

Electronic Mail Security

Two schemes used for email security:-

↳ PGP (Pretty Good Privacy)

↳ S/MIME (Secure/Multipurpose Internet Mail Extension)

PGP

PGP is mainly used for personal email security. It is an effort of a single person Phil Zimmermann. PGP provides confidentiality and authentication service that can be used for email and file storage applications.

Features:-

- 1) Uses best cryptographic mechanisms, includes RSA, DSS and DH for public key encryption, CAST-128, IDEA and 3DES for symmetric encryption, SHA-1 for hash coding.
- 2) Available free world wide via the Internet.
- 3) Platform independent
- 4) Low-cost

5) It was not developed by , nor is it controlled by government or standard organization.

6). PGP is ^{now} an Internet standard RFC3156.

Operational Description

5 Services of PGP :-

1. Authentication
2. Confidentiality
3. Compression
4. Email compatibility
5. Segmentation.

Authentication

The digital signature service provided by PGP is :-

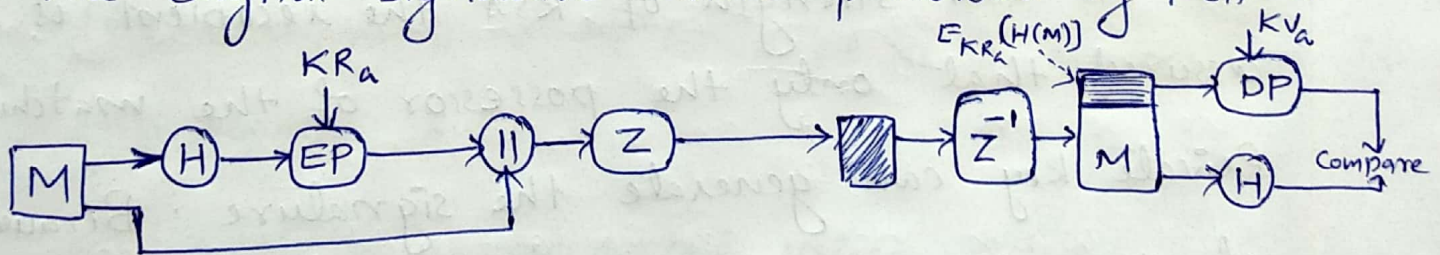


Fig:- PGP. authentication only .

where-

M - Plaintext Message

H - Hash function

EP - Public key encryption

DP - Public key decryption

KR_a - Private key of user A

KV_a - public key of user A

\parallel - Concatenation

Z - Compression using ZIP algo

Z^{-1} - Inverse Compression

Sequence is

1. 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 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.

Here the combination of SHA-1 and RSA provides an effective digital signature scheme.

Due to the strength of RSA the recipient is assured that only the possessor of the matching Private key can generate the signature. Because of the strength of SHA-1 the recipient is assured that no one else could generate a new message that matches the hash code and hence the signature of the original message.

2. Confidentiality

In PGP Confidentiality is provided by encrypting message to be transmitted or to be stored locally as files.

Confidentiality service provided by PGP:-

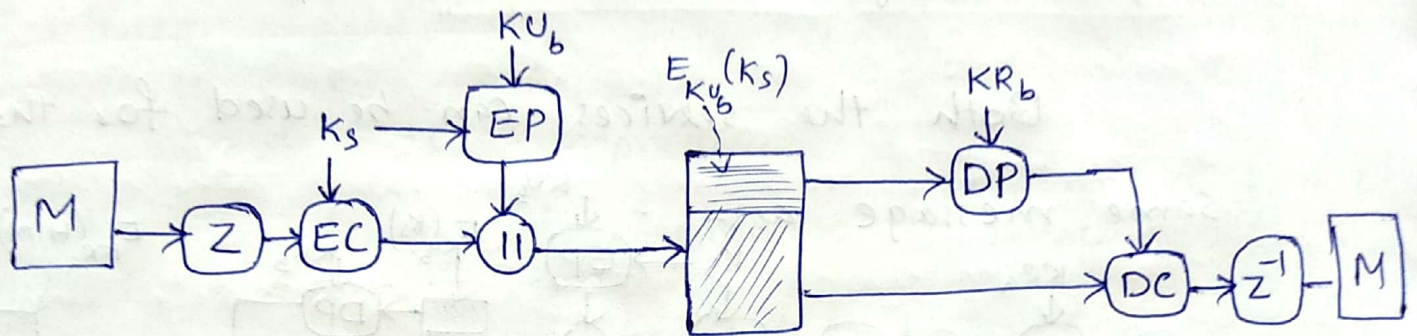


Fig: PGP Confidentiality only.

where :- EC - Symmetric Encryption

DC - Symmetric Decryption

K_s - Session key used in Symmetric Encryption algo.

