Tiến hành quá trình thiết lập hệ mật trên đường cong Elliptic

Thiết lập bộ khoá công khai

Ta chọn p có độ dài khoảng 256 bit, và p = 774101403431786789505464785594777430756945701281051993704886846934530267985607

Tìm thấy đường cong Elliptic: y^2 = x^3 + 11x + 0

Điểm sinh P của đường cong ta sẽ sử dụng: P(1, 501979195439360549144606430032399807666671973949910420832246883508662736168258)

Bob tiến hành chọn một số nguyên s làm khoá riêng của mình

Giá trị của s là 3904390461

Ta tính B = sP, khi đó B có toạ độ B(508415054307877306940184142528022706217301661114075359918197674634514699084239, 724008833095304718891910944715173802517037324252357850448301302391355039810886)

Alice tiến hành tải bộ khoá công khai

Alice có một bản tin muốn gửi với nội dung:chaomunghaimuoinamthanhlaptruongdhcn

sau đó tiến hành mã hoá bản tin thành một điểm trên Elliptic

Bản tin sau được mã hoá chính là điểm M trên đường cong, với toạ độ là M(4856054912948765854981195127206093676320084444097919, 606054926328198786072633026224512398100981378474250089667626624075872818473718)

Sau đây Alice cần chọn một số nguyên k bí mật

Giá trị của k là 8718471201

Đến đây, ta tiến hành tạo bản mã M = (M1, M2)

Ta có M1 = kP = M1(336562068653397238401545114215641678313354492568089355813978003480950984403502, 475428202595169408183276475903906234816787214154817901863675995377786997755521)

và M2 = M + kB = M2(171740270139057656012474003299717377676579162469948021317240207544717130553773, 16803233630999416413872007629345443098509241332389456051279101492628571960379)

Bob nhận được bản mã M và tiến hành giải mã

Giải mã với điểm M = M2 - sM1 = M(4856054912948765854981195127206093676320084444097919, 606054926328198786072633026224512398100981378474250089667626624075872818473718)

Bản tin được giải mã có nội dung như sau:chaomunghaimuoinamthanhlaptruongdhcn

Quá trình mã hoá và giải mã tiến hành thành công!

Quy trình thiết lập sơ đồ chữ ký trên đường cong Elliptic

Ta chọn p có độ dài khoảng 160 bit, và p = 667329633573198542835592718211457817467826187328367

Tìm thấy đường cong Elliptic: y^2 = x^3 + 19x + 17 mod 667329633573198542835592718211457817467826187328367

Số điểm thuộc đường cong E là n = 667329372500748588378524347649198375156419953964703

Điểm sinh P của đường cong ta sẽ sử dụng: P(0, 662816465626464571636452254500075910383255592142650)

Alice có một bản tin muốn gửi với nội dung:

motdieumaanhdabiettruocranglachicanconkhoangcachsekhongthaynhonhaunhungmaemdaloluusoncuaemlenbuctranhanhtomauvaythigioanhmuonduocbenemthatlauboivinanglanguoilamtraitimanhthaybotdaubabyemcugiudianhkhongcandau

Giả sử Alice là người ký trên bản rõ M. Khi đó Alice thực hiện các bước sau để tạo ra cặp khóa công khai và khóa riêng

1. Khoá riêng của Alice là d = 376855900084978807945002470127596831192897202914537

2. Khoá công khai của người gửi tổ hợp là (Ep(a,b), P, n, Q)

Alice sử dụng khóa riêng của mình để tạo chữ ký trên bản tin M bằng các bước sau:

1. Alice cần chọn một số nguyên k bí mật

Giá trị của k là 957944543225638912465992672294979586687

2. Tính kP = (x1 , y1), trong đó x1 là số nguyên

Ta có M1 = kP = M1(90819988133693160889365376696132111163196991433803, 613284359813587162442524715071621135279942405115339)

3. Tính r = x1 mod n; Nếu r = 0, thì quay lại bước 1

Ta có r = 90819988133693160889365376696132111163196991433803

4. Tính h = H(M), trong đó H là SHA-512

Ta có h = b1d1e0bd2cc9bb4de08e0b7e3f8f764a84e0f2d1a076cbad6fc4e149b41b77236c4fe234f163f2a59bb620fb3d5e36e1a9c8f94c06f7dff10254b01deb065210

Tính s = (h + d\*r)\* (k ^(- 1)) mod n; Nếu s = 0, thì quay lại bước 1

Ta có s = 115971139098691631928038696054142302777459292420006

Chữ ký của Alice trên bản tin M là cặp số nguyên (r,s) = (90819988133693160889365376696132111163196991433803,115971139098691631928038696054142302777459292420006)

Người nhận Bob có thể xác minh tính xác thực của chữ ký của Alice là (r, s) trên bản tin M bằng cách thực hiện các bước sau:

1. Nhận được chữ ký trên Khóa công khai (E, P, n, Q) của Alice

2. Xác minh rằng các giá trị r và s nằm trong khoảng [1, n-1]

3.Tính w = s ^(- 1) mod n

Ta có w = 319165693391120254465571702078845154970758998188148

4. Tính h = H (M), trong đó H là thuật toán băm an toàn tương tự được sử dụng bởi A

5. Tính u1 = hw mod n

Ta có u1 = 634623386584554570097199622551992753534879879948016

6. Tính u2 = rw mod n

Ta có u2 = 520146549491385082974941367927585286112977952501727

7. Tính F = u1P + u2Q = (x0, y0)

Ta có F = (x0, y0) = (86157288340012032276142657042869126425293053142049,645187282919430462950481321220675474036813561116826)

8. Tính v = x0mod n

Ta có v = 90819988133693160889365376696132111163196991433803

9. Chữ ký cho tin nhắn M chỉ được xác minh nếu v = r

Xác minh thành công!