Ans → 3.

PGP. (Pretty Good Privacy):

PGP stands for Pretty Good Privacy (PGP) which is invented by "Zimmermann". PGP was designed to provide all four aspects of security, i.e. privacy, integrity, authentication, and non-repudiation in sending of email.

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

PGP 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.

Following are the steps taken by PGP to Create Secure e-mail at the sender site:-

* The Email massage is hashed by using a hashing function to create a digest.

* The digest is then encrypted to form a signed digits by using the sender's private key. and then signed digest is added to original email message.
* original message and signed digest are encrypted by using a one-time secret key created by sender.
* Secret key is encrypted by using a receiver's public key.
* Both the encrypted secret key and the encrypted combination of message and digest are sent together.