8.4

Trong nhiều trường hợp, một message có thể chỉ được mã hóa và giải mã một lần, do đó, chỉ cần sử dụng bất kỳ hệ thống mật mã nào được biết là an toàn tại thời điểm tin nhắn được mã hóa là đủ. Mặt khác, một signed message có thể hoạt động như một tài liệu pháp lý như hợp đồng hoặc di chúc; vì vậy rất có thể cần phải xác minh chữ ký nhiều năm sau khi thông điệp được ký. Do đó, điều quan trọng là phải thực hiện nhiều biện pháp phòng ngừa liên quan đến tính bảo mật của sơ đồ chữ ký thay vì hệ thống mật mã. Vì Lược đồ chữ ký ElGamal không bảo mật hơn Discrete Logarithm problem nên điều này đòi hỏi phải sử dụng mô đun p lớn. Hầu hết mọi người bây giờ cho rằng độ dài của p phải ít nhất là 2048 bit để bảo mật ngày nay và thậm chí lớn hơn để bảo mật trong tương lai gần

Mô-đun 2048 bit dẫn đến chữ ký ElGamal có 4096 bit. Đối với các ứng dụng tiềm năng, trong đó có nhiều ứng dụng liên quan đến việc sử dụng thẻ thông minh và cần chữ ký ngắn hơn. Năm 1989, Schnorr đề xuất một sơ đồ chữ ký có thể được xem như một biến thể của Sơ đồ chữ ký ElGamal trong đó kích thước chữ ký được giảm đi đáng kể. Thuật toán chữ ký số (hoặc DSA) là một sửa đổi khác của Lược đồ chữ ký ElGamal, kết hợp một số ý tưởng được sử dụng trong Lược đồ chữ ký Schnorr. DSA được công bố trong Đăng ký Liên bang vào ngày 19 tháng 5 năm 1994 và được thông qua như một tiêu chuẩn vào ngày 1 tháng 12 năm 1994 (tuy nhiên, nó được đề xuất lần đầu tiên vào tháng 8 năm 1991). Chúng tôi mô tả Lược đồ chữ ký Schnorr, DSA và sửa đổi DSA thành các đường cong elip (được gọi là Thuật toán chữ ký số đường cong Elliptic, hoặc ECDSA) trong các phần phụ tiếp theo.

8.4.1. Sơ đồ chữ ký Schnorr

Giả sử p và q là các số nguyên tố sao cho $p - 1 \equiv 0 \ (mod\ q)$. Thông thường $p \sim 2^{2048}$ và $q \sim 2^{224}$. Lược đồ chữ ký Schnorr sửa đổi Lược đồ chữ ký El-Gamal một cách khéo léo sao cho bản tóm tắt (message digest) có độ dài $log_2 q$ - bit được ký bằng chữ ký $2log_2 q$ - bit, nhưng việc tính toán được thực hiện trong Z_p. Cách thực hiện điều này là làm việc trong một nhóm con Z_p^* có kích thước q. Độ an toàn giả định của lược đồ dựa trên niềm tin rằng việc tìm các logarit rời rạc trong nhóm con xác định này của Z_p^* là an toàn.

Gọi α là căn bậc q của p. Để xác định α, gọi α_0 là phần tử nguyên thủy của Z_p, khi đó $\alpha = \alpha_0^{(p-1)/q} \ mod\ p$. Khóa trong Lược đồ chữ ký Schnorr tương tự như khóa trong Lược đồ chữ ký ElGamal ở các khía cạnh khác. Tuy nhiên, Sơ đồ Chữ ký Schnorr tích hợp một hàm băm trực tiếp vào thuật toán ký. Chúng ta sẽ giả sử rằng $h: \{0, 1\}^* \longrightarrow Z_q$ là hàm băm an toàn. Một mô tả đầy đủ về Lược đồ Chữ ký Schnorr được đưa ra dưới dạng Hệ thống mật mã 8.3.

