Encapsulating Security Payload

Must support DES in CBC mode; may also support all the popular encryption algorithms

Key management

In establishing a SA, manual key distribution may be used

An automated system may be used: Oakley, based on Diffie-Hellman.

Internet Security Association and Key Management Protocol (ISAKMP) defines payloads for exchanging key generation and authentication data: many standard certificate types supported.

Email Security

- PEM: based on 7-bit mail. Kind-of dead.
- MOSS: extends PEM; very versatile, so possible to create totally incompatible mailers. Hmmm.
- PGP: Probably most widely used at present. Various versions, some free: complex issues. Author (Zimmermann) was prosecuted for exporting PGP; but case was dropped. Latest modification is GPG.
- S/MIME: Being pushed by a lot of the big players. It is a development of the ideas in PEM and MOSS.

PGP uses a web-of-trust; the others are largely ~~hierarchal~~. hierarchical.

Links: PGP: http://www.pgpi.org/http://www.pgpi.org/
S/MIME:
http://www.rsa.com/smime/html/faq.html http://www.rsa.com/smime/htm

{GNU Privacy Guard}

S/MIME and PGP: Encryption

- Both use very similar cryptographic techniques.
- Similar cryptographic strength
- S/MIME source is not public (in general)