TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN ĐIỆN TỬ - VIỄN THÔNG

BỘ MÔN ĐIỆN TỬ HÀNG KHÔNG VŨ TRỤ

LÍ THUYẾT MẬT MÃ

Báo cáo đề tài: Ứng dụng chữ kí số sử dụng hệ mật RSA vào thu thuế

Thành viên nhóm

- Nguyễn Nguyên Bách (20150239) – Điện tử 08 K60
- Trương Công Chính (20130422) – KT ĐT-TT 08 K58
- Mai Văn Hải (20141365) – Điện tử 03 K60
- Nguyễn Minh Hiếu (20151336) – Điện tử 03 K60

NỘI DUNG

I. TỔNG QUAN VỀ CHỮ KÍ SỐ VÀ ỨNG DỤNG

II. GIỚI THIỆU HỆ MẬT RSA

III. ỨNG DỤNG THU THUẾ BẰNG CHỮ KÍ SỐ

I. TỔNG QUAN VỀ CHỮ KÍ SỐ VÀ ỨNG DỤNG

1. Giới thiệu chữ kí số

Chữ kí (viết tay) được sử dụng phổ biến trong các giao dịch hang ngày, như hợp đồng, giấy tờ mua bán, đơn từ, chuyển nhượng,.. như là một hình thức xác nhận bản quyền của người kí về nội dung văn bản được kí. Tuy nhiên, chữ kí viết tay tồn tại một số nhược điểm:

- Có thể bị giả mạo chữ kí
- Trong thời đại máy tính điện tử ngày nay thì việc sử dụng chữ kí viết tay gặp một số vấn đề như: thông tin trên máy tính có thể bị thay đổi, việc thay đổi chữ kí không để lại dấu vết gì như tẩy, xóa với chữ kí viết tay, hình ảnh chữ kí có thể truyền từ máy này sang máy khác, …

=> Khái niệm chữ kí điện tử ra đời, là thông tin đi kèm dữ liệu nhằm xác định người chủ của dữ liệu đó, và chữ kí số là một tập con của chữ kí điện tử. Chữ kí số là một chuỗi dữ liệu liên kết với một thông điệp và thực thể tạo ra thông điệp.

Chữ kí số bản chất là một thông điệp dữ liệu, dựa trên lí thuyết về mật mã hóa bất đối xứng, sử dụng các hệ mật hiện đại. Việc thừa nhận chữ kí số thuộc sở hữu của cơ quan, cá nhân nào đó phải được một cơ quan công an chức thực và cơ quan này phải được thừa nhận về tính pháp lí và kĩ thuật.

