**Section 2**

{ Nonce 5 }Friend 2

{ Agent (Friend 2)}

Friend 8

Friend 2

**Section 3**

{ Nonce 5 }Friend 2

{ Agent (Friend 2)}

Friend 8

Friend 2

{ Agent (Friend 2)}

{ Nonce 5 }Friend 2

This sequence violates the protocol as the Nonce sent by Friend 8 on the second communication has already being used. You could do similar with a third party asking Friend 8 for the Nonce and Friend 8 returning an already used Nonce as well.

**Section 4**

Friend 8

Adversary

**F**

{ Nonce 5 }Friend 2

Friend 2

{ Agent (Friend 2)}

{ Agent (Friend 2)}

{ Nonce 5 }Friend 2

From the first message the adversary intercepts, it learns the identity of Friend 2. From the second message, it learns the encrypted Nonce but has no way of decrypting it to learn the value of the Nonce. It can’t decrypt as it has no knowledge of Friend 2’s private key.

**Section 5**

The second message intercepted by the adversary contains the Nonce. But the Nonce is encrypted with Friend 2’s public key, this means it can only be decrypted with Friend 2’s private key. The adversary has no knowledge of Friend 2’s private key, therefore cannot decrypt the Nonce.

**Section 6**

With this type of spy, it is only able to read messages. This means it is able to learn the identity of an initiator A. The responder B, always encrypts the Nonce with A’s public key. This ensures that the Nonce can only be decrypted with A’s private key, which is never sent anywhere by A. Thus, even if a spy intercepts the message from B, it will only learn the encrypted Nonce and it has no way of decrypting it. Hence, the Nonce is never learnt by this kind of spy.

**Section 8**

{ Nonce 5 }Adversary

{ Agent (Adversary)}

{ Agent (Friend 2)}

Friend 2

Adversary

Friend 8

The adversary can intercept the message from Friend 2 and changes the content of the message to the adversary’s identity, this then means that Friend 8 encrypts the Nonce using the adversary’s public key. The adversary then decrypts the Nonce using its own private key – thus learning the Nonce.

**Section 9**

If A encrypts its identity message using B’s public key, this means that the Adversary will only intercept an encrypted version of A’s identity and be unaware of the format and contents of the message to be sent to B. It will also only obtain an encrypted version of the Nonce from B.