**ĐỀ CƯƠNG CHI TIẾT BÀI THỰC HÀNH**

Tên học phần: An toàn và Bảo mật Hệ thống Thông tin

Tên bài thực hành: Tạo và Xác thực Chữ ký số

Thời lượng: 3 buổi (9 tiết)

Lớp học phần: INT1303-20242-13

Giảng viên phụ trách: Trần Đức Sự

Nhóm thực hiện:

* Nguyễn Khả Phong - B23DCCC129
* Phạm Tiến Công - B23DCCC025
* Đinh Hoàng Long - B23DCCC102
  1. Mục tiêu của bài thực hành
* Hiểu được cơ chế hoạt động và vai trò của chữ ký số trong bảo mật thông tin
* Nắm vững nguyên lý của các thuật toán RSA và DSA trong ứng dụng chữ ký số
* Thực hành triển khai hệ thống tạo và xác thực chữ ký số
* So sánh hiệu suất và độ an toàn giữa các thuật toán chữ ký số
  1. Nội dung thực hành
     1. Sinh khóa
* Chức năng: Tạo cặp khóa (khóa công khai, khóa riêng tư) cho người dùng
* Thực hiện:
  + Sinh số nguyên tố an toàn
  + Tạo khóa với các độ dài khác nhau (1024, 2048, 3072, 4096 bit)
  + Lưu trữ khóa dưới định dạng an toàn
  + Bảo vệ khóa riêng tư bằng mật khẩu
    1. Tạo chữ ký số
* Chức năng: Tạo chữ ký số cho dữ liệu đầu vào (văn bản, tập tin)
* Thực hiện:
* Băm dữ liệu với SHA-256/SHA-3
* Ký dữ liệu sử dụng khóa riêng
* Đóng gói chữ ký vào định dạng tiêu chuẩn
* Ký các loại tập tin khác nhau
  + 1. Xác thực chữ ký số
* Chức năng: Kiểm tra tính hợp lệ của chữ ký số
* Thực hiện:
  + Xác thực sử dụng khóa công khai
  + Kiểm tra tính toàn vẹn của dữ liệu
  + Xác minh nguồn gốc của chữ ký
  + Báo cáo kết quả xác thực chi tiết
  1. Quy trình thực hiện thuật toán
     1. Thuật toán RSA
* Sinh khóa RSA:
  + Chọn hai số nguyên tố lớn p và q
  + Tính n = p \* q
  + Tính giá trị hàm Euler φ(n) = (p-1) \* (q-1)
  + Chọn e sao cho 1 < e < φ(n) và gcd(e, φ(n)) = 1
  + Tính d = e^(-1) mod φ(n)
  + Khóa công khai: (n, e), Khóa riêng: (n, d)
* Tạo chữ ký RSA:
* Tính giá trị băm h = Hash(M) của thông điệp M
* Chuyển đổi h thành số nguyên m
* Tính chữ ký s = m^d mod n
* Kết quả là cặp (M, s)
* Xác thực chữ ký RSA:
* Tính m' = s^e mod n
* Tính giá trị băm h' = Hash(M) của thông điệp M nhận được
* Chuyển đổi h' thành số nguyên m"
* Nếu m' = m" thì chữ ký hợp lệ, ngược lại là không hợp lệ
  + 1. Thuật toán DSA
* Sinh khóa DSA:
* Chọn một số nguyên tố p (độ dài 2048 bit)
* Chọn một số nguyên tố q (độ dài 256 bit) là ước của p-1
* Tính g = h^((p-1)/q) mod p, với h < p-1 sao cho g > 1
* Chọn khóa riêng x ngẫu nhiên, 0 < x < q
* Tính khóa công khai y = g^x mod p
* Khóa công khai: (p, q, g, y), Khóa riêng: x
* Tạo chữ ký DSA:
* Tính giá trị băm h = Hash(M) của thông điệp M
* Chọn một số k ngẫu nhiên, 0 < k < q
* Tính r = (g^k mod p) mod q
* Tính s = (k^(-1) \* (h + x\*r)) mod q
* Kết quả chữ ký là cặp (r, s)
* Xác thực chữ ký DSA:
* Kiểm tra 0 < r < q và 0 < s < q, nếu không thỏa thì chữ ký không hợp lệ
* Tính w = s^(-1) mod q
* Tính giá trị băm h = Hash(M) của thông điệp M
* Tính u1 = h \* w mod q
* Tính u2 = r \* w mod q
* Tính v = ((g^u1 \* y^u2) mod p) mod q
* Nếu v = r thì chữ ký hợp lệ, ngược lại là không hợp lệ
  1. Môi trường và công cụ
* Ngôn ngữ lập trình: Python
* Thư viện mã hóa: Cryptography, PyCryptodome
* Môi trường phát triển: Visual Studio Code, PyCharm
* Công cụ kiểm thử: Pytest, Unittest
  1. Kịch bản thử nghiệm
     1. Thử nghiệm sinh khóa
* Sinh khóa RSA với các độ dài 1024, 2048, 4096 bit
* Sinh khóa DSA với các tham số khác nhau
* Đo thời gian sinh khóa và lưu trữ kết quả
  + 1. Thử nghiệm tạo chữ ký
* Tạo chữ ký cho văn bản ngắn
* Tạo chữ ký cho tập tin có kích thước khác nhau
* So sánh thời gian tạo chữ ký giữa RSA và DSA
  + 1. Thử nghiệm xác thực chữ ký
* Xác thực chữ ký hợp lệ
* Xác thực chữ ký với dữ liệu đã bị sửa đổi
* Xác thực chữ ký với khóa công khai không khớp
* So sánh thời gian xác thực giữa RSA và DSA
  1. Đánh giá kết quả
* So sánh độ an toàn lý thuyết giữa RSA và DSA
* So sánh hiệu suất về thời gian xử lý
* So sánh kích thước khóa và chữ ký
* Phân tích ưu nhược điểm của mỗi thuật toán
* Đề xuất cải tiến và ứng dụng thực tiễn
  1. Tài liệu tham khảo
* William Stallings – Cryptography and Network Security, Pearson
* https://en.wikipedia.org/wiki/Digital\_signature
* https://docs.python.org/3/library/cryptography.html