**TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI**

**VIỆN CÔNG NGHỆ THÔNG TIN&TRUYỀN THÔNG**

**🙢🙡 🕮 🙣🙠**



**BÀI TẬP LỚN**

**Môn học: Project II**

**Đề tài : Tìm hiểu và cài đặt hệ chữ ký số trên đường cong Elliptic**

Giáo viên hướng dẫn : T.S Trần Vĩnh Đức

Sinh viên thực hiện : Hà Nam Tiến - 20122545

Description: new2

HÀ NỘI 12-2015

Mục Lục

[Lời nói đầu 3](#_Toc437362647)

[Chương 1: Giới thiệu đường cong elliptic 5](#_Toc437362648)

[1 Công thức Weierstrass và đường cong Elliptic 5](#_Toc437362649)

[2 Đường cong Elliptic trên trường R2 5](#_Toc437362650)

[3 Đường cong Elliptic trên trường hữu hạn 7](#_Toc437362651)

[4 Bài toán logarith rời rạc trên đường cong Elliptic 8](#_Toc437362652)

[Chương 2: Chữ ký số trên đường cong Elliptic 9](#_Toc437362653)

[1 Sơ đồ chữ ký ECDSA 9](#_Toc437362654)

[2 Sơ đồ chữ ký Nyberg – Rueppel 10](#_Toc437362655)

[3 Sơ đồ chữ ký mù Harn trên EC 10](#_Toc437362656)

[4 Sơ đồ đa chữ ký mù Harn trên EC 11](#_Toc437362657)

[Chương 3: Cài đặt hệ chữ ký ECDSA trên đường cong Elliptic 13](#_Toc437362658)

[1 Tham số của đường cong 13](#_Toc437362659)

[2 Phép cộng điểm 13](#_Toc437362660)

[3 Phép nhân đôi điểm 14](#_Toc437362661)

[4 Phép nhân một số nguyên với một điểm 15](#_Toc437362662)

[5 Tạo cặp khóa 16](#_Toc437362663)

[6 Ký lên bản tin 16](#_Toc437362664)

[7 Xác minh chữ ký 17](#_Toc437362665)

[Kết luận 18](#_Toc437362666)

[Tài liệu tham khảo 19](#_Toc437362667)

# Lời nói đầu

Sự phát triển của công nghệ thông tin, truyền thông nói chung và Internet nói riêng đã giúp cho việc trao đổi thông tin nhanh chóng, dễ dàng. Do vậy một số vấn đề phát sinh là thông tin có thể bị trộm cắp, có thể sai lệch, có thể giả mạo. Điều đó có thể ảnh hưởng đến các tốc chức, các công ty hay cả một quốc gia. Để giải quyết tình hình trên an toàn thông tin được đặt ra cấp thiết. Kỹ thuật mật mã là một trong những giải pháp của an toàn truyền thông. Các nhà khoa học đã phát minh ra những hệ mật ma nhằm che dấu thong tin cũng như là làm rõ chúng để tránh kẻ cố tình phá hoạt các hệ mật: RSA, Elgamal …

Mục tiêu cơ bản của mật mã học là đảm bảo tính mật. Nó cho phép hai đối tác trao đổi thông tin với nhau một cách an toàn trên những kênh truyền thông công khai. Có hai hệ mật mã được sử dụng: hệ mật mã khóa bí mật và hệ mật mã khóa công khai. Trong nội dung đồ án ta chỉ xem xét về hệ mật mã khóa công khai sử dụng trong chữ ký điện tử.

Ý tưởng của các thuật toán mã hóa công khai là sử dụng hai khóa khác nhau cho 2 quá trình mã hóa và giải mã. Ý tưởng này được phát minh bởi Whitfield Diffie và Martin Hellman (1976), độc lập với Ralph Merkle (1978). Từ đó nhiều hệ mật mã khóa công khai được đưa ra, nhưng hầu hết chúng đều không an toàn hoặc không khả thi. Các thuật toán khóa công khai thường chậm hơn rất nhiều so với các thuật toán khóa bí mật.