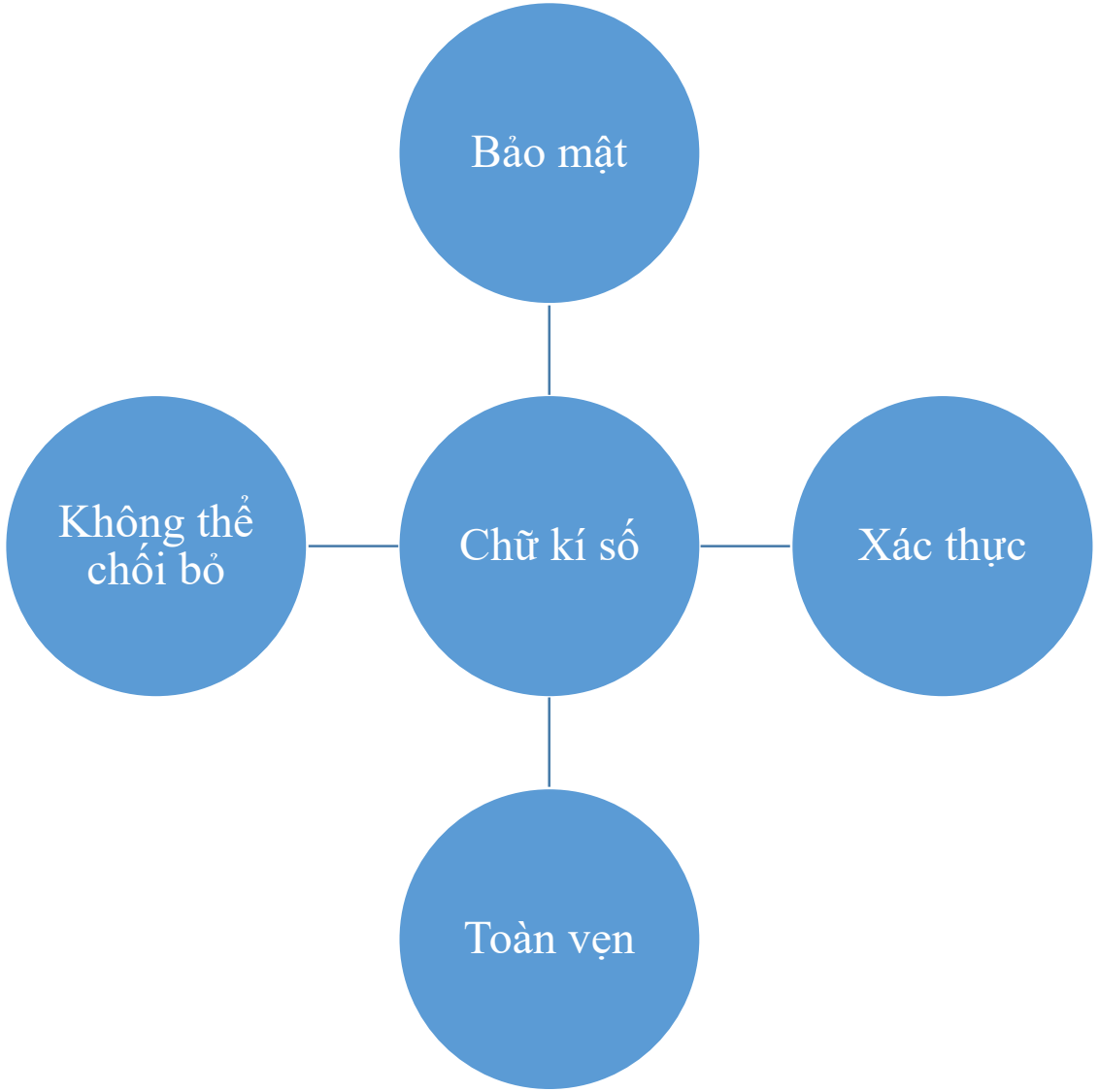
Một chữ kí số phải đảm bào các yêu cầu sau:

- Tính bảo mật: Đảm bảo dữ liệu được truyền đi một cách an toàn, không bị lộ nếu ai đó cố tình muốn có thông điệp gốc ban đầu. Chỉ những người được phép mới có khả năng đọc được nội dung đó.

- Tính xác thực: Giúp người nhận xác định được chắc chắn thông điệp mà họ hận là thông điệp gốc ban đầu. Người giả mạo không thể mạo danh để gửi thông điệp. Người nhận có khả năng kiểm tra nguồn gốc thông điệp họ nhận được.

- Tính toàn vẹn: Người nhận có thể kiểm tra thông điệp không bị thay đổi trong quá trình truyền. Người giả mạo không thể thay thế dữ liệu ban đầu bằng dữ liệu giả mạo

- Tính không thể chối bỏ: Người gửi và nhận không thể chối bỏ sau khi đã gửi và nhận thông điệp.

