Esercizio 1
Descrivere e confrontare le implementazioni e l'output di Proverif per il protocollo di Denning Sacco e per la sua versione corretta.

Esercizio 2
Implementare la cifratura ibrida con l'obiettivo di permettere lo scambio di una chiave condivisa attraverso l'utilizzo della cifratura asimmetrica.

Gli step da implementare sono i seguenti:

- Alice sceglierà una chiave K e utilizzerà la chiave pubblica di Bob per inviare K a Bob.

- Bob utilizzerà la cifratura simmetrica inviando un messaggio ad Alice cifrato con chiave K.

Obiettivi

1. *Implementare il protocollo descritto*
2. *Verificare con ProVerif eventuali criticità di sicurezza.*

3. *Implementare il protocollo corretto.*

Esercizio 3
Implementare il protocollo formato dai seguenti messaggi
A→ B: {N1}pk(B)
A→ B: {N2}pk(B)
B→ A: {x}pk(A) dove x=N1 oppure x=N2
A->B: s se A ha ricevuto cifrati attraverso la propria chiave
pubblica sia N1 che N2

Per semplicità si consideri il protocollo con soli due partecipanti A e B.
Verificare con Proverif se *s* risulta segreto. Motivare la risposta.