ĐẠI HỌC THÁI NGUYÊN

# TRƢỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

**-------o0o-------**

# PHẠM THỊ TÂM

MỘT SỐ THUẬT TOÁN CHỮ KÝ SỐ VÀ ỨNG DỤNG TRONG BẢO MẬT TÀI LIỆU ĐIỆN TỬ

# LUẬN VĂN THẠC SĨ KHOA HỌC CÔNG NGHỆ THÔNG TIN

**Chuyên ngành: Khoa học máy tính Mã số: 60.48.01.01**

# Ngƣời hƣớng dẫn khoa học: PGS.TS. Đoàn Văn Ban

**Thái Nguyên, 2017**

# LỜI CẢM ƠN

Trƣớc tiên tôi xin gửi lời cảm ơn chân thành nhất đến thầy giáo PGS. TS Đoàn Văn Ban, ngƣời đã định hƣớng và nhiệt tình hƣớng dẫn, cung cấp tài liệu, giúp đỡ tôi rất nhiều trong quá trình học tập và hoàn thiện luận văn.

Tôi xin gửi lời biết ơn sâu sắc đến các thầy, các cô đã tạo điều kiện thuận lợi và truyền đạt những kiến thức, kinh nghiệm quý báu cho chúng tôi trong suốt hai năm học cao học tại Trƣờng Đại học Công nghệ thông tin và Truyền thông – Đại học Thái Nguyên.

Tôi xin cảm ơn bạn bè, đồng nghiệp và gia đình, những ngƣời luôn gần gũi, động viên và chia sẻ cùng tôi trong suốt thời gian làm luận văn tốt nghiệp.

Tôi xin chân thành cảm ơn!

*Thái Nguyên, tháng 4 năm 2017*

# Tác giả

**Phạm Thị Tâm**

# LỜI CAM ĐOAN

Tôi là Phạm Thị Tâm, học viên cao học lớp CK14B khóa 2015-2017. Thầy giáo hƣớng dẫn là PGS.TS Đoàn Văn Ban.

Tôi xin cam đoan bản luận văn “Một số thuật toán chữ ký số và ứng dụng trong bảo mật tài liệu điện tử” là công trình nghiên cứu của tôi, dƣới sự hƣớng dẫn khoa học của PGS.TS Đoàn Văn Ban, tham khảo các nguồn tài liệu đã đƣợc chỉ rõ trong trích dẫn và danh mục tài liệu tham khảo. Các nội dung công bố và kết quả trình bày trong luận văn này là trung thực và chƣa đƣợc ai công bố trong bất kỳ công trình nào.

*Thái Nguyên, ngày tháng năm 2017*

# Phạm Thị Tâm

**MỤC LỤC**

[MỞ ĐẦU 7](#_TOC_250049)

[CHƢƠNG I: BẢO MẬT THÔNG TIN VÀ CHỮ KÝ SỐ 11](#_TOC_250048)

* 1. [Bảo mật thông tin 11](#_TOC_250047)
     1. [Vấn đề an toàn thông tin 11](#_TOC_250046)
     2. [Mã hóa tài liệu 12](#_TOC_250045)
     3. [Chữ ký số 15](#_TOC_250044)
  2. [Phân loại các lƣợc đồ chữ ký số 19](#_TOC_250043)
     1. [Lƣợc đồ chữ ký kèm thông điệp 19](#_TOC_250042)
     2. [Lƣợc đồ chữ ký khôi phục thông điệp 21](#_TOC_250041)
  3. [Một số lƣợc đồ chữ ký số cơ bản 22](#_TOC_250040)
     1. [Lƣợc đồ chữ ký RSA (Rivest, Shamir, Adleman) 22](#_TOC_250039)
     2. [Lƣợc đồ chữ ký Elgamal 25](#_TOC_250038)
  4. [Các phƣơng pháp tấn công chữ ký điện tử 28](#_TOC_250037)
  5. [Tính pháp lý và ứng dụng chữ ký số 29](#_TOC_250036)
     1. [Trong nƣớc 29](#_TOC_250035)
     2. [Ở một số nƣớc trên thế giới 31](#_TOC_250034)

[1.5.3 Ứng dụng trong thực tế 32](#_TOC_250033)

* 1. [Kết luận chƣơng 32](#_TOC_250032)

[CHƢƠNG II. THUẬT TOÁN CHỮ KÝ SỐ 34](#_TOC_250031)

* 1. [Hàm băm và thuật toán chữ ký số 34](#_TOC_250030)
     1. [Hàm băm (Hash) 34](#_TOC_250029)
     2. [Thuật toán băm SHA 35](#_TOC_250028)
     3. [Mối quan hệ giữa hàm băm và thuật toán ký số 38](#_TOC_250027)
  2. [Thuật toán chữ ký số chuẩn DSA 40](#_TOC_250026)
     1. [Tóm tắt lƣợc đồ chữ ký DSA/DSS 41](#_TOC_250025)
     2. [Thuật toán 42](#_TOC_250024)
     3. [Đặc trƣng của DSS 43](#_TOC_250023)
  3. [Thuật toán chữ ký số trên đƣờng cong Elliptic ECDSA 44](#_TOC_250022)
     1. [Lý thuyết đƣờng cong Elliptic 45](#_TOC_250021)

Các phép toán trên đƣờng cong Elliptic 46

* + 1. [Đƣờng cong eliptic trên các trƣờng hữu hạn 49](#_TOC_250020)
    2. [Miền tham số ECDSA 54](#_TOC_250019)
    3. [Cặp khóa ECDSA 61](#_TOC_250018)
    4. [Sinh và xác nhận chữ ký ECDSA 63](#_TOC_250017)
  1. [Tính bảo mật chữ ký số ECDSA 65](#_TOC_250016)
     1. [Mật mã đƣờng cong Elliptic 65](#_TOC_250015)
     2. [Vấn đề của chữ ký số trên đƣờng cong Elliptic 66](#_TOC_250014)
  2. [Kết luận chƣơng 67](#_TOC_250013)

[CHƢƠNG III. ỨNG DỤNG CHỮ KÝ SỐ TRONG BẢO MẬT TÀI LIỆU ĐIỆN TỬ 69](#_TOC_250012)

* 1. [Ý tƣởng về chƣơng trình ứng dụng 69](#_TOC_250011)
     1. [Lĩnh vực ứng dụng của chƣơng trình 69](#_TOC_250010)
     2. [Ý tƣởng xây dựng chƣơng trình 69](#_TOC_250009)
  2. [Xây dựng chƣơng trình 69](#_TOC_250008)
     1. [Chữ ký số ECDSA 69](#_TOC_250007)
     2. [Thông số và thuật toán 70](#_TOC_250006)
     3. [Giao diện chƣơng trình 71](#_TOC_250005)
  3. [Kết luận chƣơng 72](#_TOC_250004)

[Kết luận và hƣớng phát triển 73](#_TOC_250003)

[Kết quả đạt đƣợc của luận văn 73](#_TOC_250002)

[Hƣớng phát triển 73](#_TOC_250001)

[TÀI LIỆU THAM KHẢO 74](#_TOC_250000)

# DANH MỤC CÁC KÝ HIỆU VÀ CÁC TỪ VIẾT TẮT

|  |  |
| --- | --- |
| DSA | Digital Signature Algorithm |
| ECC | Elliptic Curve Cryptograpthy |
| ECDLP | Elliptic Curve Discrete Logarithm Problem |
| ECDSA | [Elliptic Curve Digital Signature Algorithm](https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm) |
| RSA | Rivesr, Shamir, Adleman |
| TCP/IP | Transfer Control Protocol/Internet Protocol |
| DES | Data Encryption Standard |
| IDEA | Internation Data Encryption Algorithm |
| AES | Advance Encryption Standard |
| P | Plaintext |
| C | Ciphertext |
| K | Key |
| E | Encrytion |
| D | Decrytion |
| DSS | Digital Signature Standart |
| SHA | Security Hash Algorithm |
| MD | Message Digest |
| FIPS | Federal Information Processing Standard |
| NIST | the National Institute of Standards and Technology |
| ISO | International Organization for Standardization |
| IEEE | Institute of Electrical and Elactronic Engineers |
| ANSI | American National Standard Institute |
| VNPT | Tập đoàn Bƣu chính viễn thông Việt Nam |

**DANH MỤC CÁC HÌNH**

Hình 1.1. Hệ mã hóa khóa bí mật 13

Hình 1.2. Hệ mã hóa khóa công khai 14

Hình 1.3. Phân loại lƣợc đồ chữ ký số 19

Hình 1.4. Mô hình lƣợc đồ chữ ký kèm thông điệp 21

Hình 1.5. Mô hình Lƣợc đồ chữ ký khôi phục thông điệp 22

Hình 1.6. Sơ đồ biểu diễn thuật toán mã hóa 24

[Hình 2.1. Xử lý thông tin trong SHA-1 37](#_bookmark0)

[Hình 2.2. Hệ sinh chữ ký điện tử có sử dụng hàm băm 38](#_bookmark1)

[Hình 2.3. Hàm băm kiểm tra tính toàn vẹn dữ liệu 39](#_bookmark2)

[Hình 2.4. Sơ đồ chữ ký DSA/DSS 41](#_bookmark3)

[Hình 2.5. Đƣờng cong Elliptic y2 = x3 - 3x + 1 45](#_bookmark4)

[Hình 2.6. Phép cộng trên đƣờng cong Elliptic 47](#_bookmark5)

[Hình 2.7. Phép nhân đôi trên đƣờng cong Elliptic 48](#_bookmark6)

[Hình 2.8. Đặc tả hình học của phép cộng của hai điểm riêng biệt trên đƣờng](#_bookmark7) [cong elliptic: P + Q = R 50](#_bookmark7)

[Hình 2.9. Mô tả hình học của phép nhân đôi của một điểm đƣờng cong](#_bookmark8) [elliptic: P + P = R 51](#_bookmark8)

[Hình 3.1. Tạo khóa ngẫu nhiên 71](#_bookmark9)

[Hình 3.2. Thực hiện ký lên tài liệu/văn bản 71](#_bookmark10)

[Hình 3.3. Kiểm tra sự toàn vẹn của tài liệu/văn bản 72](#_bookmark11)

# MỞ ĐẦU

1. **Đặt vấn đề**

Hiện nay, các giao dịch điện tử ngày càng trở nên phổ biến, việc bảo mật, bảo đảm an toàn thông tin dữ liệu trở thành vấn đề thời sự, là một chủ đề rộng có liên quan đến nhiều lĩnh vực và trong thực tế có thể có nhiều phƣơng pháp đƣợc thực hiện để đảm bảo an toàn thông tin dữ liệu. Ngày nay, với sự phát triển nhanh chóng của các hệ thống thông tin trên mạng thì các nguy cơ xâm nhập vào các hệ thống thông tin, các mạng dữ liệu ngày càng gia tăng. Vấn đề bảo mật đã và đang đƣợc nhiều ngƣời tập trung nghiên cứu, tìm mọi giải pháp để đảm bảo an toàn, an ninh cho hệ thống phần mềm, đặc biệt là các hệ thống thông tin trên mạng.

Sự phát triển mạnh mẽ của Internet về bản chất chính là việc đáp ứng lại sự gia tăng không ngừng của nhu cầu giao dịch trực tuyến trên hệ thống mạng toàn cầu. Các giao dịch trực tuyến trên Internet phát triển từ những hình thức sơ khai nhƣ trao đổi thông tin (email, message, …), quảng bá (publicshing) đến những giao dịch phức tạp thể hiện qua các hệ thống chính phủ điện tử, thƣơng mại điện tử ngày càng phát triển mạnh mẽ trên toàn cầu. Tuy nhiên, vấn đề an toàn thông tin lại đƣợc nảy sinh từ đây. Internet có những kỹ thuật cho phép mọi ngƣời truy cập, khai thác và chia sẻ thông tin với nhau. Nhƣng nó cũng là nguy cơ chính dẫn đến thông tin của chúng ta bị hƣ hỏng hay bị phá hủy hoàn toàn.

Để vừa đảm bảo tính bảo mật của thông tin lại không làm giảm sự phát triển của việc trao đổi thông tin quảng bá trên toàn cầu thì chúng ta phải có các giải pháp phù hợp. Hiện có rất nhiều giải pháp cho vấn đề an toàn thông tin trên mạng nhƣ mã hóa thông tin, chữ ký điện tử, chứng chỉ điện tử (chứng chỉ khóa công khai) , … Giải pháp chữ ký số hiện là một giải pháp an toàn và hiệu quả. Chữ ký số đƣợc sử dụng để bảo đảm tính bảo mật, tính toàn vẹn, tính chống chối bỏ của các thông tin giao dịch trên mạng Internet.

Chữ ký số tƣơng đƣơng với chữ ký tay nên có giá trị sử dụng trong các ứng dụng giao dịch điện tử với máy tính và mạng Internet cần tính pháp lý cao. Đồng thời, là một phƣơng tiện điện tử đƣợc pháp luật thừa nhận về tính pháp lý. Bên cạnh đó, chữ ký số còn là một công nghệ mã hóa và xác thực rất mạnh, thể giúp bảo đảm an toàn, bảo mật cao cho các giao dịch trực tuyến, nhất là các giao dịch chứa các thông tin liên quan đến tài chính. Ứng dụng chữ ký số sẽ đem lại cho doanh nghiệp, tổ chức rất nhiều lợi ích nhƣ: Tiết kiệm chi phí giấy tờ, thời gian luân chuyển trong hoạt động quản lý công văn, giấy tờ, thƣ điện tử; Giúp đẩy nhanh các giao dịch qua mạng trong khi vẫn đảm bảo độ an toàn và bảo mật thông tin, …

Nhận thấy sự thiết thực của chữ ký số trong các tài liệu, văn bản điện tử, trong các giao dịch qua mạng, … và đƣợc sự gợi ý của giáo viên hƣớng dẫn, em đã chọn đề tài “Ứng dụng chữ ký số và ứng dụng trong bảo mật tài liệu điện tử” làm đề tài cho luận văn thạc sỹ của mình. Luận văn tập trung vào nghiên cứu hai thuật toán chính là thuật toán chữ ký số chuẩn DSA, thuật toán chữ ký số đƣờng cong Eliptic. Đây là hai thuật toán mới mà các luận văn gần trƣớc đây chƣa đề cập đến khi nghiên cứu về thuật toán tạo chữ ký số.

# Đối tƣợng và phạm vi nghiên cứu

*\*Đối tượng nghiên cứu:*

+ Tìm hiểu về các giải pháp mã hóa để bảo mật thông tin.

+ Nghiên cứu những phƣơng pháp, kỹ thuật tạo chữ ký số trên các tài liệu, văn bản điện tử.

*\*Phạm vi nghiên cứu:*

Luận văn tập trung nghiên cứu các kiến thức có liên quan, các cơ sở lý thuyết: về một số giải pháp mã hóa và những phƣơng pháp, kỹ thuật tạo chữ ký số để ứng dụng trong bảo mật tài liệu.

# Hƣớng nghiên cứu của đề tài

Tập trung nghiên cứu hai vấn đề chính:

* + Trình bày và làm rõ hơn ý tƣởng về các hệ mật mã khóa thông dụng, việc ứng dụng của các hệ mật mã khóa trong kỹ thuật tạo chữ ký số đối với việc bảo mật, an toàn thông tin.
  + Nghiên cứu những phƣơng pháp, kỹ thuật tạo chữ ký số và ứng dụng của chữ ký số trong thƣơng mại điện tử.

# Những nội dung nghiên cứu chính

+ Nghiên cứu về các giải pháp mã hóa để bảo mật thông tin.

+ Nghiên cứu những phƣơng pháp, kỹ thuật tạo chữ ký số trên các tài liệu, văn bản điện tử. Trong đó tập trung nghiên thuật toán chữ ký số chuẩn DSA, thuật toán chữ ký số đƣờng cong Eliptic.

+ Nghiên cứu về một ngôn ngữ lập trình để viết một ứng dụng nhỏ về chữ ký số.

# Tổng quan luận văn

Luận văn đƣợc trình bày theo hình thức từ trên xuống. Bắt đầu của mỗi phần đều đƣa ra những khái niệm cơ bản và quy định cho phần trình bày tiếp sau nhằm mục đích giúp dễ dàng trong khi đọc, dần dần đi sâu vào để thảo luận rõ hơn những vấn đề liên quan, bao gồm việc bảo vệ an toàn thông tin dữ liệu dùng mật mã, mật mã khóa công khai và chữ ký số DSA, ECDSA.

Luận văn đƣợc trình bày trong 3 chƣơng và phần kết luận

*Chương 1: Bảo mật thông tin và chữ ký số*

Vấn đề bảo mật thông tin, mã hóa tài liệu, khái niệm về chữ ký số; phân loại các lƣợc đồ chữ ký số; nghiên cứu một số lƣợc đồ chữ ký số cơ bản: RSA, DSA, ElGama; các phƣơng pháp tấn công chữ ký điện tử; tính pháp lý của chữ ký số.

*Chương 2: Thuật toán chữ ký số*

Nghiên cứu về hàm băm, mối quan hệ giữa hàm băm và thuật toán chữ ký số; thuật toán chữ ký số chuẩn DSA, thuật toán chữ ký số đƣờng cong Eliptic ECDSA và tính bảo mật của chúng.

*Chương 3: Ứng dụng chữ ký số trong bảo mật tài liệu điện tử*

Chƣơng này đề cập đến việc xây dựng và cài đặt ứng dụng chữ ký số và các chức năng của chƣơng trình từ đó đƣa ra các kết quả thực hiện của chƣơng trình demo.

*Kết luận và hướng phát triển*

Tóm tắt những kết quả đạt đƣợc đồng thời nêu ra những hạn chế của luận văn và hƣớng phát triển có thể đƣợc theo hƣớng nghiên cứu của luận văn trong tƣơng lai.

# CHƢƠNG I: BẢO MẬT THÔNG TIN VÀ CHỮ KÝ SỐ

# Bảo mật thông tin

# Vấn đề an toàn thông tin

Ngày nay, với sự phát triển mạnh mẽ của công nghệ thông tin việc ứng dụng các công nghệ mạng máy tính trở nên vô cùng phổ cập và cần thiết. Công nghệ mạng máy tính đã mang lại những lợi ích to lớn cho con ngƣời. Sự xuất hiện mạng Internet cho phép mọi ngƣời có thể truy cập, chia sẻ và khai thác thông tin một cách dễ dàng và hiệu quả. Sự phát triển mạnh mẽ của Internet xét về mặt bản chất chính là việc đáp ứng lại sự gia tăng không ngừng của nhu cầu giao dịch trực tuyến trên hệ thốngmạng toàn cầu. Các giao dịch trực tuyến trên Internet phát triển từ những hình thức sơ khai nhƣ trao đổi thông tin (email, messenger, …), quảng bá (publicshing) đến những giao dịch phức tạp thể hiện qua các hệ thống chính phủ điện tử, thƣơng mại điện tử ngày cá phát triển mạnh mẽ trên toàn cầu.

Tuy nhiên vấn đề an toàn thông tin lại đƣợc nảy sinh khi Internet ra đời. Internet có những kỹ thuật cho phép mọi ngƣời truy cập, khai thác và chia sẻ thông tin với nhau. Nhƣng nó cũng là nguy cơ chính dẫn đến thông tin của chúng ta bị hƣ hỏng hay bị phá hủy hoàn toàn. Nguyên nhân là vì việc truyền thông tin qua mạng Internet hiện nay chủ yếu sử dụng giao thức TCP/IP. TCP/IP cho phép các thông tin đƣợc từ máy tính này tới máy tính khác và phải đi qua một loạt các máy tính trung gian hoặc các mạng riêng biệt trƣớc khi nó tới đƣợc đích. Chính vì vậy, giao thức TCP/IP đã tạo cơ hội cho bên thứ ba có thể thực hiện các hành động gây mất an toàn thông tin trong giao dịch.

Việc bảo vệ an toàn thông tin (dữ liệu) gồm có:

* Bảo mật: Bảo đảm tính bí mật cho tài liệu cố định hay đang di chuyển
* Bảo toàn: Bảo đảm tính toàn vẹn của dữ liệu, bảo đảm tài liệu không bị thay đổi trong bộ nhớ hay trên đƣờng truyền tin.
* Xác thực: Xác thực nguồn gốc của tài liệu, nhận dạng nguồn gốc của thông tin, cung cấp sự bảo đảm thông tin là đúng sự thực.
* Tính sẵn sàng: thông tin luôn sẵn sàng cho thực thể đƣợc phép sử dụng.

Để vừa đảm bảo tính bảo mật của thông tin lại không làm giảm sự phát triển của việc trao đổi thông tin quảng bá trên toàn cầu thì chúng ta phải có các giải pháp phù hợp. Hiện có rất nhiều giải pháp cho vấn đề an toàn thông tin trên mạng nhƣ mã hóa thông tin, chữ ký điện tử, chứng chỉ điện tử (chứng chỉ khóa công khai), … [1], [9]

# Mã hóa tài liệu

## Hệ mã hóa

Hệ mã hóa gồm 5 thành phần (P, C, K, E, D) thoả mãn các tính chất sau:

**P** (Plaintext) là tập hợp hữu hạn các bản rõ có thể, còn đƣợc gọi là không gian bản rõ.

**C** (Ciphertext) là tập hợp hữu hạn các bản mã có thể, còn đƣợc gọi là không gian bản mã. Mỗi phần tử của C có thể nhận đƣợc bằng cách áp dụng phép mã hoá Ek lên một phần tử của P, với k ∈ K.

