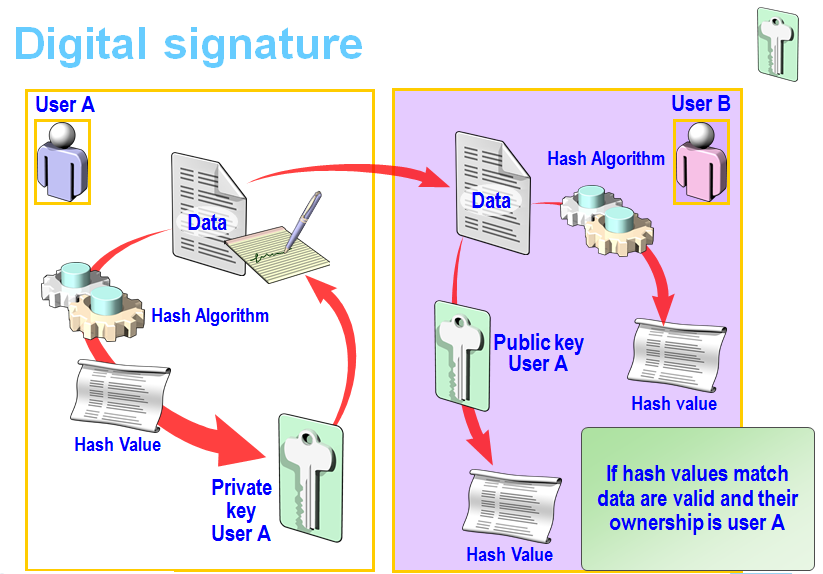
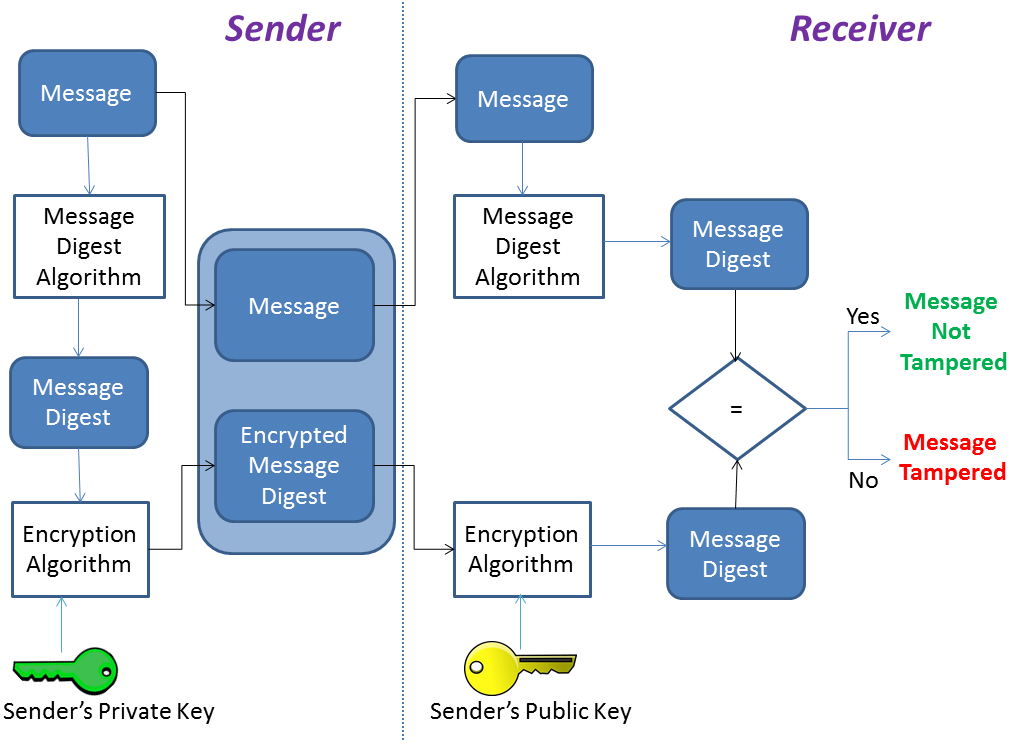
1. **Giới thiệu**

