Encrypting Files & Emails with GPG

Mai Đức Duy - 22127084
Nguyễn Trần Minh Hoàng - 22127130
Từ Chí Tiến - 22127414

I. Giới Thiệu Chung

- **PGP (Pretty Good Privacy)** được tạo ra bởi **Phil Zimmermann** năm 1991
- Do những vấn đề về bản quyền và giới hạn xuất khẩu của **PGP**, năm 1997, Werner Koch phát triển GPG như một giải pháp mã nguồn mở thay thế

GnuPG

- **GPG (GNU Privacy Guard)** là một phần mềm mã nguồn mở, dùng để mã hóa, giải mã, ký số và xác minh thông tin, tương thích với chuẩn **OpenPGP (RFC 4880)**

II. Các Khái Niệm Bảo Mật Cơ Bản

Mã hóa (Encryption)

01

Biến đổi **plaintext** thành **ciphertext**, chỉ người có khóa giải mã mới đọc được

Giải mã (Decryption)

02

Quá trình khôi phục nội dung ban đầu (**plaintext**) từ dữ liệu bị mã hóa (**ciphertext**)

Public/Private Key

03

Public Key: Dùng để mã hóa và xác minh chữ ký
Private Key: Dùng để giải mã và ký số

Ký số (Digital Signature)

04

Đảm bảo tính xác thực (**authentication**) và toàn vẹn (**integrity**) của dữ liệu

III. Công nghệ và chuẩn sử dụng

OpenPGP (RFC 4880): Chuẩn mở cho mã hóa dựa trên khóa công khai

Thuật toán bất đối xứng
RSA, ElGamal, ECDSA (Elliptic Curve), …

Thuật toán băm
SHA-256, SHA-512, MD5, …

Thuật toán đối xứng
AES, 3DES, Blowfish, …

IV. Cài đặt GPG

Trên Linux:

- sudo apt install gnupg
- sudo dnf install gnupg

Trên macOS:

- brew install gnupg

Trên Windows:

- Tải Gpg4win từ: https://www.gpg4win.org/

V. CÁC LỆNH CƠ BẢN

- gpg --full-generate-key # Tạo cặp khóa
- gpg --list-keys # Hiển thị danh sách khóa công khai
- gpg --list-secret-keys # Hiển thị danh sách khóa bí mật
- gpg --export -a KEYID > pub.asc # Xuất khóa công khai (ASCII)
- gpg --import pub.asc # Nhập khóa công khai của người khác
- gpg --encrypt -r KEYID file.txt # Mã hóa file cho người nhận
- gpg --decrypt file.txt.gpg # Giải mã file mã hóa
- gpg --sign --armor file.txt # Ký số vào một file
- gpg --verify file.txt.asc # Xác thực chữ ký

VI.
NGUYÊN LÝ HOẠT ĐỘNG

A. MÃ HÓA DỮ LIỆU

Tạo khóa phiên (session key)
GPG sẽ tự động tạo một khóa đối xứng ngẫu nhiên (ví dụ AES-256)

↓

Mã hóa nội dung
Dữ liệu gốc (file, văn bản, v.v.) được mã hóa bằng khóa phiên vừa tạo

↓

Mã hóa khóa phiên
Khóa phiên được mã hóa bằng khóa công khai (public key) của người nhận

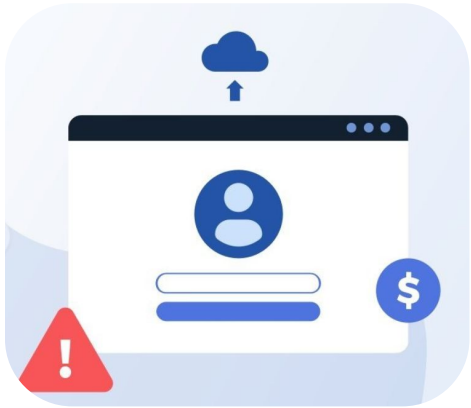
↓

Tổng hợp file đầu ra
File cuối cùng chứa cả nội dung đã mã hóa và khóa phiên đã được mã hóa

B. KÝ SỐ TÀI LIỆU (DIGITAL SIGNATURE)

BĂM TÀI LIỆU GỐC
Sử dụng thuật toán hash để băm tài liệu gốc thành một chuỗi ngắn (digest)

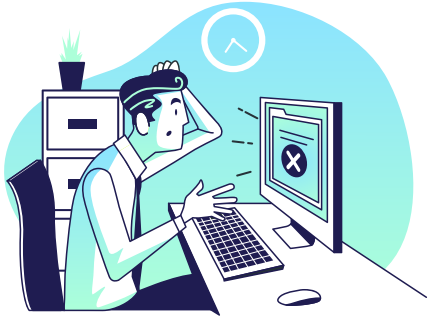
MÃ HÓA DIGEST
Dùng khóa bí mật để mã hóa digest → kết quả là chữ ký số



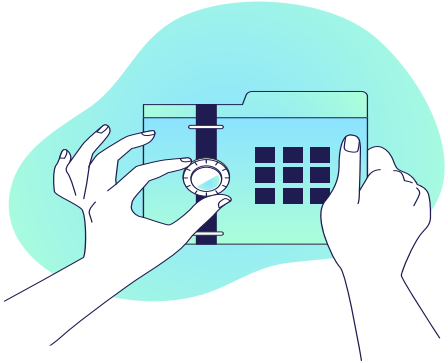
PHÂN PHỐI CHỮ KÝ
Tài liệu có thể được đính kèm chữ ký hoặc đi kèm chữ ký riêng

XÁC MINH CHỮ KÝ
Dùng khóa công khai giải mã chữ ký. Sau đó, so với digest tính lại từ tài liệu gốc.

C. MÔ HÌNH WEB OF TRUST



Người dùng tự xác minh lẫn nhau bằng cách ký vào public key của người khác



Mức độ tin tưởng được phân cấp (trust level), ví dụ: unknown, never, marginal, full, ultimate

VII. ỨNG DỤNG THỰC TẾ

Bảo Vệ Email

Xác Minh Phần Mềm

Ký Commit Git

VIII. LƯU Ý BẢO MẬT

- Không bao giờ chia sẻ khóa bí mật hoặc passphrase.
- Luôn xác minh fingerprint của khóa trước khi sử dụng.
- Tạo và lưu file chứng nhận thu hồi ngay sau khi tạo khóa.
- Cập nhật GPG thường xuyên để tránh lỗ hổng bảo mật.

IX. SO SÁNH VỚI CÁC CÔNG CỤ KHÁC

CÔNG CỤ	ƯU ĐIỂM	NHƯỢC ĐIỂM
GPG	Mã nguồn mở, mạnh mẽ, kiểm soát chi tiết	Cần hiểu rõ cách dùng, học CLI
PGP	Thân thiện người dùng, hỗ trợ thương mại	Trả phí, đóng mã nguồn
Bitlocker	Giúp bảo vệ toàn bộ ổ đĩa	Không hỗ trợ mã hóa file riêng lẻ
Age	Dễ dùng, hiện đại, nhanh	Không hỗ trợ ký số, không tương thích OpenPGP

DEMO

THANK YOU