**The two correspondents are A and B.**

**The possible intruder is X.**

**A puts the necessary data in the KEYSCAMB file, encrypts keyscamb with any key Y and sends the encrypted file to B and Y.**

**B verifies the NIDE with A and if ok decrypts keyscamb with the key Y, then creates the key KB, puts its data on keyscamb, encrypts it with Y and sends the encrypted file to A.**

**A verifies the NIDE with B and if it is ok, it decrypts the keyscamb with the key Y, then creates the key KA=KB**

**Now let's see what X could do.**

**It intercepts the key Y and the keyscamb sent by A.**

**It can decrypt it and create a key KX, put its data on the keyscamb,**

**encrypt it with Y and, let's suppose that it can replace the keyscamb sent by B to A with its own keyscamb and thus wants to replace B.**

**But it fails in its intent because once A and B have verified that their NIDEs do not match, they will discover the attempted intrusion. In fact, X has replaced the keyscamb, but the NIDE of its keyscamb cannot be the same as that of B.**