RSA加密通信小结

# 一、背景描述

2017年过完年之后回到公司，有对JAVA后端与APP端通信加密的需求。

# 二、计划与方案

1.加密方式采用RSA 1024加密。

2.发送与接收都采用RSA加密，采用两套不同的密钥。

3.统一的加解码函数。

4.H5与APP的加解密，采取特殊标识来分流。达到后端与H5通信不加解密。

进行方案参考《新版本APP与后台通信交互内容修改（改一）20170215》

# 三、关键点

1、RSA密钥的生成：包含全套的密钥生成以及安卓和IOS的密钥。[[1]](#footnote-2)

2、使用RSA对明文加密，对密文解密。[[2]](#footnote-3)

3、对安卓和IOS的密文进行解密，对明文进行加密。此处由于是对通信内容进行加密，需要进行分段加密。

4、在java后端完成拦截器的修改和返回的修改。

# 四、总结

已经完成加密，在原有的密码加密之上完成了对通信的加密。

在部署的时候 私钥须用PKCS8格式的，否则部署在linux环境报错。

1. 参考《RSA密钥生成》 [↑](#footnote-ref-2)
2. 参考《加解密代码》 [↑](#footnote-ref-3)