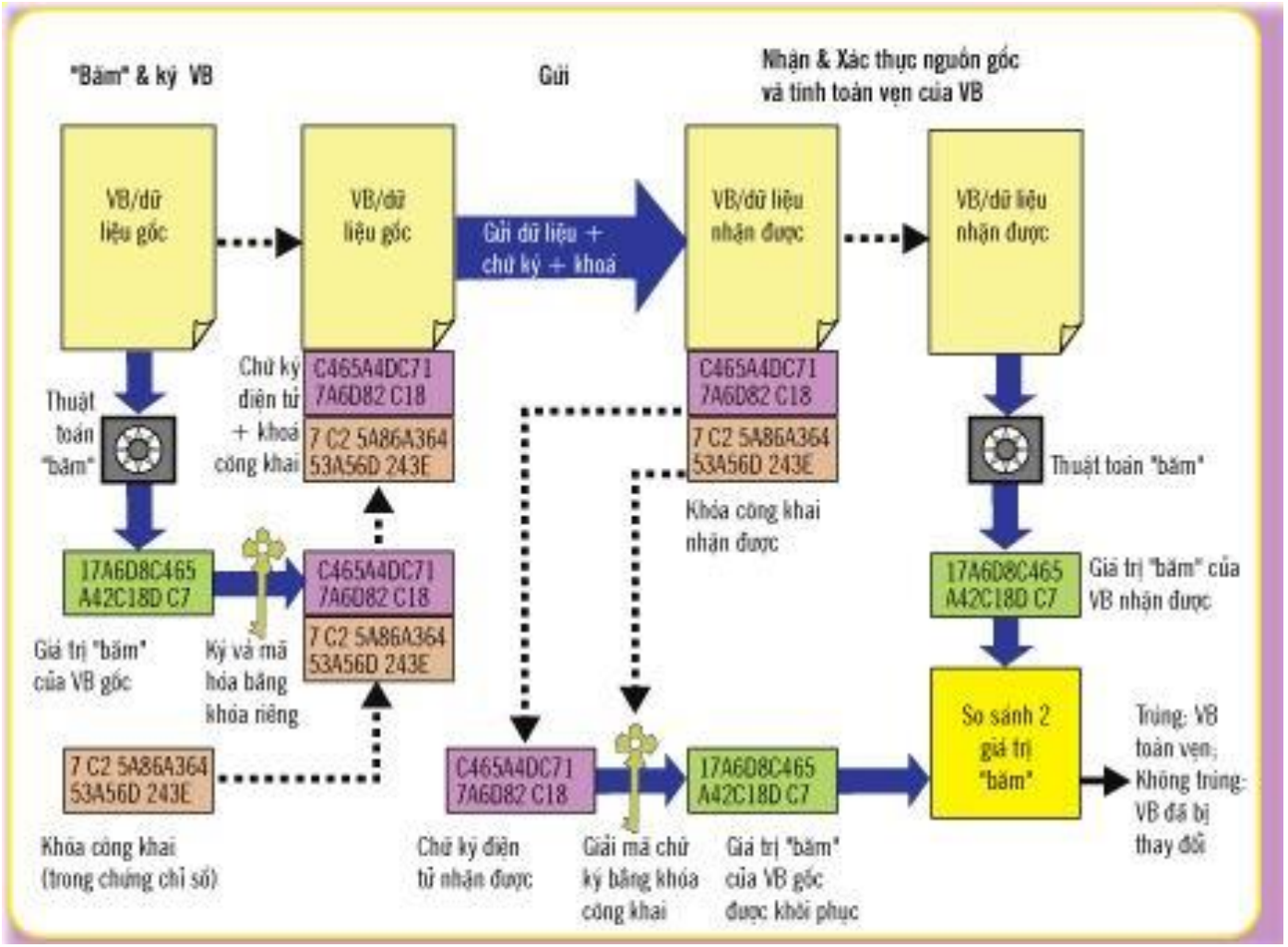


2. Ứng dụng chữ kí số

- Xác thực email trong đổi thông tin trong doanh nghiệp và giữa các doanh nghiệp với nhau
- Sử dụng trong thương mại điện tử, đặt hàng online
- Kiểm soát trong ngân hàng điện tử, thanh toán điện tử
- Áp dụng trên các thiết bị di động thông minh nhằm thực hiện các giao dịch điện tử
- Ứng dụng trong đầu tư chứng khoán, giao dịch điện tử
- Nộp thuế trực tuyến, kê khai hải quan, thông quan trực tuyến, bảo hiểm xã hội điện tử
- …

3. Sơ đồ chữ kí số

- Người gửi
- Sau khi đăng ký một chứng chỉ số,người gửi được cấp một khóa riêng (khóa bí mật).
- Trước khi gửi văn bản, người gửi áp dụng một thuật toán phần mềm để nhận giá trị băm của văn bản gốc.
- Người gửi mã hóa giá trị băm bằng khóa riêng (ký lên giá trị băm), thu được chữ ký số.
- Sau đó văn bản gốc được gửi đi cùng với chữ ký số và khóa công khai của người gửi.
- Người nhận
- Khi nhận thư, người nhận sử dụng khóa công khai giải mã chữ ký số để biết người gửi, đồng thời thu được giá trị băm của văn bản gốc.
- Người nhận cũng dùng thuật toán băm để thu được giá trị băm của văn bản nhận được.
- So sánh 2 giá trị hàm băm để xác nhận chữ kí đúng của người gửi và tính toàn vẹn của dữ liệu.