Thuật toán RSA chậm hơn 1000 lần so với các thuật toán khóa bí mật phổ biến như DES khi triển khai trên các thiết bị phần cứng, và chậm hơn 100 lần trong các phần mềm mã hóa khi mã hóa cùng một khối lượng dữ liệu như nhau. Tuy nhiên hệ mã hóa khóa công khai có một ưu điểm nổi trội là tạo chữ ký điện tử. Khóa riêng được người chủ sở hữu giữ bí mật và sử dụng để tạo ra chữ ký điện tử hoặc giải mã các thông điệp được mã hóa bằng khóa công khai. Khóa công khai không cần thiết phải giữ bí mật do tính chất “khó tính được khóa riêng từ khóa công khai” của cặp khóa. Vì vậy người dùng có thể công bố khóa công khai trên các kênh công cộng cho bất cứ ai muốn gửi thông tin cho họ hoặc muốn xác minh chữ ký của họ.

Trong lịch sử hơn 20 năm của mật mã khóa công khai, đã có nhiều bài toán khó được đưa ra xem xét ứng dụng cho các vấn đề mật mã học. Trong đó có 2 bài toán nổi bật nhất là bài toán logarith rời rạc trên trường hữu hạn và bài toán tìm ước số nguyên tố. Năm 1985, Neal Koblitz và V.S.Miller đã độc lập cùng nhau đề xuất việc sử dụng đường cong elliptic cho các hệ mã khóa công khai. Họ không phát minh ra thuật toán mã hóa mới với các đường cong elliptic trên trường hữu hạn, mà họ dùng các thuật toán đã có như Diffie – Hellman, sử dụng các đường cong elliptic. Các đường cong Elliptic có thể được sử dụng trong nhiều ứng dụng như kiểm thử số nguyên tố hoặc bài toán tìm ước số nguyên tố. Các hệ mật mã trên đường cong elliptic được dự báo là sẽ phổ biến hơn RSA do khóa nhỏ gọn hơn nhiều so với RSA. Vì vậy tốc độ mã hóa nhanh hơn so với RSA. Như vậy ECC có thể được dùng trên các thiết bị cầm tay (có bộ nhớ nhỏ và tốc độ tính toán không cao).

# Chương 1: Giới thiệu đường cong elliptic

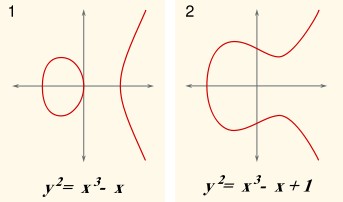
## Công thức Weierstrass và đường cong Elliptic

Gọi K là trường hữu hạn hoặc vô hạn. Một đường cong Elliptic được định nghĩa trên trường K theo công thức Weierstrass :

y2 + a1xy + a3y = x3 + a2x2 + a4x + a6

với a1, a2, a3, a4, a6 ∈ K.

Đường cong Elliptic trên trường K được ký hiệu là E(K). Số lượng các điểm nguyên trên E ký hiệu là #E. Đối với từng trường khác nhau công thức Weierstrss có thể biến đổi và đơn giản hóa thành các dạng khác nhau. Một đường cong Elliptic là tập hợp các điểm thỏa mãn công thức trên.



## Đường cong Elliptic trên trường R2

Đường cong elliptic E trên trường R2 là tập hợp các điểm (x,y) thỏa mãn công thức:

y2 = x3 + a4x + a6

cùng với một điểm đặc biệt O được gọi là điểm tại vô cực (phần tử identify). Cặp giá trị (x,y) đại diện cho một điểm trên đường cong elliptic và tạo nên mặt phẳng tọa độ 2 chiều R x R. Ký hiệu đường cong Elliptic trên trường R2 là E(R).

1. **Phép cộng**

Phép cộng trên đường cong E(R) chính là phép cộng điểm giữa 2 điểm nằm trên đường cong. Điểm O được gọi với điểm cơ sở. Với mọi điểm P(x,y) thuộc đường cong E(R) ta có:

P + O = O + P = P

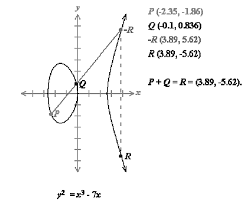
và

P + -P = O

với –P (x,-y) cũng thuộc E(R) .

