4.1 PRETTY GOOD PRIVACY

PGP provides a confidentiality and authentication service that can be used for electronic mail and file storage applications.

In essence, Zimmermann has done the following:

1. Selected the best available cryptographic algorithms as building blocks.
2. Integrated these algorithms into a general-purpose application that is independent of operating system and processor.
3. Made the package and its documentation, including the source code, freely available via the Internet.
4. Entered into an agreement with a company to provide a fully compatible, low-cost commercial version of PGP.

PGP has grown explosively and is now widely used. A number of reasons can be cited for this growth:

1. It is available free worldwide in versions that run on a variety of platforms.
2. It is based on algorithms that are extremely secure.
3. It has a wide range of applicability.
4. It was not developed by, nor is it controlled by, any governmental or standards organization
5. PGP is now on an Internet standards track.

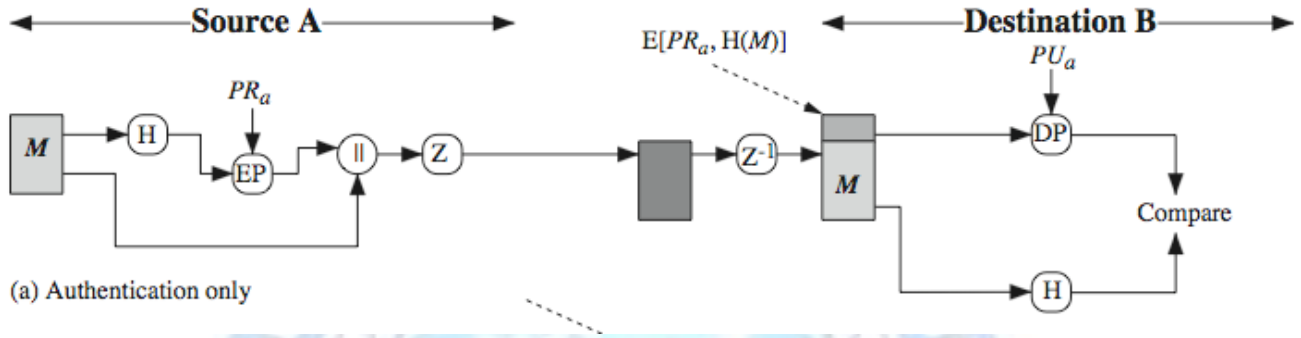
Operational Description

(i) Authentication
(ii) Confidentiality
(iii) Compression
(iv) E-Mail compatibility
(v) Segmentation

(i) Authentication

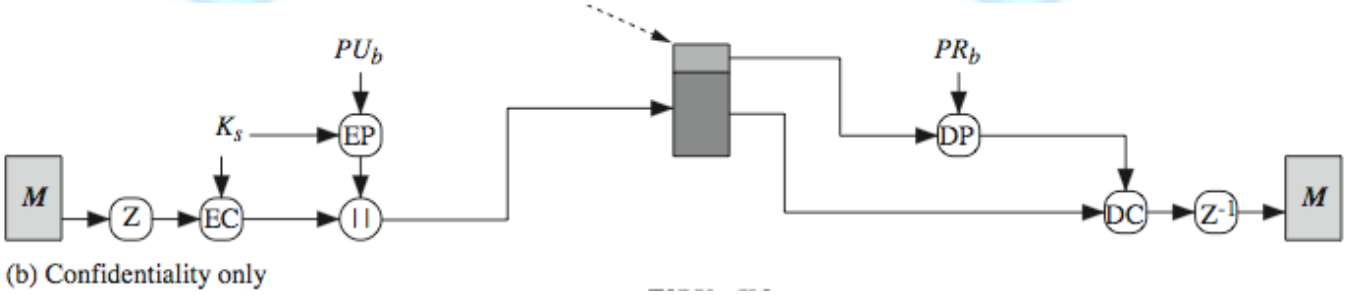
- The sender creates a message.
- SHA-1 is used to generate a 160-bit hash code of the message.
- The hash code is encrypted with RSA using the sender's private key, and the result is prepended to the message.

- The receiver uses RSA with the sender's public key to decrypt and recover the hash code.
- 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.