* Một số khái niệm:
  + Chữ kí số (Digital Signature ) là một chuỗi dữ liệu liên kết với một thông điệp (message) và thực thể tạo ra thông điệp.
  + Giải thuật tạo ra chữ ký số (Digital Signature generation algorithm) là một phương pháp sinh chữ ký số.
  + Giải thuật kiểm tra chữ ký số (Digital Signature verification algorithm ) là một phương pháp xác minh tính xác thực của chữ ký số, có nghĩa là nó thực sự được tạo ra bởi 1 bên chỉ định.
  + Một hệ chữ ký số (Figital Signature Scheme) bao gồm giải thuật tạo chữ số và giải thuật kiểm tra chữ kỹ số.
  + Quá trình tạo chữ ký số (Digital Signature signing process) bao gồm:
    - Giải thuật tạo chữ ký số.
    - Phương pháp chuyển dữ liệu thông điệp thành dạng có thể ký được
  + Quá trình kiểm tra chữ ký số (Digital signature verification process) bao gồm:
    - Giải thuật kiểm tra chữ ký số, và
    - Phương pháp khôi phục dữ liệu từ thông điệp
  + Hàm băm (Hash Funtion) làm hàm toán học chuyển đổi thông điệp (message) có độ dài bất kỳ (hữu hạn) thành một dãy bít có độ dài cố định (tùy thuộc vào thuật toán băm). Dãy bít này được gọi là thông điệp rút gọn.(message disgest) hay giá trị băm (hash value), đại diện cho thông điệp ban đầu.
    - Hàm băm SHA-1: Thuật toán SHA-1 nhận thông điệp ở đầu vào có chiều dài k<264 bit, thực hiện xử lý và đưa ra thông điệp thu gọn (message digest) có chiều dài cố định 160 bits. Quá trình tính toán cũng thực hiện theo từng khối 512bits, nhưng bộ đệm xử lý dùng 5 thanh ghi 32-bits. Thuật toán này chạy tốt với các bộ vi xử lý có cấu trúc 32 bits.
* Ví dụ minh chứng : Ta có thể mô phỏng trực quan một hệ mật mã khoá công khai như sau : Bob muốn gửi cho Alice một thông tin mật mà Bob muốn duy nhất Alice có thể đọc được. Để làm được điều này, Alice gửi cho Bob một chiếc **hộp có khóa đã mở sẵn (Khóa công khai)** và giữ lại chìa khóa. Bob nhận chiếc hộp, cho vào đó một tờ giấy viết thư bình thường và khóa lại (như loại khoá thông thường chỉ cần sập chốt lại, sau khi sập chốt khóa ngay cả Bob cũng không thể mở lại được-không đọc lại hay sửa thông tin trong thư được nữa). Sau đó Bob gửi chiếc hộp lại cho Alice. Alice mở hộp với chìa khóa của mình và đọc thông tin trong thư. Trong ví dụ này, chiếc hộp với khóa mở đóng vai trò khóa công khai, chiếc chìa khóa chính là khóa bí mật.
* Lược đồ chữ ký số RSA.
  + Trong phần này mô tả lược đồ chữ ký RSA. Độ an toàn của lược đồ chữ ký RSA dựa vào độ an toàn của hệ mã RSA. Lược đồ bao gồm cả chữ ký số kèm theo bản rõ và tự khôi phục thông điệp từ chữ ký số.
    - Thuật toán sinh khóa cho lược đồ chữ ký RSA
    - Thuật toán sinh chữ ký RSA
    - Thuật toán chứng thực chữ ký RSA