Phép cộng trên E(R) được định nghĩa theo phương diện hình học. Giả sử có 2 điểm phân biệt P,Q thuộc E(R). Phép cộng điểm trên đường cong elliptic là :

R = P + Q, R ∈ E(R)



Để tìm ra điểm R ta nối P và Q bằng đường thẳng L. Đường thẳng này sẽ cắt E(R) tại điểm thứ ba –R(x,-y). Điểm R(x,y) sẽ là tổng của 2 điểm P và Q trên đường cong E(R).

Thể hiện dưới dạng đại số ta có :

P(x1,y1), Q(x2,y2), R = P + Q (x3,y3)

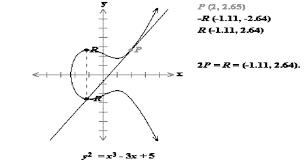
x3  = Ɵ2 - x1 - x2

y3  = Ɵ(x1 + x3) – y1

Ɵ = (y2 – y1)/(x2 – x1) nếu P ≠ Q

Hoặc Ɵ = (3x12 + a4)/(2y1) nếu P = Q

1. **Phép nhân đôi**



Phép nhân đôi chính là phép cộng 2 điểm P và Q với P = Q. Khi này đường thẳng L sẽ là tiếp tuyến của đường cong E(R) tại P.

1. **Phép nhân**

Phép nhân một số nguyên k với điểm P chính là việc thực hiện k lần cộng điểm P:

k\*P = P + P + … + P + P (k phần tử P)

## Đường cong Elliptic trên trường hữu hạn

Đường cong elliptic được xây dựng trên các trường hữu hạn. Có 2 trường hữu hạn thường được sử dụng : Trường hữu hạn Fq với q là số nguyên tố hoặc q là 2m với m là số nguyên.

Tùy thuộc vào trường hữu hạn Fq, với mỗi bậc của q tồn tại nhiều đường cong elliptic. Do đó, với một trường hữu hạn q phần tử và q lớn, có nhiều sự lựa chọn đường cong elliptic.Chúng ta ở đây chỉ xét trường hợp q là số nguyên tố

Cho q là một số nguyên tố (q>3), cho A,B thuộc Fq sao cho 4A3 + 27B2 ≠ 0. Giả sử E(Fq) là đường cong elliptic được định nghĩa trên Fq. E(Fq) có dạng như sau:

y2 = x3 + Ax + B

E(Fq) gồm các điểm (x,y) với x,y thuộc Fq và một điểm O – gọi là điểm tại vô cực.

Số lượng điểm của E(Fq) (#E(Fq)) thỏa mãn định lý Hasse:

q + 1 – 2 # E(Fq) q + 1 + 2

Các phép toán của đường cong elliptic trên Fq cũng tương tự với E(R). Tập hợp các điểm trên E(Fq) tạo thành một nhóm thỏa mãn các tính chất sau:

* Tính đóng P,Q E(Fq) thì P + Q E(Fq)
* Tính kết hợp (P + Q) + R = P + (Q + R)
* Phần tử trung hòa O : P + O = O + P = P
* Phần tử đối: với mọi P E(Fq) luôn tồn tại –P E(Fq) sao cho P + (-P) = O.
* Bậc của một điểm G trên E(Fq) là một số nguyên dương n sao cho k\*G = O.

## Bài toán logarith rời rạc trên đường cong Elliptic

Bài toán logarith rời rạc trên đường cong elliptic (ECDLP): Cho E là một đường cong elliptic và P là một điểm thuộc E có bậc n. Cho điểm Q E , tìm sô nguyên dương m thỏa mãn công thức m\*P = Q.

