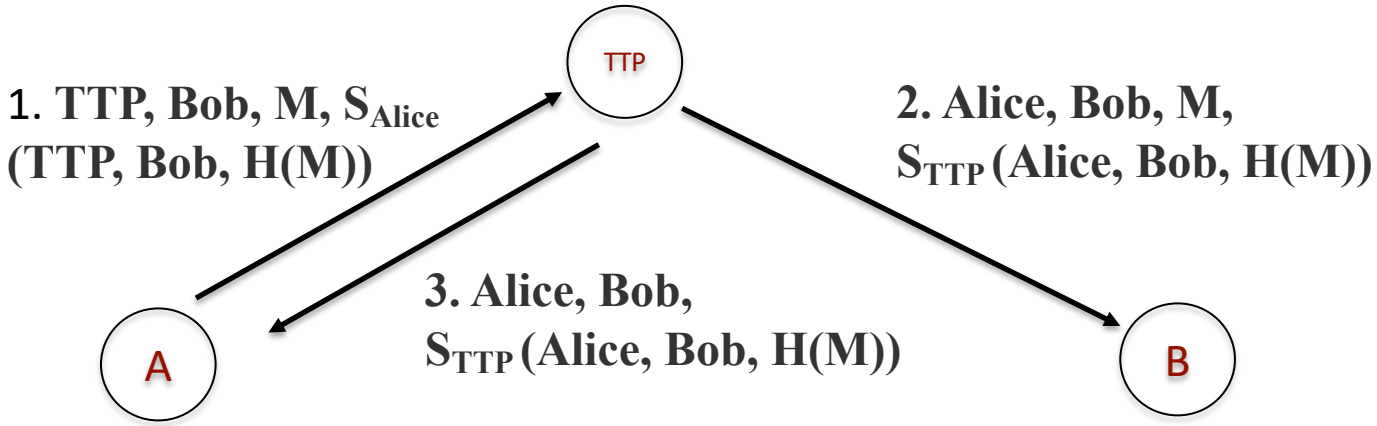
Ej. 5-(1-2)



Punto 1: el no repudio.

Punto 2: sí, en ambos lados.

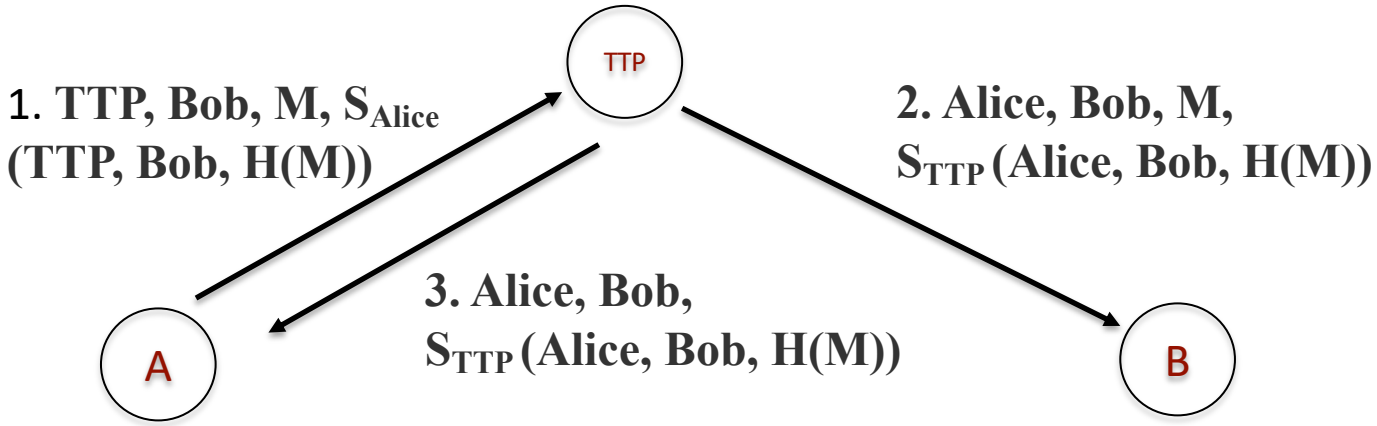
Ej. 5-(1-2)



Punto 1: el no repudio.

Punto 2: no, en todos los lados. TTP le falta la prueba de recibo por parte de B.

