Esercizio

- Si consideri il seguente protocollo di distribuzione chiavi a chiave pubblica

- A conosce la chiave pubblica di B, e_B

- A genera la chiave K_{AB} e la cifra con e_B

- A si autentica presso B usando la password P_A sul canale sicuro garantito da K_{AB}. A non invia P_A ma un suo digest

- La freschezza di tutti i messaggi è garantita per mezzo di *nonce* (numeri random).