**K** (Key) là tập hợp các khóa có thể còn gọi là không gian khóa (Khóa lập mã hay khóa giải mã).

**E** (Encrytion) là tập hợp các qui tắc mã hóa có thể.

**D** (Decrytion) là tập hợp các qui tắc giải mã có thể.

Một thông tin thƣờng ở dạng bản rõ. Ngƣời gửi thực hiện mã hóa bản rõ bằng khóa lập mã **Ke**, kết quả thu đƣợc gọi là bản mã. Ngƣời nhận đƣợc bản mã, họ giải mã bằng khóa giải mã **Kd**, để thu đƣợc bản rõ.

# EKe( P) = C và DKd( C ) = P

Có một số cách phân loại mã hóa. Nếu phân loại mã hóa theo đặc trƣng của khóa lập mã và khóa giải mã, thì có hai loại mã hóa: Mã hóa khóa đối xứng (Mã hóa khóa bí mật) và mã hóa khóa phi đối xứng (Mã hóa khóa công khai).

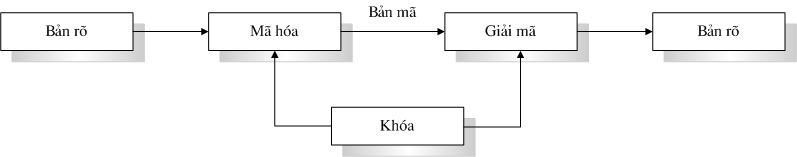
## Hệ mã hóa khóa bí mật

Hệ mã hóa khóa bí mật (secret key encryption) đƣợc đặc trƣng bởi việc *sử dụng một khóa duy nhất cho cả quá trình mã hóa và giải mã thông tin*. Hệ mã hóa này yêu cầu ngƣời gửi và ngƣời nhận phải thỏa thuận một khóa trƣớc khi thông báo đƣợc gửi đi, và khóa này phải đƣợc giữ bí mật giữa bên gửi và bên nhận (tức bên mã hoá và bên giải mã), đồng thời đƣợc giữ bí mật trong suốt thời gian sử dụng. Việc bảo mật thông tin phụ thuộc vào việc bảo mật khóa.

Kỹ thuật mã hóa dùng khoá bí mật còn đƣợc gọi là mật mã quy ƣớc (conventional encryption) hoặc mật mã đối xứng(symmetric encryption)

Ví dụ về hệ mã hóa khóa bí mật: DES, IDEA, AES, … [9].

# EK( P ) = C và DK( C ) = P



*Hình 1.1. Hệ mã hóa khóa bí mật*

## Ưu điểm:

* Mô hình khá đơn giản.
* Dễ dàng tạo ra thuật toán mã hóa đối xứng cho cá nhân.
* Dễ cài đặt và hoạt động hiệu quả.
* Hoạt động nhanh và hiệu quả do tốc độ mã hoá và giải mã cao.

## Nhược điểm:

* Dùng chung khóa nên nhiều nguy cơ mất an toàn
* Khóa dùng chung rất dễ bị hóa giải (bị “bẻ khóa”), do cũng phải truyền trên kênh truyền tin đến bên nhận.
* Việc gửi thông tin cùng khóa cho số lƣợng lớn là khó khăn, nếu số lƣợng ngƣời nhận tin lớn thì số khóa cần trao đổi lớn dẫn đến tính an toàn và bảo mật càng giảm.

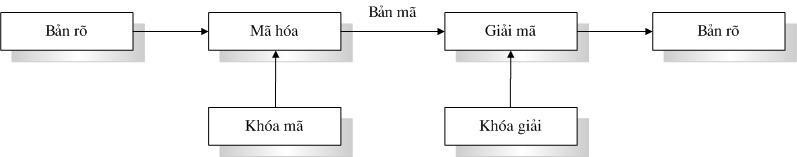
## Hệ mã hóa khóa công khai

Đặc trƣng của kỹ thuật mật mã bất đối xứng là dùng 2 khóa riêng biệt cho hai quá trình mã hóa và giải mã, trong đó có một khóa có thể đƣợc phổ biến công khai (public key hay PU) và khóa còn lại đƣợc giữ bí mật (private key hay PR). Cả hai khóa đều có thể đƣợc dùng để mã hóa hoặc giải mãvà không có khoá nào có thể suy đƣợc từ khoá kia. Trong mọi trƣờng hợp, khóa lập mã và khóa giải mã là khác nhau.

Hệ mã hóa khóa công khai (public key encryption) còn đƣợc gọi là hệ mã hóa bất đối xứng (asymmetric encryption). Hệ mã hóa này không yêu cầu ngƣời gửi và ngƣời nhận phải thoả thuận một khóa mật. Khóa công khai (public key) cho mọi ngƣời biết để lập mã, khóa mật (private key) chỉ thuộc về một ngƣời, dùng để giải mã.

Các phƣơng pháp mã hóa này khai thác những ánh xạ f mà việc thực hiện ánh xạ ngƣợc f–1 rất khó so với việc thực hiện ánh xạ f. Chỉ khi biết đƣợc mã khóa riêng thì mới có thể thực hiện đƣợc ánh xạ ngƣợc.

Ví dụ về hệ mã hóa khóa công khai: RSA, Elgamal, … [2], [3]



*Hình 1.2. Hệ mã hóa khóa công khai*

## Hệ mã hóa bảo vệ tài liệu

Hệ mã hóa có thể thực hiện đƣợc cả ba chức năng bảo vệ tài liệu, đó là: bảo mật, bảo toàn, xác thực.

1 - Bảo mật: Khi mã hóa tài liệu, kẻ gian sẽ không hiểu đƣợc thông tin 2 - Bảo toàn: Đảm bảo tài liệu không bị sửa đổi trong quá trình truyền.

+ Khi mã hóa tài liệu, kẻ gian sẽ không hiểu đƣợc thông tin, do đó không thể sửa đổi đƣợc tài liệu theo ý mình. Biện pháp này ngăn chặn kẻ gian ngay từ đầu.

+ Khi dùng mã xác thực tài liệu, nếu kẻ gian sửa đổi tài liệu, thì mã xác thực của tài liệu bị sửa đổi sẽ khác với mã xác thực của tài liệu gốc. Do đó ngƣời ta sẽ nhận ra có sự thay đổi trong tài liệu gốc. Nhƣ vậy mã xác thực dùng để kiểm tra tính toàn vẹn của tài liệu.

3 - Xác thực: Khi dùng mã xác thực với một tài liệu, mã xác thực dùng để minh chứng nguồn gốc của tài liệu đó, kẻ gian khó thể tạo ra mã xác thực giống nhƣ mã xác thực ban đầu.

# Chữ ký số

## Giới thiệu

Khi một thông điệp đƣợc truyền từ A đến B, sau khi B nhận đƣợc thì liệu thông điệp đó có đúng đƣợc gửi từ A? thông điệp có còn nguyên bản?... Để trả lời câu hỏi này cần phải có cơ chế nào đó để xác thực thông điệp. Một thông điệp đƣợc xác thực, nghĩa là:

* + - * + Thông điệp không bị thay đổi
        + Thông điệp đó đúng là của A

Nếu nhƣ cả A và B đều đồng ý, không có ý kiến gì về về xuất xứ cũng nhƣ nội dung của thông điệp thì việc trao đổi nhƣ vậy đƣợc xác nhận là hoàn tất. Cả hai bên đều tin rằng không có một kẻ thứ ba nào can thiệp vào quá trình trao đổi dữ liệu này.

Tuy nhiên, có những thông điệp gian lận xuất phát từ A hoặc do B tự tạo ra trong các giao dịch thƣơng mại, thanh toán, trao đổi trên mạng,... Chẳng hạn, B có thể thêm một đoạn tin là A đã đặt một số hàng (*mặt hàng này đang khó tiêu thụ*) tƣơng đối lớn và buộc A phải nhận số hàng đó (*trong khi thực tế số hàng đó A chỉ đặt ở mức độ vừa đủ*), các tranh chấp có thể xảy ra và cũng có nhiều trƣờng hợp ngƣời bị lừa khó mà nhận biết đƣợc, nếu không có biện pháp phòng ngừa và phát hiện hữu hiệu.

Trong thực tế, các hoạt động thƣơng mại, quản lý hành chính, hoạt động nghiệp vụ, các tài liệu trên giấy có giá trị cam kết giao hẹn với nhau (*như ngân phiếu, hợp đồng*) thì A là bên có khả năng làm giả nhiều nhất. Ngƣợc lại, cũng có khi một số trƣờng hợp phía B lại chối bỏ trách nhiệm của mình vì thấy những điều đó bất lợi cho mình. Trong các trƣờng hợp đó, việc xác thực thƣờng đƣợc dựa vào chữ ký của hai bên để xác nhận các điều khoản đã cam kết, giao hẹn với nhau trên “giấy trắng mực đen”, và đó cũng là cơ sở pháp lý để giải quyết khi có tranh chấp.

Nhƣng nếu các hoạt động trên thực hiện trao đổi với nhau trên mạng truyền số liệu thì vấn đề phức tạp hơn nhiều. Chẳng hạn, nếu bên B mang đến toà án một tài liệu nhận đƣợc qua mạng truyền số liệu (*Internet*) và bên A lại chối bỏ trách nhiệm gửi của mình thì tòa án cũng rất khó phân xử rạch ròi. Bởi vì cũng có khả năng bên B làm giả đoạn tin và cũng có khi bên A có gửi thật nhƣng lại chối bỏ trách nhiệm.

Vấn đề đặt ra là làm thế nào để phân xử đƣợc trong những trƣờng hợp nhƣ trên. Muốn giải quyết đƣợc vấn đề xác thực thì cần phải có một cơ chế nào đó giống nhƣ chữ ký tay để cả hai bên gửi và nhận cùng kiểm tra và không thể tạo giả mạo chữ ký đó. Một trong các biện pháp để thực hiện xác thực là sử dụng chữ ký số [3], [8].

## Chữ ký điện tử

Chữ ký điện tử (Electronic Signature) là thông tin đi kèm theo dữ liệu (văn bản, hình ảnh, âm thanh,…) nhằm mục đích xác định chủ nhân của dữ liệu và xác nhận sự chấp thuận của ngƣời đó đối với nội dung dữ liệu đã ký.

Chữ ký điện tử cũng giống nhƣ chữ viết tay, tức là chữ ký điện tử đƣợc dùng để xác nhận lời hứa hay cam kết của ngƣời nào đó và sau đó không thể chối bỏ đƣợc. Chữ ký điện tử không đòi hỏi phải sử dụng giấy mực mà nó gắn đặc điểm nhận dạng của ngƣời ký vào một bản cam kết nào đó. Nhƣ vậy, chữ ký điện tử sẽ chứng thực định danh ngƣời gửi và bảo vệ sự toàn vẹn dữ liệu.

Chữ ký điện tử đƣợc sử dụng trong các giao dịch số. Xuất phát từ thực tế, chữ ký điện tử cần đảm bảo các chức năng: xác định đƣợc ngƣời chủ của một dữ liệu nào đó: văn bản, âm thanh, hình ảnh,… của dữ liệu đó có bị thay đổi hay không.

Thông thƣờng chữ ký của một ngƣời trên tài liệu thƣờng đặt ở cuối bản tin để xác nhận nguồn gốc hay trách nhiệm của ngƣời ký với tài liệu đó. Với tài liệu đã đƣợc “*số hóa*” nếu chữ ký đặt ở cuối bản tin thì việc sao chép “*chữ ký số*” là dễ dàng và tính toàn vẹn dữ liệu sẽ không đƣợc đảm bảo vì vì chữ ký số là các số 0, 1 nên kẻ tấn công dễ dàng thay đổi nội dung và sao chép. Vậy một “chữ ký số” đặt cuối tài liệu “số hóa” không thể chịu trách nhiệm đối với toàn bộ nội dung văn bản. “Chữ ký số” thể hiện trách nhiệm đối với toàn bộ tài liệu phải là chữ ký đƣợc ký trên từng bit của tài liệu đó. Tuy nhiên, chữ ký số cũng không thể ký trên bất kỳ tài liệu nào với độ dài tùy ý, vì nhƣ vậy chữ ký số sẽ có độ dài rất lớn. Với tài liệu dài ngƣời ta ký trên đại diện của nó mà đại diện này đƣợc tạo ra từ *hàm băm.*

Chữ ký thông thƣờng ngƣời ta kiểm tra bằng cách so sánh với chữ ký xác thực khác. Đây không phải phƣơng pháp an toàn vì nó có thể giả mạo.Với chữ ký số, ngƣời ta có thể kiểm tra thông qua thuật toán kiểm tra công khai. Nhƣ vậy, bất kỳ ai cũng có thể kiểm tra đƣợc chữ ký số. Việc dùng một lƣợc

đồ chữ ký an toàn sẽ ngăn chặn đƣợc khả năng giả mạo bởi nó sẽ đảm bảo ba yêu cầu sau:

* Xác thực
* Toàn vẹn dữ liệu
* Không thể thóai thác trách nhiệm

Mặt khác, bản sao tài liệu đƣợc ký bằng chữ ký số đồng nhất với bản gốc, còn bản sao tài liệu có chữ ký trên giấy có thể khác với bản gốc. Điều này có nghĩa là phải cẩn thận ngăn chặn việc dùng lại một chữ ký số. Vì thế bản thân bức điện cần chứa thông tin (chẳng hạn nhƣ ngày tháng) để ngăn nó khỏi bị dùng lại.

## Tổng quan về chữ ký số

Chữ ký số (Digital Signature) là một dạng chữ ký điện tử (là tập con của chữ ký điện tử) đƣợc tạo ra bằng sự biến đổi một thông điệp dữ liệu sử dụng hệ thống mật mã công khai, theo đó ngƣời có thông điệp dữ liệu ban đầu và khóa công khai của ngƣời ký có thể xác định đƣợc:

* + - * + Việc biến đổi nêu trên đƣợc tạo ra bằng đúng khóa bí mật tƣơng ứng với khóa công khai trong cùng cặp khóa.
        + Sự toàn vẹn nội dung của thông điệp dữ liệu kể từ khi thực hiện biến đổi nhƣ trên.

Với chữ ký thông thƣờng, nó là một phần vật lý của tài liệu, nhƣng chữ số không gắn theo kiểu vật lý vào bức điện. Để chống giả mạo chữ ký số, thuật toán ký số phải là không nhìn thấy bằng mắt thƣờng trên bức điện.

Một lƣợc đồ chữ ký số là một bộ 5 (**P, A, K, S, V**) trong đó: P – Tập hữu hạn các bức điện (thông điệp) có thể

A– Tập hữu hạn các chữ ký có thể

K – Tập hữu hạn các khóa có thể (không gian khóa) S – Tập các thuật toán ký dạng

V – Tập các thuật toán kiểm tra chữ ký dạng 𝑒 𝑘 𝑥 𝐴 𝑢𝑒 𝑎𝑙𝑠𝑒

Trên thông điệp x P, với thuật toán ký 𝑆i𝑔𝑘 ∈ và khóa ký ∈ , sẽ nhận đƣợc chữ ký 𝑦 = 𝑆i𝑔𝑘(𝑥) ∈ 𝐴.

Thuật toán kiểm tra chữ ký 𝑒 𝑘 ∈ , sẽ xác minh chữ ký y nhƣ sau:

𝑒 = | 𝑢𝑒 nếu 𝑦 = 𝑠i𝑔(𝑥)

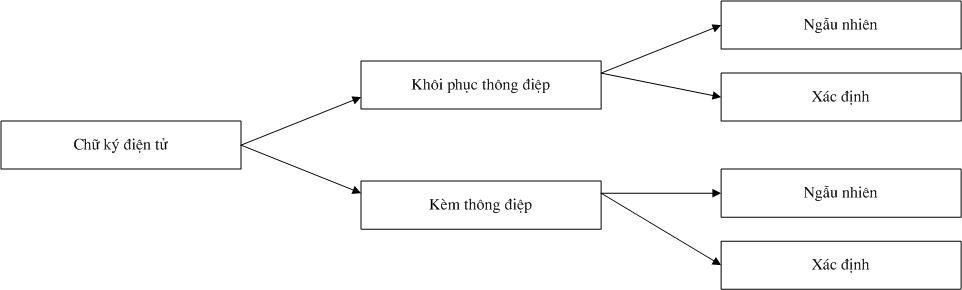
𝑘

𝐹𝑎𝑙𝑠𝑒 𝑛e𝑢 𝑦 G 𝑠i𝑔(𝑥)

𝑆i𝑔𝑘 và 𝑒 𝑘 là các hàm có thời gian đa thức trong đó 𝑒 𝑘 là hàm công khai, 𝑆i𝑔𝑘 là hàm bí mật và không thể dễ dàng giả mạo.

# Phân loại các lƣợc đồ chữ ký số

Chữ ký “số” chia thành 2 loại, chữ ký kèm thông điệp (message appendix) và chữ ký khôi phục thông điệp (message recovery).



*Hình 1.3. Phân loại lược đồ chữ ký số [7]*

# Lƣợc đồ chữ ký kèm thông điệp

Thông điệp ban đầu không thể khôi phục đƣợc từ chữ ký, do đó thông điệp phải đi kèm chữ ký, mặt khác thông điệp gốc còn dùng để kiểm tra tính đúng của chữ ký.

Loại lƣợc đồ chữ ký số này cũng đƣợc dùng phổ biến trong thực tế. Chúng dựa vào các hàm băm mật mã và ít bị tấn công giả mạo. Chữ ký này đòi hỏi thông điệp gốc là tham số quan trọng nhất cho quá trình kiểm tra chữ ký.

## Định nghĩa

Lƣợc đồ chữ ký số mà yêu cầu phải có thông điệp đầu vào cho thuật toán chứng thực chữ ký đƣợc gọi là lƣợc đồ chữ ký kèm thông điệp.

Một số lƣợc đồ kèm thông điệp nhƣ: Elgamal, DSA, Schonor, …

## Thuật toán sinh khóa

Mỗi cá thể tạo một khóa riêng để ký thông điệp và một khóa công khai tƣơng ứng để các cá thể khác trong hệ thống dùng trong quá trình xác thực chữ ký.

* + Mỗi cá thể A chọn một khóa 𝑘 = (𝑘′, 𝑘′′) ∈ 𝐾, 𝑆i𝑔𝑘𝘍 là thuật toán ký với mỗi khóa k (mỗi 𝑆i𝑔𝑘𝘍 là một ánh xạ 1-1 từ 𝑀ℎ tới 𝑀𝑠).
* Thuật toán 𝑉𝑒𝑟𝑘𝘍𝘍 tƣơng ứng là một ánh xạ từ 𝑀ℎ𝑥𝑀𝑠 đến tập hợp

{True, False} sao cho:

Với 𝑚 ∈ 𝑀ℎ, 𝑠 ∈ 𝑀𝑠: ở đây 𝑚 = ℎ(𝑃) với 𝑃 ∈ 𝑀. 𝑉𝑒𝑟𝑘𝘍𝘍 đƣợc gọi là thuật toán kiểm thử để chứng thực chữ ký, ***h*** là hàm một chiều từ ***M*** đến 𝑀ℎ (𝑀ℎ là tập hợp các giá trị băm).

Với khóa 𝑘 = (𝑘′, 𝑘′′), trong đó khóa công khai của A là 𝑘′′, khóa bí mật là 𝑘′.

𝑉𝑒𝑟𝑘

𝘍𝘍 (𝑚, 𝑠) = { 𝑇𝑟𝑢𝑒 𝑛e𝑢 𝑆i𝑔𝑘𝘍 (𝑚) = 𝑠

𝐹𝑎𝑙𝑠𝑒 𝑛e𝑢 𝑆i𝑔𝑘𝘍 (𝑚) G 𝑠

## Thuật toán sinh chữ ký và chứng thực chữ ký

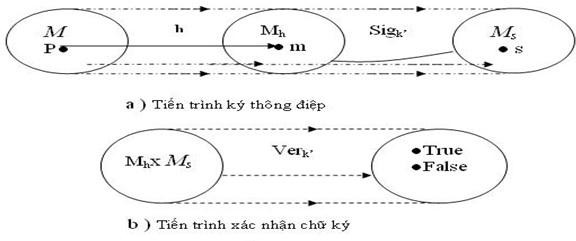
Cá thể A ký một thông điệp 𝑃 ∈ 𝑀 với chữ ký s. Một cá thể B bất kỳ có thể xác minh chữ ký đó có đúng là của A hay không?

*Quá trình sinh chữ ký*

* + Chọn một chữ ký 𝑘 = (𝑘′, 𝑘′′) ∈ 𝐾
  + Tính 𝑚 = ℎ(𝑃) và 𝑠 = 𝑆i𝑔𝑘𝘍 (𝑚)
  + Chữ ký của A cho thông điệp P là s, P và s đƣợc gửi đến B.