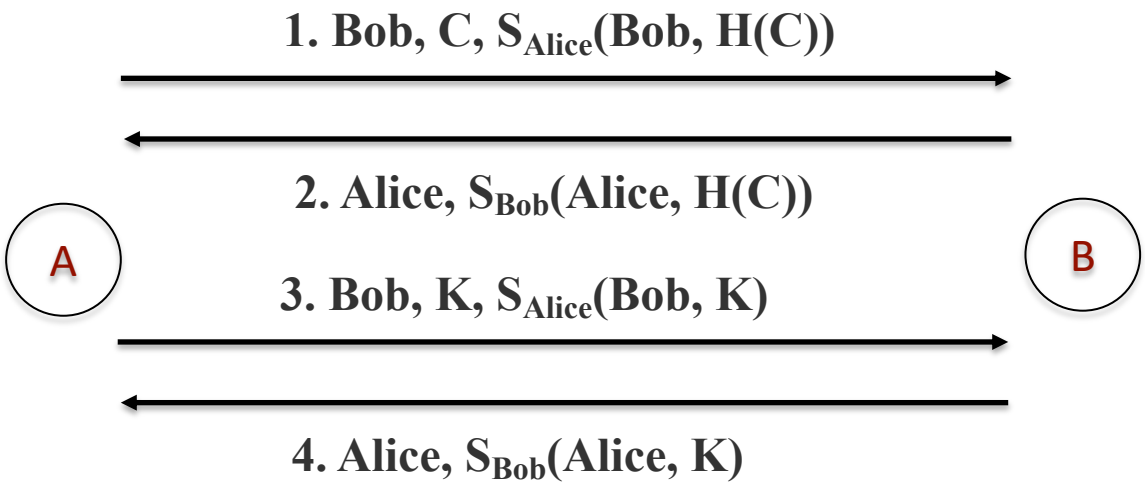
Ej. 6-(1-2)



Punto 1: el no repudio.

Punto 2: no, en todos los lados. TTP le falta la prueba de recibo por parte de B.

Ej. 7-(1-2)



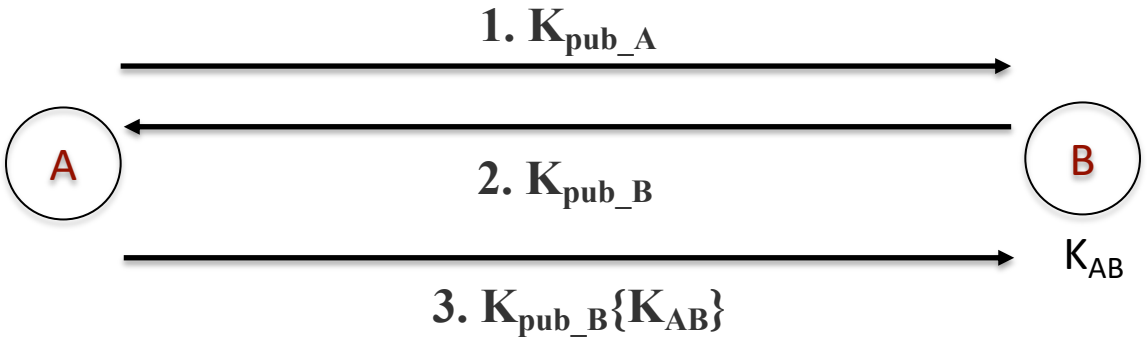
Punto 1: C es el criptograma de un mensaje cifrado por A, y K es la clave de sesión por la cual se cifro el mensaje original y está asociado al C.

Punto 2: no repudio.

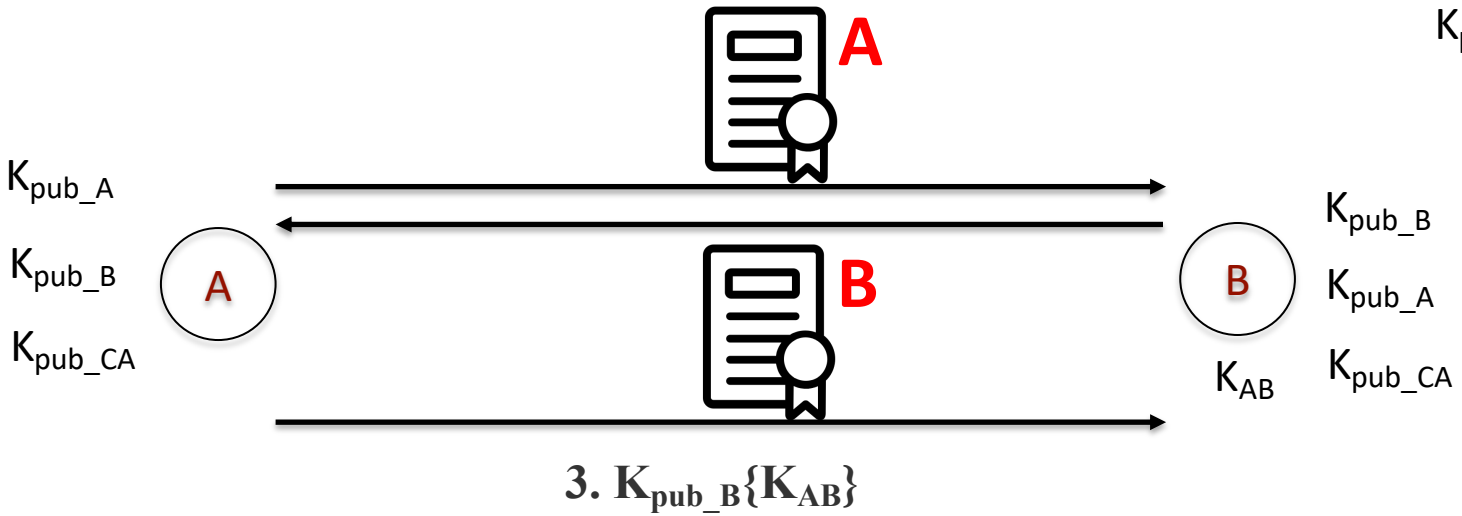
Punto 3: porque la clave de sesión es ya por sí misma pequeña.