Hiện nay chưa có thuật toán nào được xem là hiệu quả để giải quyết bài toán này. Để giải bài toán logarith rời rạc trên đường cong elliptic, cần phải kiểm tra tất cả các giá trị m [2..n-2]. Nếu điểm P được lựa chọn sao cho n khá lớn thì việc giải bài toán ECDLP xem như không khả thi. Việc giải bài toán ECDLP khó khăn hơn việc giải bài toán logarith rời rạc trên trường số nguyên thông thường.

# Chương 2: Chữ ký số trên đường cong Elliptic

## Sơ đồ chữ ký ECDSA

Để thiết lập sơ đồ chữ ký ECDSA, cần xác định các tham số: lựa chọn đường cong E trên trường hữu hạn Fq và điểm cơ sở G E(Fq). Một số khuyến nghị khi lựa chọn các tham số:

* q>3 là số nguyên tố, xác định trường hữu hạn cơ sở Fq.
* E(Fq) : y2 = x3 + Ax + B, với A,B Fq và 4A3 + 27B2 0 mod q.
* Phần tử sinh G (x,y) = (Gx,Gy) có bậc nguyên tố là n trên E(Fq) và n = # E(Fq).
* Đồng thừa số h=1

**Sinh khóa:**

* Chọn số ngẫu nhiên d trong khoảng [2…n-1] làm khóa bí mật
* Tính Q = d\*G làm khóa công khai.

**Ký trên bản rõ m:**

* Chọn số ngẫu nhiên k trong khoảng [2..n-1].
* TÍnh k\*G = (x1,y1).
* Tính r = x1 mod n. Nếu r = 0 chọn lại k.
* Tính k-1 mod n.
* Tính s = k-1 (m + d\*r) mod n. nếu s = 0 thì chọn lại k.
* Chữ ký trên thông điệp m là (r,s).

**Kiểm tra chữ ký:**

* Kiểm tra r và s xem có nằm trong khoảng 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 = O thì phủ nhận chữ ký. Ngược lại tính v = xX mod n.
* Chữ ký được chấp nhận nếu v = r.

**Chứng minh:**

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 = u1G + u2dG = (u1 + u2d)G = kG, và vì vậy v = r.

## Sơ đồ chữ ký Nyberg – Rueppel

Giả sử E là đường cong elliptic trên trường Zq (q là số nguyên tố) sao cho E chứa một nhóm con cyclic H trong đó bài toán logarith rời rạc là khó.

Chọn số ngẫu nhiên a làm khóa bí mật.

Chọn E. Tính a. là công khai.

**Tạo chữ ký cho văn bản x:**

* Chọn một số ngẫu nhiên K Z|H|.
* Tính k = (y1,y2).
* c = hash(x) mod q.
* d = k – ac mod q.
* chữ ký là (c,d)

**Kiểm tra chữ ký:**

* (y1,y2) = d + c.
* e = c – y1 mod q.
* Chữ ký được chấp nhận nếu hash(x) e mod q

Tất cả các sơ đồ chữ ký đều yêu cầu phải băm văn bản trước khi ký. Chuẩn P1363 của IEEE khuyến nghị dùng SHA-1, được định nghĩa bởi NIST, hoặc RIPEMD-160 được định nghĩa bởi ISO-IEC. Lý do để sử dụng các hàm băm là việc chúng giúp khó tìm được hai văn bản có cùng giá trị băm,hàm băm giúp chữ ký trên văn bản gốc gọn nhẹ hơn rất nhiều.

## Sơ đồ chữ ký mù Harn trên EC

Chữ ký mù là chữ ký được thực hiện trên văn bản mà người ký hoàn toàn không biết nội dung. Điều này thực hiện được vì người trình ký đã sử dụng một phương pháp nào đó để che dấu nội dung của văn bản gốc để người ký không biết. Để người ký yên tâm, người xin cấp chữ ký phải chứng minh tính hợp lệ của nội dung đã được che dấu.

