BÁO CÁO THỰC HÀNH

**Môn học: CRYPTOGRAPHY – Mật mã học**

**Tên chủ đề: Hash Functions and Digital Certificates**

*GVHD: Tô Trọng Nghĩa*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: **NT219.N21.ANTT.1**

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Họ và tên | MSSV | Email |
| 1 | Lê Đoàn Trà My | 21521149 | 21521149@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Nội dung | Tình trạng | Trang |
| 1 | Generating message digests (hash values) and HMAC | 90% | 2 - 5 |
| 2 | Hash properties: One-way vs Collision-free | 100% | 5 - 7 |
| 3 | Generating Two Different Files with the Same MD5 Hash | 75% | 8 - 10 |
| 4 | Generating Two Executable Files with the same MD5 Hash | 100% | 10 - 11 |
| 5 | Manually Verifying an X.509 Certificate | 100% | 12 - 13 |
| 6 | Programming application for X509 Certificate verification | 100% | 13 - 15 |
| Điểm tự đánh giá | | | **9 – 9.5/10** |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

**1. Generating message digests (hash values) and HMAC**

- Viết một ứng dụng (bằng C#) để tính giá trị băm với 3 loại: MD5, SHA-1, SHA3-256.

- Code hoàn chỉnh được gửi kèm báo cáo với thư mục tên: HashCaculate (dài quá nên em không chụp code).

- Giao diện:

**A screenshot of a computer

Description automatically generated**

*Hình 1. Giao diện của ứng dụng HashCaculate đơn giản*

- Kiểm thử ứng dụng:

**a, Tính giá trị băm với thông điệp bất kì có chứa MSSV và so sánh kết quả với bất kỳ tool nào:**

\* Chuỗi nhập thứ 1(dạng text): xin chao, toi la 21521149

A screenshot of a computer

Description automatically generated

*Hình 2. Giá trị băm trả về của text* ***xin chao, toi la 21521149*** *của ứng dụng tự code*

+ Kiểm thử đối chiếu với kết quả tính sử dụng bằng web <https://md5calc.com/hash>

A screenshot of a computer

Description automatically generated with medium confidence

*Hình 3. Giá trị băm trả về của text* ***xin chao, toi la 21521149*** *của web*

\* Chuỗi nhập thứ 2 (dạng hex): 21451149

A screenshot of a computer

Description automatically generated

*Hình 4. Giá trị băm trả về của text* ***21521149*** *của ứng dụng tự code*

+ Đổi kết quả 21521149 từ dạng hex sang mã ASCII: <https://www.rapidtables.org/vi/convert/number/hex-to-ascii.html>

A screenshot of a chat

Description automatically generated with medium confidence

*Hình 5. Kết quả đổi từ hex sang ASCII của* ***21521149***

+ Kiểm thử đối chiếu với kết quả tính sử dụng bằng web <https://md5calc.com/hash>

A screenshot of a computer

Description automatically generated with medium confidence

*Hình 6. Giá trị băm trả về của hex* ***21521149*** *của web*

**b, Tạo các file dữ liệu và tiến hành băm:** (băm bằng file thì chọn các hash trước rồi mở chọn file muốn băm – không nhấn Caculate)

A screenshot of a computer

Description automatically generated

*Hình 7. Tiến hành chọn file input cần băm (10KB)*

*A screenshot of a computer

Description automatically generated with medium confidence Hình 8. Kết quả băm bởi ứng dụng tự code và kết quả sử dụng tool tính*

*A screenshot of a computer

Description automatically generated with medium confidence*

*Hình 9. Kết quả băm bởi ứng dụng tự code và kết quả sử dụng tool tính với file 1MB*

**- Điểm chưa hoàn thiện:** Các file có kích thước nhỏ thì SHA3-256 băm ra giống với dùng tool web, còn các file lớn lại không chính xác.

**2. Hash properties: One-way vs Collision-free**

**a, Xét hai thông điệp ở dạng hex:**

- Sử dụng <https://text-compare.com/> để so sánh 2 thông điệp:

A screenshot of a computer

Description automatically generated with medium confidence

*Hình 10. Kết quả so sánh 2 thông điệp dạng hex*

+ Nhận thấy 2 văn bản khác nhau 6 bytes (24 bit).

- Dùng hàm băm MD5 băm 2 thông điệp, thu được:

+ Thông điệp 1: A screenshot of a computer

Description automatically generated with medium confidence

*Hình 11. Kết quả băm thông điệp 1 bằng HashCalc*

+ Thông điệp 2:

A screenshot of a computer

Description automatically generated with medium confidence

*Hình 12. Kết quả băm thông điệp 2 bằng HashCalc*

→ 2 thông điệp khác nhau nhưng kết quả băm lại giống nhau

→ Đụng độ (Collisicon).