*Quá trình xác nhận chữ ký*

* Xác thực đúng khóa công khai của A là 𝑘′′
* Tính 𝑚 = ℎ(𝑃) và 𝑢 = 𝑉𝑒𝑟𝑘𝘍𝘍 (𝑚, 𝑠)
* Chấp nhận chữ ký của A nếu u = True



*Hình 1.4. Mô hình lược đồ chữ ký kèm thông điệp [7]*

# Lƣợc đồ chữ ký khôi phục thông điệp

Đặc trƣng cho lƣợc đồ này là thông điệp ban đầu có thể đƣợc khôi phục từ chính bản thân chữ ký. Trong thực tế lƣợc đồ ký kiểu này thƣờng đƣợc ký cho các thông điệp nhỏ.

## Định nghĩa

Lƣợc đồ chữ ký khôi phục thông điệp là lƣợc đồ chữ ký số không đòi hòi hỏi phải có thông điệp gốc làm đầu vào để chứng thực chữ ký mà thông điệp gốc sẽ đƣợc phục hồi từ chính chữ ký đó.

Một số lƣợc đồ chữ ký khôi phục thông điệp nhƣ: Rabin, RSA, …

## Thuật toán sinh khóa

Mỗi cá thể tạo một khóa riêng dùng để ký thông điệp và một khóa công khai tƣơng ứng để cá thể khác trong hệ thống dùng để xác thực chữ ký.

* + Mỗi cá thể A chọn một khóa 𝑘 = (𝑘′, 𝑘′′) ∈ 𝐾, 𝑆i𝑔𝑘𝘍 là thuật toán ký với mỗi khóa k (mỗi 𝑆i𝑔𝑘𝘍 là một ánh xạ 1-1 từ ***Mh*** tới ***Ms***).

R là một hàm sao cho ***R(M)*** = ***MR*** và có nghịch đảo là ***R***-1

* + Thuật toán 𝑉𝑒𝑟𝑘𝘍𝘍 tƣơng ứng là một ánh xạ từ 𝑀𝑠 đến 𝑀 sao cho: 𝑉𝑒𝑟𝑘𝘍𝘍 𝑆i𝑔𝑘𝘍 là một ánh xạ trên MR, 𝑘 ∈ 𝐾*.* 𝑉𝑒𝑟𝑘𝘍𝘍 là thuật toán chứng thực chữ ký.
  + Cặp khóa 𝑘 = (𝑘′, 𝑘′′), trong đó khóa công khai của A là 𝑘′′, khóa bí mật của A là 𝑘′.

## Thuật toán sinh chữ ký và xác nhận chữ ký

*Thuật toán sinh chữ ký*

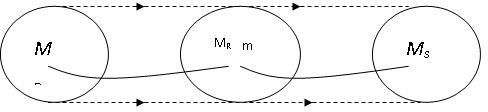
Thực thể A ký một thông điệp P***M*** với chữ ký s. Một thực thể B bất kỳ có thể xác thực chữ ký và phục hồi thông điệp P từ chữ ký đó.

* + Chọn khóa 𝑘 = (𝑘′, 𝑘′′) ∈ 𝐾
  + Tính m = R(P) và 𝑠 = 𝑆i𝑔𝑘𝘍 (𝑚) (R*,*R-1 là các hàm đƣợc công khai).
  + Chữ ký của A lên thông điệp P là s, và sau đó A gửi s cho B.

*Thuật toán xác nhận chữ ký*

B thực hiện các bƣớc sau để xác minh chữ ký:

* + Xác thực đúng khóa công khai của A là k''
  + Tính 𝑚 = 𝑉𝑒𝑟𝑘𝘍𝘍 (𝑠)
  + Xác thực m = MR (Nếu m ∈ MR thì từ chối chữ ký)
  + Phục hồi thông điệp P từ m bằng cách tính R-1(m)



*Hình 1.5. Mô hình lược đồ chữ ký khôi phục thông điệp [7]*

# Một số lƣợc đồ chữ ký số cơ bản

# Lƣợc đồ chữ ký RSA (Rivest, Shamir, Adleman)

Lƣợc đồ chữ ký RSA có độ phức tạp tính toán phụ thuộc vào việc giải quyết bài toán lũy thừa theo module các số rất lớn. Lƣợc đồ chữ ký bao gồm cả hai loại kèm thông điệp và khôi phục thông điệp [1], [14].

Lƣợc đồ chữ ký RSA đƣợc đề xuất năm 1977 bởi 3 nhà nghiên cứu Rivest, Shamir và Adleman, đây là lƣợc đồ có ứng dụng thực tế rộng rãi nhất dựa trên công nghệ sử dụng khóa chung. Các phƣơng pháp tấn công RSA đầu tiên (multicative property) và các vấn đề khác liên quan tới chữ ký RSA đƣợc đƣa ra bởi Davia và Jonge và Chaum. Sau đây là lƣợc đồ chữ ký RSA.

## Tóm tắt lược đồ ký theo RSA

* + - * Cho n = p.q với p và q là các số nguyên tố
      * Cho P = A = Zn K = {(n, p, q, a, b), n = pq, p và q là nguyên tố,

ab  1 mod (n)}. Các giá trị n, b là công khai

* + - * Với mỗi k = {(n, p, q, a, b)} Ta định nghĩa:

𝑆i𝑔𝑘(𝑥) = 𝑥𝑎 𝑚𝑜𝑑 𝑛

𝑉𝑒𝑟𝑘(𝑥, 𝑦) = true 𝑥 Ξ 𝑦 (𝑚𝑜𝑑 𝑛) với 𝑥, 𝑦 ∈

Nếu độ dài thông điệp x lớn, ta sử dụng hàm băm nhƣ trên.

## Thuật toán sinh khóa

* + - * Chọn hai số nguyên tố lớn ngẫu nhiên p và q
      * Tính 𝑛 = và ф(𝑛) = ( ) ( )
      * Chọn số tự nhiên ngẫu nhiên b sao cho ф(n) và nguyên tố cùng nhau với ф(n), tức là UCLN(b, ф(n)) = 1
* Tính số tự nhiên a là duy nhất: 1< a < ф(n) và 𝑎 𝑏 Ξ (𝑚𝑜𝑑 ф), (a là nghịch đảo duy nhất của b, tìm đƣợc duy nhất 𝑎 Ξ 𝑏−1 𝑚𝑜𝑑 ф(n) nhờ giải thuật Euclid mở rộng)
  + Khóa công khai của A là (n, b), khóa bí mật là (n, a)

***Thuật toán sinh chữ ký***: chữ ký trên thông điệp m

* + Ký trên thông điệp m (nếu m là tài liệu lớn, thì ký vào đại diện tài liệu của m là z = H(m))
* Chọn khóa bí mật a. Tính chữ ký là 𝑠 = 𝑚𝑎 𝑚𝑜𝑑 𝑛

## Thuật toán xác nhận chữ ký

* + Xác nhận chữ ký s
  + Chọn khóa công khai b. Tính mʹ = sb mod n
  + Chữ ký đúng nếu m = mʹ

M

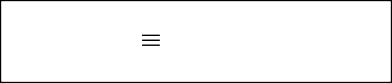
C = Mb mod n

Tính ϕ(n) = (p-1)\*(q-

Chọn 2 số nguyên tố p, q

Tính n = p\*q

*Hình 1.6. Sơ đồ biểu diễn thuật toán mã hóa [1]* **Ví dụ 1.1:** Giả sử A cần ký một chữ ký s lên thông điệp m = 2 *Sinh khóa*: Chọn số nguyên tố p = 3 và q = 5



Tính a b-1 mod ϕ(n)

Khóa bí mật (n,a)

M

M = Ca mod n

Khóa công khai (n,b)

Chọn 1 < b < ϕ(n)

Tính n = p\*q = 15, ϕ(n) = 2\*4 = 8

Chọn khóa công khai b = 3, tính khóa bí mật a = 3. *Sinh chữ ký*: Chữ ký trên m là s = ma (mod n) = 23 (mod 15) = 8 *Xác nhận chữ ký*: Tính mʹ = sb (mod n) = 83 (mod 15) = 2

Chữ ký đúng vì mʹ = m

**Ví dụ 1.2:** Giả sử A cần ký một chữ ký s lên thông điệp m = 31229978

*Sinh khóa*: Chọn số nguyên tố p = 7927 và q = 6997

Tính n = p\*q = 55465219, ϕ(n) = 7926 \* 6996 = 55450296

Chọn khóa công khai b = 5, tính khóa bí mật a = 44360237

*Sinh chữ ký*: Chữ ký trên m là s = ma (mod n)

= 3122997844360237 (mod 55465219)

= 30729435

*Xác nhận chữ ký*: Tính mʹ = sb (mod n)

= 307294355 (mod 55465219)

= 31229978

Chữ ký đúng vì mʹ = m

## Độ an toàn của RSA

Hệ mã hóa theo RSA là tất định, tức là với một bản rõ **x** và một khóa bí mật **a**, thì chỉ có một bản mã **y**.

Hệ mã hóa RSA an toàn, khi giữ đƣợc bí mật khóa giải mã **a**, **p**, **q**, **(n)**. Nếu biết đƣợc p và q, thì thám mã dễ dàng tính đƣợc ϕ(n) = ( - )\* ( - ). Nếu biết đƣợc (n), thì thám mã sẽ tính đƣợc **a** theo thuật toán Euclide mở rộng. Nhƣng phân tích n thành tích của p và q là bài toán “khó”.

Độ an toàn của Hệ mật RSA dựa vào khả năng giải bài toán phân tích số nguyên dƣơng n thành tích của 2 số nguyên tố lớn p và q.

# Lƣợc đồ chữ ký Elgamal

Lƣợc đồ Elgamal đƣợc đề xuất năm 1985. Sau đó, Viện tiêu chuẩn và Công nghệ quốc gia Mỹ sửa đổi thành chuẩn chữ ký số (Digital Signature Standart – DSS). Lƣợc đồ Elgamal [1, 9] không tất định cũng giống nhƣ hệ thống mã khóa công khai Elgamal. Điều này có nghĩa là, có nhiều chữ ký hợp lệ cho một thông điệp bất kỳ. Thuật toán kiểm thử phải có khả năng chấp nhận bất kỳ chữ ký hợp lệ nào khi xác minh.

Khác với phƣơng pháp RSA có thể áp dụng trong mã hóa khóa công khai và chữ ký số, phƣơng pháp Elgamal đƣợc xây dựng chỉ nhằm giải quyết bài toán chữ ký số.

## Tóm tắt lược đồ chữ ký Elgamal

Cho p là số nguyên tố sao cho bài toán logarit rời rạc trên Zp là khó và

cho a ∈ Z\* là phần tử nguyên thủy. Cho p = Z\*, A = Z\* x Z

và định nghĩa:

p p

K={(p, a, a, β): β = aa (mod p)}

p p-1

Giá trị p, a, β là công khai còn a là bí mật.

Với K = {(p, a, a, β) và một số ngẫu nhiên (bí mật) k Zp-1\*. Định nghĩa: 𝑆i𝑔𝑘(𝑥, 𝑘) = (𝛾, 𝛿), trong đó:

𝛾 = 𝛼𝑘 𝑚𝑜𝑑 𝑝 và 𝛿 = (𝑥 − 𝑎𝛾)𝑘−1𝑚𝑜𝑑 (𝑝 − 1).

Với 𝑥, 𝑦 ∈ 𝑍\* và 𝛿 ∈ 𝑍

ta định nghĩa:

𝑝 𝑝−1

𝑉𝑒𝑟(𝑥, 𝛾, 𝛿) = true - 𝛽𝛾𝛾ð Ξ 𝛼𝑥 (𝑚𝑜𝑑 𝑝).

## Thuật toán sinh khóa cho lược đồ chữ ký Elgamal

Mỗi cá thể trong hệ thống tạo một khóa công khai và một khóa riêng tƣơng ứng. Mỗi cá thể A thực hiện các bƣớc sau :

* Tạo số nguyên tố lớn p và chọn 𝛼 ∈ 𝑍𝑝
* Chọn số nguyên a: 1 𝑎 𝑝 −
* Tính 𝑦 = 𝛼𝑎 𝑚𝑜𝑑 𝑝

Khóa công khai là (p, a, y), khóa bí mật là a.

## Thuật toán sinh chữ ký

Cá thể A ký lên thông điệp m, A thực hiện các bƣớc:

* Chọn số nguyên k, 1 𝑘 𝑝 − , với (𝑘, 𝑝 − 1) = 1
* Tính 𝑟 = 𝛼𝑘 𝑚𝑜𝑑 𝑝
* Tính 𝑘−1 𝑚𝑜𝑑 (𝑝 − 1)
* Tính 𝑠 = 𝑘−(ℎ(𝑚) − 𝑎 \* 𝑟) 𝑚𝑜𝑑 (𝑝 − 1)
* Chữ ký của A lên thông điệp m là (r, s)

## Thuật toán chứng thực chữ ký

Cá thể B thực hiện các bƣớc sau để chứng thực chữ ký (r, s) lên m có phải là của A hay không?

* Xác nhận khóa công khai của A là (p, a, β)
* Kiểm tra r, 1 ≤ r ≤ p – 1, nếu không đúng thì từ chối chữ ký của A
* Tính 𝑣1 = 𝑦𝑟. 𝑟𝑠 𝑚𝑜𝑑 𝑝
* Tính h(m) và 𝑣2 = 𝛼ℎ(𝑚) 𝑚𝑜𝑑 𝑝
* Nếu 𝑣1 = 𝑣2 thì chấp nhận chữ ký của A

**Ví dụ 1.3**: Giả sử A cần ký lên thông điệp m có giá trị băm h(m) = 1463 để gửi cho B, sau đó B chứng thực xem chữ ký đó có phải của A hay không?

* *Tạo khóa*:
  + Chọn số nguyên tố p = 2357 và a = 2 Z2357
  + Chọn a = 1751, 1≤ a ≤ p – 2
  + Tính y = aa mod p = 21751 mod 2357 = 1185

Khóa công khai của A là (p, a, y) = (2357, 2, 1185), khóa bí mật của A là a = 1751

* *Tạo chữ ký*:

Giả sử thông điệp m sau khi dùng một thuật toán băm đƣợc giá trị băm là h(m) = 1463 sau đó:

* + Chọn k = 1529, 1≤ k ≤ p – 2
  + Tính r = ak mod p = 21529 mod 2357 = 1490
  + Tính k-1 mod (p – 1) = 245
  + Tính 𝑠 = 𝑘−1(ℎ(𝑚) − 𝑎 \* 𝑟) 𝑚𝑜𝑑 (𝑝 − 1)

= 245(1463 – 1751\*1490) mod 2356 = 1777

Vậy chữ ký của A lên thông điệp m là (1490, 1777) và gửi đến B.

* *Chứng thực chữ ký*

Để chứng thực chữ ký (1490, 1777) đúng là của A hay không thì B thực hiện:

* + Tính 𝑣1 = 𝑦𝑟. 𝑟𝑠 𝑚𝑜𝑑 𝑝 = 11851490. 14901777 mod 2357 = 1072
  + Tính 𝑣2 = 𝛼ℎ(𝑚) 𝑚𝑜𝑑 𝑝 = 21463 mod 2357 = 1072

Kết luận chữ ký (1490, 1777) đúng là của A.

# Các phƣơng pháp tấn công chữ ký điện tử

Một trong các cách tấn công chữ ký số của đối phƣơng là giả mạo chữ ký đó là đƣa ra các chữ kýđƣợc các cá thể khác chấp nhận. Tùy theo các kết quả tấn công thu đƣợc, ngƣời ta đƣa ra một tập các tiêu chuẩn dựa vào mức độ thành công của việc tấn công nhƣ sau:

1. *Bẻ gãy toàn bộ:* Ngƣời tấn công hoặc là có thể tính đƣợc khoá riêng của ngƣời ký hoặc tìm đƣợc một cách tƣơng đƣơng với thao tác sinh chữ ký.
2. *Giả mạo được chữ ký của một văn bản chọn trước*: Ngƣời tấn công có khả năng thành công khi giả mạo chữ ký cho một văn bản P nào đó đã biết trƣớc.
3. *Giả mạo được chữ ký của một văn bản nào đó:* Ngƣời tấn công có khả năng thành công khi giả mạo chữ ký cho một văn bản P nào đó (chƣa đƣợc biết trƣớc).

Có hai kiểu tấn công cơ bản vào các lƣợt đồ chữ ký số khóa công khai,

đó là:

*Tấn công vào khoá*: Đối phƣơng chỉ biết khóa công khai của ngƣời ký.

*Tấn công thông điệp:* Ngƣời tấn công biết thêm một số văn bản nào đó

và chữ ký của chúng. Tấn công thông điệp lại đƣợc chia làm ba lớp:

* Tấn công khi biết thông báo và chữ ký tƣơng ứng của thông báo nhƣng không đƣợc chọn lựa theo ý của đối phƣơng.
* Tấn công có thể chọn trƣớc một số văn bản và có chữ ký kèm theo.
* Tấn công có thể lựa chọn các văn bản để lấy chữ ký ngay trong quá trình tấn công (căn cứ trên kết quả lấy chữ ký của các văn bản trƣớc đó). Đây là kiểu tấn công đƣợc chọn văn bản thích ứng.

# Tính pháp lý và ứng dụng chữ ký số

# Trong nƣớc

## Hành lang pháp lý

Luật giao dịch điện tử ngày 29/11/2005 (có hiệu lực từ 1/3/2006). Luật giao dịch điện tử quy định về thông điệp điện tử, chữ ký số và chứng thực chữ ký số; giao kết và thực hiện hợp đồng điện tử; giao dịch điện tử của cơ quan nhà nƣớc; an ninh, an toàn, bảo vệ, bảo mật trong giao dịch điện tử; giải quyết tranh chấp và xử lý vi phạm trong giao dịch điện tử, ...

Nghị định 26/2007/NĐ-CP, ngày 15/2/2007, quy định chi tiết thi hành Luật giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số. Nghị định này quy định chi tiết về Chữ ký số và Chứng chỉ số; việc quản lý, cung cấp và sử dụng dịch vụ chứng thực chữ ký số. Áp dụng đối với cơ quan, tổ chức cung cấp dịch vụ chứng thực chữ ký số và cơ quan, tổ chức, cá nhân lựa chọn sử dụng chữ ký số và dịch vụ chứng thực chữ ký số trong giao dịch điện tử.

Nghị định 64/2007/NĐ-CP, ngày 10/4/2007 về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nƣớc. Tại Nghị định này (Điều 40) cũng quy định việc sử dụng chữ ký số trong các giao dịch điện tử của các cơ quan nhà nƣớc.

## Tình hình ứng dụng chữ ký số và chứng thực chữ ký số trong nước

Hiện nay ở Việt Nam có một số nhà cung cấp dịch vụ chữ ký số (CKS), chứng thực chữ ký số:

* Tập đoàn Bƣu chính Viễn thông Việt Nam (VNPT): nhà cung cấp dịch vụ chứng thực CKS đầu tiên tại Việt Nam sau khi nhận Giấy phép cung cấp dịch vụ Chứng thực chữ ký số công cộng của Bộ TT&TT ngày 15/9/2009. Theo giấy phép này, VNPT đƣợc cung cấp dịch vụ chứng thực CKS cho cơ quan, tổ chức, cá nhân sử dụng trong các hoạt động công cộng. Các loại chứng thƣ số đƣợc VNPT cung cấp bao gồm: Chứng thƣ số cá nhân cho cơ

quan, tổ chức, cá nhân; Chứng thƣ số SSL (chứng thƣ số danh cho website); Chứng thƣ số cho CodeSigning (chứng thƣ số dành cho ứng dụng). Trƣớc khi đƣợc cấp giấy phép, VNPT đã ký thỏa thuận cung cấp dịch vụ chứng thực CKS công cộng cho ngành tài chính, đồng thời hợp tác hỗ trợ triển khai thành công Dự án thí điểm “Ngƣời nộp thuế nộp hồ sơ qua mạng internet” và áp dụng CKS vào các thủ tục hải quan điện tử trong giai đoạn 2009 - 2010. Tiếp đến VNPT sẽ tiếp tục cung cấp dịch vụ này cho các ngân hàng, doanh nghiệp thƣơng mại điện tử, …

* Công ty cổ phẩn công nghệ thẻ NacencommSCT: chính thức là nhà cung cấp dịch vụ chứng thực CKS công khai thứ hai tại Việt Nam từ ngày 2/3/2010. NacencommSCT là công ty thành viên của công ty Điện tử Hà Nội (HANEL), hoạt động trong lĩnh vực công nghệ thẻ thông minh, phát triển các ứng dụng bảo mật và xác thực. Công ty NecencommSCT sẽ tổ chức cung cấp các dịch vụ xác thực chữ ký trong các giao dịch điện tử cho các doanh nghiệp, tổ chức, cá nhân.
* Công ty An ninh mạng Bkav là nhà cung cấp dịch vụ chứng thực CKS công cộng thứ 3 kể từ ngay 8/4/2010, với tên giao dịch BkavCA. Bkav sẽ cung cấp 3 loại chứng thƣ số gồm: Chứng thƣ số cho cơ quan, tổ chức, cá nhân; chứng thƣ số SSL và Chứng thƣ số CodeSigning.
* Viettel là nhà cung cấp dịch vụ chứng thực CKS công cộng thứ tƣ. Ngày 22/6/2010, Bộ TT&TT đã trao giấy phép cung cấp dịch vụ chứng thực CKS công cộng cho Viettel. Theo đó, Viettel đƣợc cung cấp ba loại chứng thƣ số bao gồm: Chứng thƣ số cho cơ quan, tổ chức, cá nhân giúp ngƣời dùng chứng thực cơ quan, tổ chức, cá nhân đó trong các giao dịch điện tử; Chứng thƣ số dành cho máy chủ (SSL) để chứng thực cho website và Chứng thƣ số cho phần mềm (CodeSigning) sử dụng cho các nhà sản xuất phần mềm để chứng thực và bảo đảm tính toàn vẹn của sản phẩm.
* Công ty cổ phần Hệ thống thông tin FPT (FPT IS) gia nhập thị trƣờng cung cấp dịch vụ chứng thực CKS công cộng từ ngày 10/8/2010 và là nhà cung cấp CKS thứ 5 tại Việt Nam hiện nay. FPT IS sẽ đƣợc cung cấp 3 loại chứng thƣ số gồm: chứng thƣ số cho cơ quan, tổ chức, cá nhân giúp ngƣời dùng chứng thực các giao dịch điện tử nhƣ Internet Banking, chứng khoán trực tuyến, khai báo thuế, hải quan trực tuyến, …; chứng thƣ số SSL cho các website và chứng thƣ số CodeSigning.

