

Ques-3:-1

Pretty Good Privacy (PGP)

→ PGP is a popular program used to encrypt and decrypt email over the internet as well as ~~well~~ authenticates Messages with digital signatures and Encrypted Stored files.

Steps taken by PGP to create secure e-mail

→ The Email message is hashed by using a hashing function to create a digest.

→ The digest in the encryption to form a signed digest by using the sender's private key.

→ The original message and signed digest are encrypted by using a one-time secret key create by sender.

Date: / /

- The Secret key encrypted by using a receiver's public key.
- Both the encrypted Secret key and the encrypted combination of message and digest are sent together.