Cryptosystem 8.3: Schnorr Signature Scheme

Cho p là một số nguyên tố sao cho bài toán logarit rời rạc trong Z_p^* là một bài toán khó giải, và gọi số nguyên tố q là ước của p-1. Gọi $\alpha \in Z_p^*$ là căn bậc q của p. Gọi $P = \{0, 1\}^*$ và $A = Z_q \ x \ Z_q$ và định nghĩa $K = \{(p, q, \alpha, a, \beta): \beta \equiv \alpha^a (mod\ p)\}$, trong đó $0 \le a \le q - 1$.

Các giá trị p, q, α, và β là khóa công khai, a là khóa bí mật. Cuối cùng, đặt $h: \{0, 1\}^* \longrightarrow Z_q$ là hàm băm an toàn.

Với $K = \{(p, q, \alpha, a, \beta)$ và số bí mật ngẫu nhiên k, $1 \le k \le q - 1$, định nghĩa:

$$sig_K(x, k) = (\gamma, \delta)$$

Trong đó $\gamma = h(x \,||\, \alpha^k \bmod p)$ và $\delta = k + a\gamma \bmod q$.

Với $x \in \{0,1\}^*$ và $\gamma, \delta \in Z_q$, việc xác minh được thực hiện bằng cách thực hiện các tính toán sau:

$$ver_K(x, (\gamma, \delta)) = true \Leftrightarrow h(x \,||\, \alpha^{\delta}\beta^{-\gamma} \bmod p) = \gamma.$$

Quan sát thấy mỗi thành phần trong số hai thành phần của chữ ký Schnorr là một phần tử của Z_q. Dễ dàng kiểm tra rằng $\alpha^{\delta}\beta^{-\gamma} \equiv \alpha^k \bmod p$ và do đó chữ ký Schnorr sẽ được xác minh.

Example 8.3

8.4.2 Thuật toán chữ ký số

Chúng ta sẽ trình bày các thay đổi được thực hiện trong hàm xác minh của Lược đồ chữ ký ElGamal trong đặc tả của DSA. DSA sử dụng một nhóm con có thứ tự q thuộc Z_p^*, cũng giống như Lược đồ chữ ký Schnorr. Trong DSA, khuyến nghị q là một số nguyên tố 224-bit và p là một số nguyên tố 2048-bit. Khóa trong DSA có cùng dạng như trong Lược đồ chữ ký Schnorr. Giả định rằng message sẽ được băm sử dụng SHA3-224 trước khi ký. Kết quả là một bản tóm tắt 224-bit được ký bằng một chữ ký 448-bit, và các tính toán được thực hiện trong Z_p và Z_q.

Trong Sơ đồ chữ ký ElGamal, giả sử chúng ta thay đổi "-" thành "+" trong định nghĩa của δ, do đó: $\delta = (x + a\gamma)k^{-1} \bmod (p - 1)$.

Dễ dàng nhận thấy rằng điều này thay đổi điều kiện xác minh như sau:

$$\alpha^x\beta^{\gamma} \equiv \gamma^{\delta} \pmod p \quad (8.3)$$

Bây giờ, α có bậc q, và β và γ là lũy thừa của α, nên chúng cũng có bậc q. Điều này có nghĩa là tất cả số mũ trong (8.3) có thể được rút gọn theo modulo q mà không ảnh hưởng đến tính đúng đắn của đồng dư. Vì x sẽ được thay thế bằng bản tóm tắt 224 bit trong DSA nên chúng ta sẽ giả sử rằng $x \in Zq$. Hơn nữa, chúng ta sẽ thay đổi định nghĩa của δ, sao cho $\delta \in Zq$, như sau: $\delta = (x + a\gamma)k^{-1} \bmod q$.