Để có thể đƣợc cấp phép, nhà cung cấp dịch vụ chứng thực CKS phải đạt đƣợc các tiêu chuẩn về tài chính, nhân lực, cũng nhƣ đãp ứng các yêu cầu khắt khe về hạ tầng kỹ thuật theo tiêu chuẩn quốc tế (tiêu chuẩn mật mã FIPS PUB 140 – 2 mức 3, PKCS#1 version 2.1, …).

# Ở một số nƣớc trên thế giới

Ở các nƣớc phát triển nhƣ Mỹ, Canada, … hệ thống chứng thực số đã khá hoàn thiện, với một hệ thống chính phủ điện tử hiện đại, việc quản lý sinh/tử, cấp hộ khẩu, công chứng, ... đã có thể thực hiện hoàn toàn thông qua mạng, đặc biệt những năm gần đây dịch vụ chứng thực chữ ký số (CA) ngày càng phát triển. Một số CA nổi tiếng có thể kể đến nhƣ CA của các công ty VeriSign, WISeKey, eTrust, ... có chi nhánh tại rất nhiều nƣớc trên thế giới.

Ở các nƣớc trong khu vực dịch vụ chứng thực chữ ký số phát triển khá mạnh, cụ thể: Nhật Bản đã ban hành Luật về chữ ký điện tử và các dịch vụ chứng thực vào năm 2001; Hàn Quốc ban hành luật chữ ký điện tử vào năm 1999 và sửa đổi vào năm 2001. Hiện nay Hàn Quốc có 6 CA đƣợc cấp phép hoạt động; Hồng Kông ban hành sắc lệnh về giao dịch điện tử vào năm 2000; Đài Loan ban hành luật chữ ký số vào năm 2001; Malaysia ban hành luật chữ ký số vào năm 1997, hiện nay có 3 CA đƣợc cấp phép hoạt động; Singapore ban hành luật giao dịch điện tử vào năm 1998 và Quy định về giao dịch điện tử cho các CA vào năm 1999; Thái Lan ban hành luật giao dịch điện tử năm 2001. Hiện nay chứng thực chữ ký số đƣợc sử dụng trong khá nhiều ứng dụng,

theo số liệu điều tra gần đây của tổ chức thúc đẩy các tiêu chuẩn thông tin theo cấu trúc OASIS (Organization for the Advancement of Structured Information Standards), 13,2% dùng trong thƣơng mại điện tử, 9,1% sử dụng để bảo vệ WLAN, 8% sử dụng bảo đảm an toàn cho các dịch vụ Web, 6% sử dụng bảo đảm an toàn cho Web Server, 6% sử dụng trong các mạng riêng ảo (VPN). Ngoài ra chứng thực điện tử còn đƣợc sử dụng trong một số ứng dụng khác.

# 1.5.3 Ứng dụng trong thực tế

Dựa trên các tính năng cơ bản của chữ ký số là: Tính xác thực, tính bảo mật, tính toàn vẹn dữ liệu, tính chống chối bỏ trong việc thực hiện các giao dịch điện tử qua mạng, cũng nhƣ các thủ tục hành chính với cơ quan pháp quyền, nên chữ ký số đƣợc sử dụng trong các công việc nhƣ: ký vào văn bản, tài liệu điện tử; bảo mật thƣ điện tử; bảo đảm an toàn cho Web Server (thiết lập kênh trao đổi bảo mật giữa Web client và Web server trên Internet).

Đây chính là nền tảng của Chính phủ điện tử, môi trƣờng cho phép công dân có thể giao tiếp, thực hiện các công việc hành chính với cơ quan nhà nƣớc hoàn toàn qua mạng. Có thể nói, chữ ký số là một phần không thể thiếu của Chính phủ điện tử.

Lƣợc đồ chữ ký RSA và lƣợc đồ chữ ký chuẩn DSA là hai lƣợc đồ đƣợc dùng phổ biến nhất trong các ứng dụng bảo mật do có độ an toàn và hiệu quả thực hiện tốt nhất hiện nay. Các thuật toán cũng đơn giản và dễ thực hiện.

# Kết luận chƣơng

Trong chƣơng 1 chúng ta đã nghiên cứu về hệ mã hóa khóa bí mật và hệ mã hóa khóa công khai. Hai loại mã hóa này khác nhau ở số lƣợng khóa. Mã hóa khóa bí mật sử dụng một khóa duy nhất cho cả quá trình mã hóa và giải mã thông tin. Trong khi đó, mã hóa khóa công khai sử dụng hai khóa khác nhau để mã hóa và giải mã thông tin. Mỗi hệ thống mã hóa có ƣu nhƣợc điểm riêng.

Đối với hệ mã hóa khóa bí mật, mô hình đơn giản, dễ thai tác, cài đặt,

tốc độ xử lý nhanh nhƣng độ an toàn không cao. Trong quá trình trao đổi thông tin, cả bên nhận và bên gửi đều đã biết về khóa bí mật, cho phép trao đổi thông tin từ A đến B hoặc từ B đến A, không phân đƣợc A và B vì thế kênh truyền phải đƣợc bảo vệ từ 2 phía. Do đó vấn đề bảo mật thông tin khi sử dụng kỹ thuật mã hóa khóa bí mật là việc bảo mật khóa (nếu khóa lập mã bị lộ thì ngƣời khác dễ dàng tìm ra khóa giải mã). Với n ngƣời sử dụng cần trao đổi thông tin với nhau dùng mã hóa khóa bí mật thì mỗi cá thể cần biết n- 1 khóa bí mật. Thế thì với n cá thể đòi hỏi phải có số khóa ít nhất là n\*(n-1)/2 khóa. Khi tăng số ngƣời sử dụng thì số khóa sẽ tăng rất nhanh, gây nên hậu quả kém an toàn.

Sự ra đời của hệ mã hóa khóa công khai đã khắc phục đƣợc nhƣợc điểm của hệ mã hóa khóa bí mật, điển hình của hệ mật này có thể kể đến nhƣ RSA, Elgama, … Mã hóa khóa công khai xử lý chậm hơn nhƣng độ an toàn và tính thuận tiện trong quản lý khóa cao. Trong các ứng dụng mã hóa hiện tại, ngƣời ta thƣờng kết hợp các ƣu điểm của hai loại mã hóa này.

Bên cạnh đó, chúng ta cũng đã nghiên cứu về chữ ký số (là tập con của chữ ký điện tử) đƣợc tạo ra bằng sự biến đổi thông điệp sử dụng hệ thống mật mã công khai. Chữ ký số đƣợc chia thành hai loại là chữ ký kèm thông điệp và chữ ký khôi phục thông điệp. Với lƣợc đồ chữ ký kèm thông điệp, thông điệp ban đầu không thể khôi phục đƣợc từ chữ ký do đó thông điệp phải đi kèm chữ ký. Lƣợc đồ này sử dụng các hàm băm mật mã và ít bị giả mạo, đồng thời thông điệp gốc cũng là tham số quan trọng nhất cho quá trình kiểm tra chữ ký. Ngƣợc lại, thông điệp ban đầu có thể đƣợc khôi phục từ chính bản thân chữ ký với lƣợc đồ chữ ký khôi phục thông điệp. Lƣợc đồ này không đòi hỏi thông điệp gốc làm đầu vào để chứng thực chữ ký. Một số lƣợc đồ chữ ký số cơ bản của lƣợc đồ chữ ký khôi phục thông điệp nhƣ RSA, Elgamal cũng đã đƣợc nghiên cứu, tìm hiểu kỹ trong chƣơng này.

# CHƢƠNG II. THUẬT TOÁN CHỮ KÝ SỐ

# Hàm băm và thuật toán chữ ký số

# Hàm băm (Hash)

Thông thƣờng chữ ký số có độ dài lớn hơn văn bản ký, nhƣ vậy thời gian ký lâu, tốn bộ nhớ để lƣu chữ ký, tốn thời gian và băng thông để truyền chữ ký trên mạng máy tính. Nhƣ vậy lƣợc đồ chữ ký số chỉ cho phép ký trên tài liệu nhỏ mà thực tế ta cần ký trên các tài liệu rất dài, có thể dài nhiều Megabyte.

Để giải bài toán trên, cách đơn giản là chia tài liệu dài thành nhiều đoạn, sau đó ký lên từng đoạn. Với cách này, một tài liệu dài vẫn phải có một chữ ký rất lớn. Mặt khác tốc độ ký chậm vì các lƣợc đồ chữ ký hiện nay phải tính các số mũ module rất lớn. Nhƣng khó khăn hơn là tài liệu đã ký có thể bị sắp xếp lại các đoạn khác nhau. Trong khi đó ta cần bảo vệ tính nguyên vẹn của tài liệu, điều này không thể thực hiện đƣợc bằng cách ký độc lập từng đoạn nhỏ của chúng.

Giải pháp cho các vấn đề này là dùng hàm băm (Hash) để tạo ra “đại diện” tài liệu (message digest). Từ tài liệu có độ dài tùy ý, hàm băm tạo ra một tóm lƣợc (đại diện tài liệu) có kích thƣớc quy định (ví dụ 128 bit). Sau đó ký trên đại diện tài liệu này, thay vì ký trực tiếp trên tài liệu gốc.

Tài liệu X có độ dài bất kỳ

Bản tóm lƣợc thông báo z = h(X)

Chữ ký y = sigk(z)

Ký vào đại diện z của X (z = h(X)) thay vì ký trực tiếp trên X, tức y = sigk(z)

## \* Đặc điểm hàm băm và đại diện tài liệu

* + - * Hàm băm cho kết quả duy nhất đối với mỗi giá trị đầu vào
      * Hàm băm là hàm “một chiều” (“one-way”)

Nhƣ vậy từ đại diện tài liệu “khó” tính đƣợc tài liệu gốc.

Tóm lại, với hàm băm y = h(x), tính xuôi y = h(x) thì dễ, tính ngƣợc x = h-1(y) thì khó.

# Thuật toán băm SHA

SHA (Security Hash Algorithm) đƣợc chuẩn hoá năm 1993, sau đó đƣợc chỉnh sửa năm 1995 và đặt tên là SHA-1, từ đó phiên bản cũ đƣợc gọi là SHA-0 [12].

SHA-1 tạo ra mã băm có chiều dài cố định là 160 bit. Về sau, có nhiều nâng cấp đối với SHA, chủ yếu là tăng chiều dài mã băm, từ đó xuất hiện các phiên bản khác nhau của SHA, bao gồm: SHA-256 (mã băm dài 256 bit), SHA-384 (mã băm dài 385 bit) và SHA-512 (mã băm dài 512 bit).

Bảng 2.1. Tóm tắt các phiên bản của SHA

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Thông số** | **SHA-1** | **SHA-256** | **SHA-384** | **SHA-512** |
| Kích thƣớc mã băm (bit) | 160 | 256 | 384 | 512 |
| Kích thƣớcthông tin gốc (bit) | < 264 | < 264 | < 2128 | <2128 |
| Kích thƣớc khối (bit) | 512 | 512 | 1024 | 1024 |
| Độ dài từ (bit) | 32 | 32 | 64 | 64 |
| Số bƣớc thực hiện (bƣớc) | 80 | 64 | 80 | 80 |

Phần này chỉ mô tả thuật toán băm SHA-1, các phiên bản khác của SHA cũng đƣợc thiết kế theo nguyên lý tƣơng tự.

SHA-1 chấp nhận các khối thông tin có kích thƣớc tối đa là 264 bit để tạo ra mã băm với độ dài cố định 160 bit. Toàn bộ khối thông tin đƣợc xử lý theo từng khối 512 bit, qua 5 công đoạn nhƣ sau:

1. *Gắn bit đệm – Append padding bit*: Thông tin gốc đƣợc gắn thêm các bit thừa để có chiều dài (448 modulo 512) bit, tức là tất cả các khối trƣớc có chiều dài bằng nhau là 512 bit, riêng khối cuối cùng là 448 bit. Chú ý rằng việc chèn thêm bit vào khối thông tin đƣợc thực hiện đối với tất cả các khối thông tin gốc, kể cả khi khối thông tin gốc có số bit chính xác bằng 448 mod 512 (khi đó chuỗi bit chèn vào sẽ có chiều dài là 512 bit).
2. *Gắn chiều dài – Append length*: Một chuỗi 64 bit đƣợc gắn thêm vào khối thông tin. 64 bit này đƣợc xử lý nhƣ một số nguyên không dấu, cho biết chiều dài của khối thông tin gốc (tức chiều dài thật sự khi chƣa thực hiện công đoạn 1).

Sau công đoạn này, khối thông tin nhận đƣợc có chiều dài là bội số của 512 bit, đƣợc chia thành các nhóm, mỗi nhóm tƣơng đƣơng với 16 thanh ghi 32 bit (16\*32 = 512 bit).

1. *Khởi tạo bộ đệm MD – Initialize MD buffer:* Bộ đệm MD (message digest) là bộ nhớ có dung lƣợng 160 bit dùng để chứa các kết quả trung gian và kết quả cuối cùng của mã băm. Bộ nhớ này đƣợc tổ chức thành 5 thanh ghi 32 bit và đƣợc khởi tạo các giá trị ban đầu nhƣ sau (Hex):

A = 67452301 B = EFCDAB89 C = 98BADCFE D = 10325476

E = C3D2E1F0

1. *Xử lý thông tin theo từng khối 512 bit – Process message:* Đây là công đọan trung tâm quả hàm băm, còn đƣợc gọi là hàm nén (compress function), bao gồm 4 vòng, mỗi vòng 20 bƣớc. Hình 2.1 trình trình bày sơ đồ khối của bƣớc 4.

Cả 4 vòng có cấu trúc tƣơng tự nhau, nhƣng mỗi vòng sử dụng một hàm luận lý khác nhau là f1, f2, f3 và f4.

Cổng vào của mỗi vòng là khối bit Y (512 bit) đang xử lý cùng với giá trị của bộ đệm MD. Mỗi vòng sử dụng một biến cộng Kt khác nhau, với 0  t  79 biểu diễn cho 80 bƣớc của 4 vòng. Tuy nhiên, thực tế chỉ có 4 giá trị K khác nhau nhƣ sau:

**Yq**

**CVq**

160

512

32

**A**

**B**

**C D**

**E**

**f1, K, W[0…19]**

**20 vòng**

**A**

**B**

**C D**

**E**

**f2, K, W[20…39]**

**20 vòng**

**A**

**B**

**C D**

**E**

**f3, K, W[40…59]**

**20 vòng**

**A**

**B**

**C D**

**E**

**f4, K, W[60…79]**

**20 vòng**

160

**CVq+1**

*Hình 2.1. Xử lý thông tin trong SHA-1 [12]*

# Bƣớc Giá trị K (Hexa)

0  t  19 Kt = 5A827999

20  t  39 Kt = 6ED9EBA11

40  t  59 Kt = 8F1BBCDC

60  t  79 Kt = CA62C1D6

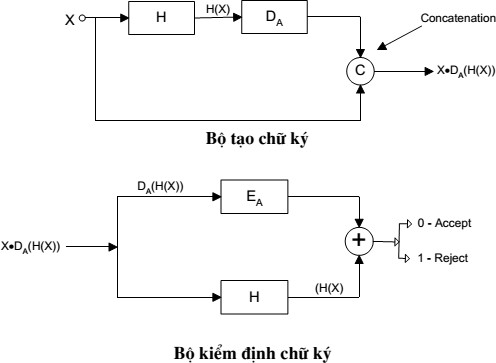
Cổng ra của vòng thứ tƣ (tức bƣớc 80) đƣợc cộng với ngõ vào của vòng đầu tiên để tạo ra CVq+1. Thao tác cộng đƣợc thực hiện một cách độc lập, ứng với từng thanh ghi trong bộ đệm MD với một từ tƣơng ứng trong CVq, sử dụng phép cộng modulo 232.

1. *Xuất kết quả - Output:* Sau khi tất cả các khối 512 bit đã đƣợc xử lý, ngõ ra của bƣớc cuối cùng chính là giá trị của mã băm.

Một thuộc tính quan trọng của giải thuật băm SHA-1 là mỗi bit trong mã băm đều có quan hệ với tất cả các bit trong thông tin gốc. Việc lặp lại các hàm f một cách phức tạp nhƣ vậy nhằm mục đích đảm bảo rằng dữ liệu đã đƣợc trộn một cách kỹ lƣỡng và do đó rất khó tìm đƣợc 2 khối thông tin gốc khác nhau có thể tạo ra cùng một mã băm.

# Mối quan hệ giữa hàm băm và thuật toán ký số

Hàm băm có ứng dụng chủ chốt trong các hệ chữ ký điện tử đƣợc sử dụng hiện nay. Thay vì ký (tức là thực hiện thuật toán DzA) lên văn bản X, ta cần thực hiện việc ký lên hX nhƣ vậy văn bản đã ký sẽ có dạng X || DzA(H(X)).



*Hình 2.2. Hệ sinh chữ ký điện tử có sử dụng hàm băm*

Để đảm bảm an toàn cao, chống đƣợc tấn công giả mạo chữ ký, chúng ta cần sử dụng các hàm băm mật mã (cryptographic hash function) với các thuộc tính nhƣ sau:

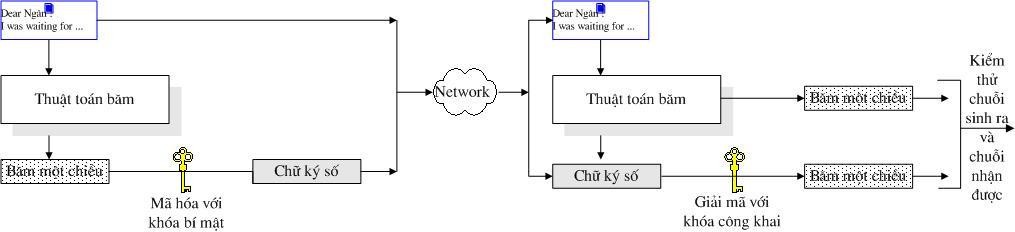
* Lấy đầu vào là một xâu với độ dài bất kỳ và sinh ra một xâu với độ dài cố định.
* Có tính một chiều (one - way): biết X, có thể dễ dàng tính đƣợc giá trị băm hX, nhƣng không thể tính ngƣợc đƣợc X khi chỉ biết hX, với công cụ tính toán hiện nay (bất khả thi về tính toán).
* Có tính phi đụng độ cao (collision free), tức là thực tế không thể tim đƣợc hai thông tin X ≠ X" sao cho H(X) = H(X"). Tất nhiên, đây là bất khả thi về mặt tính toán.

## \* Hàm băm và hàm băm dùng để kiểm tra tính toàn vẹn của dữ liệu

Nhƣ đã biết, hàm băm dùng để tạo đại diện tài liệu trƣớc khi “ký số”.

Hàm băm còn dùng để kiểm tra tính toàn vẹn của dữ liệu.

Trong hình dƣới có hai phần đƣợc gửi cho ngƣời nhận: dữ liệu gốc và chữ ký số. Ngƣời nhận sử dụng khóa công khai của ngƣời ký để giải mã đại diện bản tin (chính là “chữ ký” hay bản mã của đại diện bản tin, với loại chữ ký khôi phục thông điệp gốc). Dựa vào hàm băm đã biết, ngƣời nhận tạo ra đại diện bản tin gốc. Nếu 2 đại diện này giống nhau tức là bản tin gốc không bị thay đổi từ lúc đƣợc ký. Nếu chúng khác nhau, tức là bản tin gốc đã bị thay đổi.



*Hình 2.3. Hàm băm kiểm tra tính toàn vẹn dữ liệu*

Chữ ký số chỉ có thể đảm bảo khi khóa bí mật không bị lộ. Khi khóa bí mật bị lộ thì ngƣời sở hữu chữ ký không thể ngăn chặn đƣợc việc bị giả mạo chữ ký.

