Nhập môn mã hóa

Đồ án cuối kì

Bộ môn Công nghệ tri thức
Khoa Công nghệ thông tin
Đại học Khoa học tự nhiên TP HCM

Thông tin nhóm

MSSV	Họ Tên	Email	Điện thoại
1512112	Tôn Thất Tâm Định	1512112@student.hcmus.edu.vn	
1412261	Đinh Nguyên Khôi	1412261@student.hcmus.edu.vn	

MỤC LỤC

1 Mã hóa Symcrypt

1.1 Phần Encrypt

- Nhóm sử dụng thư viện bên thứ 3 là aes.h để mã hóa aes 128bit có khóa là 16 bit.
- Đầu vào của chương trình encrypt là file encrypt.inp gồm:
  - Dòng đầu chứa khóa đối xứng ở dạng thập phân
  - Dòng tiếp theo là đoạn message
- Kết quả sau khi chạy chương trình encrypt.exe được ghi vào 2 file: file key.txt chứa khóa ở dạng hex, file encrypt.txt chứa ciphertext ở dạng hex.
- Chi tiết cài đặt được chứa trong file Source/Encrypt

1.2 Phần Decrypt

- Nhóm sử dụng thư viện bên thứ 3 là aes.h để mã hóa aes 128bit có khóa là 16 bit.
- Đầu vào của chương trình decrypt là file decrypt.inp có định dạng:
  - Dòng đầu chứa khóa đối xứng ở dạng hex
  - Dòng tiếp theo là đoạn ciphertext
- Kết quả sau khi chạy chương trình encrypt.exe được ghi vào 1 file decrypt.txt: chứa đoạn message sau khi đã giải mã

2 Thiết kế cơ chế truyền tin

2.1 TN1

- Tạo 1 folder trên Google drive đặt tên là Y1 – Y2 và chia sẻ quyền được cập nhật cho 2 máy Y1, Y2.
- Y1 nhận file key.txt và thực hiện việc mã hóa đối xứng bằng rsa được file encryptkey.txt và gửi lên drive.
- Đồng thời Y1 gửi bản ciphertext chứa trong file encrypt.txt lên drive.
- Y2 nhận file encryptkey.txt thực hiện việc dịch mã để có được khóa đối xứng.

- Y2 tiến hành ghi vào file decrypt.inp theo định dạng như đã đề cập ở trên.

Link folder:

https://drive.google.com/drive/folders/1unM8Z0OKx6Gig2cVyodAXJ2rH1eEgLww?usp=sharing

2.2 TN2

- Thiết kế trên google drive các thư mục để các máy liên lạc với nhau, các máy sẽ gửi và nhận file trên từng folder tương ứng.
- Folder X – Y2: https://drive.google.com/drive/folders/1MtNHGwOp1_U-BQ3Er7-nFbV38WOC948W?usp=sharing
- Folder X – Y1: https://drive.google.com/drive/folders/1ZMNIaH4pH_bWZgMbsDsjeD85SRoyLzuI?usp=sharing
- Folder Y1 – Y3: https://drive.google.com/drive/folders/1AAfnviPyWDhwtwZ7nOU_5qpTWCVLlcR2?usp=sharing
- Folder Y2 – X, Y1, Y3: https://drive.google.com/drive/folders/1GB5CDsmslvMYLbnHfM-RKj8uNQjVwgRM?usp=sharing

2.3 TN3

- Thiết kế trên google drive các thư mục để các máy liên lạc với nhau, các máy sẽ gửi và nhận file trên từng folder tương ứng.
- Folder X- Y2: https://drive.google.com/drive/folders/17vBciGmd-q9Rw1bEo8SIYFrEM0ef_wEJ?usp=sharing
- Folder X- Y1: https://drive.google.com/drive/folders/1GUTx3CmIaEsmk5XRxnA8PyJr0YecEP_s?usp=sharing
- Folder X-Y3: https://drive.google.com/drive/folders/1wSeYBtnOAGhH63uUqwzZMPY9MfS7Kn3g?usp=sharing
- Folder Y1-Y3:

https://drive.google.com/drive/folders/1lEQ4igfiTjW4Ob20uy6Ol0wMRpftji00?usp=sharing

2.4 TN4

- Thiết kế trên google drive các thư mục để các máy liên lạc với nhau, các máy sẽ gửi và nhận file trên từng folder tương ứng.
- Folder X- Y1: https://drive.google.com/drive/folders/1FxKlsPxQ-FEn2wFjmuYpXWeb73RnUAGz?usp=sharing
- Folder X – Y2: https://drive.google.com/drive/folders/1a82gRpFCW_-e4cCGjp-ydn7kli8n6hNl?usp=sharing
- Folder X – Y3: https://drive.google.com/drive/folders/1a82gRpFCW_-e4cCGjp-ydn7kli8n6hNl?usp=sharing
- Folder Y1 – Y3: https://drive.google.com/drive/folders/1b-EySNUPdiyqWT8z0KOGrkTJW9HMSVhb?usp=sharing

3 Tài liệu tham khảo

1. https://github.com/kokke/tiny-AES-c