**Pretty Good Privacy** (qu'on pourrait traduire en français assez bon niveau de confidentialité), plus connu sous le sigle PGP, est un logiciel de chiffrement cryptographique, développé et diffusé aux États-Unis par Philip Zimmermann en 1991.

**PGP** se propose de garantir la **confidentialité** et **l'authentification** pour la communication des données. Il est souvent utilisé pour la **signature** de données, le chiffrement et le déchiffrement des textes, des **courriels**, **fichiers**, **répertoires** et **partitions de disque** entier pour accroître la sécurité des communications par courriel. Utilisant la cryptographie asymétrique mais également la cryptographie symétrique, il fait partie des logiciels de cryptographie hybride.

**PGP** et les produits similaires suivent **le standard OpenPGP** pour le chiffrement et le déchiffrement de données.

Avec PGP, il est possible de vérifier si un message provient bien de l'origine (via les signatures cryptographiques), ainsi que de chiffrer des messages afin qu'un seul destinataire puisse les lire. En bref, **chaque utilisateur** crée une paire de **clés de chiffrement asymétriques** (une publique, l'autre privée), et distribue la clé publique. Les signatures effectuées avec la clé privée peuvent être vérifiées en utilisant la clé publique correspondante et les messages chiffrés utilisant la clé publique sont déchiffrables en utilisant la clé privée correspondante.

PGP offre des services d'authentification, de confidentialité, de compression et de segmentation, tout en étant compatible avec de nombreux systèmes de messagerie électronique :

* **authentification** : l'expéditeur crée un condensat de son message , chiffre ce condensat avec sa clé privée et l'ajoute en début de message. Le destinataire déchiffre l'ajout en début de message avec la clé publique de l'émetteur et en extrait le condensat. ​Le couple clé publique/clé privée peut être fourni par RSA ou DSA ;
* **confidentialité** : génération d'une clé secrète nommée clé de session, valable pour un seul fichier ou un seul message. Le message ou le fichier est chiffré au moyen de cette clé de session avec un algorithme de cryptographie symétrique. Pour que la sécurité de l'échange soit plus sûre il ne faudrait pas utiliser le chiffrement sans authentification ;
* **compression** : utilisation de ZIP appliqué après la signature mais avant le chiffrement ;
* **compatibilité** : comme certains systèmes de messagerie ne permettent l'utilisation que du format ASCII, PGP contourne cette limitation en convertissant chaque flot binaire de 8 bits en caractères ASCII imprimables ;
* **segmentation** et **ré-assemblage** : pour outrepasser certaines contraintes (taille maximum des messages), après tous les traitements précédents PGP peut tronçonner le message original en segments de taille fixe. L'en-tête contenant la clé secrète ne sera positionnée que dans le premier segment. Le destinataire met en mémoire la clé secrète, récupère tous les segments, en retire les en-têtes inutiles, ré-assemble le message avant de le déchiffrer, le décompresser et vérifier sa signature.

En juin 2010, la société PGP Corporation a été acquise par Symantec. Symantec n'offre plus de version gratuite du logiciel.

**GnuPG** (ou **GPG**, de l'anglais GNU Privacy Guard) est l'implémentation GNU du standard OpenPGP, distribuée selon les termes de la licence publique générale GNU.

Ce logiciel permet la transmission de messages électroniques **signés** et **chiffrés**, garantissant ainsi leur **authenticité**, **intégrité** et **confidentialité**.