This how GPG works

As of versions 2.0.26 and 1.4.18, GnuPG supports the following algorithms:

- Pubkey: RSA, ElGamal, DSA
- Cipher: IDEA (since versions 1.4.13 and 2.0.20), 3DES, CAST5, Blowfish, AES-128, AES-192, AES-256, Twofish, Camellia-128, -192 and -256 (since versions 1.4.10 and 2.0.12)
- Hash: MD5, SHA-1, RIPEMD-160, SHA-256, SHA-384, SHA-512, SHA-224
- Compression: Uncompressed, ZIP, ZLIB, BZIP2

More recent releases of GnuPG 2.x ("stable" and "modern" series) expose most cryptographic functions and algorithms Libgcrypt (its cryptographic library) provides, including support for elliptic curve cryptography (ECDSA, ECDH and EdDSA)[10] in the "modern" series (i.e. since GnuPG 2.1).

source *"GNU_Privacy_Guard"* on *Wikipedia*

Asymmetric encryption for key exchange

Should we use asymmetric encryption for key exchange?

- ✓ Simple solution for non-interactive protocol (e.g GPG)
- ◉ But not a good solution for interactive protocols