KHOA CÔNG NGHỆ THÔNG TIN & TRUYỀN THÔNG

**BÁO CÁO**

**AN TOÀN VÀ BẢO MẬT THÔNG TIN**

🙜 🕮 🙞

***Đề tài*: CHỮ KÝ SỐ RSA VÀ HASH 256**

Giảng viên hướng dẫn : Huỳnh Tuấn Hảo

Nhóm 25

Lê Thanh Lương – B1609830

Trần Sĩ Đạt – B1611134

Ông Minh Thuận – B1609847

Nguyễn Phạm Anh Duy – B1611133

Cần Thơ 11 - 2019

**Mục lục**

[**Giới thiệu** 3](#_Toc25678013)

[**1)** **Mật mã bất đối xứng RSA** 3](#_Toc25678014)

[**a)** **Tổng quan** 3](#_Toc25678015)

[**b)** **Lịch sử** 3](#_Toc25678016)

[**2)** **Hàm băm** 4](#_Toc25678017)

[**3)** **Chữ ký số** 4](#_Toc25678018)

[**Nội dung** 5](#_Toc25678019)

[**1.** **Cài đặt giải thuật và giao diện chương trình chữ ký số RSA và Hash 256** 5](#_Toc25678020)

[**a)** **Tạo chữ ký số** 5](#_Toc25678021)

[**b)** **Xác thực chữ ký số** 6](#_Toc25678022)

[**Kết quả** 7](#_Toc25678023)

[**1)** **Giao diện tạo chữ ký số** 7](#_Toc25678024)

[**2)** **Giao diện xác thực chữ ký số** 8](#_Toc25678025)

[**Tài liệu tham khảo** 8](#_Toc25678026)

**Giới thiệu**

1. **Mật mã bất đối xứng RSA**
2. **Tổng quan**

Trong mật mã học, RSA là một thuật toán mã hóa công khai. Đây là thuật toán đầu tiên phù hợp với việc tạo chữ ký điện tử đồng thời với việc mã hóa. Nó đánh dấu một sự tiến bộ vượt bậc của lĩnh vực mật mã học trong việc sử dụng khóa công cộng. RSA đang được sử dụng phổ biến trong lĩnh vực thương mại điện tử và được cho là đảm bảo an toàn với điều kiện độ dài khóa đủ lớn.

Phương pháp mã hóa công khai RSA là một dạng mã hóa cho phép người sử dụng trao đổi các thông tin mật mà không cần phải trao đổi các khóa chung bí mật trước đó. Điều này được thực hiện bằng cách sử dụng cặp khóa có quan hệ toán học với nhau. Một hệ mã hóa công khai sử dụng hai loại khóa:

**Khóa công khai (public key**) được công bố rộng rãi và được sử dụng trong việc mã hóa.

**Khóa riêng (private key)** chỉ do một người nắm giữ và được sử dụng để giải mã thông tin đã được mã hóa bằng khóa công khai

1. **Lịch sử**

Thuật toán RSA được Ron Rivest, Adi Shamir và Len Adleman mô tả lần đầu tiên năm 1977 tại Học viện Massachusetts (MIT). Tên thuật toán này lấy từ 3 chữ cái đầu tên của các tác giả.

Trước đó, vào năm 1973, Clifford Cocks, một nhà toán học người Anh làm việc tại GCHQ (Government Code and Cypher School – Cơ quan tình báo lớn nhất nước anh), đã mô tả thuậ toán tương tự. Với khả năng tính toán tại thời điểm đó thì thuật toán này không khả thi và chưa bao giờ được thực nghiệm. Tuy nhiên, phát minh này chỉ được công bố vào năm 1997 vì được xếp vào loại tuyệt mật.

Thuật toán RSA được đăng ký bằng sáng chế tại Hoa Kỳ vào năm 1983 (Số đăng ký 4.405.829) . Bằng sáng chế này hết hạn vào ngày 21 tháng 9 năm 2000. Tuy nhiên, có giá trị bên ngoài Hoa Kỳ. Ngoài ra, nếu như công trình của Clifford Cocks đã được công bố trước đó thì bằng sáng chế RSA đã không thể đăng ký.

1. **Hàm băm**

Băm là một trong những yếu tố cốt lõi của hệ thống chữ ký số. Quá trình băm bao gồm chuyển đổi dữ liệu có kích thước bất kỳ thành đầu ra có kích thước cố định. Điều này được thực hiện bởi một loại thuật toán đặc biệt gọi là hàm băm. Đầu ra được tạo ra bởi hàm băm được gọi là giá trị băm.