**b, Tải 2 file PDF, xem và so sánh 2 file, tính toán hàm băm SHA-1 cho 2 file PDF và quan sát:**

A picture containing text, screenshot, businesscard, font

Description automatically generated

*Hình 13. File Shattered-1.pdf và file Shattered-2.pdf*

- Nhận thấy, 2 file có sự khác nhau về màu sắc ở nửa phần trên (Shattered-1.pdf có màu xanh và Shattered-2.pdf có màu đỏ).

- Sử dụng HashCalc thu được các kết quả:

A screenshot of a computer

Description automatically generated with medium confidence

*Hình 14. Kết quả băm file Shattered-1.pdf*

*A screenshot of a computer

Description automatically generated with medium confidence*

*Hình 15. Kết quả băm file Shattered-2.pdf*

→ Kết quả khi băm bằng SHA-1 của 2 file là giống nhau.

**c, Rút ra kết luận và giải thích vì sao có sự đụng độ (conllision) trong MD5 và SHA-1:**

- Kết luận: Ở hai câu a, b có thể thấy dù 2 thông điệp (băm MD5) hay 2 file pdf (băm SHA-1) có những điểm khác nhau nhưng sau khi băm lại cùng trả về một kết quả.

- Giải thích: Sự đụng độ này xảy ra là do thiết kế và kích thước đầu ra (output) của hàm băm.

+ Output đầu ra: các giá trị băm MD5 và SHA-1 đều có độ dài cố định và khá nhỏ, tương ứng là 128 bit và 160 bit. Khi các thông điệp được đưa vào hàm băm, chúng sẽ được ánh xạ thành các giá trị băm có độ dài cố định này.

+ Thiết kế: Trong cơ chế hoạt động của các giải thuật băm này, các thông điệp được chia thành các khối và sau đó áp dụng các phép biến đổi để tạo ra giá trị băm. Một số phép biến đổi có thể dẫn đến việc các thông điệp khác nhau tạo ra cùng một giá trị băm.

**3. Generating Two Different Files with the Same MD5 Hash**

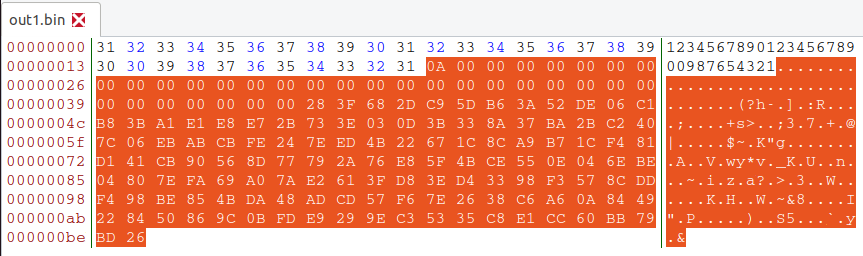
**a, Độ dài tệp tiền tố (prefix) không là bội của 64 thì chuyện gì xảy ra?**

- Khởi tạo file prefix.txt 31 bytes, sau đó sử dụng md5collgen sinh ra file out1.bin và out2.bin

A picture containing text, screenshot, font

Description automatically generated

*Hình 16. Kết quả sử dụng md5collgen sinh ra file out1.bin và out2.bin với prefix không là bội 64*



*Hình 17. Kết quả file out1.bin khi mở bằng lệnh bless*

A picture containing text, screenshot, font, parallel

Description automatically generated

*Hình 18. Kết quả file out2.bin khi mở bằng lệnh bless*

→ Nếu độ dài của tệp prefix không là bội số của 64, md5collgen sẽ padding thêm các ký tự vào cuối tệp cho đến khi độ dài của tệp là bội số của 64 byte. Điều này là do thuật toán MD5 xử lý dữ liệu đầu vào theo các khối 64 byte.

A picture containing text, screenshot, font, line

Description automatically generated

*Hình 19. Kích thước các file*

**b, Tạo tệp tiền đố bằng 64 bytes, chạy tool conllision và quan sát**

**A picture containing text, screenshot, font

Description automatically generated**

*Hình 19. Tiến hành chạy lệnh*

**A picture containing text, screenshot, receipt, font

Description automatically generated**

*Hình 20. Kích thước các file*

**A screenshot of a computer

Description automatically generated with medium confidence**

*Hình 21. Nội dung các file out13.bin và out23.bin mở bằng bless*

→ Hai file đụng độ có giá trị băm MD5 giống nhau nhưng nội dung của chúng khác nhau.