# Thuật toán chữ ký số chuẩn DSA

Giải thuật ký số DSA (Digital Signature Standard) là chuẩn cho các chữ ký số của chính phủ Mỹ hay tiêu chuẩn xử lý thông tin liên bang (Federal Information Processing Standard – FIPS). Giải thuật này đƣợc đề nghị bởi Viện các tiêu chuẩn và công nghệ quốc gia (the National Institute of Standards and Technology – NIST) vào tháng 8/1991 để sử dụng trong chuẩn chữ ký số (DSS – Digital Signature Standard) đƣợc chỉ ra trong FIPS 186 đƣợc chấp nhận năm 1993, Một sửa đổi nhỏ đƣợc đƣa ra năm 1996 trong FIPS 186-1, chuẩn đƣợc mở rộng hơn năm 2000 và đƣợc xem là tiêu chuẩn xử lý thông tin liên bang trong FIPS 186-2 [4], [13].

Đặc điểm của giải thuật này là đều sử dụng chữ ký theo kiểu chọn lựa ngẫu nhiên. Tất cả các lƣợc đồ DSA kèm thông điệp đều có thể cải biến thành các lƣợc đồ ký khôi phục thông điệp. Để tìm hiểu về lƣợc đồ DSA ta đi sâu tìm hiểu vào chuẩn chữ ký số DSS do khả năng cài đặt thực tế của nó.

Sơ đồ chữ ký DSS dựa trên giải thuật chữ ký số DSA. Chữ ký số DSS phải đi kèm thông điệp vì bản thân chữ ký không khôi phục đƣợc thông điệp gốc.

Trƣớc khi ký một thông điệp dài, phải tạo ra đại diện thông điệp nhờ hàm băm (đƣợc tìm hiểu trong chƣơng 2). Hàm băm tạo ra một dạng nén của dữ liệu (condensed version of data) gọi là đại diện thông điệp (message digest). Với sơ đồ chữ ký DSS, hàm băm là SHA (Security Hash Algorithm) đƣợc miêu tả trong FIPS 186. Hàm băm SHA tạo ra một giá trị số nguyên 160 bit đặc trƣng cho một thông điệp.

|  |  |  |
| --- | --- | --- |
| **Sinh chữ ký số** | | |
|  | Thông điệp |  |
|  | SHA - 1 |  |
|  | Thông điệp đại diện |  |
| Khoá |  | Chữ ký |
|  | Sinh chữ |  |
| Riêng | Ký số | số |

Thông điệp

Thông điệp đại diện

Chữ ký

Khoá công

số

khai

Chấp nhận hoặc

từ chối

**Xác thực chữ ký số**

Xác thực chữ ký số

SHA - 1

*Hình 2.4. Sơ đồ chữ ký DSA/DSS*

# Tóm tắt lƣợc đồ chữ ký DSA/DSS

Giả sử p là số nguyên tố 512 bit sao cho bài toán logarit rời rạc trong Zp là khó giải.

Có q là số nguyên tố 160 bit là ƣớc của (p – 1) Giả thiết 𝛼 ∈ 𝑍𝑝 là căn bậc q của 1 modulo p Cho 𝑝 ∈ 𝑍𝑝 và 𝑎 = 𝑍 𝑥 𝑍𝑝 và định nghĩa:

A= {(p, q, a, a, β) : β ≡ aa (mod p)}

Các số p, q, a và β là công khai, có a mật

Với = (𝑝, 𝑞, 𝛼, 𝑎, 𝛽) và với một số ngẫu nhiên (bí mật) k, 1 𝑘

𝑞 − 1, ta định nghĩa:

Quá trình ký số sigk (x, k) = (y, δ) trong đó: y = (ak mod p) mod q và

δ = (x +ay)k-1 mod q với 𝑥 ∈ 𝑍𝑝 và 𝛾, 𝛿 ∈ 𝑍

Quá trình xác minh sẽ hoàn toàn sau các tính toán: e1 = xδ-1 mod q

e2 = yδ-1 mod q

𝑉𝑒𝑟𝑘(𝑥, 𝛾, 𝛿) = true - (𝛼𝑒1 𝛽𝑒2 mod 𝑝) mod 𝑞 = 𝛾

# Thuật toán

## Thuật toán sinh khóa

* + - * + Chọn số nguyên tố 512 bit p, sao cho bài toán logarit rời rạc trong Zp là khó giải, 2511+64t < p < 2512+64t, t  [0, 8].
        + Chọn số nguyên tố 160 bit q, là ƣớc của (p – 1), (2159 < q < 2160).
        + Chọn số a = g(p-1)/q mod p, a ≠ 1, (g là phần tử nguyên thủy trong Zp).
        + Chọn khóa bí mật **a**: 1 ≤ a ≤ q – 1. Tính khóa công khai **β = α a** mod p.
        + Công khai (p, q, a, β).

## Thuật toán sinh chữ ký

* + - * + Chọn ngẫu nhiên bí mật số nguyên k, 0 < k < q – 1.
        + Chữ ký trên **x** là cặp (δ, y), trong đó:

y = (ak mod p) mod q,δ = k-1(**x** + ay) mod q.

Chú ý: Nếu x lớn, thì phải tạo đại diện z = H(x), và ký trên z.

## Thuật toán xác minh chữ ký

* + - * + Xét khoá công khai (p,q, a, β): Nếu điều kiện: 0 < δ, y < q không thoả mãn, thì từ chối chữ ký.
        + Tính e1 = wx mod q, e2 = yw mod q, với w = δ -1 mod q.

- Tính v = (𝛼𝑒1 𝛽𝑒2 mod 𝑝) mod 𝑞.

* + - * + Chữ ký đúng nếu v = y.

***í dụ 2.1.*** Chữ ký trên thông điệp x = 1234.

* *Sinh khóa:*

- Chọn q = 101, p = 78q + 1 = 7879

* + Chọn a = 378 mod 7879 = 170, g = 3 là phần tử nguyên thuy trong Z7879
  + Chọn khóa bí mật a =75. Khóa công khai β = a a mod 7879 = 4576
* *Sinh chữ ký*: Chữ ký trên thông điệp **x** = 1234.
  + Chọn ngẫu nhiên k = 50, tính k-1 mod 101 = 99

- Tính y = (17030 mod 7879) mod 101 = 2518 mod 101 = 94

δ = (1234 +75\*94)\*99 mod 101 = 97

- Chữ kí trên **x** = 1234 là (94, 97).

* *Xác minh chữ ký*:

- Tính w = δ -1 mod q = 97-1 mod 101 = 25 e1= w x mod q = 25 \* 1234 mod 101 = 45, e2 = y w mod q = 94 \* 25 mod 101 = 27.

v = (𝛼𝑒1 𝛽𝑒2 mod 𝑝)mod 𝑞 = 17045 456727 mod 7879) mod 101

= 2518 mod 101 = 94.

* + Chữ ký đúng vì v = y = 94.

# Đặc trƣng của DSS

## Ðộ an toàn

Độ an toàn của chữ ký phụ thuộc vào việc bảo vệ khóa bí mật. Mặt khác, từ khoá công khai “khó” tính đƣợc khoá bí mật. Cụ thể là biết khóa công khai **β,** “khó” tính đƣợc khoá bí mật **a**, vì **β = αa** mod p.

## Tính hợp lệ

Tính hợp lệ của chữ ký DSS dựa trên 2 định lý sau [13]:

*Định lý 1:* Cho p, q là số nguyên tố thoả mãn q\(p-1), h là số nguyên dƣơng h < p. Nếu g ≡ h(p-1)/q mod p thì gq ≡ 1 mod p.

Thật vậy gq ≡ (h(p-1)/q)q ≡ h(p-1) mod p ≡ 1 mod p (theo định lý Fermat nhỏ).

*Định lý 2:* Với g, p, q xác định nhƣ trên, ta có:

Nếu m ≡ n mod p thì gm ≡ gn mod p.

Thật vậy không mất tính tổng quát ta đặt m = n + kq, ta có:

gm ≡ gn + kq ≡ (gn mod p)(gkq mod p) ≡ gn mod p => điều phải chứng minh.

## Nhược điểm:

* Kích thƣớc modulo p bị cố định = 512 bit. Để đáp ứng yêu cầu kích thƣớc này có thể đƣợc thay đổi nếu cần, NIST đã chọn tiêu chuẩn cho phép có nhiều cỡ modulo, cỡ modulo bất kỳ chia hết cho 64 trong phạm vi từ 512 đến 1024 bit.
* Chữ ký đƣợc tạo ra nhanh hơn việc xác minh nó, dẫn đến hai vấn đề:

+ Bức điện chỉ đƣợc ký một lần, song nhiều khi cần xác minh chữ ký nhiều lần trong nhiều năm. Gợi ý nhu cầu có thuật toán xác minh nhanh hơn.

+ Những kiểu máy tính nào có thể dùng để ký và xác minh chữ ký? Nhiều ứng dụng, ví dụ thẻ thông minh tính toán hạn chế nhƣng liên lạc với máy tính mạnh hơn. Tuy nhiên, có tình huống cần hệ thống thông minh tạo chữ ký, trong tình huống khác lại cần thẻ thông minh kiểm tra chữ ký.

# Thuật toán chữ ký số trên đƣờng cong Elliptic ECDSA

Hệ thống mã hóa khóa công khai dựa trên việc sử dụng các bài toán khóa giải quyết. Vấn đề khó ở đây chính là số lƣợng phép tính cần thiết để tìm ra một lời giải cho bài toán là rất lớn. Trong lịch sử 20 năm của ngành mã hóa bất đối xứng đã có nhiều đề xuất khác nhau cho dạng bài toán nhƣ vậy, tuy nhiên chỉ có hai trong số các đề xuất đó còn tồn tại vững đến ngày nay. Hai bài toán đó bao gồm: bài toán logarit rời rạc và bài toán phân tích thừa số nguyên tố.

Cho đến năm 1985, hai nhà khoa học Neal Koblitz và Victor S.Miller đã độc lập nghiên cứu và đƣa ra đề xuất ứng dụng lý thuyết toán học đƣờng cong Elliptic trên trƣờng hữu hạn. Đƣờng cong Elliptic đƣợc nghiên cứu một cách rộng rãi trong vòng 150 năm trở lại đây và đã đạt đƣợc một số kết quả lý thuyết có giá trị [8].

Chữ ký số dựa trên mật mã đƣờng cong Elliptic (ECDSA) đƣợc giới thiệu lần đầu vào năm 1991 bởi các công trình nghiên cứu độc lập của Neals Koblitz và Victor Miller. Từ những năm 2000, các nƣớc Mỹ, Nga, Nhật Bản, Hàn Quốc và một số nƣớc Châu Âu đã đầu tƣ nghiên cứu về vấn đề này và đƣa vào các hệ thống tiêu chuẩn nhƣ ISO, ANSI, IEEE, SECG, FIPS. Một trong những quốc gia sử dụng ECDSA nhiều nhất là Liên bang Nga. Năm 2001, Nga đã đƣa ra chuẩn chữ ký số GOST R34-10-2001 sử dụng mật mã Elliptic với độ dài khóa 256 bit. Phiên bản mới nhất của Nga về chữ ký số là GOST R34-10 năm 2012 với độ dài khóa trong khoảng từ 256 bit đến 512 bit.

# Lý thuyết đƣờng cong Elliptic

Gọi K là một trƣờng hữu hạn hoặc vô hạn. Một đƣờng cong Elliptic là một tập các điểm có tọa độ (𝑥, 𝑦) ∈ 𝑥 thỏa mãn phƣơng trình có dạng:

y2 + a1xy + a3y = x3 + a2x2 + a4x + a6 (2.1) trong đó ai ∈ K, 4a 3 + 27a 2 ≠ 0.

4 6

Với một điểm O gọi là điểm tại vô cùng [8].

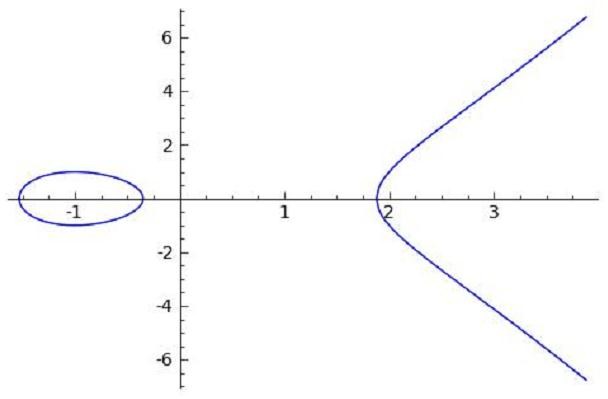
Xét đƣờng cong Elliptic trên trƣờng nguyên tố hữu hạn Fp (p nguyên tố, p > 3) với công thức biến đổi sau:

X→ X – a2 , Y→ Y – a1X + a3

3 2

Khi đó, phƣơng trình Weierstrass có dạng: X3 + aX + b Vậy trong trƣờng Fp, (2.1) trở thành:

Y2 = X3 + aX + b (2.2)



## Định nghĩa

*Hình 2.5. Đường cong Elliptic y2 = x3 - 3x + 1*

Giả sử K là một trƣờng có đặc số khác 2 và khác 3, xét đa thức: X3 + aX + b (với a, b ∈ K)

Khi đó, đƣờng cong Elliptic trên trƣờng K: Y2 = X3 + aX + b là tập hợp tất cả các điểm (x, y) với x, y ∈ K sao cho (2.2) không có các nghiệm bội. Tức là 4a3+ 27b2 ≠ 0 mod p cùng với phần tử 0 – điểm 0 này đƣợc gọi là điểm vô hạn.

Nếu K là trƣờng đặc số 2 thì ta định nghĩa:

𝑆 = {(𝑥, 𝑦): 𝑦2 + 𝑦 = 𝑥3 + 𝑎𝑥 + 𝑏} 𝖴 {0} (2.3) Nếu K là trƣờng đặc số 3 thì ta định nghĩa:

𝑆 = {(𝑥, 𝑦): 𝑦2 + 𝑦 = 𝑥3 + 𝑏𝑥 + 𝑐} 𝖴 {0} (2.4)

## Tính chất của đường cong Elliptic [8]

- Nếu hai điểm P1(x1, y1) và P2 (x2, y2) với x1 ≠ x2 nằm trên cùng một đƣờng cong elliptic E, thì đƣờng thẳng qua hai điểm P1 và P2 sẽ cắt một điểm duy nhất P3(x3, y3) có thể xác định thông qua P1 và P2.

. - Tiếp tuyến của đƣờng cong tại điểm bất kỳ P(x, y) trên đƣờng cong E cũng cắt đƣờng cong elliptic E tại một điểm duy nhất nằm trên đƣờng E, điểm này cũng có thể xác định đƣợc thông qua P.

Dựa vào những tính chất đó, ngƣời ta đã nghiên cứu và phát hiện ra một khả năng mới cho kỹ thuật mã hóa nói chung và chứng thực nói riêng, kỹ thuật mã hóa dựa trên đƣờng cong elliptic.

## Các phép toán trên đường cong Elliptic

Giả sử E là đƣờng cong Elliptic trên trƣờng Zp và P, Q là 2 điểm trên E. Xét các phép toán sau trên E [8].

*a/ Phần tử không*

Nếu P là điểm 0 thì -P cũng là 0. Với mọi điểm Q ta định nghĩa 0 + Q = Q.

*b/ Phần tử nghịch đảo*

Trong Zp chúng ta định nghĩa nghịch đảo của P(x, y) là -P(x, -y). Nếu Q = -P thì P + Q = 0.

*c/ Phép cộng*

Giả sử, ta có P(x1, y1) và Q(x2, y2) là hai điểm thuộc E. Nếu x1 = x2 và y1 = -y2 thì ta định nghĩa P + Q = 0 Ngƣợc lại thì P + Q = S(x3, y3) ∈ E trong đó:

𝑥3 = 𝜆2 − 𝑥1 − 𝑥2

{𝑦3 = 𝜆(𝑥1 − 𝑥3) − 𝑦1

Với:

𝜆 =

𝑦2 − 𝑦1 , nếu P ≠ Q

𝑥2 − 𝑥1

ﻟ

2

❪3 𝑥 +

1 , nếu P = Q

𝗅 2𝑦1

Vậy nếu P ≠ Q thì:

ﻟ

= (𝑦2 − 𝑦1)2 − 𝑥

− 𝑥

𝑆 =

3

❪ 𝑦

𝑥2 − 𝑥1

= (𝑦2 − 𝑦1) (𝑥

1

− 𝑥

2

) − 𝑦

(2.5)

𝗅 3

Nếu P = Q thì:

𝑥2 − 𝑥1 1 3 1

3𝑥2 + 𝑎 2

𝑆 =

𝑥3 = ( 1 )

2𝑦1

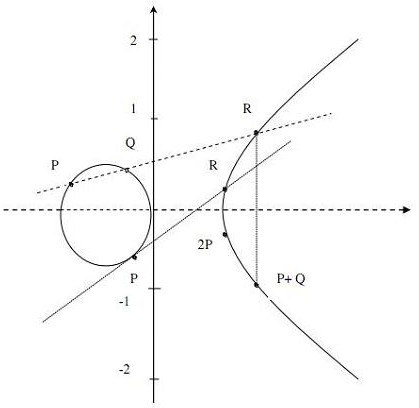
3𝑥2 + 𝑎

− 2𝑥1

(2.6)

𝑦3 = ( 1 ) (𝑥1 − 𝑥3) − 𝑦1

𝗅 2𝑦1



*Hình 2.6. Phép cộng trên đường cong Elliptic*

Chú ý rằng các điểm (x3, y3), (x3,-y3) cũng nằm trên đƣờng cong E và xét về mặt hình học, thì các điểm (x1, y1), (x2, y2), (x3,-y3) cũng nằm trên cùng một đƣờng thẳng.

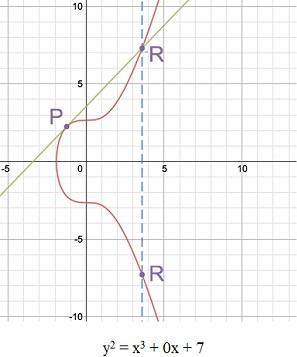
***Tính chất***: Dễ thấy rằng tập E với phép toán cộng tạo thành một nhóm Abelian:

* Tính đóng: Nếu P, Q ∈ E thì P + Q ∈ E
* Tính kết hợp: Nếu P, Q, R ∈ E thì P + (Q + R) = (P + Q) + R
* ∃ phần tử trung hòa 0: ✯P(x, y) ∈ E thì P + 0 = 0 + P = P
* ∃ phần tử nghịch đảo: ✯P(x, y) ∈ E thì ∃ -P(x, -y) ∈ E để P + (-P) = 0
* Tính chất giao hoán: Nếu P, Q ∈ E thì P + Q = Q + P

*d/ Phép nhân*

Phép nhân một số nguyên k với một điểm P thuộc đƣờng cong Elliptic E là điểm Q (Q ∈ E) đƣợc xác định bằng cách cộng k lần điểm P:

kP = P + P + … + P (k lần phép cộng điểm P)

Vì vậy nếu G là một điểm thuộc đƣờng cong Elliptic E thì với mỗi số nguyên dƣơng k luôn dễ dàng xác định đƣợc điểm Q = k x G.

*Hình 2.7. Phép nhân đôi trên đường cong Elliptic*

***í dụ 2.2.*** Xét đƣờng cong Elliptic y2 = x3 – 36x

Lấy P = (-3, 9), Q(-2, 8). Hãy tìm P + Q và 2P?

Ta có: x1 = -3, x2 = -2, y1 = 9, y2 = 8

Áp dụng công thức (2.5), ta có P + Q = (x3, y3) trong đó:

𝑥 = ( 8 – 9 )

3

2

–2 + 3

+ 3 + 2 = 1 + 3 + 2 = 6

𝑦3

= ( 8 – 9 ) (- 3 – 6) – 9 = (–1)(–9) – 9 = 0

–2 + 3

Vậy P + Q = (6, 0)

Áp dụng công thức (2.6), ta có 2P = (x4, y4) trong đó:

3(–3)2– 36 2

–9 2 25

𝑥4 = (

18 )

+ 6 = ( )

18

+ 6 = 4

3(- 3)2 - 36 25 1 25 35

𝑦4 = (

25

Vậy 2P = ( 4 , -

18 ) (- 3 −

35

8 )

4 ) − 9 = (− 2) (- 3 −

4 ) − 9 = − 8

# Đƣờng cong eliptic trên các trƣờng hữu hạn

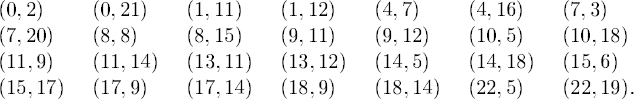
## Đường cong elliptic trên Æ𝑝

Cho *p>3* là số nguyên tố. Một đƣờng cong elliptic E trên Æ𝑝 đƣợc biểu diễn bởi phƣơng trình có dạng:

𝑦2 = 𝑥3 + 𝑎𝑥 + 𝑏

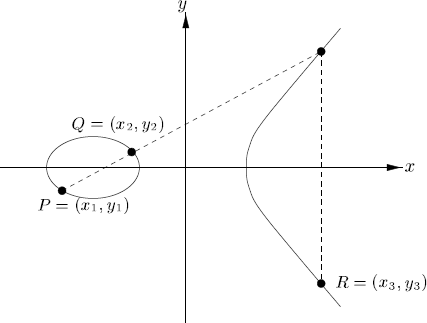
Trong đó 𝑎, 𝑏 ∈ Æ𝑝 và 4𝑎3 + 2 𝑏2 0 (𝑚𝑜𝑑 𝑝). Thiết lập E(Æ𝑝) bao gồm tất cả các điểm (𝑥, 𝑦), 𝑥 ∈ Æ𝑝, 𝑦 ∈ Æ𝑝 thỏa mãn phƣơng trình xác định (2.2), cũng nhƣ điểm đặc biệt đƣợc gọi là điểm vô cùng.