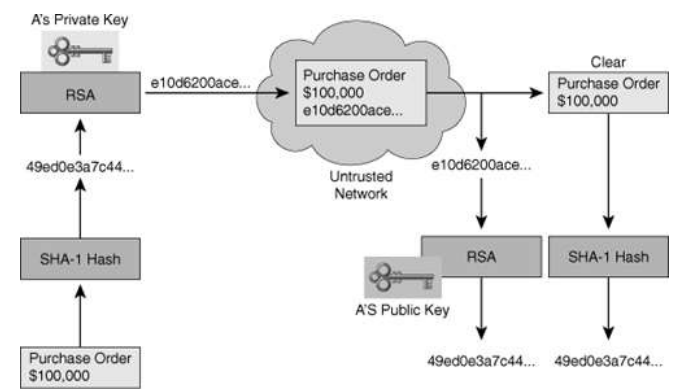
1. **Nội dung**
2. **Kiến trúc**

**1.1 Kiến trúc chữ ký số tổng quát**

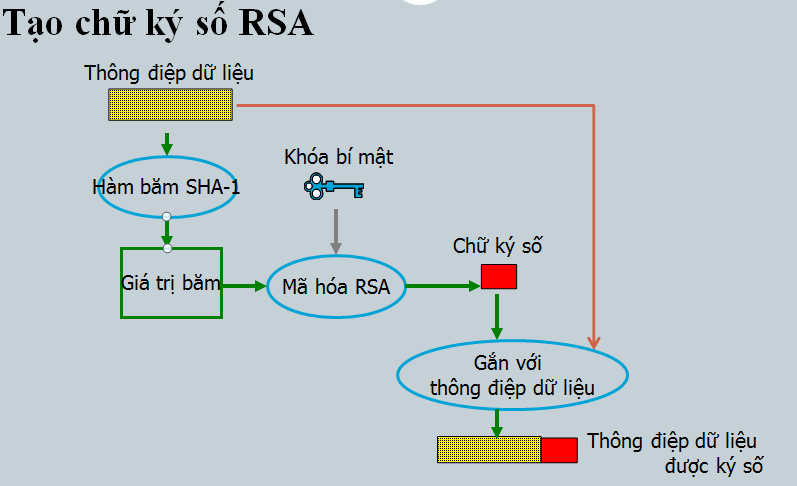


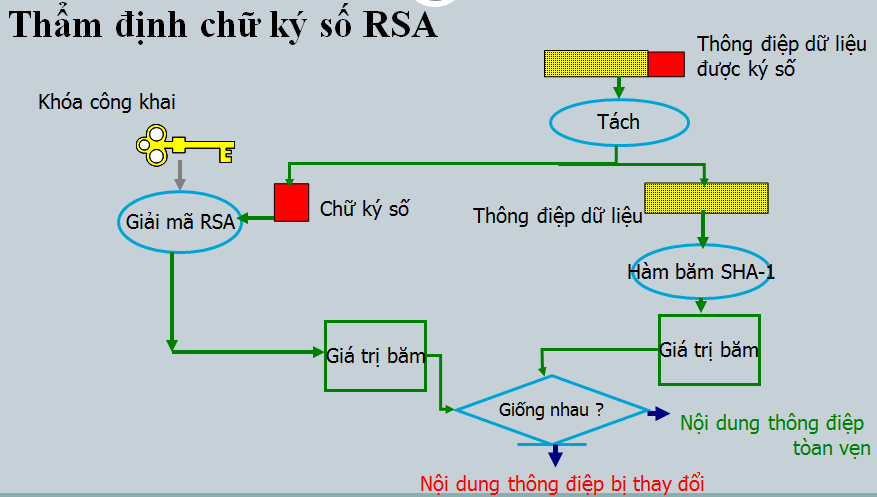


* 1. Quá trình ký (bên gửi)
* Tính toán chuỗi đại diện (message digest/ hash value) của thông điệp sử dụng một giải thuật băm (Hashing algorithm)
* Chuỗi đại diện được ký sử dụng khóa riêng (Priavte key) cảu người gửi va 1 giải thuật tạo chữ ký (Signature/ Encryption algorithm). Kết quả chữ ký số (Digital signature) của thông điệp hay còn gọi là chuỗi đại diện được mã hóa (Encryted message digest)
* Thông điệp ban đầu (message) được ghép với chữ ký số( Digital signature) tạo thành thông điệp đã được ký (Signed message)
* Thông điệp đã được ký (Signed message) được gửi cho người nhận
  1. Quá trình kiểm tra chữ ký (bên nhận)
* Tách chữ ký số và thông điệp gốc khỏi thông điệp đã ký để xử lý riêng;
* Tính toán chuỗi đại diện MD1 (message digest) của thông điệp gốc sử dụng giải thuật băm (là giải thuật sử dụng trong quá trình ký)
* Sử dụng khóa công khai (Public key) của người gửi để giải mã chữ ký số -> chuỗi đại diện thông điệp MD2
* So sánh MD1 và MD2:
  + Nếu MD1 =MD2 -> chữ ký kiểm tra thành công. Thông điệp đảm bảo tính toàn vẹn và thực sự xuất phát từ người gửi (do khóa công khai được chứng thực).
  + Nếu MD1 <>MD2 -> chữ ký không hợp lệ. Thông điệp có thể đã bị sửa đổi hoặc không thực sự xuất phát từ người gửi.
