Paillier私钥管理方案

该文档给出了用户对自身Paillier私钥管理的技术方案，主要思路是利用口令对私钥加密，再并将密文存储在本地，同时计算密文的mac值来验证私钥的完整性。

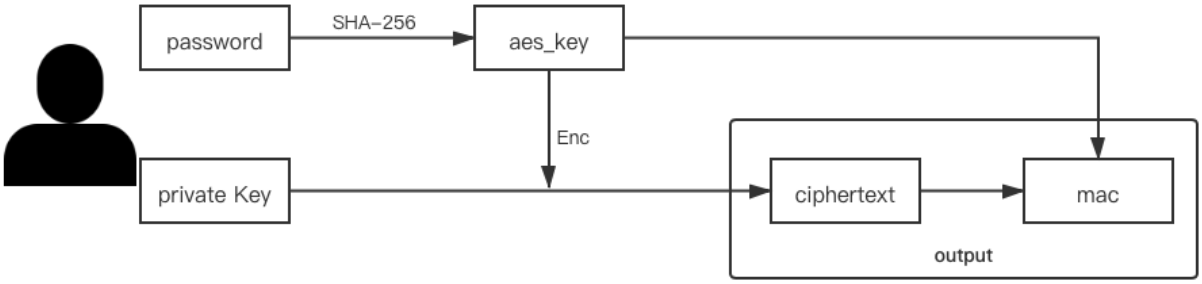
一、私钥保存过程

1、用户随机生成Paillier公私钥对，并设置一个口令password

2、计算SHA-256(password)得到AES秘钥aes_key，加密用户私钥并得到ciphertext

3、计算SHA-256(aesKey||ciphertext)得到一个mac值作为私钥完整性验证依据

4、将ciphertext和mac值一同存储在本地文件中



二、私钥恢复过程

1、从本地读取ciphertext和mac值

2、计算SHA-256(password)得到AES秘钥aes_key

3、计算SHA-256(aesKey||ciphertext)并和读取的mac值做比对，相同即表示密文未被篡改

4、利用aes_key解密ciphertext得到私钥明文