**Nhập môn An toàn thông tin - Assignment 3**

**Họ và tên:** Lê Hữu Đức Anh

**Mssv:** 20215304

1. **Giải thích quá trình**
2. **Lý thuyết**

Lý thuyết đã được nêu rất kỹ trong file bài tập, yêu cầu băm 1 file video .mp4 thành các block kích thước 1kb, từ mỗi block và 1 giá trị băm h của block sau nó, ta tính được h của block hiện tại. Từ đó tính được h0 và truyền đi đến đích. Dựa vào h0, tiến hành kiểm tra các block tiếp theo xem nó có đúng là các block video được gửi không.

A diagram of a block

Description automatically generated

***Quá trình băm file***

Vì vậy ở bài tập này, em sẽ cài đặt chương trình với các hàm tìm h0, băm file video thành các khối kích thước 1 Kb block 0, block 1,... và lưu chúng cùng các giá trị băm h1, h2,... tương ứng. Cuối cùng, em sẽ tiến hành kiểm tra các block video từ đầu tới cuối, nếu có lỗi ở 1 video, quá trình kiểm tra sẽ tạm dừng.

1. **Cài đặt chương trình**

Do thư viện Pycrypto đã bị outdated nên em sử dụng thư viện Cryptography để thay thế với việc băm file bằng SHA256.

A close up of a sign

Description automatically generated

***Cài đặt thư viện***

Tiếp theo tiến hành cài đặt các hàm để băm dữ liệu và tính toán h0, sử dụng các công cụ có sẵn của Cryptography.

A computer screen shot of a code

Description automatically generated

Dữ liệu của video sẽ được đọc từ file video theo đơn vị 1 block là 1024 bytes = 1 Kb. Tính toán h[-1] sẽ được tính trực tiếp từ block cuối cùng (block có thể không đạt 1Kb). Các giá trị băm h tiếp theo của 1 block sẽ được tính từ sau ra trước dựa trên việc băm dữ liệu từ block đó và giá trị băm h của block trước nó. Kết quả h0 thu được từ hàm calculate\_h0 cho file video mẫu:



Tiếp theo, cài đặt hàm băm file video, chia video thành rất nhiều block, lưu chúng vào 1 file .mp4 kèm giá trị băm h của block phía sau chúng.

*Note: Việc mở file block này với dạng video là không thể, vì file .mp4 có định dạng header nằm ở đâu đó, trong khi 1Kb block có nơi có nơi không.*

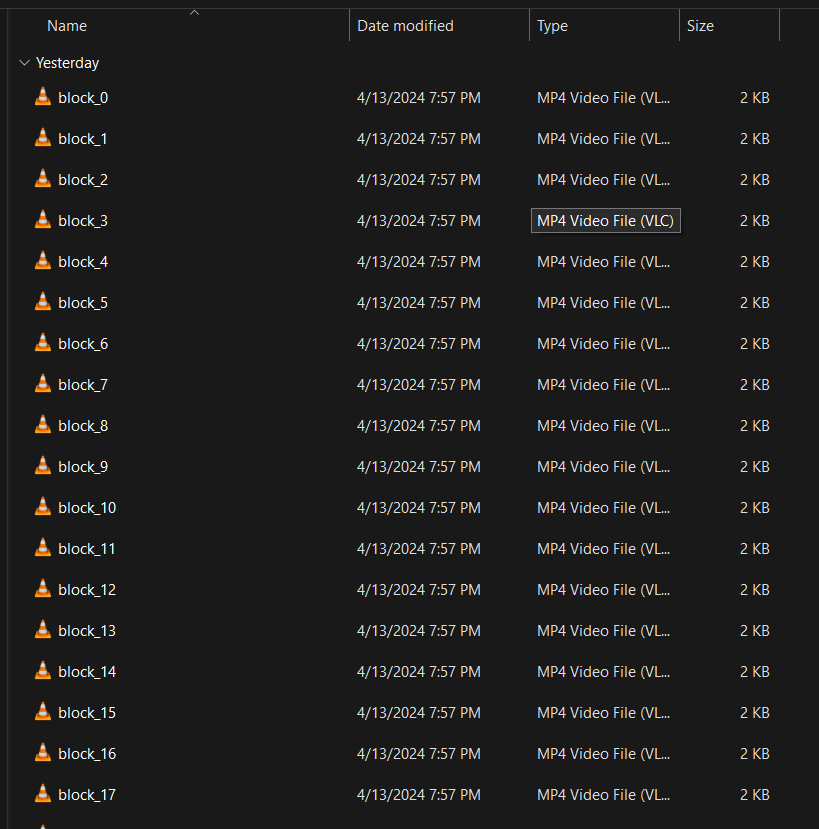
*A screenshot of a computer program

Description automatically generated*

***Hàm băm file video***

A screenshot of a computer

Description automatically generated



Tiến hành băm thu được 16530 file block .mp4

*Note: 2Kb trong hình là làm tròn, thực chất chỉ 1056 = 1024 + 32 byte*

Cuối cùng là các hàm để kiểm tra tính hợp lệ của các file block. Gồm các hàm check\_data, check\_video\_part, và hàm check\_all\_video để kiểm tra các video block, kiểm tra dữ liệu hợp lệ tại từng block theo thứ tự từ 1 đến hết.

A screenshot of a computer code

Description automatically generated

***Hàm kiểm tra các file video***

Kết quả chạy thử với thư mục các block được sinh ra ban đầu bởi hàm hash\_video đạt kết quả là hợp lệ.

A screen shot of a computer

Description automatically generated

***Chạy thử với file hoàn chỉnh là hợp lệ***

Thử nghiệm thay đổi ngẫu nhiên 10 byte trong file block\_100 rồi tiến hành kiểm tra tính hợp lệ, nhân được kết quả video không hợp lệ. Như vậy quá trình băm file và kiểm tra đã thực hiện đúng.

A computer screen shot of text

Description automatically generated

***Sửa ngẫu nhiên 1 số byte trên file block***

A screen shot of a computer

Description automatically generated

***Chạy thử file đã sửa đổi cho ra kết quả không hợp lệ***