The sequence is :-

1. The sender generates a message and a random 128-bit number to be used as a session key for this message only.
2. The message is encrypted using 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.

Confidentiality and Authentication

Both the services can be used for the

same message as:-

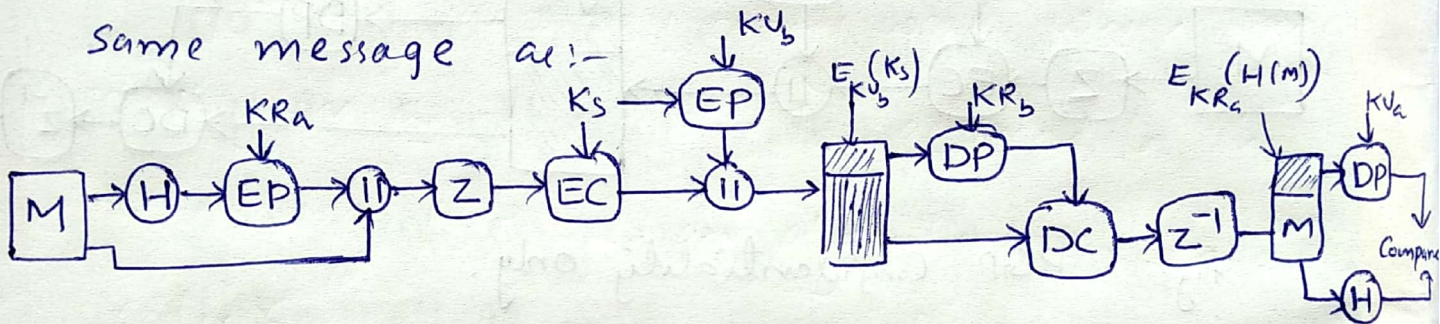


Fig- Confidentiality & authentication in PGP.

Here first a signature is generated for the Plaintext message and prepended to the message then the plaintext message plus signature is encrypted using CAST-128 (or IDEA or 3DES) and the session key is encrypted using RSA.

ie when both services are used, the sender first sign 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.

mission and for file storage. Compression algo used in pcap is **ZIP**.

z - indicates compression
 z^{-1} - indicates decompression

} placement of z and z^{-1} in algo is critical:-

* ① The signature is generated before compression for two reasons:-

a) It is preferable to sign an uncompressed message so it is free of the need for a compression algorithm for later verification.

5) Different version of PGP produce different compressed forms. Applying the hash function and signature after compression would constrain all PGP implementations to the same version of the compressed algorithm.

② Message encryption is applied after compression to strengthen cryptographic security. Because the compressed message has less redundancy than the original plaintext, cryptanalysis is difficult.

