TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI TP. HỒ CHÍ MINH

KHOA CÔNG NGHỆ THÔNG TIN

AN TOÀN THÔNG TIN- INFORMATION SECURITY

CHƯƠNG 4

CÁC THUẬT TOÁN CHỮ KÝ SỐ

Giảng viên: TS. Trần Thế Vinh

LƯỢC ĐỒ CHỮ KÝ SỐ ELGAMAL

Khái niệm:

Lược đồ chữ ký số Elgamal được thiết kế dựa trên các tính chất đại số của phép lũy thừa modulo, cùng với bài toán logarit rời rạc. Nó được Taher Elgamal mô tả vào năm 1985.
Thuật toán sử dụng một cặp khóa chung và khóa riêng. Khóa riêng được sử dụng để tạo chữ ký số cho tin nhắn và chữ ký đó có thể được xác minh bằng cách sử dụng khóa chung tương ứng của người ký.

Nhắc lại về cơ sở toán học trong mật mã. Cho một số nguyên tố p, nếu một phần tử $\alpha \in G_p^* = \{1, 2, \dots, p-1\}$ được coi là phần tử sinh (hay căn nguyên thủy) của nhóm G_p^* nếu như tập các lũy thừa của α cũng chính là nhóm này, tức là 2 tập sau đây trùng nhau

$$\{\alpha, \alpha^2, \dots, \alpha^{p-1}\}, \{1, 2, \dots, p-1\}$$

Có thể chỉ ra rằng nếu α là căn nguyên thuỷ của p thì:

1. Với mọi số nguyên m, $\alpha^m \equiv 1 (mod\ p)$ nếu và chỉ nếu $m \equiv 0\ (mod\ p-1)$
2. Với mọi số nguyên i, j: $\alpha^i \equiv \alpha^j\ (mod\ p)$ nếu và chỉ nếu $i \equiv j\ (mod\ p-1)$

Sinh khóa:

Với mã hóa Elgamal, các yếu tố cần có của chữ ký số Elgamal là số nguyên tố p và α, với α là căn nguyên thủy của p trong trường G_p^*. Alice tạo ra một cặp khóa riêng/khoá chung như sau:

1. Tạo một số nguyên ngẫu nhiên X_A, sao cho 1 < X_A < p-1
2. Tính toán $Y_A = \alpha^{X_A}$ mod p.
3. Khoá riêng của Alice là X_A , Khoá công khai của Alice là {p, α, Y_A}

LƯỢC ĐỒ CHỮ KÝ SỐ ELGAMAL

Để ký tin nhắn M, Alice đầu tiên tính toán hàm băm m = H(M), sao cho m là một số nguyên trong phạm vi $0 \leq m \leq p - 1$. **Alice sau đó tạo thành một chữ ký số như sau:**

1. Chọn một số nguyên ngẫu nhiên K sao cho $1 < K < p - 1$ và $\gcd(K, p - 1) = 1$.
2. Tính $S_1 = \alpha^K \bmod p$.
3. Tính $K^{-1} \bmod (p - 1)$. Nghĩa là, tính nghịch đảo của K modulo p - 1.
4. Tính $S_2 = K^{-1} (m - X_A S_1) \bmod (p - 1)$.
5. Chữ ký bao gồm cặp (S_1, S_2).

Bob có thể xác thực chữ ký bằng cách sau

1. Tính $V_1 = \alpha^m \bmod p$
2. Tính $V_2 = (Y_A)^{S_1} (S_1)^{S_2} \bmod p$

Chữ ký hợp lệ nếu $V_1 = V_2$. Chúng ta chứng minh điều này như sau.
Giả sử rằng $V_1 = V_2$ là đúng.
Thay vào ta có:

$\alpha^m \bmod p = (Y_A)^{S_1} (S_1)^{S_2} \bmod p$	Giả sử $V_1 = V_2$
$\alpha^m \bmod p = \alpha^{X_A S_1} \alpha^{K S_2} \bmod p$	Thay thế cho Y_A và S_1
$\alpha^{m - X_A S_1} \bmod p = \alpha^{K S_2} \bmod p$	Sắp xếp lại hệ số
$m - X_A S_1 \equiv K S_2 \bmod (p-1)$	Tính chất của căn nguyên thuỷ
$m - X_A S_1 \equiv K K^{-1} (m - X_A S_1) \bmod (p-1)$	Thay thế cho S_2

LƯỢC ĐỒ CHỮ KÝ SỐ ELGAMAL

Ví dụ:

Cho trường hữu hạn G_{19}^{*} nghĩa là, p = 19. Ta có
căn nguyên thủy {2, 3, 10, 13, 14, 15}. Ta chọn α = 10.
Alice tạo ra một cặp khóa như sau:
1. Alice chọn X_A = 16.
2. Sau đó $Y_A = \alpha^{X_A} \bmod p = \alpha^{16} \bmod 19 = 4$.
3. Khoá bí mật của alice là 16; Khoá công khai của Alice là {p, α, Y_A } = {19, 10, 4}.
Giả sử Alice muốn ký một tin nhắn có giá trị băm m = 14.
1. Alice chọn K = 5, ta có gcd(5, 18)=1.
2. $S_1 = \alpha^K \bmod p = 10^5 \bmod 19 = 3$
3. $K^{-1} mod(p-1) = 5^{-1}\ mod\ 18 = 11$
4. $S_2 = K^{-1}(m - X_A S_1) \bmod (p\text{-}1) = 11\ (14 - (16)(3)) \bmod 18 = -374 \bmod 18 = 4$
Bob có thể xác minh chữ ký như sau.
1. $V_1 = \alpha^m mod\ p = \ 10^{14}\ mod\ 19 = 16$
2. $V_2 = (Y_A)^{S_1}\ (S_1)^{S_2} mod\ p = (4)^3\ (3)^4 mod\ 19 = 5184\ mod\ 19 = 16$

Do đó, chữ ký là hợp lệ bởi vì $V_1 = V_2$

LƯỢC ĐỒ CHỮ KÝ SỐ SCHNORR

Như với lược đồ chữ ký số Elgamal, lược đồ chữ ký Schnorr dựa trên logarit rời rạc. Lược đồ Schnorr giảm thiểu số lượng tính toán phụ thuộc vào thông điệp cần thiết để tạo ra một chữ ký. Nó là một hệ thống chữ ký số nổi tiếng vì dễ sử dụng và là một trong những hệ thống đầu tiên có tính bảo mật được phát hiện bằng các bài toán logarit rời rạc cụ thể. Lược đồ chữ ký số Schnorr tạo ra các chữ ký ngắn gọn và hiệu quả. Phần phụ thuộc thông điệp của quá trình tạo chữ ký yêu cầu nhân số nguyên 2n-bit với số nguyên n-bit.

Lược đồ dựa trên việc sử dụng module số nguyên tố p, với p – 1 ta có thừa số nguyên tố q có kích thước thích hợp; nghĩa là, p -1 $\equiv$ 0 (mod q). Thông thường, sử dụng p $\approx 2^{1024}$ và q $\approx 2^{160}$. Do đó, p là số 1024-bit và q là số 160-bit, cũng là độ dài của giá trị băm SHA-1.

Sinh khóa:

Phần đầu tiên của sơ đồ này là việc tạo ra một cặp khóa riêng tư / công khai, bao gồm các bước sau.

1. Chọn số nguyên tố p và q, sao cho q là thừa số nguyên tố của p - 1.

2. Chọn một số nguyên α, sao cho $\alpha^q = 1$ mod p. Giá trị của α, p, and q bao gồm một khóa công khai toàn cầu có thể dùng chung cho một nhóm người dùng.

