PGP Questions

1. I'm trying to import a RSA encryption master key in PGP Desktop version X and I can't use it for encryption. What can I do?

In later versions of PGP Desktop a master key is always considered to be a signing only key, regardless of the algorithm, unless there is a KeyFlags subpacket on its certification that says otherwise.

In the case of a BC created key this means you need something like:

```
PGPSignatureSubpacketGenerator    hashedGen = new PGPSignatureSubpacketGenerator();

hashedGen.setKeyFlags(true, KeyFlags.CERTIFY_OTHER | KeyFlags.SIGN_DATA
                          | KeyFlags.ENCRYPT_COMMS |
KeyFlags.ENCRYPT_STORAGE);
```

And then pass hashedGen.generate() to the keyring/secret key generator as the hashed subpackets argument.

Note: a master key must always be available for use as a signing key. For this reason it is generally better to add a subkey for use for encryption where possible.