***Ví dụ 2.3.*** (Đƣờng cong elliptic trên Æ23) cho p = 23 và xét đƣờng cong

elliptic : 𝑦2 = 𝑥3 + 𝑥 + 4 xác định đặc điểm trên Æ23 (trong các ký hiệu của phƣơng trình (2.2), chúng ta có a = 1 và b = 4). Chú ý ở đây 4𝑎3 + 2 𝑏2 = 4 + 432 Ξ 22(𝑚𝑜𝑑 23), nhƣ vậy E là một đƣờng cong elliptic thực sự. Những điểm trong E(Æ23) là và đƣợc hiện thị sau đây:

***Công thức cộng****:* Đây là một quy tắc, gọi là quy tắc *cung – và – đường tiếp tuyến*, cộng hai điểm trên đƣờng cong elliptic E(Æ𝑝) để cung cấp ba điểm trên đƣờng cong elliptic. Cùng tạo ra toán tử cộng, thiết lập các điểm mẫu của E(Æ𝑝) thành một nhóm đồng nhất với . Nó là nhóm sử dụng cấu trúc của mật mã đƣờng cong elliptic. Quy tắc cộng là tốt nhất về giải thích hình học. Cho P = (x1,y1) và Q = (x2, y2) là hai điểm khác biệt trên đƣờng cong elliptic

E. Tổng của P và Q, đƣợc biểu diễn *R = (x3, y3)* đƣợc định nghĩa nhƣ sau. Đầu tiên ta vẽ đƣờng thẳng P và Q; đƣờng thẳng này cắt các đƣờng cong elliptic trong một điểm thứ ba. Sau đó R phản chiếu điểm này trong trục – x. Điều này đƣợc mô tả trong hình 1. Đƣờng cong elliptic trong hình bao gồm hai phần, hình giống nhƣ elliptic và đƣờng cong vô hạn.



*Hình 2.8. Đặc tả hình học của phép cộng của hai điểm riêng biệt trên đường cong elliptic: P + Q = R*

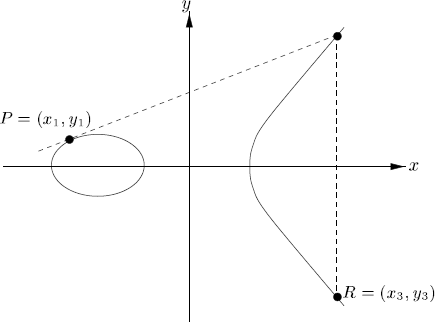
Nếu *P = (x1,y1)* thì nhân đôi của P đƣợc biểu diễn *R=(x3,y3),* đƣợc định nghĩa nhƣ sau. Đầu tiên vẽ một đƣờng tiếp tuyền đến đƣơng cong elliptic tại

P. Đƣờng thẳng giao với đƣờng cong elliptic tại điểm thứ 2. R là phản chiếu của điểm đó trên trục – x. Xem mô tả trong hình 2.9.

Công thức đại số sau đây cho tổng của hai điểm và nhân đôi của một điểm bây giờ có thể đƣợc rút ra từ mô tả hình học.

1. 𝑃 + = + 𝑃 = 𝑃 cho tất cả 𝑃 ∈ 𝐸(Æ𝑝)

2. Nếu 𝑃 = (𝑥, 𝑦) ∈ 𝐸(Æ𝑝) thì (𝑥, 𝑦) + (𝑥, −𝑦) = (ở đây điểm (x,-y) đƣợc đặc tả bởi –P và gọi là phần phủ định của P; quan sát thấy –P là điểm thực trên cung).



*Hình 2.9. Mô tả hình học của phép nhân đôi của một điểm đường cong elliptic: P + P = R*

3. (Phép cộng điểm) Cho 𝑃 = (𝑥1, 𝑦1) ∈ 𝐸(Æ𝑝) và = (𝑥2, 𝑦2) ∈

𝐸(Æ𝑝) ở đó 𝑃 G thì P + Q = (x3, y3), trong đó:

𝑥 = (𝑦2 − 𝑦1)2 − 𝑥

− 𝑥

và 𝑦

= (𝑦2 − 𝑦1)2 (𝑥

− 𝑥

) − 𝑦

3 𝑥2 − 𝑥1

1 2 3

𝑥2 − 𝑥1 1 3 1

4. (Phép nhân đôi) Cho 𝑃 = (𝑥1, 𝑦1) ∈ 𝐸(Æ𝑝) ở đó 𝑃 G −𝑃 thì 2P = (x3,y3), trong đó:

3𝑥2 − 𝑎 2 3𝑥2 − 𝑎 2

𝑥3 = ( 1 )

2𝑦1

− 2𝑥1 và 𝑦 3 = ( 1 )

2𝑦1

(𝑥1 − 𝑥3) − 𝑦1

Quan sát rằng các bổ sung của hai đƣờng cong elliptic trong 𝐸(Æ𝑝) đòi hỏi một vài phép tính toán học (cộng, trừ, nhân, và nghịch đảo) trong các cơ bản Æ𝑝.

## Đường cong elliptic trên Æ2𝑚

Một đƣờng cong elliptic E trên Æ2𝑚 đƣợc biểu diễn bằng phƣơng trình

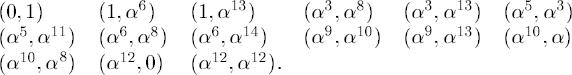
dạng:

𝑦2 + 𝑥𝑦 = 𝑥3 + 𝑎𝑥2 + 𝑏 (2.7)

Trong đó 𝑎, 𝑏 ∈ Æ2𝑚 và 𝑏 G 0. Thiết lập E(Æ2𝑚) bao gồm tất cả các

điểm (𝑥, 𝑦), 𝑥 ∈ Æ2𝑚𝑝, 𝑦 ∈ Æ2𝑚 thỏa mãn phƣơng trình xác định (2.7), cũng nhƣ điểm đặc biệt 𝐺 đƣợc gọi là điểm vô cùng.

***Ví dụ 2.4****.* Xét Æ24 đại diện tối giản các tam thức ƒ(𝑥) = 𝑥4 + 𝑥 + 1. Xét đƣờng cong elliptic E: 𝑦2 + 𝑥𝑦 = 𝑥3 + 𝛼4𝑥2 + 1 trên Æ24 (trong chú giải của phƣơng trình (2.7), chúng ta có 𝛼 = 𝑎4 và 𝑏 = 1) chú ý là 𝑏 G 0 nhƣ vậy E là một đƣờng cong elliptic thực. Các điểm trong E(Æ24 ) là 𝐺 và đƣợc tính ở phía dƣới:



***Công thức cộng:*** Với đƣờng cong elliptic trên Æ𝑝, gọi là quy tắc cung và tiếp tuyến cho các phép thêm các điểm trên đƣờng cong elliptic 𝐸(Æ2𝑚) cho ba điểm trên đƣờng cong elliptic. Với cả hai công thức cộng, thiết lập các điểm

𝐸(Æ2𝑚) trong mẫu nhóm với 𝐺 nhƣ là định dạng của nó.

Công thức đại số sau đây cho tổng của hai điểm và tăng gấp đôi của một điểm bây giờ có thể đƣợc rút ra từ mô tả hình học.

1. 𝑃 + 𝐺 = 𝐺 + 𝑃 = 𝑃 cho tất cả 𝑃 ∈ 𝐸(Æ2𝑚).

2. Nếu 𝑃 = (𝑥, 𝑦) ∈ 𝐸(Æ2𝑚) (𝑥, 𝑦) + (𝑥, 𝑥 + 𝑦) = 𝐺 (điểm (x, x+y) đƣợc đặc tả bởi –P và gọi là phần phủ định của P; quan sát thấy –P là điểm thực trên cung).

3. Phép cộng điểm: Cho 𝑃 = (𝑥1, 𝑦1) ∈ 𝐸(Æ2𝑚) và = (𝑥2, 𝑦2) ∈

𝐸(Æ2𝑚) trong đó 𝑃 G thì 𝑃 + = (𝑥3, 𝑦3), trong đó:

𝑥 = (𝑦1 + 𝑦2)

2

3 𝑥1 + 𝑥2

+ 𝑦1 + 𝑦2 + 𝑥 + 𝑥 + 𝑎 𝑣à 𝑦

𝑥1 + 𝑥2 1 2 3

= (𝑦1 + 𝑦2) (𝑥 + 𝑥 ) + 𝑦

𝑥1 + 𝑥2 1 3 1

4. Phép nhân đôi: Cho 𝑃 = (𝑥1, 𝑦1) ∈ 𝐸(Æ2𝑚) trong đó 𝑃 G −𝑃 thì

2𝑃 = (𝑥3, 𝑦3), trong đó:

𝑥 = 𝑥2 + 𝑏

và 𝑦

= 𝑥2 + (𝑥

+ 𝑦1) 𝑥 + 𝑥

3 1 𝑥2

1

3 1 1

𝑥1 3 3

***Ví dụ 2.5.*** (Phép cộng trong đƣờng cong elliptic) Hãy xem đƣờng cong elliptic đã đƣợc định nghĩa trong ví dụ 2.4.

1. Cho 𝑃 = (𝛼6, 𝛼8) và = (𝛼3, 𝛼13) thì 𝑃 + = (𝑥3, 𝑦3) đƣợc tính nhƣ sau:

𝛼8 + 𝛼13 2 𝛼8 + 𝛼13

𝑥3 = ( 𝛼6 + 𝛼3 ) + 𝛼6 + 𝛼3 + 𝛼6 + 𝛼3 + 𝛼4

𝛼3 2

= ( )

2

𝛼

Và

𝛼3

+ 𝛼2 + 𝛼6 + 𝛼3 + 𝛼4 = 1

𝛼8 + 𝛼13 ( 6 )

8 𝛼3 13

2 13

𝑦3 = ( 𝛼6 + 𝛼3 ) 𝛼 + 1 + 1 + 𝛼

2

= ( ) (𝛼

𝛼

) + 𝛼

= 𝛼

Từ đó suy ra 𝑃 + = (1, 𝛼13)

2. Cho 𝑃 = (𝛼6, 𝛼8) thì 2𝑃 = (𝑥3, 𝑦3) đƣợc tính nhƣ sau:

𝑥3

= (𝛼6)2 + 1

(𝛼6)2

= 𝛼12 + 𝛼3 = 𝛼10

𝑦3 = (𝛼

6)2

+ (𝛼6

𝛼8

+ 𝛼6) 𝛼10

+ 𝛼10

= 𝛼12

+ 𝛼13

+ 𝛼10

= 𝛼8

Từ đó suy ra 𝑃 + = (𝛼10, 𝛼11).

## Thông tin cơ bản

***Nhóm bậc****:* Cho E là đƣờng cong elliptic trên trƣờng hữu hạn Æ𝑝. Định lý Hasse có nói rằng số lƣợng các điểm trên một đƣờng cong elliptic (bao gồm cả các điểm ở vô cùng) là G 𝐸(Æ𝑞) = 𝑞 + 1 − trong đó | | 2√𝑞 G 𝐸(Æ𝑞) gọi là bậc của E và *t* gọi là vệt của *E*. Trong một số từ, bậc của đƣờng cong elliptic 𝐸(Æ𝑞) là xấp xỉ bằng với kích thƣớc của *q* trong các trƣờng dƣới.

***Cấu trúc nhóm***: 𝐸(Æ𝑞) là nhóm giao hoán giữa bậc 1 hoặc 2. Đó là,

𝐸(Æ𝑞) là đẳng cấu từ Æ𝑛1 Æ𝑛2 , trong đó 𝑛2 chia cho 𝑛1 cho cùng một số nguyên dƣơng 𝑛1 và 𝑛2. Æ𝑛 biểu thị theo chu kỳ trên *n*. Ngoài ra, 𝑛2 chia cho

𝑞 − 1. Nếu 𝑛2 = 1 thì 𝐸(Æ𝑞) đƣợc gọi là chu kỳ. Một lựa chọn 𝐸(Æ𝑞) là đẳng cấu từ Æ𝑛1 và nó bao gồm một điểm 𝑃 ∈ 𝐸(Æ𝑞) nhƣ vậy 𝐸(Æ𝑞) =

{𝑘𝑃: 0 𝑘 𝑛1 − 1}; vì vậy điểm đó đƣợc gọi là điểm khởi đầu (bộ sinh)

của 𝐸(Æ𝑞).

# Miền tham số ECDSA

Cho các miền tham số ECDSA bao gồm một đƣờng cong elip E lựa chọn phù hợp đƣợc xác định trên một tập hữu hạn Æq đƣợc đặc trƣng bởi *p*, và một điểm cơ bản *G* thuộc *E* (Æq). Các miền tham số có thể đƣợc chia sẻ bởi một nhóm các thực thể, hoặc cụ thể cho một ngƣời dùng duy nhất.

## Miền tham số

Để tạo điều kiện thuận lợi cho khả năng tƣơng tác, một số hạn chế đƣợc đặt trên trƣờng kích thƣớc *q* cơ bản và đại diện đƣợc sử dụng cho các yếu tố của Æ𝑞. Hơn nữa, để tránh một số đƣợc biết đến các cuộc tấn công cụ thể, giới hạn đƣợc đặt trên đƣờng cong elliptic và thứ tự của các điểm cơ sở.

***Những yêu cầu của trường***. Trình tự của trƣờng hữu hạn cơ bản *q = p*,

là một số nguyên tố, hoặc *q = 2m* là lũy thừa của 2. Trong trƣờng hợp *q = p,*

các tập hữu hạn cơ bản là Æ𝑞, các số nguyên *modulo p*. Trong trƣờng hợp

*q = 2m,* tập hữu hạn cơ bản là Æ2𝑚 mà các thành phần đại diện đối với một đa thức hoặc một cơ sở bình thƣờng nhƣ mô tả trong mục 3.

***Yêu cầu đường cong Elliptic***. Để tránh sự tấn công của Pollard [10] và các Pohlig-Hellman [10] vào đƣờng cong elip logarit rời rạc là cần thiết về điểm Æ𝑞- hợp lý đƣợc chia hết cho một *n* đủ lớn. ANSI X9.62 chỉ ra rằng *n>2160*. Sau khi cố định một tập cơ bản Æ𝑞, *n* nên đƣợc lựa chọn để đƣợc càng lớn càng tốt, tức là ta nên có *n ≈ q,* vì vậy # E(Æ𝑞) là gần nhƣ chính. Trong phần còn lại của bài viết này, chúng ta sẽ giả định rằng *n > 2160* và *n > 4 √ q*. Các hệ số đều đƣợc định nghĩa là *h = # E(*Æ𝑞*)/n*.

Một số biện pháp phòng ngừa cần tiếp tục đƣợc thực hiện khi lựa chọn các đƣờng cong elip. Để tránh các thuật toán giảm Menezes, Okamoto và Vanstone [10], Frey và Ruck [10], các đƣờng cong không nên supersingular (tức là *p* không nên chia *(q + 1 -* # E(Æ𝑞)). Tổng quát hơn, ta nên xác minh rằng *n* không chia *qk - 1*cho tất cả 1 ≤ k ≤ C, C là đủ lớn để nó tính toán khả thi nhằm tìm logarit rời rạc trong Æ𝑞C. Cuối cùng, để tránh các cuộc tấn công của Semaev [10], Smart [10], Satoh và Araki [10] trên tập Æ𝑞 đƣờng cong bất thƣờng, đƣờng công không nên là tập Æ𝑞 bất thƣờng (ví dụ, # E(Æ𝑞)≠ q).

Một cách thận trọng để bảo vệ và chống lại các cuộc tấn công, và các cuộc tấn công tƣơng tự đối với các loại đặc biệt của các đƣờng cong có thể đƣợc phát hiện trong tƣơng lai, chọn đƣờng cong eliptic E tại điểm ngẫu nhiên với điều kiện # E(Æ𝑞) chia hết cho một số nguyên tố đủ lớn có khả năng bị khuất phục và đƣờng cong ngẫu nhiên các cuộc tấn công có mục đích đặc biệt là không đáng kể. Đƣờng cong có thể đƣợc lựa chọn xác minh một cách ngẫu nhiên bằng cách chọn các hệ số của phƣơng trình xác định đƣờng cong elliptic là kết quả đầu ra của một hàm chức năng một chiều nhƣ SHA-1 theo một số thủ tục xác định trƣớc. Một thủ tục cho việc này có tinh thần

tƣơng tự với phƣơng pháp đƣợc đƣa ra trong FIPS 186 để chọn số nguyên tố DSA xác minh một cách ngẫu nhiên.

## Tóm lại, các thông số miền bao gồm:

* + - * 1. Một tập có kích thƣớc *q*, hoặc *q = p*, một nguyên tố lẻ, hoặc *q = 2m*.
        2. Một dấu hiệu cho thấy FR (tập đại diện) của các đại diện đƣợc sử dụng cho các nhân tố của Æ𝑞. Chọn ngẫu nhiên một chuỗi bit *seedE* (nguồn E) chiều dài ít nhất 160 bit, nếu các đƣờng cong elliptic đƣợc tạo ra theo phƣơng pháp mô tả trong mục 3.2.
        3. Hai lĩnh vực yếu tố *a* và *b* trong Æ𝑞 xác định phƣơng trình của đƣờng cong elliptic *E* trên Æ𝑞 (tức là, 𝑦2 = 𝑥3 + 𝑎𝑥 + 𝑏 trong trƣờng hợp *p > 3*,

𝑦2 + 𝑥𝑦 = 𝑥3 + 𝑎𝑥2 + 𝑏 trong trƣờng hợp *p = 2*).

* + - * 1. Hai lĩnh vực yếu tố xG và yG trong Æ𝑞 xác định một điểm hữu hạn G = (xG, yG) của bậc nguyên (thứ tự số nguyên tố) trong E(Æ𝑞).
        2. Thứ tự *n* của điểm G, với n > 2160 và *n > 4*√𝑞.
        3. Phần phụ đại số *h = # E(*Æ𝑞) *n*.

## Tạo một đường cong Elliptic xác định ngẫu nhiên

1. ***Trường hợp q = p***

Các ký hiệu sau đây đƣợc sử dụng: t = [log2p], s = [(t-1)/160], v = t-160.s

***Thuật toán 2.1***: Tạo ra một đƣờng cong ellip ngẫu nhiên về Fp. INPUT: Kích thƣớc trƣờng p, trong đó p là một nguyên tố lẻ.

OUTPUT: Một chuỗi bit *seedE* (thiết lập E) chiều dài ít nhất là 160 bit và các nhân tố a, b thuộc Æ𝑞 xác định một đƣờng cong ellip E trên Æ𝑞.

* 1. Chọn một chuỗi *seedE* bit tùy ý có chiều dài g ≥ 160 bit.
  2. Tính H = SHA-1 (seedE), và cho *c0* biểu thị các chuỗi bit có chiều dài *v*

bit thu đƣợc bằng cách lấy *v* bit ngoài cùng bên phải của H.

* 1. Cho w0 biểu thị các chuỗi bit có chiều dài *v* bit thu đƣợc bằng cách thiết lập bit tận cùng bên trái *c0* đến 0. (Điều này đảm bảo r < p).
  2. Cho Z là số nguyên nhị phân mở rộng đƣợc đƣa ra bởi độ dài g bit seedE.
  3. Cho i từ 1 đến s ta có:
* Cho si thiết lập bởi độ dài chỗi g-bit là phần mở rộng của nhị phân của các số nguyên *(z+i)mod 2g*.
* Tính Wi = SHA-1(si).
  1. Cho W là chuỗi bit thu đƣợc bằng cách nối W0, W1,….Ws nhƣ sau:

W = W0 " W1 " ⋯ " W𝑠.

* 1. Cho r là 1 số nguyên mà nhị phân mở rộng đƣợc cho bởi W.
  2. Nếu r = 0 hoặc 4r + 27 = 0 (mod p) thì quay lại bƣớc 1.
  3. Chọn tuỳ ý các số nguyên a,b Є Æ𝑞 ≠ 0 sao cho𝑟. 𝑏2 Ξ 𝑎3 𝑚𝑜𝑑 𝑝, (ví dụ, chúng ta có thể lấy a = r và b = r).
  4. Đƣờng cong eliptic trên Æ𝑞 đƣợc cho bởi phƣơng trình E: 𝑦2 = 𝑥3 +

𝑎𝑥2 + 𝑏.

* 1. Đầu ra (seedE, a, b).

***Thuật toán 2.2***: Xác minh rằng một đƣờng cong elliptic đƣợc tạo ra ngẫu nhiên trên Æ𝑝

INPUT: Một kích thƣớc trƣờng p (một số nguyên tố), một chuỗi bit seedE của độ dài 𝑔 160 bit, và các trƣờng phần tử 𝑎, 𝑏 ∈ Æ𝑝 với định nghĩa đƣờng cong elliptic E: 𝑦2 = 𝑥3 + 𝑎𝑥 + 𝑏 trên Æ𝑝.