Relación de ejercicios

Ej. 8-(1-2)



Punto 1: usando certificados.



Relación de ejercicios

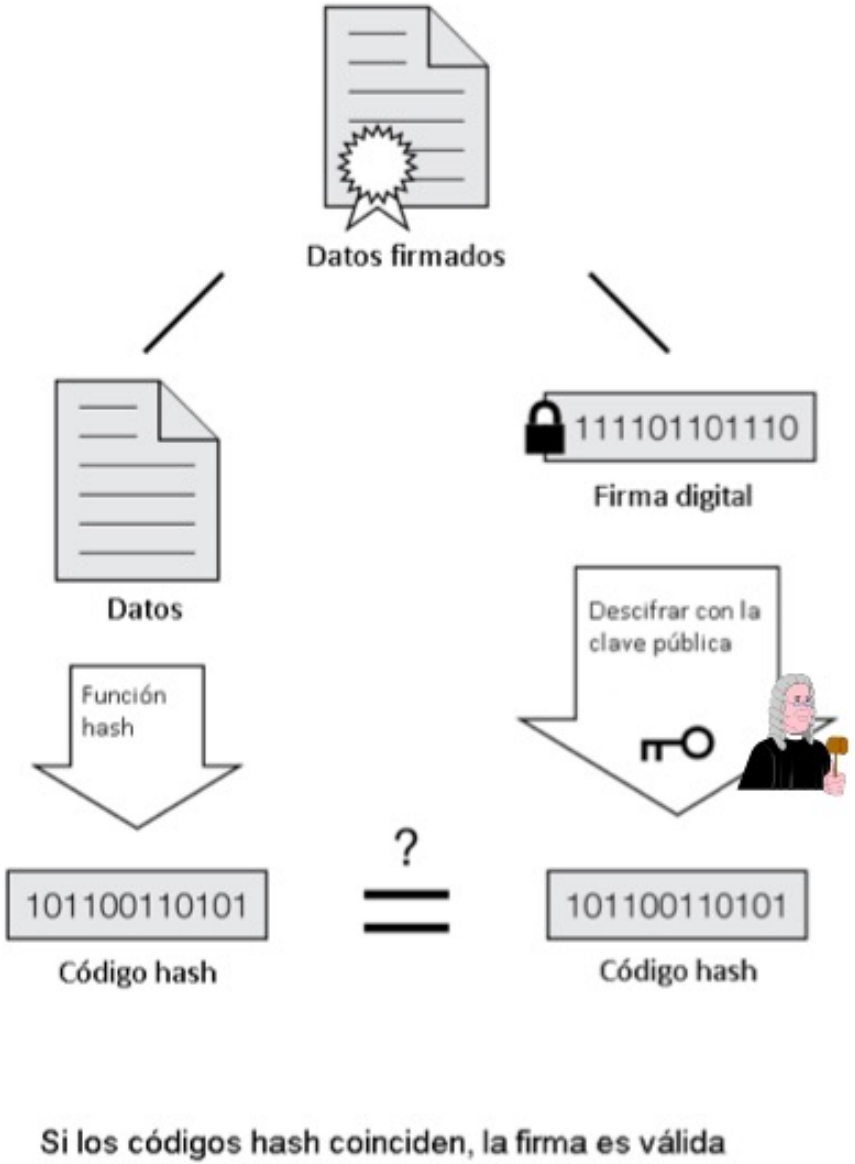
Ej. 8-(1-2)

Punto 2: verificar la firma de la CA:

1) A cuando recibe el certificado aplica un proceso de verificación, Equivalente a ➔

2) Extrae la clave K_{pub_B}

3) Opera como siempre



Ej. 9-(1-2)

Punto 1: sí, siempre y cuando tenga alguna forma de conseguir la clave pública de CA2 (ej. a través de un servidor público, etc.). Sin embargo, si A no conoce a CA2 puede que "no confíe" en el $Cert_{B\_CA2}$

Punto 2: sí, por cualquier medio sería posible. Son claves públicas.

Sin embargo, una forma de que A pueda "confiar" en CA2 sería que tanto $Cert_{B\_CA1}$ y $Cert_{B\_CA2}$ sean certificados por una CA común a CA1 y CA2, creando una **cadena de confianza**

$Cert_{B\_CA3}$ → $Cert_{B\_CA1}$ → A

$Cert_{B\_CA3}$ → $Cert_{B\_CA2}$ → B