**Sinh khóa:**

Chọn các tham số cho đường cong elliptic:

1. Chọn số nguyên tố p và số nguyên n. Giả sử f(x) là một hàm đa thức trên trường GF(p) bậc n tạo thành trường hữu hạn GF(pn) và a là một nghiệm của f(x) trong GF(pn).
2. Với 2 phần tử a,b của GF(pn), xác định phương trình của E trên GF(pn) y2 = x3 + ax + b với 4a3 + 27b2 0
3. Với 2 phần tử xp và yp trong GF(pn), xác định một điểm G = (xG,yG) trên E (GO).
4. Giả sử điểm G có bậc q.
5. Hàm chyển c(x): GF(pn) được cho bởi:

c(x) = , x = GF(pn), 0.

Việc sinh khóa bao gồm:

1. Chọn khóa bí mật d là một số nguyên ngẫu nhiên trong [2…q-1].
2. Tính khóa công khai Q = dG.

**Ký mù:**

Giả sử Bob yêu cầu Alice ký lên một văn m0 mà m là đại diện của văn bản này(m = H(m0) với H là một hàm băm nào đó).Giao thức ký được thực hiện như sau:

1. Alice sinh ra cặp khóa( , ) theo cách sau: chọn ngẫu nhiên [1…q-1] và tính = G = (,). Đặt = , rồi gửi và cho Bob
2. Bob chọn các tham số làm mù a,b [1…q-1] , tính R trên E sao cho R = a + bG = (xk, yk) và tính r = c(xk) và = (. Sau đó gửi cho Alice ( là m sau khi đã bị làm mù).
3. Alice tính , rồi gửi cho Bob.
4. Bob nhận được , xóa mù để có được chữ ký s trên m bằng cách tính .

Cặp (r,s) là chữ ký trên m.

## Sơ đồ đa chữ ký mù Harn trên EC

Đa chữ ký hiểu là chữ ký được tạo thành bởi nhiều người ký. Có văn bản cần được ký bởi một số người thay vì một người nhằm bảo đảm tính an toàn. Những người ký không biết về nội dung văn bản ký.

**Sinh khóa**

Việc chọn các tham số cho đường cong elliptic tương tự như sơ đồ chữ ký Harn. Giả sử rằng có t người ký là Ui , với i = 1 … t . Việc sinh khóa được thực hiện qua các bước:

1. Mỗi người ký Ui chọn ngẫu nhiên một khóa bí mật di là một số nguyên thuộc [2, q – 1].
2. Khóa công khai của người ký Ui là điểm: Qi = diG = ( xdi , ydi ), i = 1 , … ,t.
3. Khóa công khai cho tất cả người ký là: Q = Q1+…+ Qt = dG = (xd, yd) với d = d1+ …+ dt (mod q).

**Ký mù trên m**

1. Người ký Ui sinh một lần cặp (, ) bằng cách chọn ngẫu nhiên ∈ [2…q – 1] và tính tính = G = (,). Đặt = , rồi gửi và cho Ban thư ký.
2. Ban thư ký chọn các tham số làm mù a,b ∈ [1…q-1] , tìm điểm R trên E sao cho ( , ) R = a + bG = (xk, yk) trong đó = và Q = Q1 + … + Qt. và tính r = c(xk) và = (. Sau đó gửi và cho từng người ký Ui.
3. Ui tính tính . Gửi tới ban thư ký.
4. Ban thư ký tính G − Qi = () và kiểm tra . Chữ ký mù nhóm ECC là cặp (r, s) trong đó s = a (mod q) và =

# Chương 3: Cài đặt hệ chữ ký ECDSA trên đường cong Elliptic

Đê cài đặt thử nghiệm hoạt động của hệ chữ ký ECDSA em sử dụng ngôn ngữ C++ cùng với sự hỗ trợ của 2 thư viện:

NTL: thư viện hỗ trợ các phép toán với số nguyên lớn.

OpenSSL: thư viện hỗ trợ các hàm bảo mật (em sử dụng hàm băm sha256 trong thư viện OpenSSL).