**c, Dữ liệu do md5collgen tạo ra có khác hoàn toàn với đầu ra của 2 file? Xác định tất cả các bytes khác nhau**

- Dữ liệu do md5collgen tạo ra của 2 file không khác hoàn toàn với nhau.

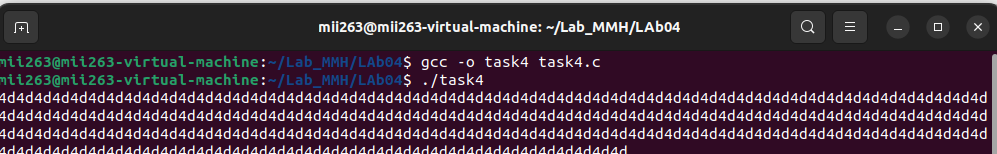
A screenshot of a computer

Description automatically generated*Hình 22. Các bytes khác nhau giữa out13.bin và out23.bin*

**d, Viết lại chương trình md5collgen**

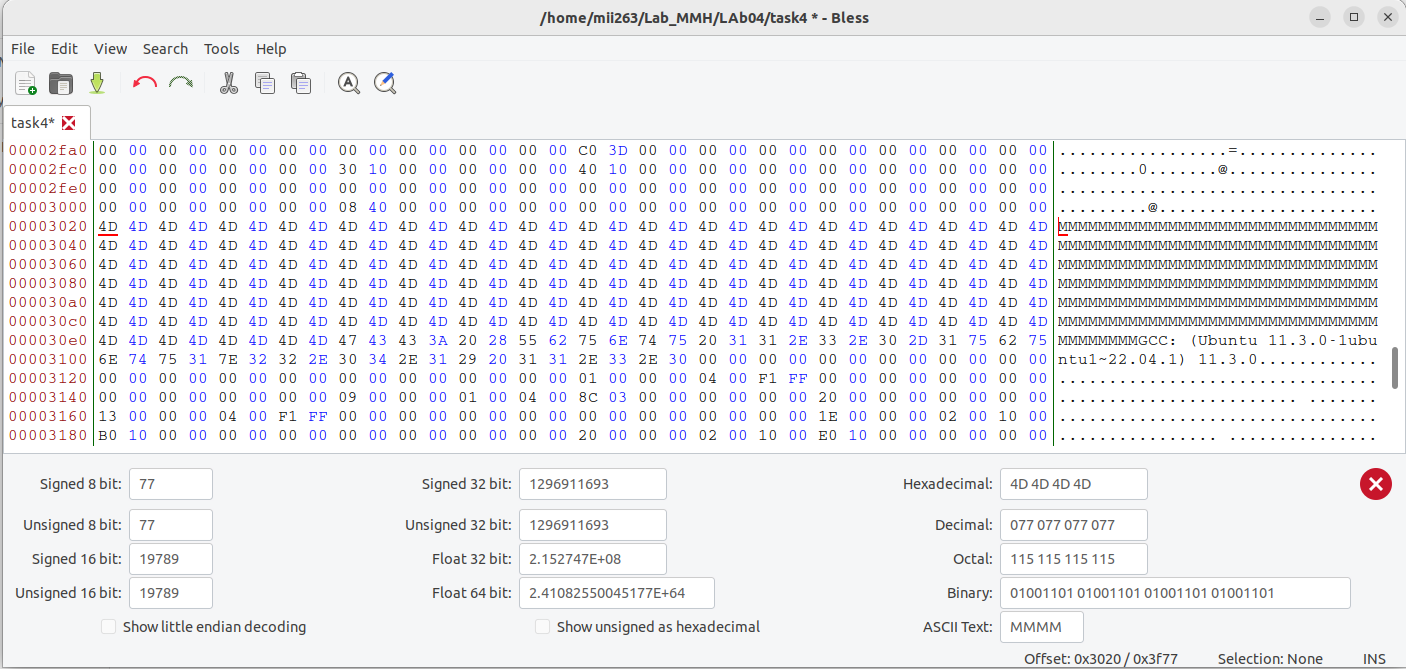
**4. Generating Two Executable Files with the same MD5 Hash**

- Chạy file task4.c in ra 200 ký tự biểu diễn chữ M (dạng hex: 4D)



*Hình 23. Kết quả thực thi file task4.c*

- Dùng lệnh bless để mở file task4 và xác định vị trí của mảng:



*Hình 24. Kết quả mở file task4 bằng bless*

→ Offset = 0x3020 = 12320, mảng bắt đầu tại byte thứ 12320, kết thúc tại offset = 0x30e7 (byte thứ 12519).