II. Giới thiệu hệ mật RSA

1. Hệ mật RSA

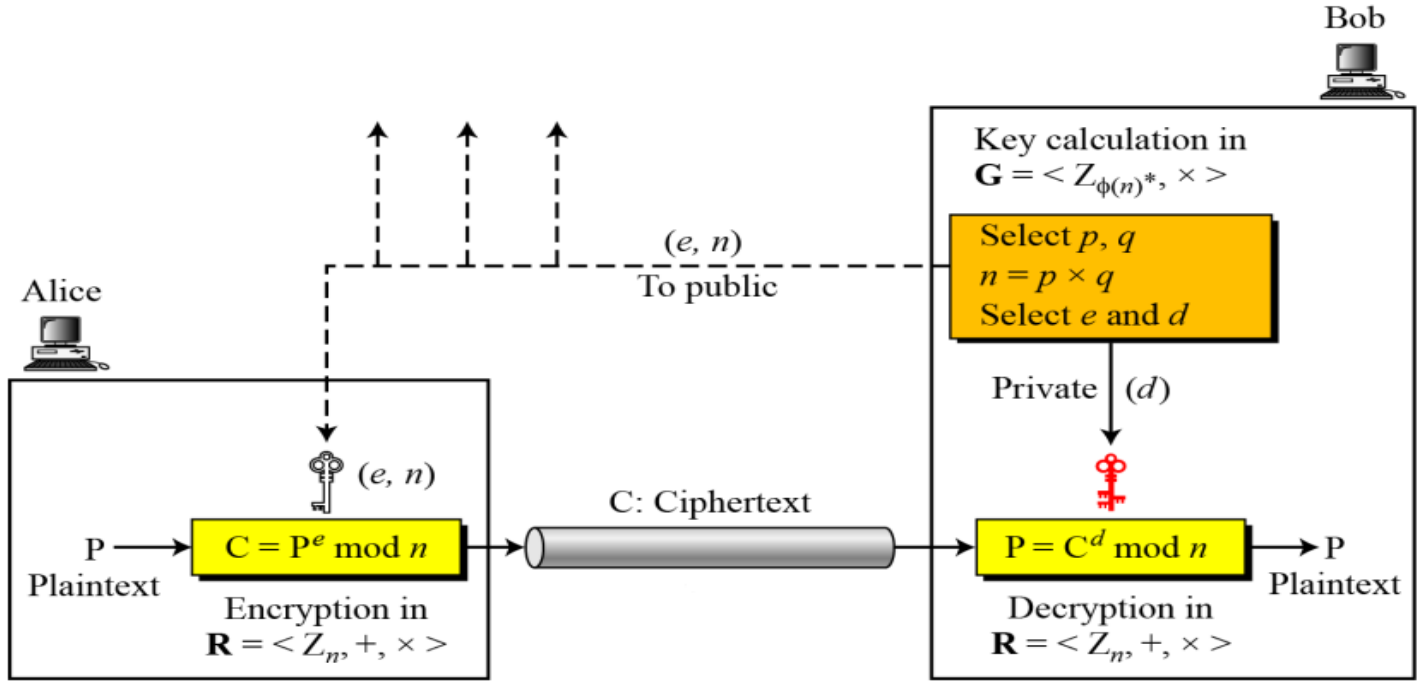
RSA là một hệ mật hiện đại, tên được lấy từ 3 tác giả Ron Rivest, Adi Shamir và Len Adleman công bố lần đầu năm 1977 tại Viện Công nghệ Massachusetts (MIT).

Về cơ bản, RSA hoạt động trên cơ chế sử dụng 2 khóa: khóa công khai và khóa bí mật. Khóa công khai được công khai cho mọi người biết, được sử dụng trong quá trình mã hóa. Tuy nhiên tất cả các thông tin mã hóa bằng khóa công khai chỉ có thể được giải mã bằng khóa bí mật tương ứng với khóa công khai đó.