OUTPUT: Chấp nhận hoặc từ chối rằng E đƣợc tạo một cách ngẫu nhiên bằng cách sử dụng thuật toán 2.1.

1. Tính H = SHA-1 (seedE), và cho *c0* biểu thị các chuỗi bit có chiều dài *v*

bit thu đƣợc bằng cách lấy *v* bit ngoài cùng bên phải của H.

1. Cho w0 biểu thị các chuỗi bit có chiều dài *v* bit thu đƣợc bằng cách thiết lập bit tận cùng bên trái *c0* đến 0.
2. Cho z là số nguyên nhị phân mở rộng đƣợc đƣa ra bởi độ dài g bit seedE
3. Cho i từ 1 đến s ta có:

* Để si là chuỗi g-bit là sự mở rộng nhị phân của (Z + i) mod 2g.
* Tính Wi = SHA-1(si).

1. Cho W là chuỗi bit bao gồm 1 chuỗi liên tiếp nhau W 0, W1, ...,Ws nhƣ sau: W′ = W0 " W1 " ⋯ " W𝑠.
2. Cho r' là số nguyên nhị phân mở rộng đƣợc tạo ra bởi W'.
3. Nếu r'.b2 ≡ a3 (mod *p*) thì chấp nhận, nếu không thì từ chối.

## Trường hợp q = 2m

Theo ký hiệu đƣợc sử dụng: 𝑠 = ⌊(𝑚 − 1)/160⌋𝑣à 𝑣 = 𝑚 − 160. 𝑠

***Thuật toán 2.3***: Tạo ra một đƣờng cong elliptic ngẫu nhiên trên Æ2𝑚. INPUT: Kích thƣớc trƣờng q = 2m.

OUTPUT: Một chuỗi bit seedE có độ dài ít nhất 160 bit và các phần tử trƣờng

𝑎, 𝑏 ∈ Æ2𝑚 xác định một đƣờng cong elliptic E trên Æ2𝑚.

* 1. Chọn một chuỗi bit tùy ý seeE có chiều dài g ≥ 160 bit.
  2. Tính H = SHA-1(seedE), và để cho bo biểu thị chuỗi bit dài *v* bit thu đƣợc bằng cách dùng *v* bit ngoài cùng bên phải của H.
  3. Z là số nguyên nhị phân mở rộng đƣợc đƣa ra bởi seedE chuỗi g-bit.
  4. Cho i chạy từ 1 đến s ta có:
* Cho si là chuỗi g-bit mà nó có phần mở rộng nhị phân của số nguyên (z + i) mod 2g.
* Tính bi = SHA-1(si).
  1. Cho b là phần tử trƣờng thu đƣợc bằng cách nối bo, b1, ..., bs nhƣ sau: b = b0 | | b1 | | ... | | bs.
  2. Nếu b = 0 quay lại bƣớc 1.
  3. Cho a là một phần tử tùy ý của Æ2𝑚.
  4. Đƣờng cong elliptic đƣợc lựa chọn trên Æ2𝑚 là E: y 2 + xy = x 3 + ax2 + b.
  5. Output (seedE, a, b).

***Thuật toán 2.4:*** Xác minh rằng một đƣờng cong elliptic đƣợc tạo ngẫu nhiên trên Æ2𝑚.

INPUT: Kích thƣớc trƣờng q = 2m, một chuỗi bit seedE chiều dài g ≥160 bit, và các trƣờng hệ số 𝑎, 𝑏 ∈ Æ2𝑚. Xác định một đƣờng cong eliptic E: y2 + xy = x2 + ax2 + b trên Æ2𝑚.

OUTPUT: Chấp nhận hoặc từ chối rằng E là ngẫu nhiên tạo ra bằng cách sử dụng thuật toán 2.3.

1. Tính H = SHA-1(seedE), và để cho bo biểu thị chuỗi bit của bit v, chiều dài thu đƣợc bằng cách v bit ngoài cùng bên phải của H.
2. Cho z là số nguyên nhị phân mở rộng đƣợc đƣa ra bởi seedE chuỗi g-bit.
3. Cho i từ 1 đến s:

* Để si là chuỗi g-bit có mở rộng nhị phân của số nguyên (z + i) mod 2g.
* Tính bi = SHA - 1(si).

1. Để b' là phần tử trƣờng hiện thực thu đƣợc bằng cách nối b0,b1, ..., bs vào nhau nhƣ sau: b = b0 | | b1 | | ... | | bs.
2. Nếu b = b ' thì chấp nhận, nếu không từ chối.

## Sinh miền tham số

Sau đây là một trong những cách để tạo ra các miền tham số bảo mật:

* + - * 1. Chọn hệ số a và b từ Æ𝑞 có thể nhận một cách ngẫu nhiên bằng cách sử dụng thuật toán 1 hoặc 3. Cho E là đƣờng cong 𝑦2 = 𝑥3 + 𝑎𝑥 + 𝑏 trong trƣờng hợp q = p và 𝑦2 + 𝑥𝑦 = 𝑥3 + 𝑎𝑥2 + 𝑏 trong trƣờng hợp q = 2m.
        2. Tính N = # E(Æ𝑞).
        3. Xác minh rằng N có chia hết cho một nguyên tố lớn n (n > 2160 và N > 4√q). Nếu không, quay lại bƣớc 1.
        4. Xác minh rằng n không chia qk -1 cho mỗi k, 1 ≤ k ≤ 20. Nếu không, quay lại bƣớc 1.
        5. Xác minh rằng n # q. Nếu không, quay lại bƣớc 1.
        6. Chọn một điểm tùy ý 𝐺𝑡 ∈ 𝐸(Æ𝑞) và thiết lập G = (N/n)Gt. Lặp lại cho đến khi G # O.

## Xác định miền tham số

Đảm bảo rằng một bộ *D = (q, FR, a, b, G, n, h)* của miền tham số EC có giá trị có thể đƣợc cung cấp cho một thực thể bằng cách sử dụng một trong các phƣơng pháp sau đây:

* + - * 1. Thực hiện rõ ràng một tham số xác nhận miền bằng cách sử dụng thuật toán 2.5 (hiển thị bên dƣới).
        2. Một D đƣa ra bằng cách sử dụng một hệt thống đáng tin cậy.
        3. Nhận đƣợc một sự đảm bảo từ phần đáng tin cậy phía T (ví dụ nhƣ một thành phần chứng nhận) rằng T đã thực hiện rõ ràng tham số xác nhận miền của D bằng cách sử dụng thuật toán 2.5.
        4. Nhận đƣợc sự đảm bảo từ một phần đáng tin cậy của T là D đƣợc tạo ra bằng cách sử dụng một hệ thống cũ.

***Thuật toán 2.5***: Xác nhận rõ ràng của bộ miền tham số EC

INPUT: Thiết lập một miền tham số D của EC, D = (q, FR, a, b, n, h). OUTPUT: Chấp nhận hoặc từ chối tính hợp lệ của D.

1. Xác nhận rằng q là một nguyên tố hoặc một lũy thừa của 2 (q=2m).
2. Xác nhận rằng FR là đại diện hợp lệ cho Æ𝑞.
3. Xác nhận rằng G # O.
4. Xác nhận rằng a, b, xG và yG đƣợc đại diện thực sự các nguyên tố của Æ𝑞 (ví dụ, số nguyên trong khoảng [0, p-1] trong trƣờng hợp q = p, và chuỗi các bit dài m bits trong trƣờng hợp q=2m.
5. (Tùy chọn) Nếu các đƣờng cong elliptic đƣợc tạo ngẫu nhiên phù hợp

với thuật toán 2.1 hoặc thuật toán 2.3, xác nhận rằng seedE là một chuối dài bit gồm ít nhất 160 bít và sử dụng thuật toán 2.2 hoặc thuật toán 2.4 để xác nhận rằng a và b là phù hợp với seedE.

1. Xác nhận rằng a và b xác định một đƣờng cong elliptic trên Æ𝑞 (VD: 4a2 + 27 # 0 (mod p) if q = p; b # 0 nếu q = 2m).
2. Xác nhận rằng G nằm trên đƣờng cong ellip bởi a và b (VD, yG2 = xG3

+ axG + b trong trƣờng hợp q = p, và yG2 + xGyG = xG3 + axG2 + b trong trƣờng hợp q = 2m).

1. Xác minh rằng n là số nguyên tố.
2. Xác minh rằng n > 2160 và n > 4√q.
3. Xác minh rằng nG = O.
4. Tính h’= [(√q + 1)2/n] và xác minh rằng h = h’.
5. Xác minh n không chia qk - 1 cho mỗi k, 1≤ k ≤ 20.
6. Xác minh n # q.
7. Nếu nhận thấy bất kì sai sót nào, thì D là không phù hợp, nếu không D là phù hợp.

# Cặp khóa ECDSA

Một cặp khóa ECDSA chính liên kết với một tập hợp các tham số miền EC. Khóa công khai là một trong nhiều lựa chọn ngẫu nhiên của điểm cơ sở, trong khi khóa riêng là một số nguyên lựa chọn ngẫu nhiên.

## Sinh cặp khóa

Một cặp khoá của một thực thể A liên quan với một tập hợp các tham số miền EC, *D = (q, FR, a, b, G, n, h)*. Liên kết đã đƣợc đảm bảo trong mật mã (chứng nhận) hoặc bởi nội dung (tất cả các thực thể sử dụng cùng tham số miền). Mỗi một thực thể A phải đảm bảo cho tham số miền một giá trị trƣớc khi sinh khóa.

***Sinh cặp khóa ECDSA***. Mỗi thực thể đƣợc làm nhƣ sau:

* + - * 1. Chọn ngẫu nhiên hoặc giả ngẫu nhiên một số nguyên *d* ∈ *[1, n-1].*
        2. Tính *Q = dG.*
        3. A Có một khóa công khai Q; A có một khóa riêng d.

## Xác nhận khóa công khai

Xác nhận khóa công khai, đã đƣợc đề xuất lần đầu tiên bởi Johnson, đảm bảo rằng một khóa công khai có tính chất số học cần thiết. Thực nghiệm thành công này cho thấy rằng một khóa riêng có liên quan tồn tại một cách hợp lý, mặc dù nó không chứng minh rằng ai đó thực sự có khóa riêng cũng không phải là chủ sở hữu đã tuyên bố thực sự sở hữu khóa riêng.

Lý do để thực hiện xác nhận khóa công khai là quan trọng trong thực tế bao gồm:

1. Phòng ngừa chèn mã độc hại của một khóa công khai không hợp lệ mà có thể cho phép một số cuộc tấn công.
2. Phát hiện mã hóa hoặc lỗi vô ý truyền. Sử dụng một khóa công khai không hợp lệ có thể hủy bỏ tất cả các tài sản bảo đảm dự kiến.

## Phương thức sinh các khóa công khai:

Bảo đảm rằng một khóa công khai *Q* là hợp lệ có thể đƣợc cung cấp cho một thực thể A bằng cách sử dụng một trong các phƣơng pháp sau đây:

1. Một thực hiện khóa công khai A xác nhận rõ ràng bằng cách sử dụng thuật toán 2.6 (trình bày dƣới đây).
2. A tạo ra *Q* nó sử dụng một hệ thống đáng tin cậy.
3. A nhận đƣợc bảo đảm từ một bên đáng tin cậy *T* (một chứng thực chữ ký số) *T* biểu diễn tƣờng minh việc xác nhận khóa công khai của A sử dụng thuật toán 2.6.
4. A nhận đƣợc bảo đảm từ một bên đáng tin cậy *T* cái mà *Q* có thể đƣợc tạo ra khi sử dụng hệ thống.

***Thuật toán 2.6***: Xác nhận tƣờng minh của khóa công khai ECDSA.

INPUT: Một khóa công khai *Q =(xQ, yQ )* liên kết với tham số miền giá trị

*(q, FR, a, b ,G, m, h).*

OUTPUT: Chấp nhận hoặc từ chối giá trị của *Q*.

1. Đầu tiên kiểm tra *Q ≠ O*.
2. Kiểm tra *xQ* và *yQ* là đại diện cho các phần tử của Æ𝑞 (các số nguyên trong khoảng *[0, p-1]* trong mỗi lựa chọn *q = p* và sâu bit có độ dài *m* bit trong mỗi lựa chọn *q = 2m*).
3. Kiểm tra *Q* có nằm trên đƣờng cong elliptic tại điểm *a* và *b*.
4. Kiểm tra *nQ = O*.
5. Nếu một kiểm tra lỗi, thì *Q* là không hợp lệ, nếu không *Q* có giá trị.

# Sinh và xác nhận chữ ký ECDSA

## Sinh chữ ký ECDSA

Để ký hiệu một thông điệp *m*, một thực thể *A* với vùng tham số *D = (q, FR, a, b, G, n, h)* và cặp khóa liên kết *(d, Q)* ta tính nhƣ sau:

* + - * 1. Chọn ngẫu nhiên hoặc giả ngẫu nhiên số nguyên *k,* 1 ≤ 𝑘 ≤ 𝑛 − 1.
        2. Tính *kG = (x1,y1)* và chuyển đổi *x1* từ số nguyên thành 𝑥̅̅1̅.
        3. Tính *r = x1 mod n*. Nếu *r = 0* thì quay lại bƣớc 1.
        4. Tính *k-1 mod n.*
        5. Tính SHA-1*(m)* và chuyển đổi chuỗi bit sang số nguyên *e*.
        6. Tính *s = k-1(e + dr) mod n.* Nếu *s = 0* thì quay lại bƣớc 1.
        7. Chữ ký của thông điệp *m* là *(r,s)*.

## Xác nhận chữ ký ECDSA

Để xác minh một chữ ký của *A (r,s)* trên *m*. B có đƣợc một bản sao xác thực của A trong vùng tham số *D = (q, FR, a, b, G, n, h)* và liên kết khóa công khai Q. Đó là khuyến cáo rằng B cũng có xác nhận các giá trị D và Q. B đƣợc thực hiện nhƣ sau:

* + - * 1. Xác minh rằng r và s là các số nguyên trong khoảng [1, n-1].
        2. Tính SHA-1*(m)* và chuyển đổi chuỗi bit sang số nguyên *e*.
        3. Tính *w =s -1 mod n*.
        4. Tính *u1 = ew mod n* và *u2 = rw mod n.*
        5. Tính *X = u1G + u2Q.*
        6. Nếu *X =* 𝐺, thì từ chối chữ ký. Ngƣợc lại, chuyển đổi x – ngang bằng

x1 của X từ số nguyên

𝑥̅̅1̅, và tính *v* = 𝑥1 𝑚𝑜𝑑 𝑛.

* + - * 1. Thừa nhận chữ ký nếu và chỉ nếu *v = r*.

## Bằng chứng xác thực làm việc chữ ký số

Nếu mốt chữ ký *a (r, s)* trên thông điệp *m* đƣợc tạo ra bởi A, thì

*s = k-1(e + dr) mod n*, đƣợc sắp xếp cho:

𝑘 Ξ 𝑠−1(𝑒 + 𝑑𝑟) Ξ 𝑠−1𝑒 + 𝑠−1𝑟𝑑 Ξ 𝑤𝑒 + 𝑤𝑟𝑑 Ξ 𝑢1 + 𝑢2𝑑 (𝑚𝑜𝑑 𝑛)

Nhƣ vậy, *u1G + u2Q = (u1 + u2d)G = kG* và nhƣ vậy *v = r* là cần thiết.

## Chuyển đổi giữa các loại dữ liệu

ANSI X9.62 xác định một phƣơng pháp để chuyển đổi trƣờng các phần tử phải là các số nguyên. Nó sử dụng để chuyển đổi trƣờng phần tử *x1* từ số nguyên trong bƣớc 2 của phần tạo chữ ký và bƣớc 6 của phần xác nhận chữ ký trƣớc khi tính toán *x1 mod n*.

ANSI X9.62 xác định phƣơng thức chuyển đổi chuỗi bit sang các số nguyên. Nó sử dụng chuyển đổi đầu ra *e* của SHA-1 sang số nguyên trƣớc khi sử dụng trong tính toán modulo trong bƣớc 5 của phần tạo chữ ký và bƣớc 2 của phần xác nhận chữ ký.

## Chứng nhận khóa công khai

Trƣớc khi xác minh chữ ký A trên thông điệp, B cần có đƣợc một bản sao của A trên vùng tham số D và liên quan đến khóa công khai Q. ANSI X9.62 không chỉ thị một cơ chế để đạt đƣợc điều này. Trong thực tế, xác thực khóa công khai thƣờng đƣợc phân phối thông qua giấy chứng nhận. Chứng nhận khóa công khai bao gồm một chuỗi các thông tin xác định duy nhất A, miền tham số D, khóa công khai Q và một cơ quan xác nhận chữ ký (CA) trên các thông tin. B có thể sử dụng bản sao xác thực khóa công khai của CA để xác minh A đã đƣợc xác nhận, do đó có đƣợc một bản sao xác thực khóa công khai tĩnh của A.

## Cơ sở cho kiểm tra r và s trong xác minh chữ ký

Bƣớc 1 của việc kiểm tra xác nhận chữ ký là *r* và *s* phải là các số nguyên trong khoảng *[1, n-1]*. Sau đây là sự hợp lý tấn công trên ECDSA nếu kiểm tra *r ≠ 0* (và nói chung, 𝑟 0 (𝑚𝑜𝑑 𝑛) là không thể thực hiện). Giả sử A sử dụng đƣờng cong elliptic 𝑦2 = 𝑥3 + 𝑎𝑥2 + 𝑏 bậc (Æ𝑞), ở đây b là dƣ

bậc hai của modulo *p* và giả sử A sử dụng điểm cơ sở 𝐺 = (0, √𝑏) của số nguyên tố bậc *n*. (Đó là hợp lý mà tất cả các thực thể có thể lựa chọn một điểm cơ sở 0 tọa độ x để giảm thiểu bậc của kích thƣớc của các thông số miền). Một nhƣợc điểm bây giờ có thể giả mạo một chữ ký A trên thông điệp m của lựa chọn tính toán A = SHA-1(m). Nó có thể dễ dàng kiểm tra tất cả (r = 0, s = e) là chữ ký hợp lệ từ m.

# Tính bảo mật chữ ký số ECDSA

# Mật mã đƣờng cong Elliptic

Sau lần đầu mật mã đƣờng cong elliptic (ECC – Elliptic Curve Cryptograpthy) đƣợc giới thiệu năm 1991 bởi các công trình nghiên cứu độc lập của Neals Koblitz và Victor Miller, đƣờng cong Elliptic đã đóng vai trò quan trọng đối với lý thuyết số và mật mã trong vài thập ky gần đây. Độ an toàn của ECC dựa vào bài toán logarit rời rạc trên nhóm các điểm của đƣờng cong Elliptic (ECDLP). Đối với bài toán logarit rời rạc trên trƣờng hữu hạn hoặc bài toán phân tích số, tồn tại các thuật toán dƣới dạng dạng hàm mũ để giải các bài toán này (tính chỉ số hoặc sàng trƣờng số). Tuy nhiên, đối với bài toán ECDLP cho đến nay vẫn chƣa tìm đƣợc thuật toán dƣới hàm mũ để giải. Nhà toán học nổi tiếng J. Silverman cũng nhƣ nhiều nhà thám mã khác đã nghiên cứu các thuật toán tƣơng tự, nhƣ thuật toán tính chỉ số để áp dụng cho ECDLP nhƣng đều không thành công. Điều này đã tạo ra những ƣu việt của hệ mật ECC so với các hệ mật khóa công khai khác.

Mật mã ECC cung cấp tính an toàn tƣơng đƣơng với các hệ mật khóa công khai truyền thống, trong khi độ dài khóa nhỏ hơn nhiều lần. ECC là khả năng bảo mật cao với kích thƣớc khóa nhỏ dựa vào mức độ khó giải quyết của vấn đề ECDLP. Đây chính là một tính chất rất hữu ích đối với xu hƣớng ngày nay là tìm ra phƣơng pháp tăng độ bảo mật của mã hóa khóa công cộng với kích thƣớc khóa đƣợc rút gọn. Kích thƣớc khóa nhỏ hơn giúp thu gọn đƣợc kích thƣớc của chứng nhận giao dịch trên mạng và giảm kích thƣớc tham số củahệ thống mã hóa. Kích thƣớc khóa nhỏ giúp các hệ thống bảo mật dựa trên ECC giảm thời gian tạo khóa. Thời gian tạo khóa thƣờng rất lớn ở các hệ thống RSA. Ngoài ra, việc mã hóa và giải mã trong ECC cũng đƣợc thực hiện nhanh hơn. Ngƣời ta đã ƣớc lƣợng rằng cỡ khóa 3248 bit của hệ mật RSA cho cùng một độ an toàn nhƣ 256 bit của hệ mật ECC. Điều đó có nghĩa là việc cài đặt ECC sử dụng tài nguyên hệ thống ít hơn, năng lƣợng tiêu thụ nhỏ hơn... Với ƣu thế về độ dài khóa nhỏ, ECC đang đƣợc ứng dụng rộng rãi trong nhiều lĩnh vực.