Khi kết hợp với mật mã, các hàm được gọi là hàm băm mật mã có thể được sử dụng để tạo giá trị băm (digest) hoạt động như một dấu vân tay kỹ thuật số duy nhất. Điều này có nghĩa là bất kỳ thay đổi nào trong dữ liệu đầu vào (tin nhắn) sẽ dẫn đến đầu ra hoàn toàn khác (giá trị băm). Và lý do đó là các hàm băm mật mã được sử dụng rộng rãi để xác minh tính xác thực của dữ liệu số.

1. **Chữ ký số**

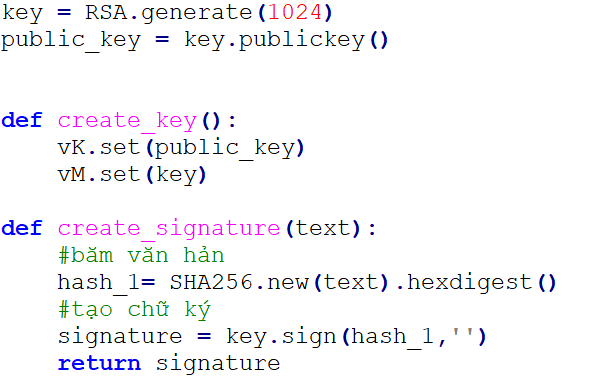
Chữ ký số là một cơ chế mã hóa được sữ dụng để xác minh tính xác thực và toàn vẹn của dữ liệu kỹ thuật số. Nó có thể côi là một phiên bản kỹ thuật số viết tay thông thường, nhưng mức độ phức tạp và bảo mật hơn.

Nói một cách đơn giản, chữ ký viết tay được mã hóa, đính kèm với tin nhắn hoặc tài liệu. Sau khi được tạo, mã đóng vai trò là bằng chứng cho thấy thông tin được gởi đi tới người nhận không bị giả mạo.

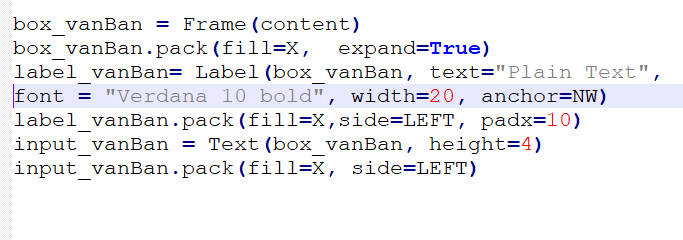
**Nội dung**

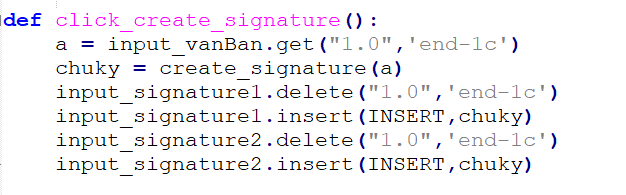
1. **Cài đặt giải thuật và giao diện chương trình chữ ký số RSA và Hash 256**
2. **Tạo chữ ký số**

