Họ và tên: Nguyễn Duy Hưng MSSV: 20020108

Lớp: K65CB

Môn học: Nhập môn An toàn thông tin – INT3213 1

BỔ SUNG BÀI TẬP LỚN GIỮA KỲ - PHẦN QUÁ TRÌNH THIẾT LẬP SƠ ĐỒ CHỮ KÝ TRÊN ĐƯỜNG CONG ELLIPTIC

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

Ta chọn p có độ dài khoảng 160 bit, và p = 980305116056896295692277965934189882265112841974339

Tìm thấy đường cong Elliptic: y^2 = x^3 + 2x + 11 mod 980305116056896295692277965934189882265112841974339

Số điểm thuộc đường cong E là n = 980304585885089881261823807590448889865106540782193

Điểm sinh P của đường cong ta sẽ sử dụng: P(0, 194869307919875665664795546482245457211764932260957)

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 = 229023971259573298277853087774020756796934441692483

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 5459044464128716521860494175268905582109

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

Ta có M1 = kP = M1(418938334930377819666706091857544506488817304550199, 25892712989919139649541964633199153296317794994925)

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

Ta có r = 418938334930377819666706091857544506488817304550199

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 = 776980012940506761725304546389911567663960033405282

Chữ ký của Alice trên bản tin M là cặp số nguyên (r,s) = (418938334930377819666706091857544506488817304550199,776980012940506761725304546389911567663960033405282)

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 = 638509205124842339412556513368278939783481611182247

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 = 261580800695763439862279221738398240957917515568593

6. Tính u2 = rw mod n

Ta có u2 = 259031733970688550655871305152068516849714452626829

7. Tính F = u1P + u2Q = (x0, y0)

Ta có F = (x0, y0) = (823222364920314752871114603804631462296597450403308,586686438556207002878695457703297931185891130681289)

8. Tính v = x0mod n

Ta có v = 418938334930377819666706091857544506488817304550199

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

Xác minh chữ ký thành công!