# Vấn đề của chữ ký số trên đƣờng cong Elliptic

Độ an toàn của sơ đồ chữ ký ECDSA tƣơng ứng với độ phức tạp của bài toán logarit rời rạc trên đƣờng cong elliptic: cho trƣớc hai điểm Q và G nằm trên đƣờng cong elliptic E, tìm số tự nhiên d sao cho Q = dG.

Cho đến nay sơ đồ chữ ký ECDSA đã đƣợc chỉ ra là khá an toàn và hiệu quả. Đối với bài toán logarit rời rạc đƣờng cong elliptic thì có nhiều thuật toán giải nó. Ngƣời ta đã phân tích và chỉ ra rằng với cùng độ an toàn, hệ mã hoá dựa trên bài toán logarit rời rạc đƣờng cong elliptic có độ dài khoá ngắn hơn rất nhiều so với hệ mã hoá dựa trên bài toán phân tích số nguyên thành các thừa số nguyên tố (nhƣ RSA). Ví dụ với hệ mã hoá RSA có chiều dài khoá là 3248 bit thì hệ mật đƣờng cong elliptic chỉ cần độ dài khoá 256 bit sẽ có độ an toàn tƣơng đƣơng.

Thuật toán giải bài toán logarit rời rạc đƣờng cong elliptic tốt nhất tính đến trƣớc năm 2006 là thuật toán Pollard’s Rho, phiên bản thiết kế theo hƣớng tính toán song song. Đến năm 2006, Jung Hee Cheon đã đƣa ra một tấn công hiệu quả hơn hẳn thuật toán Pollard sử dụng giả thuyết Diffie-Hellman mạnh. Tấn công này áp dụng đối với các lƣợc đồ mật mã mà tạo ra một bộ tiên đoán có thể trả về lũy thừa khóa bí mật của nó với một đầu vào bất kỳ (ví dụ nhƣ lƣợc đồ chữ ký số mù sử dụng trong an toàn giao dịch điện tử). Đến năm 2009, tấn công này mới đƣợc xem xét đƣa vào chuẩn ISO và FIPS. Các chuẩn khác nhƣ ANSI hoặc SECG không đƣợc cập nhật về tấn công. Ngay cả trong chuẩn ISO và FIPS, các điều kiện đƣa ra đối với tiêu chuẩn chống tấn công này cũng có những điểm khác nhau cơ bản. Năm 2012, sử dụng giả thuyết Diffi-Hellman, Masaya Yasuda và các cộng sự đã đƣa ra một bằng chứng phá vỡ mật mã elliptic dựa trên cặp (pairing-based cryptography) với độ dài khóa là 160 bit (độ dài khóa 131 bit hiện vẫn chƣa giải đƣợc theo các công bố công khai, 160 bit là độ an toàn mà hầu hết các chuẩn trên thế giới đƣa ra.

Do đó, để ứng dụng và triển khai chữ ký số trên đƣờng cong Elliptic, chúng ta phải thƣờng xuyên cập nhật những nghiên cứu phân tích và đánh giá mới nhất về các tiêu chuẩn an toàn, các tấn công đối với hệ mật để có đủ cơ sở lý thuyết, cơ sở toán học vững chắc, đƣa ra các tiêu chuẩn an toàn riêng cho các tham số.

# Kết luận chƣơng

ECDSA chỉ đơn giản là thu đƣợc từ DSA bằng cách thay thế trong phân nhóm theo thứ tự (bậc) *q* của Æ\* sinh ra bới *q* với phân nhóm của các điểm trên đƣờng cong elliptic đƣợc sinh ra bởi G. Sự khác biệt đáng kể duy nhất giữa ECDSA và DSA là đƣợc sinh ra trong *r*. DSA thực hiện điều này bằng cách tham gia phần tử ngẫu nhiên X = 𝑔𝑦𝑚𝑜𝑑 𝑝 và việc giảm modulo *q*, nó đạt đƣợc số nguyên trong khoảng *[1, q-1].* ECDSA tạo ra r trong

𝑝

khoảng *[1, n-1]* thực hiện điều này trên tọa độ x của lựa chọn ngẫy nhiêu điểm *kG* và việc giảm *modulo n*.

Các hệ mã hoá đƣờng cong elliptic đầu tiên đƣợc phát minh năm 1985 bởi Neal Kobliz và Victor Miller. Tuy nhiên sơ đồ chữ ký ECDSA do Scott Vanstone đƣa ra năm 1992, đƣợc chấp nhận là chuẩn ISO vào năm 1998, là chuẩn ANSI vào năm 1999, và là chuẩn IEEE vào năm 2000.

Độ an toàn của sơ đồ ký ECDSA dựa trên bài toán logarit rời rạc đƣờng cong elliptic. Cho đến nay độ an toàn của các hệ mã hoá đƣờng cong elliptic đã đƣợc chỉ ra là rất an toàn và hiệu quả. Đối với bài toán logarit rời rạc đƣờng cong elliptic thì có nhiều thuật toán giải nó. Tuy nhiên chƣa có thuật toán nào có độ phức tạp tính toán trong thời gian đa thức.

Thuật toán giải bài toán logarit rời rạc đƣờng cong elliptic tốt nhất hiện nay là thuật toán Pollard’s Rho, phiên bản thiết kế theo hƣớng tính toán song song. Theo đó với nhóm đƣờng cong elliptic cấp n và có r máy tính cùng tính toán thì phải mất √ . 𝑛 /2.r phép toán.

Mặt khác ngƣời ta đã phân tích và chỉ ra rằng với hệ mã hoá dựa trên

bài toán logarit rời rạc đƣờng cong elliptic có cùng độ bảo mật với hệ mã hoá dựa trên bài toán phân tích số nguyên thành các thừa số nguyên tố (nhƣ RSA) thì độ dài khoá của hệ mã hoá dựa trên đƣờng cong elliptic có chiều dài khoá ngắn hơn rất nhiều. Chẳng hạn với hệ mã hoá RSA có chiều dài khoá là 1024 bit thì hệ mã hoá bằng đƣờng cong elliptic chỉ cần độ dài khoá 163 bit sẽ có độ bảo mật tƣơng đƣơng. Và do đó việc tính toán các tiến trình đối với các hệ mã hoá đƣờng cong elliptic là nhanh hơn rất nhiều.

# CHƢƠNG III. ỨNG DỤNG CHỮ KÝ SỐ TRONG BẢO MẬT TÀI LIỆU ĐIỆN TỬ

# Ý tƣởng về chƣơng trình ứng dụng

# Lĩnh vực ứng dụng của chƣơng trình

Chƣơng trình ứng dụng trong các hoạt động trao đổi tài liệu, văn bản thông qua hình thức điện tử, đảm bảo tính an toàn và toàn vẹn dữ liệu khi trao đổi thông tin bằng các tài liệu điện tử.

Chƣơng trình đáp ứng nhu cầu đảm bảo tính kịp thời, toàn vẹn dữ liệu trong hoạt động giao dịch điện tử trƣớc sự phát triển mạnh mẽ của Internet cùng sự gia tăng không ngừng của các giao dịch điện tử.

# Ý tƣởng xây dựng chƣơng trình

Xây dựng một giao diện ngƣời dùng để ngƣời dùng có thể sử dụng chữ ký số một cách thuận tiện.

Ngƣời gửi có thể dùng phần mềm để chọn văn bản cần ký, bấm vào nút ký để ký (sử dụng khóa bí mật do chƣơng trình sinh ra). Sau đó gửi văn bản đã ký với khóa công khai đi.

Ngƣời nhận khi nhận đƣợc văn bản có thể dùng phần mềm để kiểm tra chữ ký có đúng có đúng của ngƣời gửi không, văn bản có toàn vẹn hay không.

# Xây dựng chƣơng trình

# Chữ ký số ECDSA

Để thiết lập sơ đồ chữ ký ECDSA (Elliptic Curve Digital Signature Algorithm) cần xác định các tham số:

* + - * Lựa chọn một đƣờng cong Elliptic trên trƣờng số Fq với O là điểm ở vô cùng.
      * Điểm cơ sở G thuộc E(Fq)và n là bậc của G (nG = O).

## Tạo khóa

* + - * Chọn số ngẫu nhiên d ∈ [2, n – 1] làm khóa bí mật
      * Tính Q(xq, yq) = dG làm khóa công khai

## Thuật toán ký

* + - * Chọn số ngẫu nhiên k, 2 ≤ k ≤ n – 1
      * Tính kG = (x1, y1)
      * Tính r = x1 mod n, nếu r = 0 quay lại bƣớc 1
      * Tính k – 1 mod n
      * Tính s = k – 1 (m + dr) mod n. Nếu s = 0 quay lại bƣớc 1
      * Chữ ký trên thông điệp m là (r, s)

## Thuật toán kiểm tra

* + - * Kiểm tra r và s có là các số tự nhiên ∈[2, n – 1] không
      * Tính w = s – 1 mod n
      * Tính u1 = mw mod n và u2 = rw mod n
      * Tính X = u1G + u2Q = (xX, yX)
      * Nếu X = 0 thì phủ nhận chữ ký. Ngƣợc lại tính v = xX mod n
      * Chữ ký đƣợc chấp nhận nếu v = r

*\* Quá trình kiểm tra chữ ký được thực hiện như trên bởi*

Nếu chữ ký (r, s) trên m là đúng thì s = [k-1 (m + dr)] mod n k ≡ s-1 (m + dr) ≡ s-1m + s-1dr ≡ wm + wdr ≡ u1 + u2d (mod n) Vì vậy, u1G + u2Q = (u1 + u2d)G = kG và vì vậy v = r

# Thông số và thuật toán

Chƣơng trình sử dụng EC đã đƣợc kiểm chứng độ bảo mật an toàn trong quá trình sử dụng. Đó là EC 𝑃1 2: 𝑃1 2−𝑃64 − 1 có các thông số nhƣ sau:

P = 6277101735386680763835789423207666416083908700390324961279

a = -3

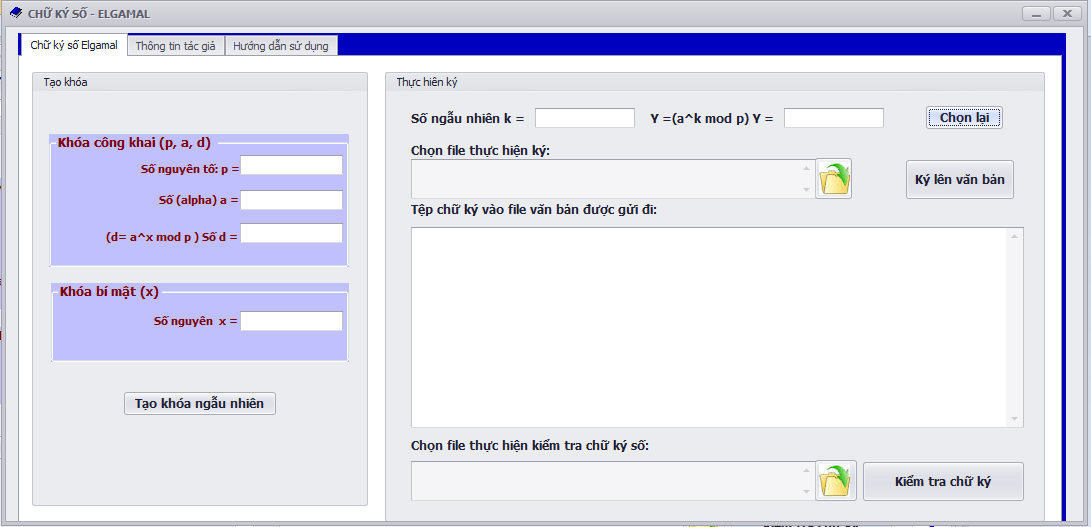
b = *0x*64210519E59C80E70FA7E9AB72243049FEB8DEECC146B9B1 Gx = *0x* 188DA80EB03090F67CBF20EB43A18800F4FF0AFD82FF1012 Gy = *0x* 07192B95FFC8DA78631011ED6B24CDD573F977A11E794811

N = 6277101735386680763835789423176059013767194773182842284081

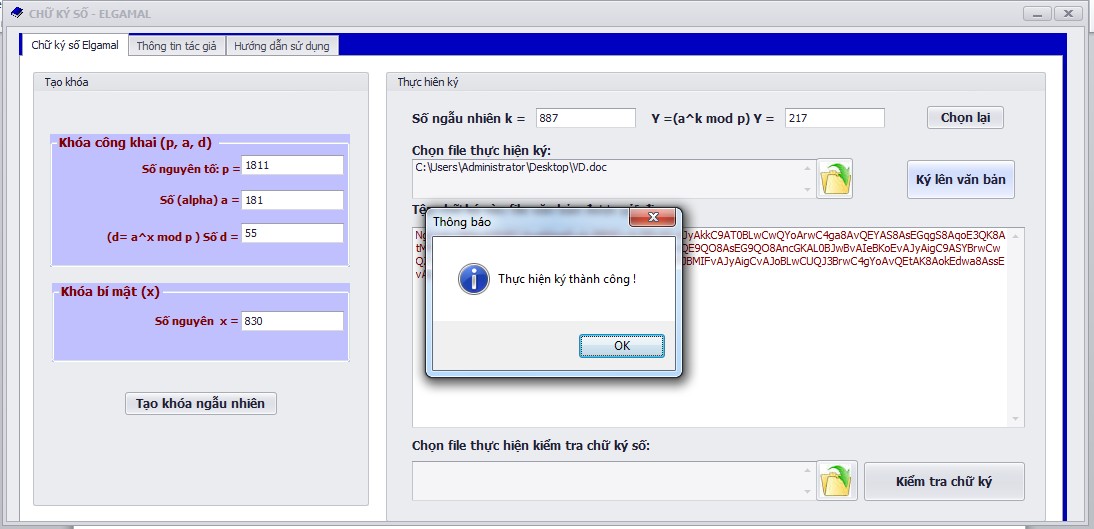
Các thuật toán sinh cặp khóa, sinh và xác nhận chữ ký đã trình bày ở chƣơng II.

Thuật toán hàm băm SHA-1 tạo một tóm tắt cho văn bản gửi đi. Ngƣời nhận cũng sẽ dùng hàm băm để kiểm tra xem văn bản gửi đi có toàn vẹn không.

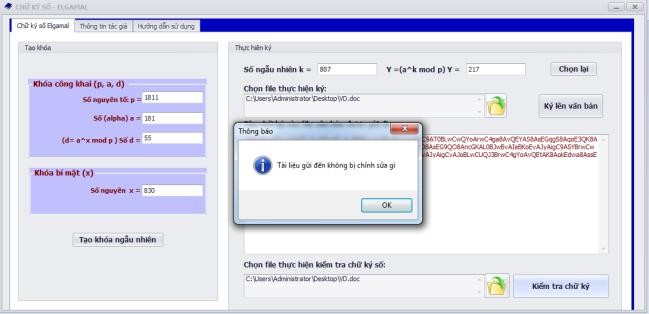
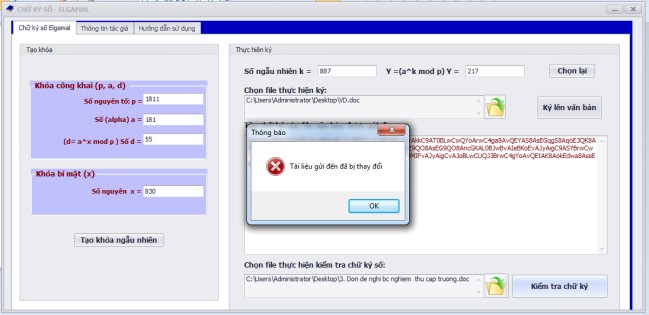
# Giao diện chƣơng trình



*Hình 3.1. Tạo khóa ngẫu nhiên*



*Hình 3.2. Thực hiện ký lên tài liệu/văn bản*

*Hình 3.3. Kiểm tra sự toàn vẹn của tài liệu/văn bản*

# Kết luận chƣơng

Chƣơng III đã đề cập đến việc xây dựng và cài đặt ứng dụng chữ ký số trong mã hóa, bảo mật thông tin; Mã hóa và giải mã một tệp tin, dùng chữ ký số để ký vào văn bản. Sau khi ký vào văn bản và gửi đến cho ngƣời nhận nào đó, ngƣời nhận dùng chức năng xác thực để kiểm tra chính xác chữ ký đó có phải xuất phát từ ngƣời gửi đã biết trƣớc không, dữ liệu đƣợc nhận đƣợc có đảm báo tính toàn vẹn không.

# Kết luận và hƣớng phát triển

Cho đến nay hệ mã hóa đƣờng cong elliptic đƣợc xem là hệ mã hoá an toàn và hiệu quả nhất. So với các hệ mã hoá công khai khác, ECDSA đƣợc xem là ƣu việt hơn bởi ở cùng độ bảo mật nhƣ nhau thì độ dài khoá trong ECDSA nhỏ hơn nhiều so với các hệ mã hoá khác. Điều này dẫn tới các hệ mã hoá ECDSA có khả năng thực thi nhanh hơn, hiệu quả hơn các hệ mã hóa công khai khác.

# Kết quả đạt đƣợc của luận văn

* Luận văn trình bày về an toàn thông tin và các giải pháp về bảo mật an toàn thông tin. Hai hệ mật mã phổ biến là hệ mã hóa khóa bí mật và hệ mã hóa khóa công khai.
* Giới thiệu thuật toán đƣờng cong Elliptic ECDSA và phân tích tính bảo mật của ECDSA.
* Xy dựng chƣơng trình ứng dụng mang tính chất minh họa việc bảo mật thông tin, ký số và xác thực chữ ký số.

# Hƣớng phát triển

Đối với lĩnh vực nghiên cứu của luận văn có thể mở rộng, phát triển theo hƣớng xây dựng mô hình kiểm soát tính toàn vẹn thông tin và các lƣợc đồ mã hóa khóa công khai, đảm bảo độ an toàn cao và tiên tiến hơn.

Hƣớng phát triển của đề tài là xây dựng chƣơng trình để có thể kết nối trực tiếp vào một số phần mềm gửi nhận email và phần mềm quản lý văn bản. Đồng thời xây dựng một hệ thống chứng thực khóa công khai cho các thành viên, nhằm tránh trƣờng hợp bị ngƣời khác giả mạo khóa công khai của ngƣời nhận khi thực hiện trao đổi thông tin.

Tuy còn những hạn chế nhất định, nhƣng trong quá trình nghiên cứu, hoàn thành luận văn đã giúp tôi trang bị thêm nhiều kiến thức cơ bản về bảo mật thông tin. Từ đó có thể xây dựng các ứng dụng bảo mật hoàn chỉnh hơn, phục vụ cho việc tham mƣu ứng dụng công nghệ thông tin vào công tác quản lý tại đơn vị mình đang công tác.

# TÀI LIỆU THAM KHẢO

**Tài liệu tiếng Việt**

[1]. Phan Đình Diệu (2006), *Lý thuyết mật mã và an toàn thông tin*, NXB Đại học Quốc gia Hà Nội.

[2]. Nguyễn Khanh Văn (2012), *An toàn & Bảo mật thông tin*, Đại học Bách khoa Hà Nội.

[3]. Dƣơng Anh Đức, Trần Minh Triết (2005), *Mã hóa và ứng dụng*, NXB Đại học Quốc gia TP Hồ Chí Minh.

[4]. Thái Thanh Tùng (2015), *Giáo trình Mật mã học & An toàn thông tin*, NXB Thông tin và Truyền thông.

[5]. Phạm Huy Điển, Hà Huy Khoái (2004), *Mã hóa thông tin cơ sở toán học và ứng dụng*, NXB Đại học Quốc gia Hà Nội.

# Tài liệu tiếng Anh

[6]. A. MENEZES, P. VAN OORSCHOT, AND S. VANSTONE, 1996

“Handbook of Applied Cryptography”, CRC Press, See.

[7]. J. BUCHMANN, December 2001, *The Digital Signature Algorithm*. [8]. D. Johnson, A. Menezes And S. Vanstone, *1554 (2005), The Eliptic*

*Curve Digital Signature Algorithm, Lecture Notes in Computer Science, Springer-Verlag.*

[9]. W. Stallings, 2011, *Cryptography And Network Security 5th Edition*, Prentice Hall Pearson Education, Inc.

# Địa chỉ trên internet

[10]. https://vi.wikipedia.org/

[11]. https://vi.wikipedia.org/wiki/M%E1%BA%ADt\_m%C3%A3\_h%C 3%B3a\_kh%C3%B3a\_c%C3%B4ng\_khai

[12]. <http://www.cit.ctu.edu.vn/~pnkhang/cours/atbmtt/chuong%204->

%20ham%20bam.pdf

[13]. https://vi.wikipedia.org/wiki/Gi%E1%BA%A3i\_thu%E1%BA%A Dt\_k%C3%BD\_s%E1%BB%91

[14]. [http://vi.wikipedia.org/wiki/Ch%E1%BB%AF\_k%C3%BD\_s%E1%B](http://vi.wikipedia.org/wiki/Ch%E1%BB%AF_k%C3%BD_s%E1%25B) B%91

[15]. <http://vi.wikipedia.org/wiki/RSA_(m%C3%A3_h%C3%B3a)>