3. Chọn một số nguyên ngẫu nhiên s với $0 < s < q$. Đây là khóa riêng của người gửi.

4. Tính $v = \alpha^{-s}$ mod p. Đây là khóa công khai của người gửi.

LƯỢC ĐỒ CHỮ KÝ SỐ SCHNORR

Người gửi có khóa riêng s và khóa công khai v tạo chữ ký như sau.

1. Chọn một số nguyên ngẫu nhiên r với 0 < r < q và tính x = α^{-r} mod p. Tính toán này là một giai đoạn tiền xử lý độc lập với thông điệp M sẽ được ký.

2. Đính kèm thông điệp M với x và băm kết quả được đính kèm để tính giá trị e:

e = H(M||x) (đính kèm văn bản M với x). H là hàm băm

3. Tính y = (r + se) mod q. Chữ ký bao gồm cặp (e, y).

Bất kỳ người nhận nào khác cũng có thể xác minh chữ ký như sau.

1. Tính x′ = $a^y v^e$mod p.

2. Xác minh rằng e = H(M$\|x'$) .

Để thấy rằng việc xác minh hoạt động, hãy quan sát phương trình sau:

$$x' \equiv a^y v^e \equiv a^y a^{-se} \equiv a^{y-se} \equiv a^r \equiv x \ (mod\ p)$$

Do đó, H(M$\|x'$) = H(M||x) .

LƯỢC ĐỒ CHỮ KÝ SỐ DSA

Tổng quan:

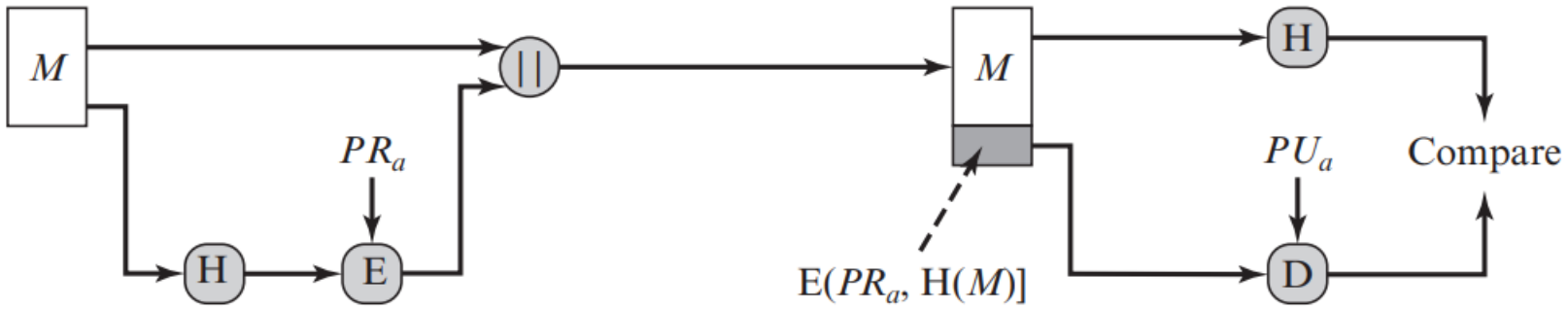
Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) đã xuất bản Tiêu chuẩn Xử lý Thông tin Liên bang FIPS 186, được gọi là Thuật toán Chữ ký Số (DSA). DSA sử dụng Thuật toán băm an toàn (SHA). DSA ban đầu được đề xuất vào năm 1991 và được sửa đổi vào năm 1993 để đáp lại phản hồi của công chúng liên quan đến tính bảo mật của chương trình. Có một bản sửa đổi nhỏ hơn nữa vào năm 1996. Năm 2000, một phiên bản mở rộng của tiêu chuẩn được ban hành là FIPS 186-2, sau đó được cập nhật thành FIPS 186-3 vào năm 2009 và FIPS 186-4 vào năm 2013. Phiên bản mới nhất cũng kết hợp các thuật toán chữ ký số dựa trên RSA và mật mã đường cong Elliptic.

