ĐẠI HỌC QUỐC GIA TPHCM

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

KHOA CÔNG NGHỆ THÔNG TIN

BỘ MÔN CÔNG NGHỆ TRI THỨC

Lab

1

Môn học: Seminar Công Nghệ Tri Thức

Sinh viên thực hiện:

Trần Quốc Thuận – 20127349

Giáo viên hướng dẫn:

TS. Ngô Minh Nhựt

TS. Trần Hoàng Quân

Ngày 9 tháng 11 năm 2024

Mục lục

1 Giới thiệu

Báo cáo này nói về hybrid encryption - là hệ thống mã hoá kết hợp mã hóa bất đối xứng để trao đổi khóa an toàn với mã hóa đối xứng để mã hóa dữ liệu nhanh. Báo cáo này giải thích động cơ, mục tiêu và phương pháp mã hóa lai cụ thể được triển khai.

2 Mô tả hệ thống:

Hệ thống này bao gồm ba thành phần chính: **Tạo khóa**, **Mã hóa**, và **Giải mã**.

- **Tạo khóa (keygen.py):** Module này tạo một cặp khóa RSA có kích thước 2048 bit. Khóa riêng được lưu trong tệp `receiver_private_key.key`, và khóa công khai được lưu trong tệp `receiver_pub_key.pub`.[1]
- **Mã hóa (encryptor.py):** Chương trình này thực hiện mã hóa tệp, quá trình bắt đầu bằng việc tạo một khóa AES ngẫu nhiên 128-bit (sử dụng AES-128 với chế độ EAX để mã hóa). Khóa đối xứng này sau đó được mã hóa bằng khóa công khai RSA [2], đảm bảo bảo mật cho quá trình trao đổi khóa. Khóa đối xứng AES đã được mã hóa cùng với nội dung tệp đã được mã hóa sẽ được xuất ra 2 tệp riêng biệt
- **Giải mã (decryptor.py):** Chương trình này giải mã các tệp đã được mã hóa bằng `encryptor.py`. Đầu tiên, nó giải mã khóa AES bằng khóa riêng RSA. Sau đó, nó sử dụng khóa AES đã giải mã để giải mã dữ liệu tệp, đồng thời kiểm tra tính toàn vẹn của nó bằng *nonce* và *tag* đã cung cấp của mode EAX (của AES) [3]

3 Tham số và cài đặt

- **Kích thước khoá RSA:** 2048 bit
- **Kích thước khoá AES:** 128 bit
- **Chế độ AES:** EAX để xác minh tính toàn vẹn
- **Các loại tệp được hỗ trợ:** Văn bản (`.txt`) và mọi loại tệp nhị phân (`.jpg, .png, .jpeg`)
- **Kiểm tra tính bảo mật:** Số ngẫu nhiên dùng 1 lần và mã xác thực (authen tag)

4 Tiêu chí đánh giá:

Content	Percentage
Keygen (symmetric & asymmetric)	20%
Encryption & Decryption (symmetric & asymmetric)	40%
Application (command-line)	10%
Demo video	10%
Report	20%
Multiple filetype support (bonus)	0%
File integrity verification (bonus)	0%

Tài liệu

[1] PyCryptodome Documentation, "Examples of Encryption and Decryption."

[2] Stack Overflow, "RSA Encryption and Decryption in Python."

[3] R. Jesus, "Hybrid-Cryptography."