

科研平台数据安全检查

科研平台数据安全检查

背景

某高校建立了一个科研成果平台，用于共享和备份科研成果，使用FTP协议。平台规定，所有的成果上传到平台都需要使用每个人对应的aes256密钥进行加密，且同时上传sha256哈希文件，用于校验恢复后文件的完整性。为了保证平台数据安全，需要对平台流量进行审计。

题干说明

1. 分析提供的流量文件，找到哪些研究成果只上传了成果文档，但是没有上传哈希文件。

【评测标准】 将找到的研究成果编号按照数字部分从小到大进行排序，使用“-”连接，最后转为32位小写md5提交，注意计算md5时，输入字符应为UTF-8编码且行尾不带换行符。

举例说明，若找到的编号如下：

代码块

```
1 RES456881
2 RES223341
3 RES333333
```

排序连接后可以使用下面命令转换为md5：

代码块

```
1 echo -n "RES223341-RES333333-RES456881" | md5sum
```

最终答案为：acab254fff6c6d3b487d937540c90b7e

2. 科研成果在提交到平台之前，都会进行审核并记录哈希，现在检查发现有些成果上传的和提交审查的文件存在区别，请使用提供的aes256密钥解密文件，并校验哈希，找到哪些科研成果存在区别。

【评测标准】 将找到的研究成果编号按照数字部分从小到大进行排序，使用“-”连接，最后转为32位小写md5提交，注意计算md5时，输入字符应为UTF-8编码且行尾不带换行符。

举例说明，若找到的编号如下：

代码块

```
1 RES456881
2 RES223341
3 RES333333
```

排序连接后可以使用下面命令转换为md5：

代码块

```
1 echo -n "RES223341-RES333333-RES456881" | md5sum
```

最终答案为：acab254fff6c6d3b487d937540c90b7e

3. 近期在平台上发现了一些.eml后缀的垃圾邮件，检查流量，找到登录并上传这些eml垃圾邮件的用户名数量。

【评测标准】 提交上传垃圾文件的用户名数量。若找到了24个用户名上传垃圾文件，则提交答案为：24