Electronic Mail Security

- Authentication and confidentiality problems
- Two systems:
  - PGP (Pretty Good Privacy)
  - S/MIME (Science Multipurpose Internet Mail Extension).

- System utilization

S/MIME Industrial Standard for business utilization

PGB personal electronic mail

• Philip R. Zimmermann created the first version of PGP encryption in 1991.
• Shortly after its release, PGP encryption found its way outside the United States and in February 1993 Zimmermann became the formal target of a criminal investigation by the US Government for “munition export without a license".
• Cryptosystems using keys larger than 40 bits were then considered munitions within the definition of the US export without a license; PGP has never used keys smaller than 128 bits so it qualified at that time. Penalties for violation, if found guilty, were substantial. After several years, the investigation of Zimmermann was closed without filing criminal charges against him or anyone else.
•After the Federal criminal investigation ended in 1996, Zimmermann and his team started a company to produce new versions of PGP encryption.

PGP is based on:

• RSA, DSS, and Diffie- Helman algorithms for public key encryption and CAST-128, IDEA e TDEA algorithms for symmetric key encryption.

•SHA-1 for hash functions.

•PGP services:

- Authentication
- Confidentiality
- Compression
- E-mail compatibility
- Segmentation

Authentication (digital signature)

1. The sender creates a message
2. SHA-1 is used to generate a 160 bit hash code of the message
3. The hash code is encrypted with RSA using the sender's private key and the result is prepended to the message.
4. The receiver uses RSA with the sender's public key, to decrypt and recover the hash code.
5. The receiver generates a new hash code for the message and compares it with the decrypted hash code. If the two match, the message is accepted as authentic

Confidentiality

1. The sender generates a message and a random 128-bit number to be used as a session key for this message only. (one time key)

2. The message is encrypted, using a symmetric algorithm (CAST-128 or IDEA or 3DES) with the session key

3. The session key is encrypted with RSA, using the recipient's public key, and is prepended to the message

4. The receiver uses RSA with its private key to decrypt and recover the session key

5. The session key is used to decrypt the message.

Authentication and Confidentiality

The sender

- Signs the message with its private key

-Encrypts the message with the session key

-Encrypts the session key with the public key of the receiver

- **Compression**

A message may be compressed, for storage or transmission using ZIP

- **Email compatibility**

An encrypted message may be converted to an ASCII string using radix-e conversion

- **Segmentation**

To accomodate maximum message size limitations, PGP performs segmentation and reassembly