  1. **Kiến trúc chữ ký số RSA**



Cụ thể hơn:



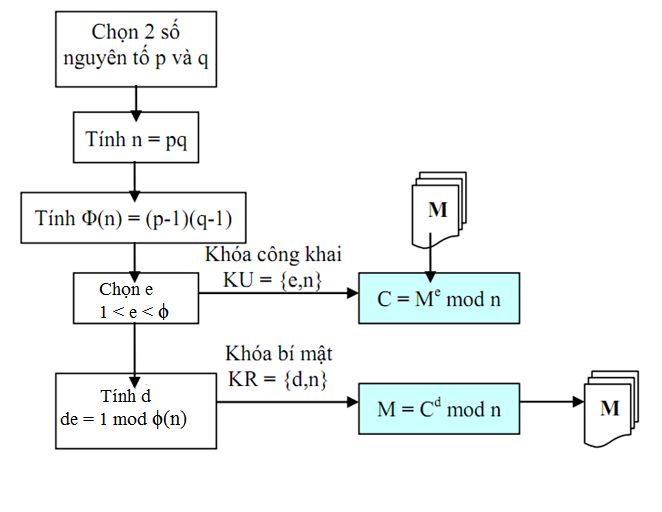


* 1. Quá trình ký (bên gửi)
* Tính toán chuỗi đại diện (message digest/ hash value) của thông điệp sử dụng một giải thuật băm (Hashing algorithm) SHA-1
* Chuỗi đại diện được ký sử dụng khóa riêng (Priavte key) của người gửi và giải thuật tạo chữ ký (Signature/ Encryption algorithm) RSA. Kết quả chữ ký số (Digital signature) của thông điệp hay còn gọi là chuỗi đại diện được mã hóa bởi giải thuật RSA (Encryted message digest)
* Thông điệp ban đầu (message) được ghép với chữ ký số( Digital signature) tạo thành thông điệp đã được ký (Signed message)
* Thông điệp đã được ký (Signed message) được gửi cho người nhận
  1. Quá trình kiểm tra chữ ký (bên nhận)
* Tách chữ ký số RSA và thông điệp gốc khỏi thông điệp đã ký để xử lý riêng;
* Tính toán chuỗi đại diện MD1 (message digest) của thông điệp gốc sử dụng giải thuật băm (là giải thuật sử dụng trong quá trình ký là SHA-1)
* Sử dụng khóa công khai (Public key) của người gửi để giải mã chữ ký số RSA-> chuỗi đại diện thông điệp MD2
* So sánh MD1 và MD2:
  + Nếu MD1 =MD2 -> chữ ký kiểm tra thành công. Thông điệp đảm bảo tính toàn vẹn và thực sự xuất phát từ người gửi (do khóa công khai được chứng thực).
  + Nếu MD1 <>MD2 -> chữ ký không hợp lệ. Thông điệp có thể đã bị sửa đổi hoặc không thực sự xuất phát từ người gửi.

