**I due corrispondenti sono A e B.**

**L’eventuale intruso è X.**

**A mette nel file KEYSCAMB i dati necessari, cifra keyscamb con una chiave qualsiasi Y e invia a B il file cifrato e Y.**

**B verifica il NIDE con A e se ok decifra keyscamb con la chiave Y, quindi crea la chiave KB, mette i suoi dati su keyscamb, lo cifra con Y e invia ad A il file cifrato.**

**A verifica il NIDE con B e se ok decifra keyscamb con la chiave Y, quindi crea la chiave **KA=KB****

**Ora vediamo cosa potrebbe fare X.**

**Intercetta la chiave Y e keyscamb spedito da A.**

**Può decifrarlo e creare una chiave KX, mettere i suoi dati su keyscamb,**

**cifrarlo con Y e, ipotizziamo che possa sostituire col suo keyscamb quello inviato da B ad A e voglia così sostituirsi a B.**

**Ma non riesce nel suo intento perchè una volta che A e B avranno verificato che i loro NIDE non corrispondono, scopriranno il tentativo di intrusione. Infatti X ha sì sostituito keyscamb, ma il NIDE del suo keyscamb non può essere uguale a quello di B.**