- Chọn đoạn prefix thoả size(prefix) % 64 = 0 → Prefix từ 0 đến 12352.

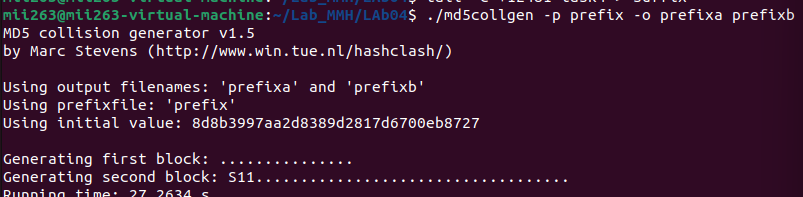
+ Đoạn 128 byte ở giữa từ 12353 tới 12480.

+ Suffix từ 12481 tới hết file.

****

*Hình 25. Thực thi “tạo” prefix và suffix*

- Dùng md5collgen tạo prefixa và prefix:



*Hình 26. Thực thi “tạo” prefixa và prefixb*

- Nối suffix vào các prefix:



*Hình 27. Thực thi nối prefix và suffix*

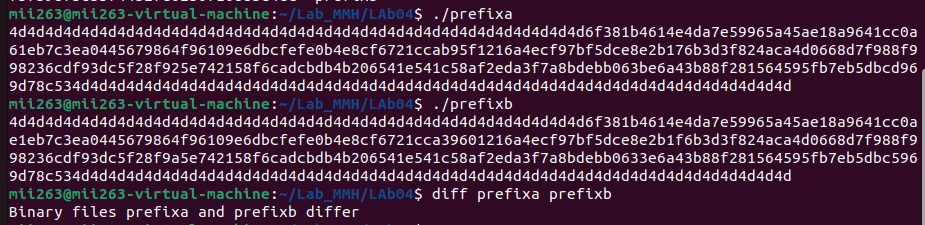
- Kiểm tra md5sum của 2 file prefixa và prefix: kết quả trả vê flaf giống nhau.

A screen shot of a computer program

Description automatically generated with low confidence

*Hình 28. Sự giống nhau của kết quả md5sum của 2 file prefix*

- So sánh 2 file prefix: 2 file prefix có sự khác nhau.



A screenshot of a computer

Description automatically generated with low confidence

*Hình 29, 30. So sánh 2 file prefixa và prefixb*

**5. Manually Verifying an X.509 Certificate**

**A picture containing text, screenshot, font

Description automatically generated**

*Hình 31. Thực hiện Bước 1 theo hướng dẫn bài lab*

**A screenshot of a computer screen

Description automatically generated with low confidence**

*Hình 32. Thực hiện Bước 2 theo hướng dẫn bài lab*

**A picture containing text, screenshot, font

Description automatically generated**

*Hình 33. Thực hiện Bước 3 theo hướng dẫn bài lab*

**A picture containing text, screenshot, font, information

Description automatically generated**

*Hình 34. Thực hiện Bước 3, Bước 4 theo hướng dẫn bài lab*

- Bước 5: Verify

+ Code (được gửi đính kèm báo cáo với tên Task5.cpp):

A screenshot of a computer code

Description automatically generated with low confidence

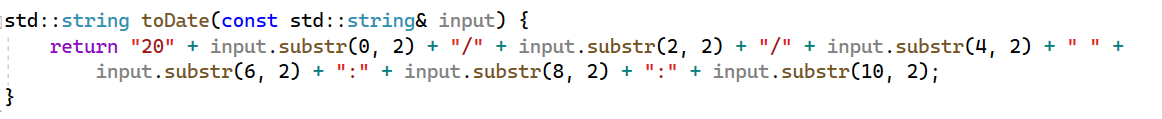
*Hình 35. Code verify*

**A screen shot of a computer

Description automatically generated with medium confidence**

*Hình 36. Kết quả thực thi*

**6. Programming application for X509 Certificate verification**

****

*Hình 37. Code chuyển đổi ngày tháng*

*A screen shot of a computer code

Description automatically generated with medium confidence*

*Hình 38. Code in thông tin chứng chỉ*

**A picture containing text, screenshot, font

Description automatically generated**

*Hình 39. Code tiến hành verify*

**A screenshot of a computer program

Description automatically generated with low confidence**

*Hình 40. Nội dung hàm main*

**A screenshot of a computer

Description automatically generated**

*Hình 41. Kết quả thực thi*

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)