## Tham số của đường cong

Đường cong elliptic E trên trường hữu hạn Fq : y2 = x3 + Ax + Bcó các tham số như sau:

q = FFFFFFFF00000001000000000000000000000000FFFFFFFFFFFFFFFFFFFFFFFF

A = FFFFFFFF00000001000000000000000000000000FFFFFFFFFFFFFFFFFFFFFFFC

B = 5AC635D8AA3A93E7B3EBBD55769886BC651D06B0CC53B0F63BCE3C3E27D2604B

Gx = 6B17D1F2E12C4247F8BCE6E563A440F277037D812DEB33A0F4A13945D898C296

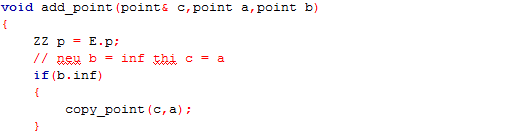
Gy = 4FE342E2FE1A7F9B8EE7EB4A7C0F9E162BCE33576B315ECECBB6406837BF51F5

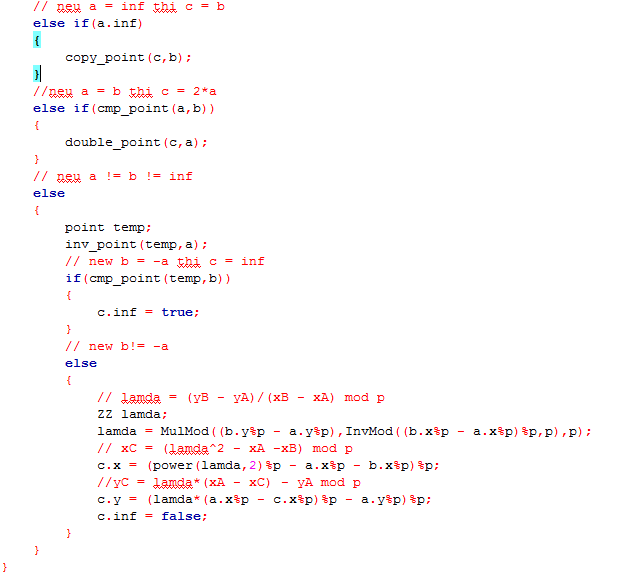
n = FFFFFFFF00000000FFFFFFFFFFFFFFFFBCE6FAADA7179E84F3B9CAC2FC632551

h = 01

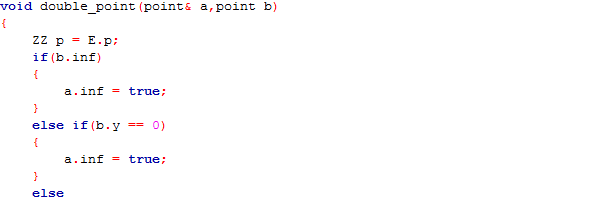
Đây là đường cong Elliptic trên trường Fq với các tham số q,A,B như trên, điểm cơ sở G(Gx,Gy) ∈ E(Fq) với bậc là n, h = #E/n.