Coi $\gamma = \alpha^k \bmod p$. Giả sử chúng ta tạm thời xác định $\gamma' = \gamma \bmod q = (\alpha^k \bmod p) \bmod q$. Để ý $\delta = (x + a\gamma)k^{-1} \bmod q$ nên δ không đổi. Chúng ta có thể viết phương trình xác minh như sau: $\alpha^x\beta^{\gamma'} \equiv \gamma^{\delta} \pmod p$. (8.4)

Cryptosystem 8.4: Digital Signature Algorithm

Cho p là một số nguyên tố 2048-bit sao cho bài toán logarit rời rạc trong Z_p^* là một bài toán khó giải, và gọi số nguyên tố 224-bit q là ước của p-1. Gọi $\alpha \in Z_p^*$ là căn bậc q của p. Gọi $P = \{0, 1\}^*$ và $A = Z_q \, x \, Z_q$ và định nghĩa $K = \{(p, q, \alpha, a, \beta) : \beta \equiv \alpha^a \pmod p\}$, trong đó $0 \le a \le q - 1$. Các giá trị p, q, α, và β là khóa công khai, a là khóa bí mật.

Với $K = \{(p, q, \alpha, a, \beta)$ và số bí mật ngẫu nhiên k, $1 \le k \le q - 1$, định nghĩa:

$$sig_K(x, k) = (\gamma, \delta)$$

Trong đó $\gamma = (a^k \bmod p) \bmod q$ và $\delta = (SHA3\_224(x) + a\gamma)k^{-1} \bmod q$. (Nếu $\gamma = 0$ hoặc $\delta = 0$, giá trị ngẫu nhiên k sẽ được chọn lại.

Với $x \in \{0,1\}^*$ và $\gamma, \delta \in Z_q^*$, việc xác minh được thực hiện bằng cách thực hiện các tính toán sau:

$$e_1 = SHA3\_224(x)\,\delta^{-1} mod\ q,\ e_2 = \gamma\delta^{-1} mod\ q$$

$$ver_K(x, (\gamma, \delta)) = true \Leftrightarrow (\alpha^{e1}\beta^{e2} mod\ p) \bmod q = \gamma$$

Lưu ý rằng chúng ta không thể thay thế sự xuất hiện còn lại của γ bằng γ'. Bây giờ chúng ta tiến hành viết lại (8.4), bằng cách tăng cả hai vế lên lũy thừa δ^{-1} mod q (điều này đòi hỏi $\delta^{-1} \neq 0$). Chúng tôi có được những điều sau đây: $\alpha^{x\delta^{-1}}\beta^{\gamma'\delta^{-1}} \equiv \gamma \pmod p$ (8.5)

Bây giờ chúng ta có thể rút gọn cả hai vế của (8.5) cho modulo q, thu được kết quả sau:

$(\alpha^{x\delta^{-1}}\beta^{\gamma'\delta^{-1}} mod\ p) \bmod q \equiv \gamma'$ (8.6).

Mô tả đầy đủ về DSA được đưa ra dưới dạng Cryptosystem 8.4, trong đó chúng tôi đổi tên γ' thành γ và thay thế x bằng bản tóm tắt SHA3-224 (x). Lưu ý rằng nếu Alice tính giá trị $\delta \equiv 0 \pmod q$ trong thuật toán ký DSA, cô ấy nên tạo chữ ký mới với k ngẫu nhiên mới. Chúng ta nên chỉ ra rằng điều này khó có thể gây ra vấn đề trong thực tế: xác suất $\delta \equiv 0 \pmod q$ có thể ở mức 2^{-224}; vì vậy, xét về mọi ý định và mục đích, điều đó sẽ không bao giờ xảy ra.

Example 8.4

Khi DSA được đề xuất vào năm 1991, đã có một số lời chỉ trích được đưa ra. Một khiếu nại là quy trình lựa chọn của NIST không được công khai. Tiêu chuẩn này được Cơ quan An ninh Quốc gia (NSA) phát triển mà không có sự tham gia của ngành công nghiệp Hoa Kỳ. Bất kể giá trị của kế hoạch đạt được là gì, nhiều người vẫn phẫn nộ với cách tiếp cận "đóng cửa".