=> Mọi người đều có thể sử dụng khóa công khai để mã hóa dữ liệu nhưng chỉ có ngươi nắm giữ khóa bí mật mới có thể giải mã

2. Sơ đồ hệ mật RSA

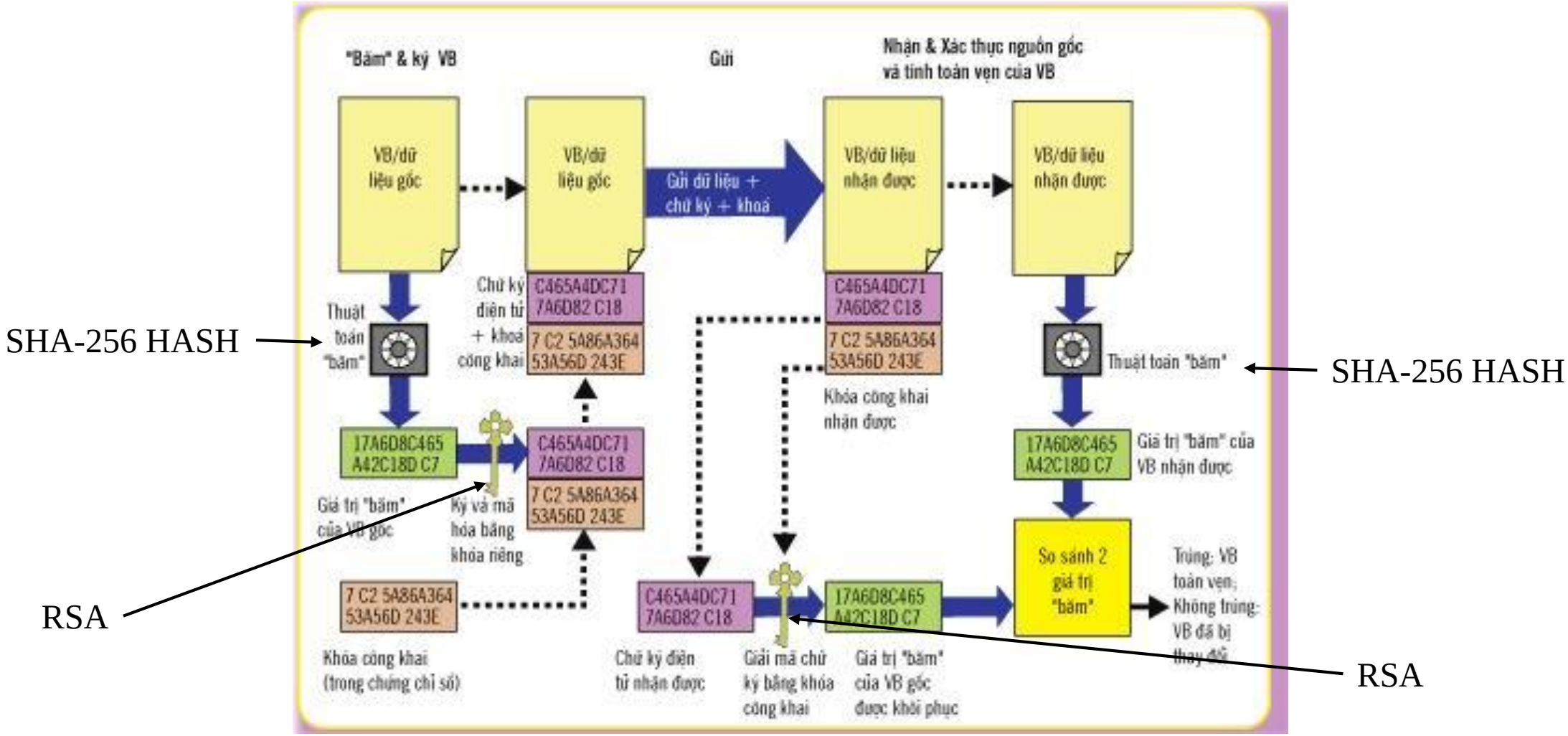
- p,q là 2 số nguyên tố đủ lớn
- n=p*q
- Φ(n)= Φ(p)*Φ(q)
- e và Φ(n) là 2 số nguyên tố cùng nhau
- d=e^{-1}mod Φ(n)
- Khóa công khai là e và n
- Khóa bí mật là d