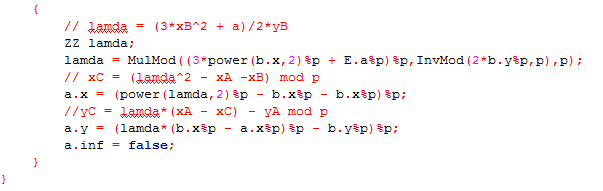
## Phép cộng điểm



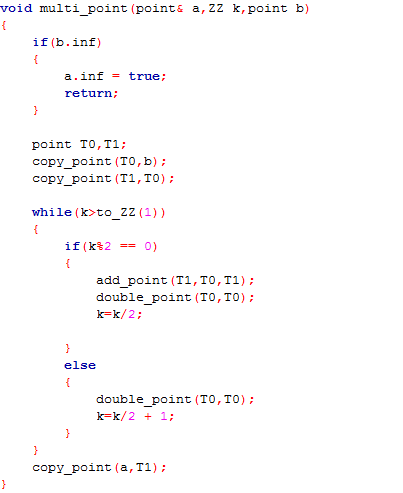


## Phép nhân đôi điểm





## Phép nhân một số nguyên với một điểm



## Tạo cặp khóa

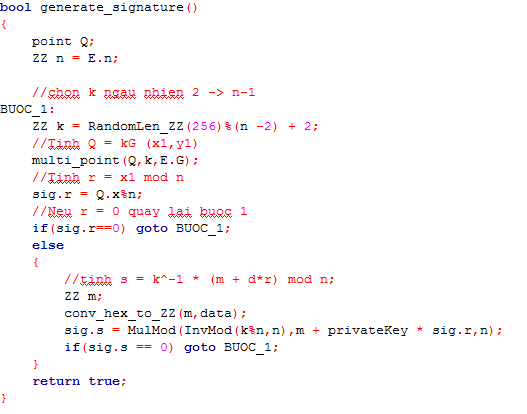
Để tạo cặp khóa bí mật và công khai cần sử dụng các tham số đường cong nêu ở trên

Khóa bí mật là một sô nguyên tùy ý do người dùng nhập vào (privateKey)

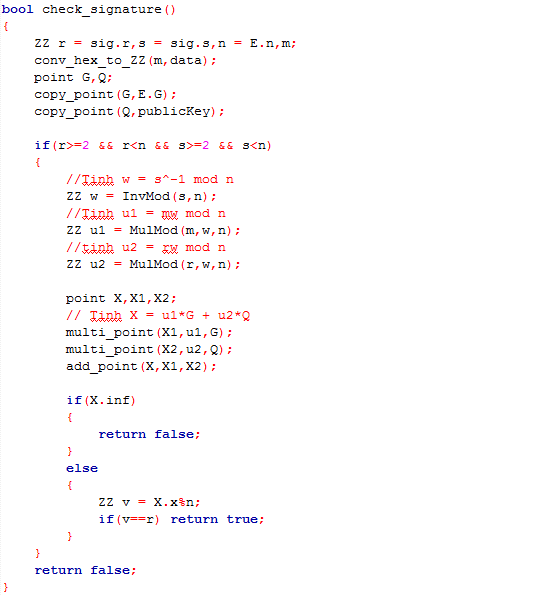
Khóa công khai là một điểm nằm trên đường cong E được tính theo công thức nhân nêu trên:

publicKey = privateKey\*G. (G là điểm cơ sở của đường cong E)

## Ký lên bản tin



## Xác minh chữ ký



# Kết luận

Qua đồ án này, em đã thu được một số kết quả chính như sau:

1. Hiểu được khái niệm về đường cong Elliptic và chữ ký số trên đường cong Elliptic
2. Nắm được một số sơ đồ chữ ký sô trên đường cong Elliptic đang được sử dụng hiện nay
3. Mô phỏng được hoạt động của sơ đồ chữ ký số ECDSA bằng ngôn ngữ lập trình C++

Trong tương lai hệ chữ ký điện tử trên đường cong Elliptic sẽ ngày càng được phát triển và ứng dụng rộng rãi như trong các hệ thống bỏ phiếu điện tử và thanh toán điện tử. Việc hiểu được khái niệm và biết các cài đặt hệ chữ ký điện tử trên đường cong Elliptic sẽ là rất quan trọng đối với những ai muốn xây dựng các hệ thống nói trên trong tương lai.

Trong quá trình làm Project, em xin cảm ơn sự hướng dẫn tận tình của T.S Trần Vĩnh Đức, cả về chuyên môn cũng như định hướng để em có thể hoàn thành được đề tài.

Dù đã cố gắng nhưng đồ án vẫn còn nhiều thiếu sót. Em rất mong thầy góp ý để em có thể rút kinh nghiệm và hoàn thành hơn trong tương lai.

# Tài liệu tham khảo

<http://repositories.vnu.edu.vn/jspui/bitstream/123456789/39410/1/TT_00050000892.pdf>

<http://luanvan.net.vn/luan-van/luan-van-nghien-cuu-tim-hieu-va-trinh-bay-ve-chu-ky-so-tren-duong-cong-elliptic-ung-dung-cua-duong-cong-elliptic-trong-53140/>

<http://www.secg.org/SEC2-Ver-1.0.pdf>

<http://www.ecc-brainpool.org/download/Domain-parameters.pdf>