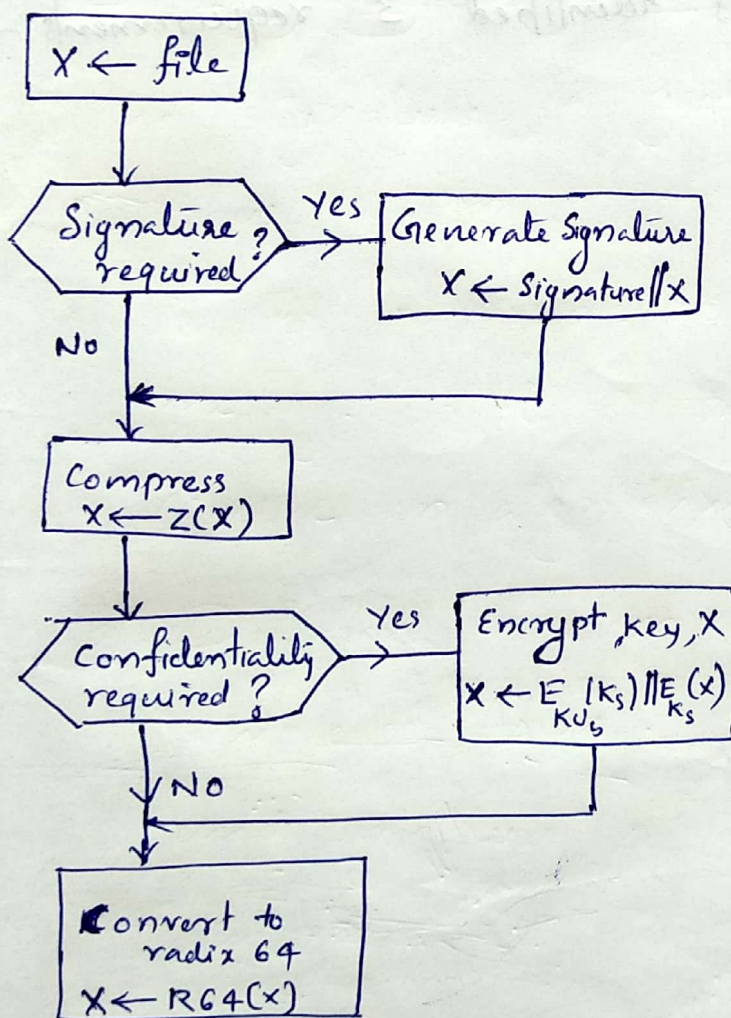
4. Email Compatibility

Many electronic mail systems only permit the use of blocks consisting of ASCII text. When PGP is used, at least part of the block to be transmitted is encrypted. This basically produces a sequence of arbitrary binary words which some mail systems won't accept. To accommodate this restriction PGP uses an algorithm known as radix 64 which maps 6 bits of binary data into 8 bit ASCII character. Unfortunately this expands the message by 33% however with the compression algorithm overall compression will be about one third.

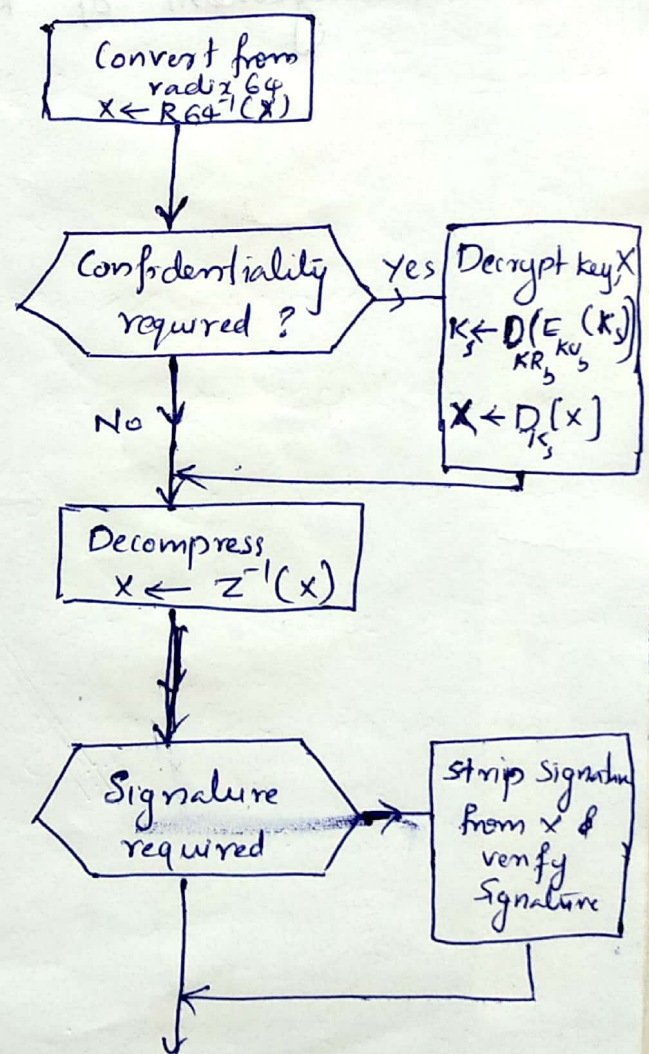
5. Segmentation

Email facilities are often restricted to a maximum message length. For example, many of the facilities accessible throughout the internet impose a maximal length of 50,000 octets. Any msg longer than that must be broken up into smaller segments, each of which is mailed separately.

To accommodate this restriction, PGP automatically subdivides a message that is too large into segments that are small enough to send via e-mail. The segmentation is done after all of the other processing including the radix-64 conversion, which is illustrated as follows:



(a) Transmission diagram (from A)



b) Reception diagram (to B)

Fig.- Transmission & Reception of PGP messages.