工业协议分析1

发表于 2021-02-16 分类于 Challenge ， 2019 ， 工业信息安全技能大赛 ， 深圳站
Challenge | 2019 | 工业信息安全技能大赛 | 深圳站 | 工业协议分析1

点击此处获得更好的阅读体验

WriteUp来源

https://www.jianshu.com/p/008e08547ae5

题目描述

> *工业网络中存在异常流量，尝试通过分析pcap流量包，分析出流量中的异常数据点，拿到flag*

题目考点

- *流量分析*
- *MMS规约*

解题思路

打开pacp文件，看到有mms协议，先过滤一下mms协议，同时搜索flag字符串

看到NO.1764里有flag.txt，功能码是fileDirectory

猜测有可能会用fileopen打开该文件，所以对fileopen进行过滤

第1771、1798、1813、4034条都对flag.txt进行了打开操作。接下来去每条报文后边一条看是否有fileread进行了读取。最终在1800处发现，其读取了flag.txt，1801是回复报文

内容是一张base64编码的图片，对其进行解码得到flag

Flag

```
flag{ICS-mms104}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2019/工业信息安全技能大赛/深圳站/ocTMi3RFTYB9rkYqZvwcFi.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2019 # 工业信息安全技能大赛 # 深圳站
工业协议分析2
对称加密问题