**使用 OpenSSL 对文件进行加密和解密**

<https://my.oschina.net/u/728245/blog/789761>

我们在平时的 Linux 运维管理的时候，经常会进行各种数据备份任务。将数据导出然后打包。通常在安全性要求比较高的环境下，我们可以借助 OpenSSL 工具对打包后的数据进行加密，这样能进一步的保障数据的安全性。

**1. OpenSSL 使用密码方式加密或解密文件**

1. 使用 openssl 加密一个文件 (data.zip 为原始文件，back.zip 为加密之后的文件)

# openssl enc -e -aes256 -in data.zip -out back.zip

解释: enc 表示对文件进行对称加密或解密， -e 表示对一个文件进行加密操作，-aes256 表示使用 aes256 算法进行加密，-in 表示需要被加密的文件，-out 表示加密之后生成的新文件。加密过程中会要求输入一个加密密码，重复输入两次即可完成对文件的加密

2. 使用 openssl 解密一个文件 (back.zip 为加密的文件，data.zip 为解密之后的文件)

# openssl enc -d -aes256 -in back.zip -out data.zip

解释: enc 表示对文件进行对称加密或解密， -d 表示对文件进行解密操作，-aes256 表示使用 aes256 算法进行解密，-in 表示需要被解密的文件，-out 表示解密之后生成的新文件，解密一个文件的时候会要求输入加密文件时设置的密码才能进行解密。

**2. OpenSSL 使用密钥方式加密或解密文件**

1. 首先需要使用 openssl 生成一个 2048 位的密钥 rsa.key 文件 (rsa.key 密钥文件中包含了私钥和公钥)

# openssl genrsa -out rsa.key 2048

2. 然后从 rsa.key 密钥文件中提取出公钥 pub.key

# openssl rsa -in rsa.key -pubout -out pub.key

3. 使用 pub.key 公钥加密一个文件 (data.zip 为原始文件，back.zip 为加密之后的文件)

# openssl rsautl -encrypt -inkey pub.key -pubin -in data.zip -out back.zip

4. 使用 rsa.key 私钥解密一个文件 (back.zip 为加密的文件，data.zip 为解密之后的文件)

# openssl rsautl -decrypt -inkey rsa.key -in back.zip -out data.zip

最后我们使用 OpenSSL 工具，对所有备份的数据文件进行加密存储，就能保证业务系统数据进行保护，防止泄漏。我们也可以使用其他的加密工具比如 GPG，VeraCrypt，trueCrypt 这些工具来对数据进行加密，但相比而言，使用 OpenSSL 更加方便，因为几乎每种 Linux 发行版都预装了 OpenSSL 软件包。