Date.....

Sol

Pretty Good privacy (PGP) :-

- PGP stands for pretty good privacy (PGP) which is invented by Phil Zimmermann.
- PGP was designed to provide all four aspects of security, i.e privacy, integrity, authentication, and non-repudiation in the sending of email.
- It uses a digital signature (a combination of hasing and public key encryption) to provide integrity authentication, and non-repudiation.

It is an open source and freely available software package for email security.

It provides authentication through the use of Digital Signature.

- It provides compression by using the ZIP algorithm, and Email compatibility using the radix-64 encoding scheme.

Date.....

- It provides confidentially through the use of Symmetric block encryption.
- The Secret key is encrypted by using a receiver's public key.
- The e-maid message is hashed by using a hashing function to create a digest.
- PGP ~~is~~ uses a combination of Secretkey encryption and public key encryption to provide privacy. Therefore, we can Say that the digital Signature use one hash function, one Secret key, and two private - public key pairs.