3. Chữ kí số sử dụng hệ mật RSA

Sử dụng sơ đồ chữ kí số ở phần trước, với một số đặc điểm

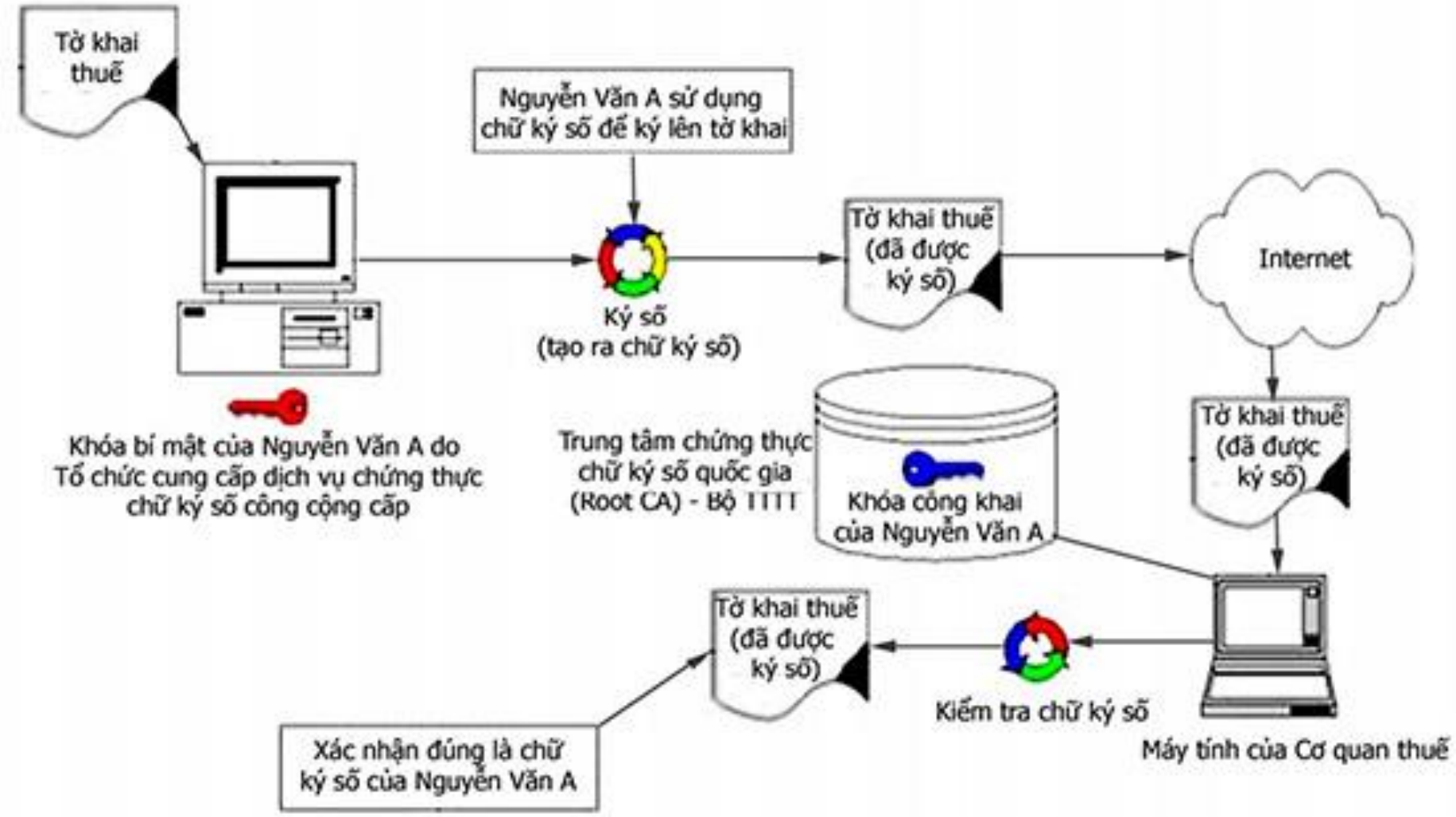
- Hàm băm là SHA-256 HASH
- Hệ mật là RSA



