实验报告5

陈旻 SA18225036

1 具体思路

1.1 实验原理

现在，浏览器以每次一个块的方式下载文件F，其中每个块包含上图中的附加哈希值。当接收到第一个块(B0 —— h1)后，浏览器检查H(B0 —— h1)是否等于h0；假如相等，浏览器就开始播放第一个视频块。当接受到第二个块(B1 —— h2)后，浏览器检查H(B1 —— h2)是否等于h1；假如相等，浏览器就开始播放第二个视频块。此过程一直持续到最后一个块。这样，每个块都会在接收时进行认证和播放，无需等到整个文件下载完毕。显然，如果哈希函数H时抗碰撞的，则攻击者无法在不被浏览器检测到的情况下修改任何视频块。事实上，由于h0 = H(B0 k h1)，攻击者无法找到一对(B00; h01) 6= (B0; h1)使得h0 = H(B00 k h01)，因为这是违反哈希抗碰撞的。因此，在第一次哈希核验后，浏览器确信B0和h1都是可信的。相同的证明方法可以表明，浏览器确信B1和h2都是可信的，并以此类推剩余的所以块。

1.2 实验步骤

整体思路安装实验要求逐步完成即可

1. 将文件分成1KB块
2. 计算最后一个块的哈希值
3. 将所得值附加到倒数第二个块末尾
4. 依次计算

程序代码

```
from Crypto.Hash import SHA256

h = SHA256.new()

with open("test.mp4",'rb') as file_b:
    while True:
        data_flow=file_b.read(1)
        if not data_flow:
            break
        h.update(data_flow)
file_b.close()
return md5_value.hexdigest()
```