1. PGP provides for 1) privacy through encryption 2) authentication using signatures and 3) compression to reduce message size.
   (a) What is the order in which encryption, compression and compression are performed. (2 points)
   (b) Why? (4 points)

2. State true or false, and provide a brief explanation: (4 points)
   (a) Both PGP and TLS are intended for application layer authentication
   (b) Both TLS and PGP rely on PKI

3. Host A, with a private IP address is behind a NAT N. Host B (with a public IP address) is behind a firewall F. Now consider a scenario where Host A establishes a TCP connection with Host B. Assume that A, N, F and B are IPSec capable. Discuss at least four different combinations in which IPSec SAs can be bundled in this scenario. (10 points)