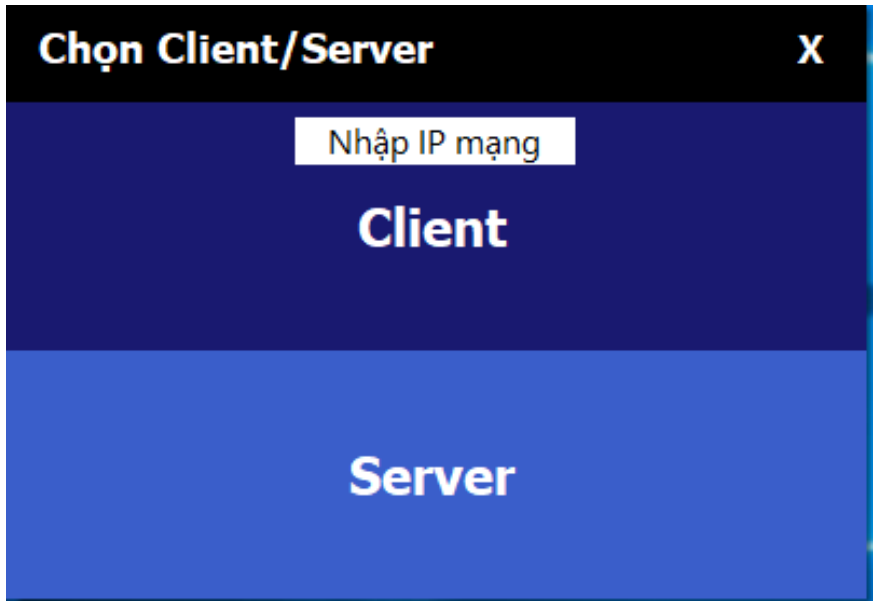
III. ỨNG DỤNG THU THUẾ BẰNG CHỮ KÍ SỐ

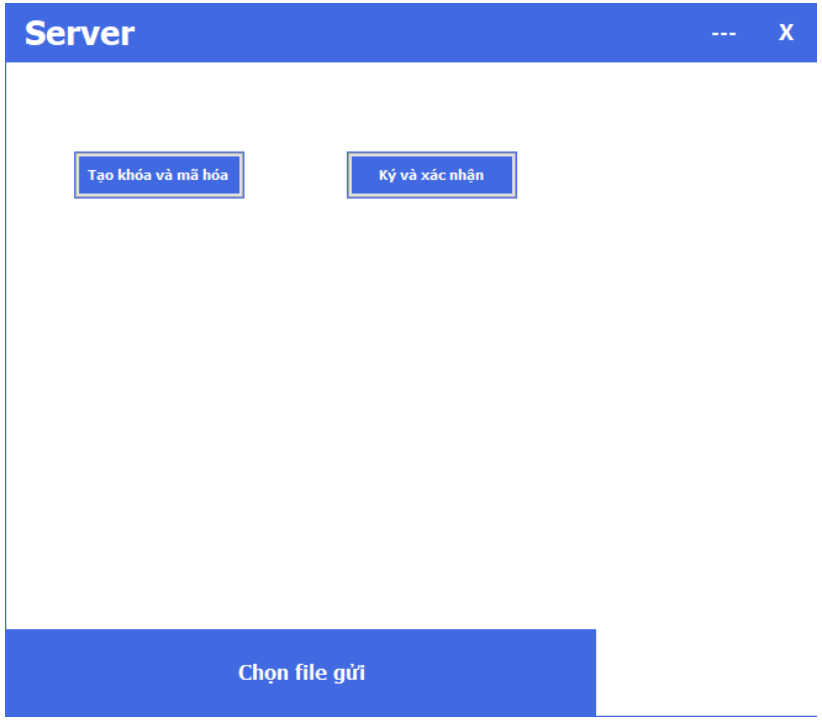
1. Sơ đồ thu thuế bằng chữ kí số

- Nguyễn Văn A sử dụng khóa bí mật do trung tâm chứng thực chữ kí số quốc gia cấp để kí lên tờ khai thuế.
- Tờ khai thuế được gửi đến máy tính của cơ quan thuế.
- Cơ quan thuế sử dụng khóa công khai của trung tâm chứng thực chữ kí số quốc gia để kiểm tra chữ kí số, xác nhận xem chữ kí số đúng của Nguyễn Văn A không.