1. **Giải thuật và cài đặt giải thuật**

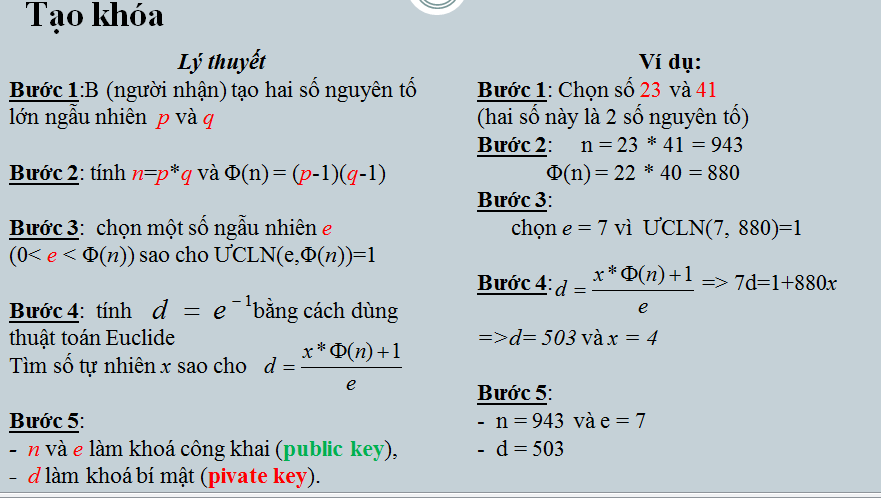
**2.1 Giải thuật RSA được dùng trong việc tạo khóa, mã hóa, giải mã.**

Sơ đồ giải thuật :

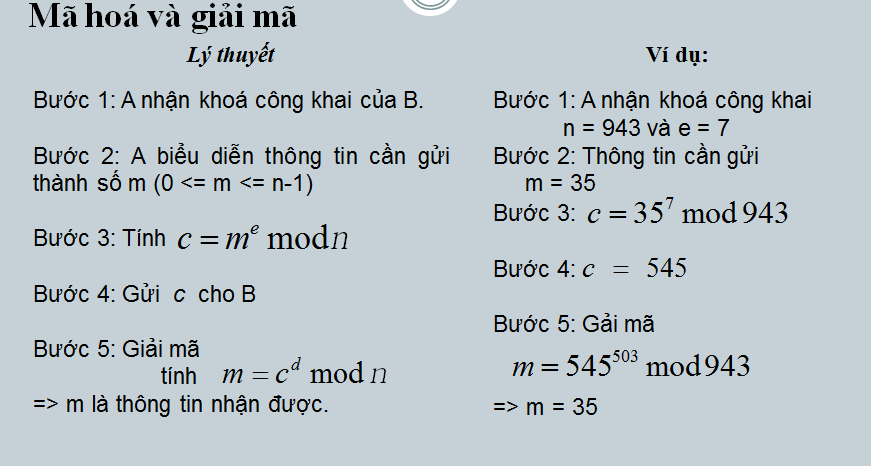
******

|  |  |
| --- | --- |
| Thuật toán RSA có hai Khóa:  **- *Khóa công khai*** (**Public key**): được công bố rộng rãi cho mọi người và được dùng để mã hóa  **-** ***Khóa bí mật*** (**Private key**):  Những thông tin được mã hóa bằng khóa công khai chỉ có thể  được giải mã bằng khóa bí mật tương ứng | C:\Users\Mr Khiem\Desktop\RSA\Báo cáo\TQRSA.png |

* 1. Tạo khóa



* 1. Mã hóa và giải mã



**3.Ứng dụng chữ ký số sử dụng giải thuật RSA**

-Sử dụng trong việc đảm bảo vẹn toàn dữ liệu: Chữ ký, công văn, file, tệp tin của người gửi qua môi trường Internet của các cá nhân , cơ quan tổ chức ….