* **Tạo khóa công khai và khóa bí mật**

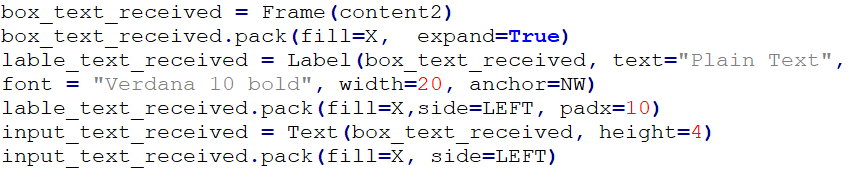


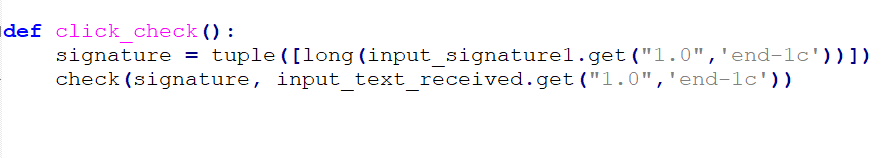
* **Nhập bản rõ gửi đi**



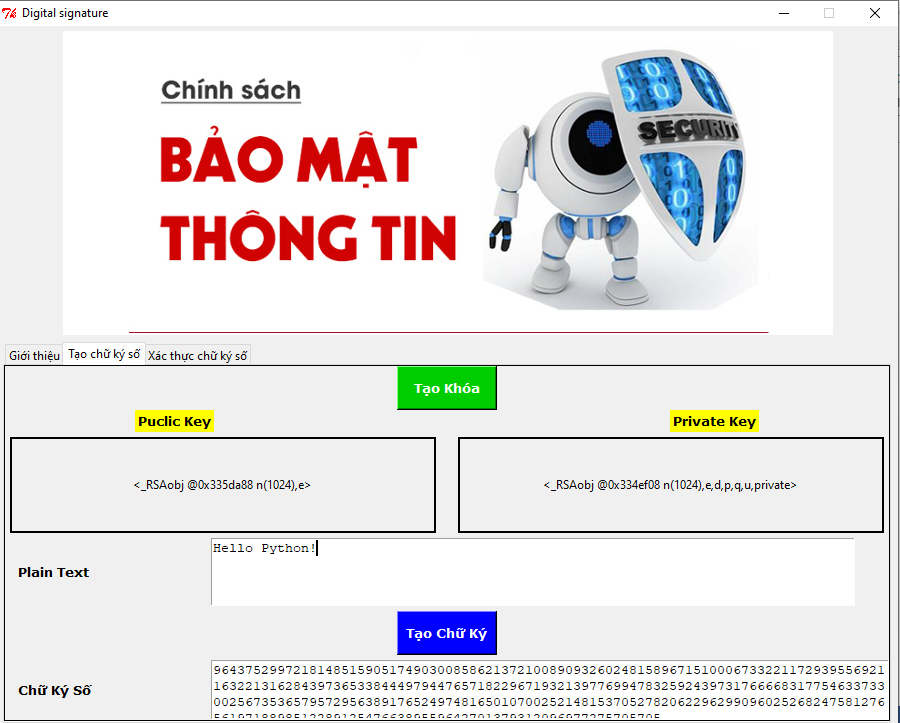
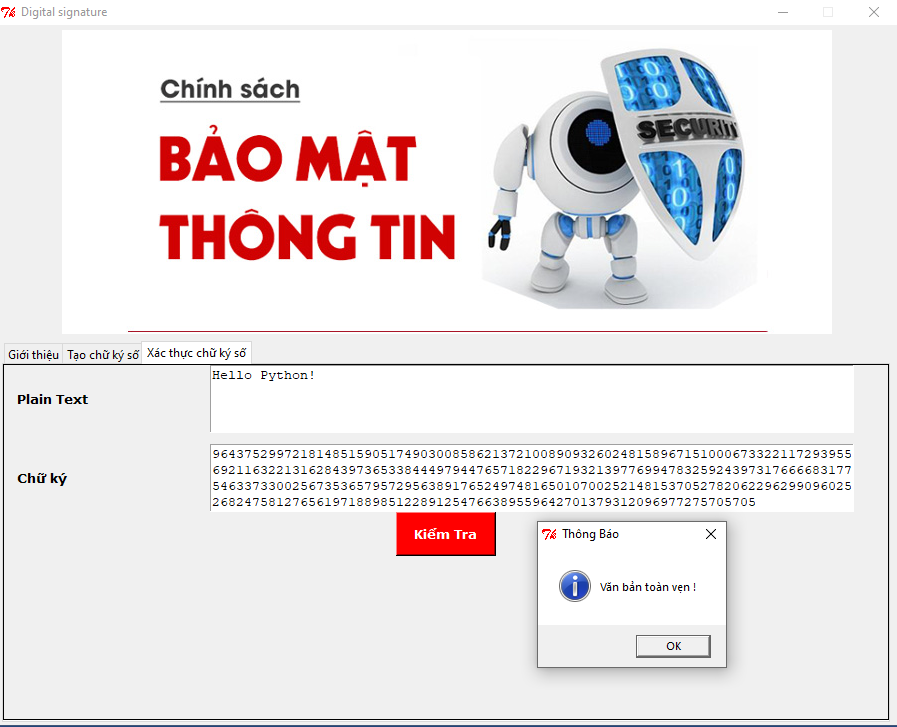
* **Tiến hành tạo chữ ký số cho bản rõ gửi đi**

1. **Xác thực chữ ký số**

* **Nhập bản rõ kiểm tra**
* **Tiến hành kiểm tra**

****

**Kết quả**

1. **Giao diện tạo chữ ký số**
2. **Giao diện xác thực chữ ký số**

**Tài liệu tham khảo**

1. <https://www.dlitz.net/software/pycrypto/api/current/>
2. <https://www.geeksforgeeks.org/python-gui-tkinter/>
3. <https://stackoverflow.com/>
4. <https://github.com/>