DSA sử dụng thuật toán được thiết kế để cung cấp chức năng chữ ký số. Không giống như RSA, nó không thể được sử dụng để mã hóa hoặc trao đổi khóa. DSA phù hợp cho việc ký và giải mã.

LƯỢC ĐỒ CHỮ KÝ SỐ DSA

Cách tiếp cận của RSA:

- Theo cách tiếp cận RSA, thông điệp cần ký được đưa vào một hàm băm tạo ra mã băm an toàn có độ dài cố định.
- Mã băm này sau đó được mã hóa bằng khóa riêng của người gửi để tạo thành chữ ký.
- Cả tin nhắn và chữ ký đều được truyền đi.
- Người nhận nhận tin nhắn và tạo mã băm.
- Người nhận cũng giải mã chữ ký bằng khóa chung của người gửi.
- Nếu mã băm được tính khớp với chữ ký được giải mã, chữ ký được chấp nhận là hợp lệ.

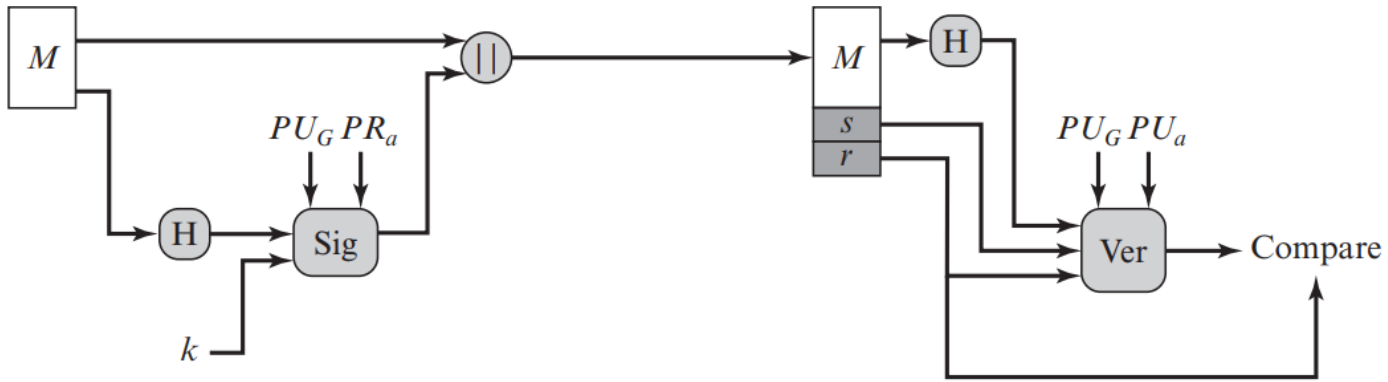


(a) RSA approach

LƯỢC ĐỒ CHỮ KÝ SỐ DSA

Cách tiếp cận của DSA:

- Cách tiếp cận DSA cũng sử dụng hàm băm
- Mã băm được cung cấp làm đầu vào cho hàm chữ ký cùng với số k ngẫu nhiên được tạo cho chữ ký cụ thể này.
- Chức năng chữ ký cũng phụ thuộc vào khóa riêng của người gửi (PR_a) và một tập hợp các tham số được biết đến với một nhóm nguyên tắc giao tiếp.
- Chúng ta có thể coi tập hợp này tạo thành khóa công khai toàn cầu (PU_G).
- Kết quả là một chữ ký bao gồm hai thành phần, được gắn nhãn s và r.
- Ở đầu nhận, mã băm của tin nhắn đến được tạo.
- Chữ ký được nhập vào hàm xác minh.
- Hàm xác minh cũng phụ thuộc vào khóa chung toàn cầu cũng như khóa chung của người gửi (PU_a), khóa này được ghép nối với khóa riêng(PR_a) của người gửi.
- Đầu ra của hàm xác minh là một giá trị bằng với thành phần chữ ký r, nếu chữ ký hợp lệ.
- Hàm chữ ký sao cho chỉ người gửi, biết về khóa riêng, mới có thể tạo ra chữ ký hợp lệ.



