E4.44/ISE4.45/SO21 Network Security Problem Sheet 4

1. Fig 1 shows a protocol in which the identity of the server B is hidden from an attacker. Explain how an attacker could ascertain the identity of the client which initiates this transaction. How could this protocol be modified so that the identity of the client be hidden at the expense of the server? If A knows B's public key in advance of the transactioin how could the protocol be modified further so that both identities be modified further so that both identities are hidden from an attacker?
2. Which security features (privacy, integrity protection, repudiability, non-repudiability, source authentication) would be desirable in the following electronic mail messages:
    - submitting am expense claim
    - inviting a friend to lunch
    - selling illegal merchandise on the network
    - sending a purchase order, and
    - sending a message to the tax authorities about a neighbour's alleged tax evasion.

Figure 1