PGP - Pretty Good Privacy and Privacy Enhanced Mail (PEM)

PGP, Pretty Good Privacy, a program invented by Philip Zimmermann, is a popular method used to encrypt data. It uses MD5 (message-digest 5) and RSA cryptosystems to generate the key pairs. PGP is a popular program that can run on UNIX, DOS, and Macintosh platforms. It offers some variations of functionality, like compression, that other cryptosystems do not. Multiple key pairs can be generated and placed on public and private key rings.

What is PGP?

- PGP is Pretty Good Privacy, by Phil Zimmerman, an encryption program that uses the MD5, RSA and IDEA algorithms for data encryption and integrity checking. It can be used to encrypt, with very high security, a message or a binary file to someone, without having to exchange a set of private encryption keys before-hand.

Background

- No Privacy in Standard Internet E-mail.
- Message travels a number of sites before reaching the destination. Anyone can read the contents of the message.
- Cryptography provides secrecy so it could be applied to secure e-mails.
- Strong opposition from government to such a move.

What PGP Gives You

- PGP serves the following objectives:
  - **confidentiality of communication (secrecy)** with other people, in a way that prevents other people to read the message in plain text except of the intended addressee,
  - **reliability of the source of information** (authenticity), in a way that prevents someone to masquerade as the author of a message actually having been created by somebody else (protection of intellectual property),
  - you intend to guarantee the **integrity of a message**, in a way that a composed message cannot be changed accidentally or deliberately.

How PGP Works

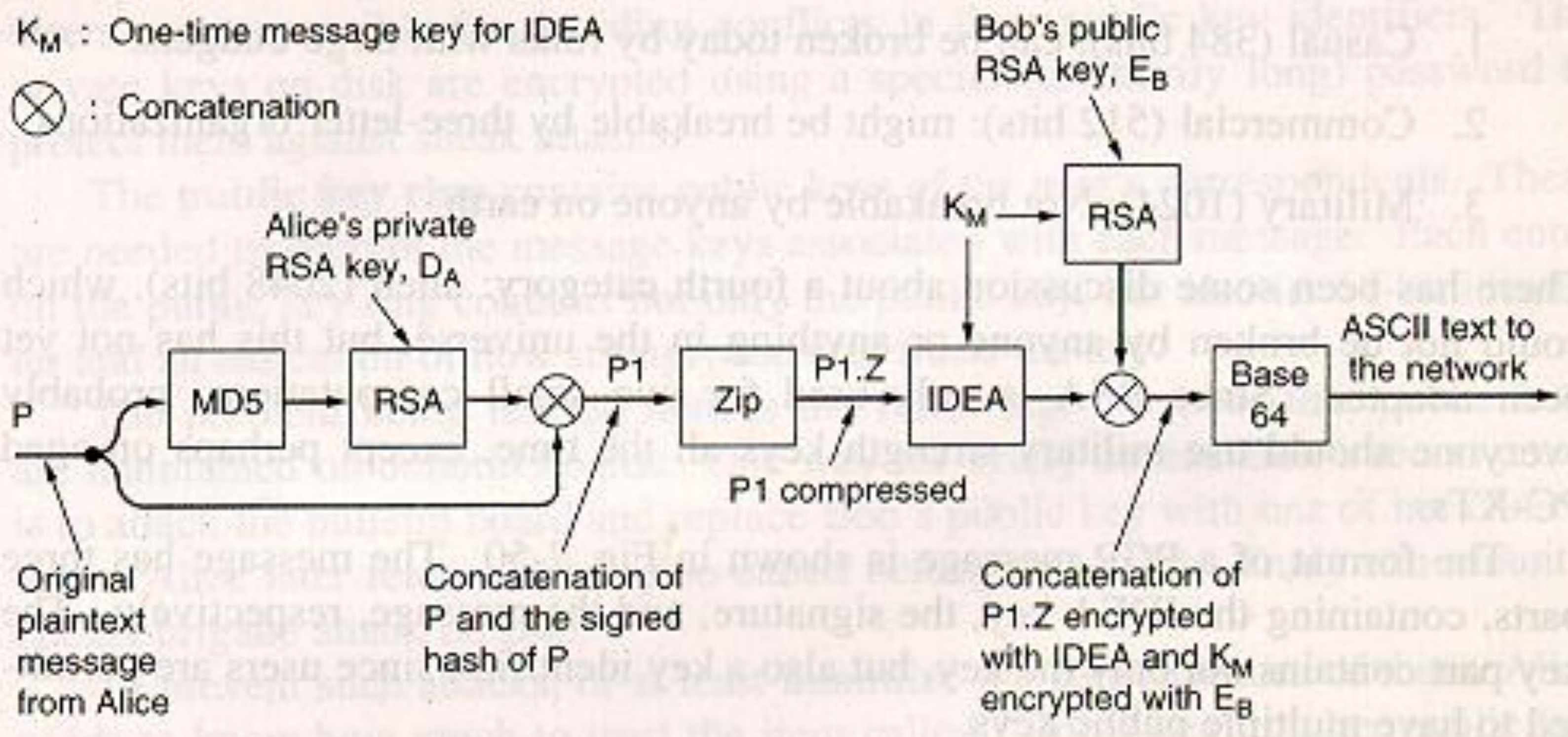
K_M : One-time message key for IDEA
⊗ : Concatenation
Bob's public RSA key, E_B
K_M
RSA
Alice's private RSA key, D_A
ASCII text to the network
P
MD5
RSA
P1
Zip
P1.Z
IDEA
Base 64
P1 compressed
Original plaintext message from Alice
Concatenation of P and the signed hash of P
Concatenation of P1.Z encrypted with IDEA and K_M encrypted with E_B

Fig. 7-49. PGP in operation for sending a message.