(b) DSA approach

LƯỢC ĐỒ CHỮ KÝ SỐ DSA
THUẬT TOÁN DSA

Sinh khóa:

Các thành phần khóa công khai toàn cầu

p số nguyên tố ở đây $2^{L-1} < p < 2^{L}$ Trong đó 512 ≤L ≤ 1024 và L là bội số của 64; tức là, độ dài bit L từ 512 đến 1024 bit với tăng dần 64 bit

q ước số nguyên tố của (p - 1), Trong đó $2^{N-1} < q < 2^{N}$ độ dài bit của N bit (SHA-1, có N=160 bit)

$g = h^{(p-1)/q} mod\ p$, trong đó h là số nguyên bất kỳ với $1 < h < (p - 1)$ sao cho $h^{(p-1)/q} mod\ p > 1$

Khoá bí mật

x là số nguyên ngẫu nhiên hoặc giả ngẫu nhiên với 0 < x < q

Khoá công khai

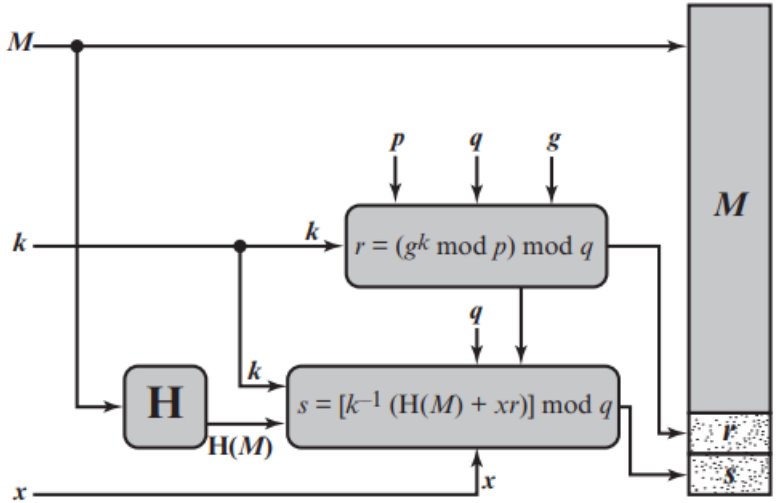
Y = g^{x} mod p

LƯỢC ĐỒ CHỮ KÝ SỐ DSA

Tạo chữ ký:

Số bí mật cho mỗi tin nhắn
k là số nguyên ngẫu nhiên hoặc giả ngẫu nhiên với 0 < k < q

Ký
r = $(g^k \bmod p) \bmod q$
s = $[k^{-1} (H(M) + xr)] \bmod q$
Signature = (r, s)



(a) Signing

LƯỢC ĐỒ CHỮ KÝ SỐ DSA

Xác thực chữ ký:

Xác thực

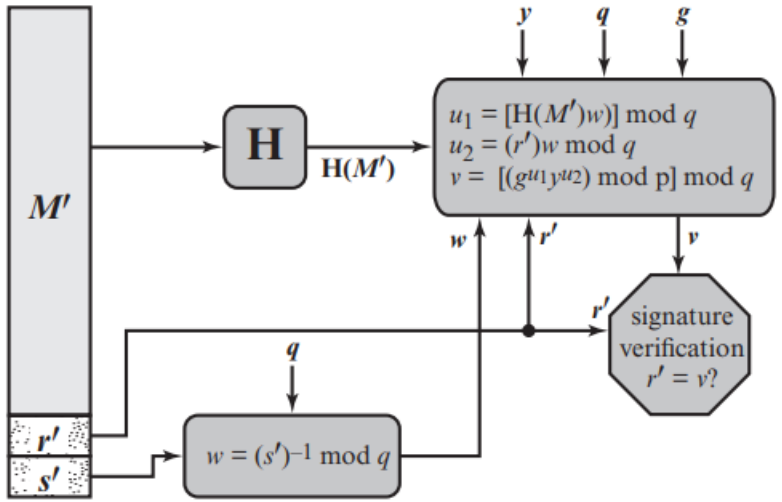
w = $(s')^{-1}$ mod q

u_1 = [H(M′)w] mod q

u_2 = (r′)w mod q

v = [$(g^{u_1} y^{u_2})$ mod p] mod q

TEST: v = r′



(b) Verifying

M = tin nhắn đã được ký

H(M) = băm của M sử dụng SHA-1

M′, r′, s′ = nhận được từ M, r, s

THUẬT TOÁN CHỮ KÝ SỐ TRÊN ĐƯỜNG CONG ELLIPTIC

Khái niệm:
Phiên bản 2009 của FIPS 186 bao gồm một kỹ thuật chữ ký số mới dựa trên mật mã đường cong elipptic, được gọi là Thuật toán chữ ký số đường cong Elliptic (ECDSA). ECDSA đang được chấp nhận ngày càng tăng do lợi thế hiệu quả của mật mã đường cong elip, mang lại bảo mật tương đương với các sơ đồ khác với độ dài bit khóa nhỏ hơn.

Bốn yếu tố có liên quan trong chữ ký số dựa trên đường cong Elliptic:

1. Tất cả những người tham gia vào sơ đồ chữ ký số sử dụng cùng một tham số miền, xác định một đường cong elliptic và một điểm (x, y) trên đường cong.

2. Trước tiên, người ký phải tạo một cặp khóa công khai/riêng tư. Đối với khóa riêng tư, người ký sẽ chọn một số ngẫu nhiên hoặc giả ngẫu nhiên. Sử dụng số ngẫu nhiên đó và điểm xuất phát, người ký sẽ tính toán một điểm khác trên đường cong elliptic. Đây là khóa công khai của người ký.

3. Một giá trị băm được tạo ra từ tin nhắn được ký. Sử dụng khóa riêng, các tham số miền và giá trị băm để tạo ra chữ ký số. Chữ ký bao gồm hai số nguyên, r và s.

4. Để xác minh chữ ký, người xác minh sử dụng khóa công khai của người ký làm đầu vào, các tham số miền và số nguyên s. Đầu ra là một giá trị v được so sánh với r. Chữ ký được xác minh nếu v = r.

THUẬT TOÁN CHỮ KÝ SỐ TRÊN ĐƯỜNG CONG ELLIPTIC

Tham số miền ECDSA:

Các tham số miền cho ECDSA như sau:

- Tham số miền có thể được chia sẻ cho một nhóm người hoặc dành riêng cho một người dùng.
- Tạo một trường GF có kích thước q là số nguyên tố lẻ, hoặc $q = 2^m$
- (tùy chọn) một chuỗi bit seedE có độ dài ít nhất là 256 bit, nếu đường cong elliptic được tạo theo các phương pháp tạo ngẫu nhiên.
- a, b là các số nguyên xác định phương trình đường cong elliptic được xác định trên trường GF_q với phương trình $y^2 = x^3 + ax + b$ với q>3 và $y^2 + xy = x^3 + ax + b$ với $q = 2^m$
- G là một điểm cơ sở được biểu thị bằng G =(x_g, y_g) trên phương trình đường cong elliptic.
- Thứ tự n của điểm G, với $n > 2^{256}$ và $n > 4\sqrt{q}$.
- n thứ tự điểm G; có nghĩa n là số nguyên dương nhỏ nhất sao cho nG = O. Đây cũng là số điểm trên đường cong.