Trong số những lời chỉ trích kỹ thuật được đưa ra, nghiêm trọng nhất là kích thước của mô đun p ban đầu được cố định ở mức 512 bit. Nhiều người cho rằng không nên cố định kích thước mô đun mà có thể sử dụng kích thước mô đun lớn hơn nếu muốn. Để đáp lại những nhận xét này, NIST đã thay đổi mô tả tiêu chuẩn để cho phép có nhiều kích cỡ mô đun khác nhau.

8.4.3. Đường cong Elliptic DSA

Năm 2000, Thuật toán chữ ký số đường cong Elliptic (ECDSA) đã được phê duyệt là FIPS 186-2. Sơ đồ chữ ký này có thể được xem như một sự sửa đổi của DSA đối với việc thiết lập các đường cong elliptic. Chúng ta có hai điểm A và B trên đường cong elliptic xác định trên Z_p với một số nguyên tố p. Logarit rời rạc $m = log_A B$ là khóa bí mật. (Điều này tương tự với quan hệ $\beta \equiv \alpha^a \pmod p$ trong DSA, trong đó a là khóa bí mật.) Cấp của A là số nguyên tố lớn q. Việc tính toán chữ ký trước tiên bao gồm việc chọn một giá trị ngẫu nhiên k và tính toán kA (điều này tương tự như việc tính toán α^k trong DSA).

Đây là điểm khác biệt chính giữa DSA và ECDSA. Trong DSA, giá trị $\alpha^k \pmod p$ được giảm modulo q để tạo ra giá trị γ là thành phần đầu tiên của chữ ký (γ, δ). Trong ECDSA, giá trị tương tự là r, là tọa độ x của điểm kA trên đường cong elliptic, rút gọn modulo q. Giá trị *r* này là thành phần đầu tiên của chữ ký *(r, s)*.

Cuối cùng, trong ECDSA, giá trị *s* được tính từ *r, m, k* và message *x* theo cách giống hệt như δ được tính từ γ, *a, k* và message *x* trong DSA. Bây giờ chúng tôi trình bày mô tả đầy đủ về ECDSA dưới dạng Hệ thống mật mã 8.5.

Cryptosystem 8.5: Elliptic Curve Digital Signature Algorithm

Cho p là một số nguyên tố lớn và Ɛ là đường cong Elliptic định nghĩa trong Z_p. Gọi A là một điểm thuộc Ɛ có bậc q nguyên tố, sao cho bài toán Logarit rời rạc trong <A> không thể giải được. Gọi $P = \{0, 1\}^*$ và $A = Z_q \, x \, Z_q$ và định nghĩa

$K = \{(p, q, Ɛ, A, m, B) : B = mA$, trong đó $0 \leq m \leq q - 1$.

Các giá trị p, q, Ɛ, A, B là khóa công khai, m là khóa bí mật.

Với $K = \{(p, q, Ɛ, A, m, B)$ và số bí mật ngẫu nhiên $k, 1 \leq k \leq q - 1$, định nghĩa:

$$sig_K(x, k) = (r, s)$$

Trong đó $kA = (u, v), r = u \bmod q$ và $s = k^{-1}(SHA3\_224(x) + mr) \bmod q$. (Nếu $r = 0$ hoặc $s = 0$, giá trị ngẫu nhiên k sẽ được chọn lại.

Với $x \in \{0, 1\}^*$ và $r, s \in Z_q^*$, việc xác minh được thực hiện bằng cách thực hiện các tính toán sau:

$$w = s^{-1} \bmod q$$
$$i = w \times SHA3\_224(x) \bmod q$$
$$j = wr \bmod q$$
$$(u, v) = iA + jB$$
$$ver_K(x, (r, s)) = true \Leftrightarrow u \bmod q = r$$
