Hashing

Câu 1: Hàm một chiều (one-way function) là gì?

Hàm một chiều là hàm mà rất dễ mã hóa nhưng không giải mã được, ta không thể tính lại được bản gốc khi có bản mã.

Câu 2: Cho một ví dụ để minh hoạ việc sử dụng hàm băm có thể giúp kiểm tra tính toàn vẹn của thông điệp.

Gợi ý: mã hoá thông điệp, tạo ra thay đổi trên ciphertext và sử dụng hàm băm để kiểm tra thông điệp được giải mã có thay đổi so với thông điệp gốc ban đầu.

Có thể dùng hàm băm để tạo chữ kí số giúp xác thực tính toàn vẹn của thông điệp cũng như xác minh được người gửi. Ví dụ với việc gửi thông điệp M. Bên gửi: sẽ gửi dùng hàm Hash để tính h = Hash(M), sau đó lấy h đi mã hóa bằng khóa riêng người gửi để được chữ ký số S. Người gửi sẽ gửi cả M và S.

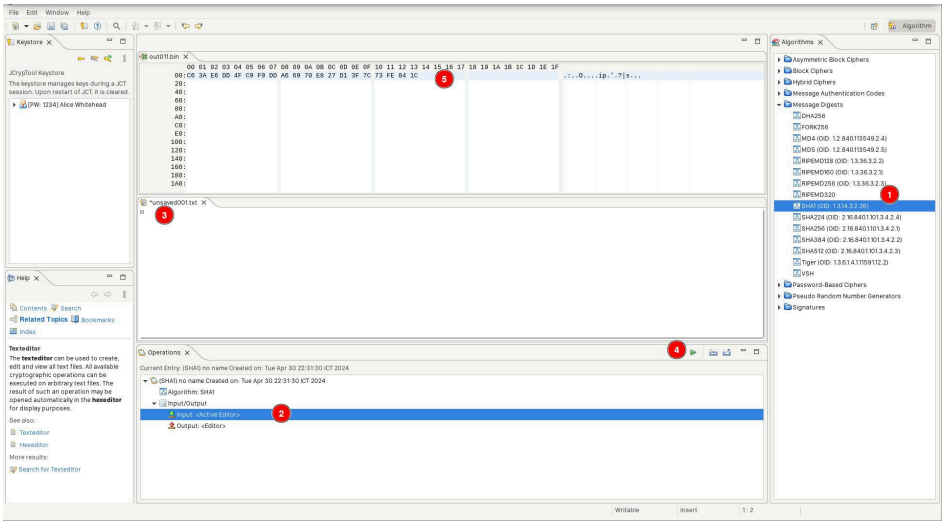
Bên nhân: lấy ra M và tính h = Hash(M), sau đó sẽ lấy khóa công khai người gửi để giải mã S ta được h'. Cuối cùng so trùng h = h' để xem tính toàn vẹn của dữ liệu.

Câu 3: Hàm băm H(·) là hàm có chức năng chuyển thông điệp có kích thước bất kì bất kỳ về kích thước cố định:

a) Xem xét giá trị hash được tạo ra bằng cách áp dụng giải thuật hash SHA-1 trên một ký tự trong bảng chữ cái tiếng Anh: C6 3A E6 DD 4F C9 F9 DD A6 69 70 E8 27 D1 3F 7C 73 FE 84 1C. Hãy tìm ký tự chữ cái tiếng anh được sử dụng và mô tả cách làm? (dùng công cụ CrypTool)

NOTE: Ở đây sinh viên đang sử dụng hệ điều hành **ArchLinux** nên sử dụng phiên bàn Cryptool dành cho Linux.

- Bước 1: Mở công cụ, và chọn vào phần Algorithms, và chọn giải thuật **SHA1**
- Bước 2: Ở tab Operations > Input/Ouput, chọn Input là Active Editor
- Bước 3: Nhập các ký tự cần thử để dùng giải thuật hashing và nhấn Execute
- Bước 4: Ta theo dõi kết quả ở oupt editor



b) Giả sử bạn đã tìm ra được ký tự ở câu a, như vậy có thể kết luận hàm hash SHA-1 không thoả mãn tính chất một chiều (one-way) được hay không, giải thích câu trả lời? SHA-1 vẫn thỏa mãn tính chất một chiều, chúng ta tìm được ký tự ban đầu dựa vào phép thử, và nếu message trở nên lớn hơn, rất khó để tìm ra được giá trị hash.

Câu 4: Thực hiện lại bước 3 cho các giải thuật hash khác và đánh giá giá trị hash nhận được với giá trị hash ban đầu.

•