Cặp khóa ECDSA:

- Cặp khóa ECDSA được liên kết với một bộ tham số miền EC cụ thể.
- Khóa chung là bội số ngẫu nhiên của điểm cơ sở, trong khi khóa riêng là số nguyên được sử dụng để tạo bội số.
- Cặp khóa của thực thể A được liên kết với một bộ tham số miền EC cụ thể D=(q, FR, a,b, G, n, h).
- Liên kết này có thể được đảm bảo bằng mật mã (ví dụ: bằng chứng chỉ) hoặc theo ngữ cảnh (ví dụ: tất cả các thực thể sử dụng cùng tham số miền).
- Thực thể A phải đảm bảo rằng các tham số miền hợp lệ trước khi tạo khóa

THUẬT TOÁN CHỮ KÝ SỐ TRÊN ĐƯỜNG CONG ELLIPTIC

Sinh khóa

Mỗi người ký phải tạo một cặp khóa, một khóa riêng tư và một khóa công khai. Người ký, chúng ta hãy gọi anh ta là Bob, tạo hai khóa bằng các bước sau:

1. Chọn một số nguyên ngẫu nhiên hoặc giả ngẫu nhiên d, $d \in [1, n - 1]$

2. Tính Q = dG. Đây là một điểm trong Eq(a, b)

3. Khóa công khai của Bob là Q và khóa riêng tư là d.

THUẬT TOÁN CHỮ KÝ SỐ TRÊN ĐƯỜNG CONG ELLIPTIC

Tạo chữ ký số

Với các tham số miền, khóa công khai(Q) và khóa riêng tư (d) trong tay, Bob tạo chữ ký số 320 byte cho tin nhắn m bằng các bước sau:

1. Chọn một số nguyên ngẫu nhiên hoặc giả ngẫu nhiên k, k ∈ [1, n - 1]

2. Tìm điểm P = (x, y) = kG và r = $\bar{x}$ mod n. If r = 0 thì quay lại bước 1. (chuyển đổi x thành số nguyên $\bar{x}$ (ANSI X9.62 chỉ định phương pháp chuyển đổi các phần tử trường thành số nguyên)

3. Tính t = k^{-1} mod n

4. Tính e = H(m), trong đó H là một trong những hàm băm SHA-2 hoặc SHA-3 và chuyển đổi chuỗi bit này thành số nguyên e.

5. Tính s = k^{-1} (e + dr) mod n. Nếu s = 0 thì quay lại bước 1

6. Chữ ký của tin nhắn m là cặp (r, s).

THUẬT TOÁN CHỮ KÝ KỸ THUẬT SỐ ĐƯỜNG CONG ELLIPTIC

Xác thực chữ ký số

Alice biết các thông số miền và khóa công khai của Bob. Alice nhận tin nhắn và chữ ký cố của Bob, tiếp đến xác minh chữ ký bằng các bước sau:

1. Xác minh rằng r và s là các số nguyên trong phạm vi [1, n – 1]

2. Tính Hash(m) và chuyển chuỗi bit này sang số nguyên e = H(m)

3. Tính toán w = s^{-1} mod n

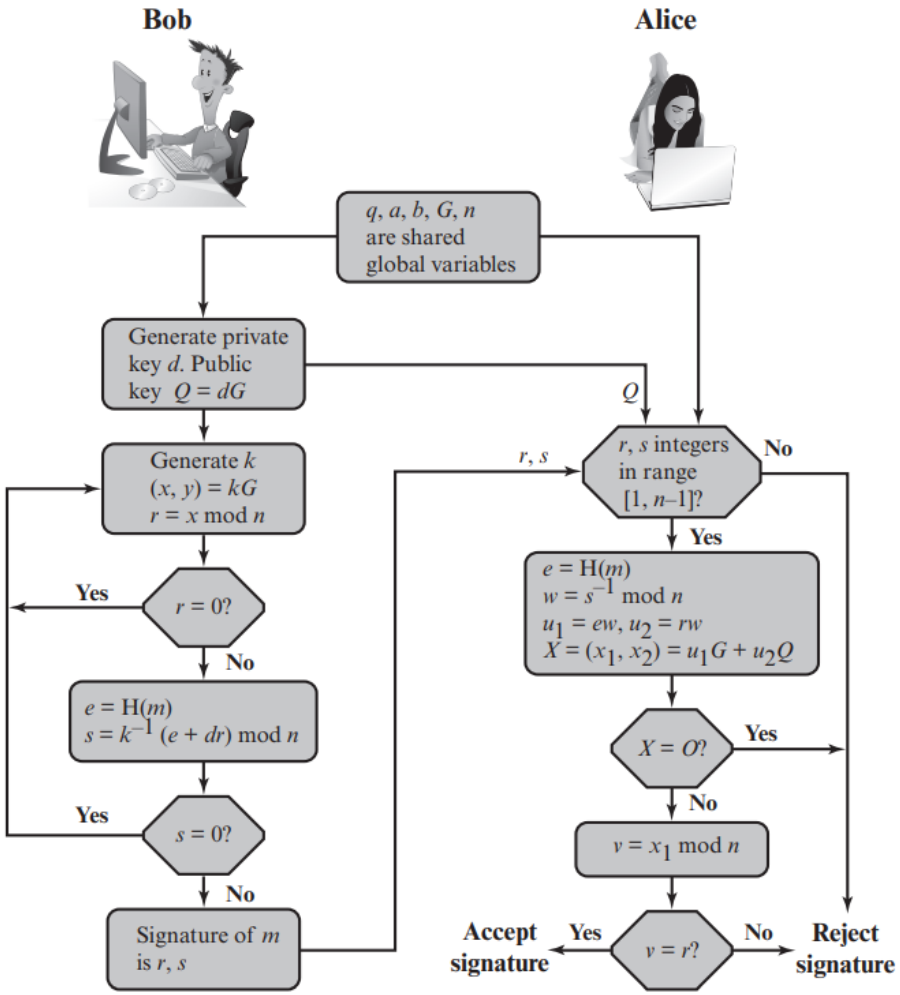
4. Tính toán $u_1 = ew(mod\ n)$ và $u_2 = rw(mod\ n)$

5. Tính toán điểm X(x_1, y_1) = u_1 G + u_2 Q

6. Nếu X = 0, từ chối chữ ký nếu X ≠ 0 tính v = x_1 mod n

7. Chấp nhận chữ ký của Bob khi và chỉ khi v = r

THUẬT TOÁN CHỮ KÝ KỸ THUẬT SỐ ĐƯỜNG CONG ELLIPTIC



Hình bên: Minh họa quá trình xác thực chữ ký. Chúng ta có thể xác minh rằng quá trình này là hợp lệ như sau. Nếu thư Alice nhận được trên thực tế có chữ ký của Bob, sau đó:

s = $k^{-1}(e + dr) mod\ n$

Sau đó:

k = $s^{-1}(e + dr) mod\ n$

k = $(s^{-1}e + s^{-1}dr) mod\ n$

k = $(we + wdr) mod\ n$

k = $(u_1 + u_2 d) mod\ n$

Bây giờ hãy xem xét rằng:

$$\boldsymbol{u_1 G + u_2 Q = u_1 G + u_2 dG = (u_1 + u_2 d)G = kG}$$

Trong bước 6 của quy trình xác minh, ta có v = x_1 mod n, trong đó điểm X = (x_1 , y_1) = $u_1 G + u_2 Q$. Vì vậy, chúng tôi thấy rằng v = r since r = x mod n và x là tọa độ x của điểm kG và chúng tôi đã thấy rằng $u_1 G + u_2 Q$ = kG