PGP Message Format

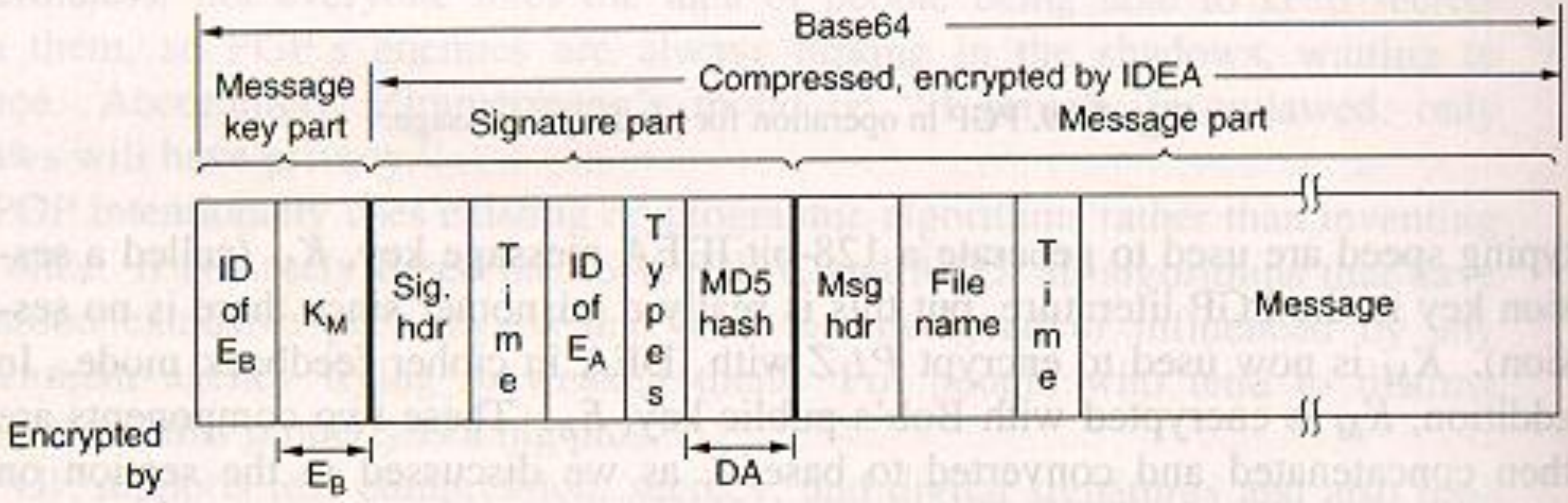

Fig. 7-50. A PGP message.

Alternatives to PGP

- PEM - Privacy Enhanced Email
- Defined in RFC 1421 through 1424
- Official Internet Standard

What are secure messages?

- As more and more people send confidential information via e-mail, it is becoming increasingly important to know that your messages cannot be intercepted and read by anyone other than the intended recipient. It is equally important to know that documents sent by e-mail such as checks and credit cards cannot be forged.
- By using "digital IDs" with Outlook Express, you can prove your identity in electronic transactions, similar to showing your driver’s license when you cash a check. You can also use your digital ID to encrypt messages to keep them private. Digital IDs incorporate the S/MIME specification for secure electronic mail.

How do digital IDs work?

- ⌘ A digital ID is composed of a "public key," a "private key," and a "digital signature." When you send your digital ID to others, you are actually giving them your public key, so they can send you encrypted mail which only you can decrypt and read with your private key.
- ⌘ The digital signature component of a digital ID is your electronic identity card. The digital signature tells the message recipient that the message actually came from you and has neither been forged nor tampered with.
- ⌘ Before you can start sending encrypted or digitally signed messages, you must obtain a digital ID and set up your mail account to use it. If you are sending encrypted messages, your address book must contain a digital ID for the recipient.

Where do you get digital IDs?

- Digital IDs are issued by an independent certifying authority. When you apply for a digital ID from a certifying authority's Web site, they have a process to verify your identity before issuing an ID. There are different classes of digital IDs, each one providing a different level of credibility. For more information, use the Help at the certifying authority's Web site.
- To get someone else's digital ID, they can send you digitally signed mail (which will include their ID); you can search through the database on a certifying authority's Web site; some directory services also list digital IDs along with other properties.

Advanced security information

- Outlook Express is compatible with the S/MIME version 2 specification. Outlook Express supports the following encryption algorithms: RC2 (40-bit and 128-bit), DES (56-bit), and 3DES (168-bit). The RC2 40-bit encryption algorithm is the only algorithm available on non-U.S./Canadian versions of Outlook Express. Outlook Express can decrypt 3DES (168-bit) and RC2 (64-bit) encrypted mail, but cannot send messages using these algorithms.
- Outlook Express uses SHA-1 as the hashing algorithm when signing messages. The bit length of your private key varies, depending on the certifying authority from which you obtain it. A certifying authority that uses the Microsoft Enrollment wizard will generate private keys that are at least 512 bits in length.
- The private keys are stored on your computer and are only as secure as your computer. Private keys installed using Microsoft cryptographic system components will not be transmitted to the certifying authority which issues the digital ID; the keys are not stored in escrow with any government agency.