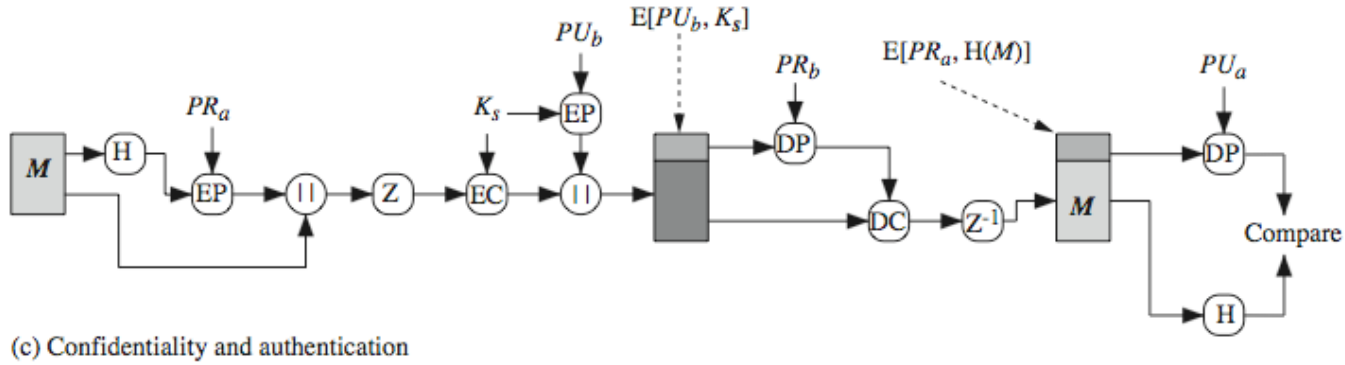
(ii) Confidentiality

- The sender generates a message and a random 128-bit number to be used as a session key for this message only.
- The message is encrypted, using CAST-128 (or IDEA or 3DES) with the session key.
- The session key is encrypted with RSA, using the recipient's public key, and is prepended to the message.
- The receiver uses RSA with its private key to decrypt and recover the session key.
- The session key is used to decrypt the message.



(iii) Confidentiality and Authentication

When both services are used, the sender first signs the message with its own private key, then encrypts the message with a session key, and then encrypts the session key with the recipient's public key.



(c) Confidentiality and authentication

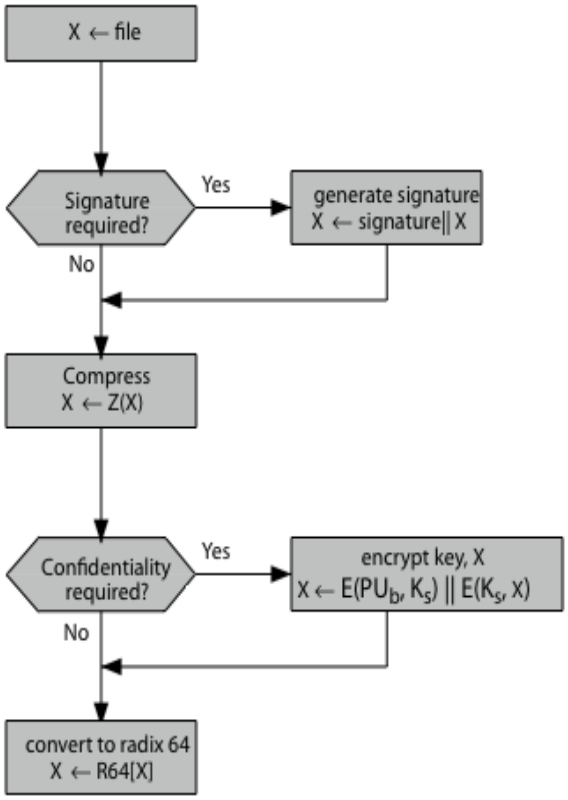
(iv) Compression

PGP compresses the message after applying the signature but before encryption. The compression algorithm is indicated by Z for compression and Z^{-1} for decompression. The signature is generated before compression for two reasons:

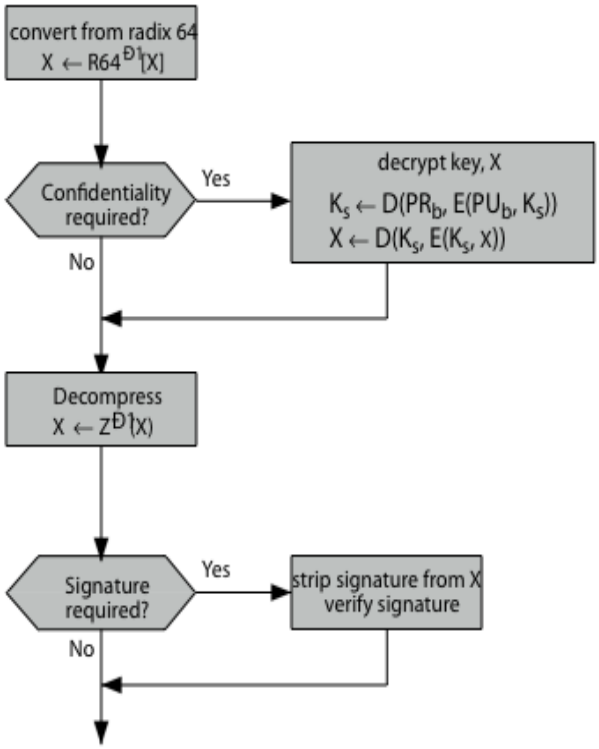
a) It is preferable to sign an uncompressed message so that one can store only the uncompressed message together with the signature for future verification.

b) Even if one were willing to generate dynamically a recompressed message for verification, PGP's compression algorithm presents a difficulty. The algorithm is not deterministic.

c) Message encryption is applied after compression to strengthen cryptographic security. Because the compressed message has less redundancy than the original plaintext, cryptanalysis is more difficult.



(a) Generic Transmission Diagram (from A)



(b) Generic Reception Diagram (to B)

v) E-mail Compatibility

When PGP is used, at least part of the block to be transmitted is encrypted. PGP provides the service of converting the raw 8-bit binary stream to a stream of printable ASCII. For this PGP using radix- 64 conversion. Each group of 3 octets of binary data is mapped in to 4 ASCII characters. The uses of radix 64 expands a message by 33%

(vi) Segmentation and reassembly

Any message longer than that must be broken up into smaller segments, each of which is mailed separately. At the receiving end, the PGP must strip off all e-mail header and retrieve the essential block. The header is separated from the body by a blank line, a header line consists of a keyword, followed by a colon followed by keyword's arguments.

Date:

From: To: Subject: