1) DIFFIE-HELLMAN

a)

Sicuramente la risposta giusta è "B. $q=5$ $\alpha=2$" perchè "q" deve essere primo mentre "α" deve essere radice primitiva di "q".

b) Se $Y_A=1$ è la chiave pubblica di A, trovare la Key privata di A

$q=5$ $\alpha=2$ $Y_A=1$

$$Y_A = \alpha^{X_A} \bmod q \rightarrow 1 = 2^4 \bmod 5 \rightarrow X_A=4$$

c) Se $Y_B=3$ è la chiave pubblica di B, trovare shared Key K

$$K = Y_B^{X_A} \bmod q \rightarrow 3^4 \bmod 5 = 1 \rightarrow K=1$$

2)

(a) C

(c) E, G

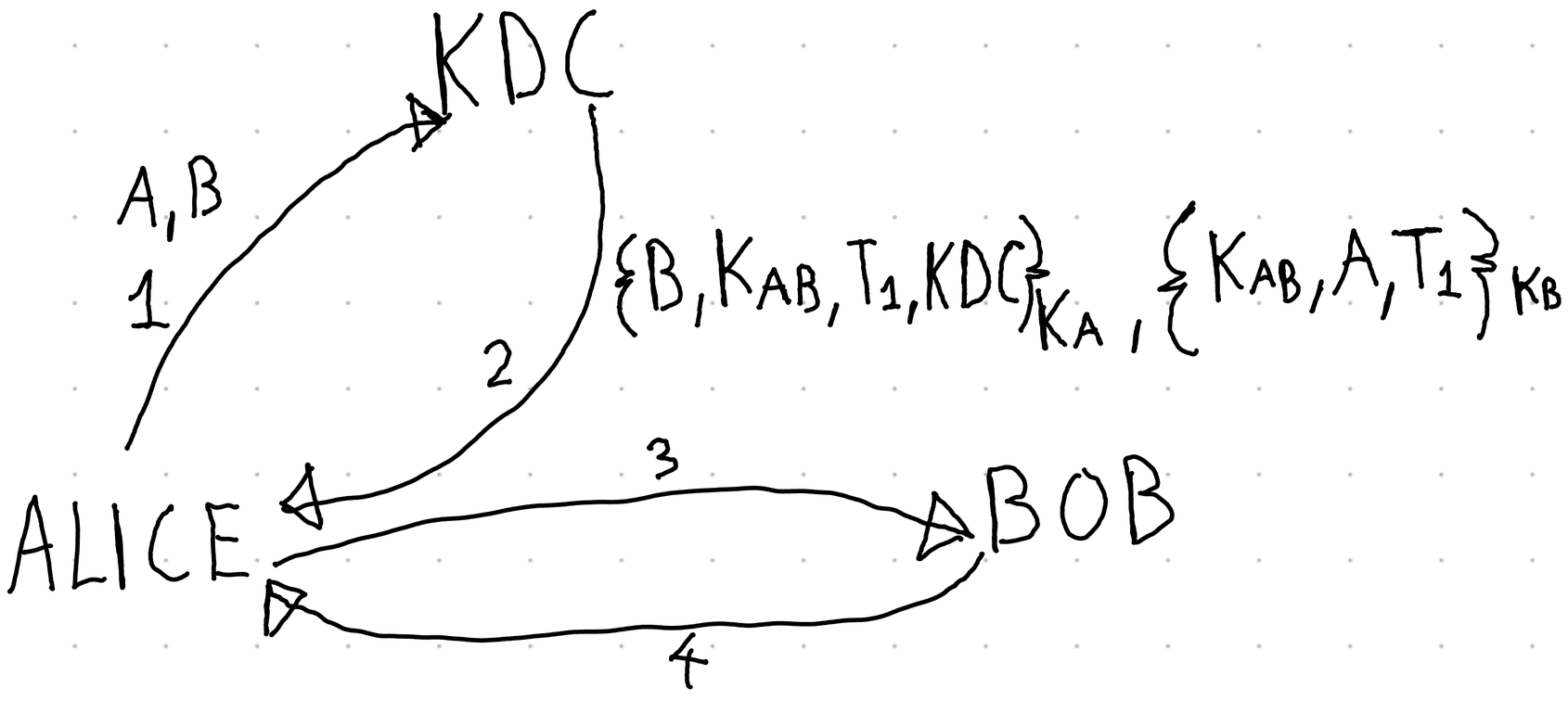
3) SECURITY PROTOCOLS

1)

Il secondo protocollo non è sicuro perché può essere vittima di attacchi man-in-the-middle, infatti se si utilizza solo K_A che è una chiave pubblica, Alice non può essere sicura della autenticità, infatti così facendo non gli viene garantita l'autenticità di KDC.

2)

Per ovviare il problema io utilizzerei il protocollo a chiave pubblica che garantisce sia segretezza che autenticità.

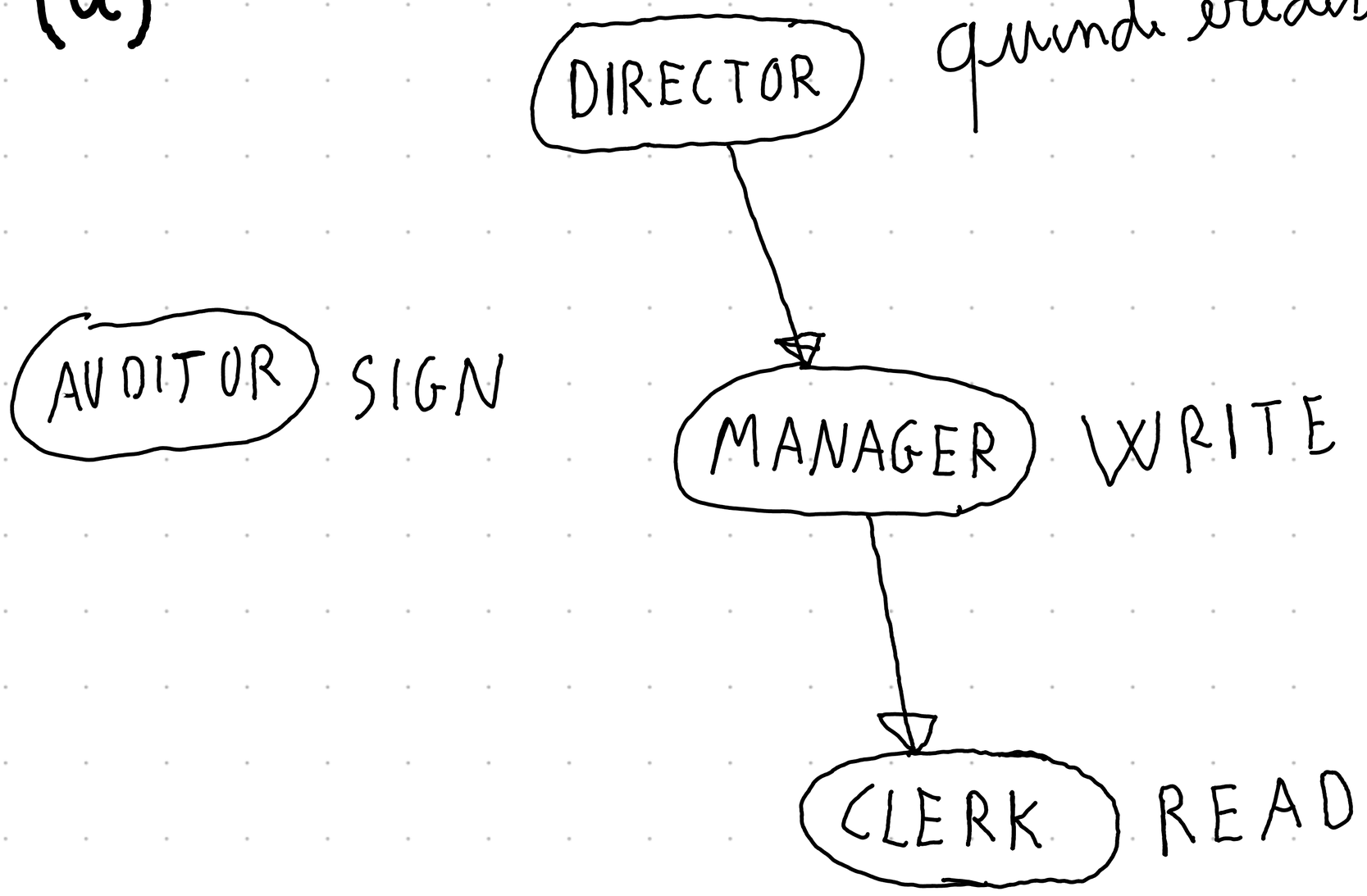


(REPLAY ATTACK SOLO SE ABBIAMO SOLO TIME

SLIDE 44)

4)

(a)



A David has permission to READ

(b)

Basta aggiungere nella tabella "Permission Assignment"

DIRECTOR	SIGN