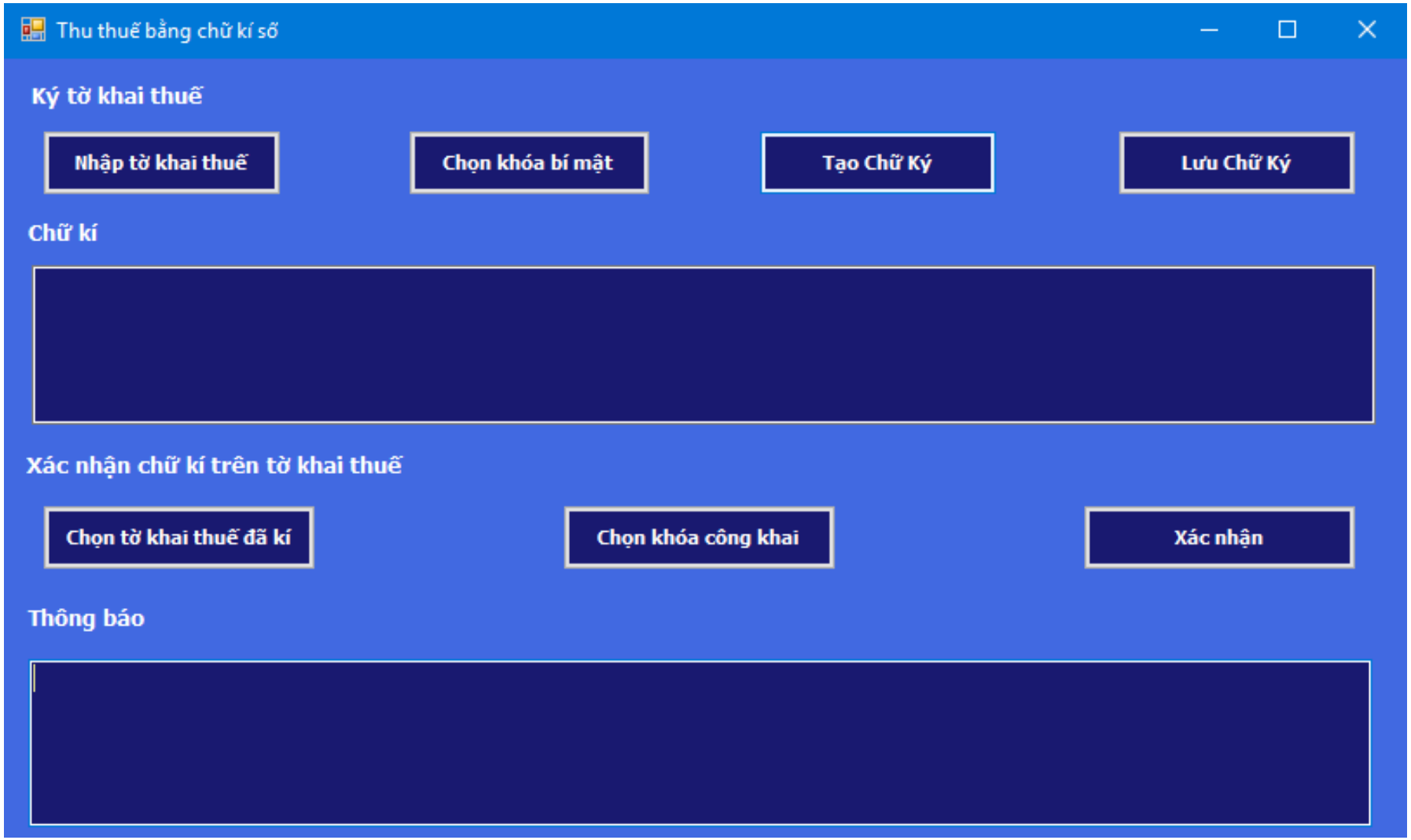


2. Phần mềm mô phỏng






Tạo khóa và mã hóa
Kích thước khóa
Tạo khóa
Làm lại
Khóa công khai
Khóa bí mật
Mã hóa
Bản rõ
Mã hóa
Bản mã hóa
Giải mã
Bản mã hóa
Giải mã
Bản rõ


Thu thuế bằng chữ kí số
Ký tờ khai thuế
Nhập tờ khai thuế
Chọn khóa bí mật
Tạo Chữ Ký
Lưu Chữ Ký
Chữ kí
Xác nhận chữ kí trên tờ khai thuế
Chọn tờ khai thuế đã kí
Chọn khóa công khai
Xác nhận
Thông báo

CẢM ƠN CÁC BẠN ĐÃ XEM VÀ LẮNG NGHE !