

按照此结构，实现PGP方案

于是在代码中可以体现出:

在加密函数encrypt中：

我们随机产生密钥k

对data进行hash等操作后进行sm4对称加密。然后用sm2对k进行加密

拼接发送

在解密函数decrypt中：

按照顺序分开解密，验证公钥

最后结果为：



