# 1 IPSec and IKE

## 1.1 Security Associations

- Describe all the security associations that are neccessary to allow a machine to sucessfuly ping another machine over an IPSec protected network.
- How many Diffie-Hellman operations have to be carried out to establish these associations?

## 1.2 Cookies and Nonces

IKE make use of cookies and nonces.

- Use the main mode exchange to explain the attacks that cookies and nonces should prevent.
- Are cookies and nonces still efficient if agressive mode is used?

## 1.3 IPSec Authentication

The following three methods of authentication are specified in IPSec:

- Pre-Shared Key: provide the same key to all parties
- Digital Signature: provide each party with the public key of the other
- Public Key Cryptography: provide each party with a certificate of its public key.

For each authentication method find a scenario where that particular method would be specially recommended.

## 1.4 PSK attack on IKE Main Mode

In the seminar we have seen an attack against IKE agressive mode with PSK authentication which allows a passive attacker to retrieve the preshared key just by listening to the exchange.

- Explain why this attack does not work with main mode.
- Modifiy the attack such that it works in main mode for an attacker located between the two parties. Describe the packets that are exchanged and the operations that are carried out.
- What should be done to prevent these attacks against the PSK.