0.1 Mật mã trong đường cong elliptic

1. Sơ bộ

Alice muốn gửi một tin nhắn, thường được gọi là **bản rõ**, cho Bob. Để ngăn không cho kẻ nghe trộm Eve đọc được tin nhắn, cô đã mã hóa nó để lấy được **bản mã**. Khi Bob nhận được bản mã, anh ta sẽ giải mã nó và đọc tin nhắn. Để mã hóa tin nhắn, Alice sử dụng một **khóa mã hóa**. Bob sử dụng **khóa giải mã** để giải mã bản mã. Có hai loại mã hóa cơ bản.

Có hai loại mã hóa cơ bản.

- Mã hoá đối xứng: Trong mã hóa đối xứng, khóa mã hóa và khóa giải mã giống nhau, hoặc cái này có thể dễ dàng suy ra từ cái kia. Các phương pháp mã hóa đối xứng phổ biến bao gồm Tiêu chuẩn Mã hóa Dữ liệu (DES) và Tiêu chuẩn Mã hóa Nâng cao (AES, thường được gọi bằng tên ban đầu là Rijndael). Trong trường hợp này, Alice và Bob cần có một số cách thiết lập khóa. Ví dụ, Bob có thể gửi một người đưa tin cho Alice trước vài ngày. Sau đó, khi đến lúc gửi tin nhắn, cả hai sẽ có chìa khóa. Rõ ràng điều này là không thực tế trong nhiều tình huống.
- Mã hóa khóa công khai hoặc mã hoá không đối xứng Trong trường hợp này, Alice và Bob không cần phải liên hệ trước. Bob xuất bản một khóa mã hóa công khai, mà Alice sử dụng. Anh ta cũng có một khóa giải mã riêng cho phép anh ta giải mã các bản mã. Vì mọi người đều biết khóa mã hóa, nên không thể suy ra khóa giải mã từ khóa mã hóa. Hệ thống khóa công khai nổi tiếng nhất được biết đến là RSA và dựa trên khó khăn của việc tính các số nguyên thành số nguyên tố. Một hệ thống nổi tiếng khác là do ElGamal và dựa trên độ khó của bài toán logarit rời rạc.

Nói chung, các hệ thống khóa công khai chậm hơn các hệ thống đối xứng tốt. Do đó, người ta thường sử dụng hệ thống khóa công khai để thiết lập một khóa sau đó được sử dụng trong hệ thống đối xứng. Việc cải thiện tốc độ là rất quan trọng khi lượng lớn dữ liệu đang được truyền.

2. Trao đổi khoá **Elliptic Diffie–Hellman (**

Mô hình trao đổi khóa Elliptic Diffie-Hellman tương tự mô hình trao đổi khóa Diffie-Hellman.

Trao đổi khóa Elliptic Diffie-Hellman cũng dựa vào nguyên lý của bài toán logarit rời rạc nhưng áp dụng trên đường cong elliptic. Mô hình này dùng để thiết lập một hoặc nhiều khóa quy ước chung giữa hai đối tác A và B.

Các thao tác để trao đổi khóa được thực hiện như sau:

• Một bên tin cậy chọn ra một số nguyên tố lớn, đường cong elliptic $E(Fp)$ và điểm $P \in E(F_p)$
• Alice chọn một giá trị n_A ngẫu nhiên. Alice tính giá trị điểm $Q_A = n_A P$
• Bob chọn một giá trị n_B ngẫu nhiên. Alice tính giá trị điểm $Q_B = n_B P$
• Alice và Bob trao đổi Q_A và Q_B cho nhau sau đó tính $n_A Q_B$ và $n_B Q_A$
• Giá trị $G = n_A \times Q_B = (n_A n_B) \times P = n_B \times Q_A$ chính là giá trị bí mật được quy ước chung.

Ví dụ: Alice và Bob quyết định sử dụng Diffie – Hellman trên đường cong elliptic với số nguyên tố, đường cong và điểm:

$$p = 3851, E : Y^2 = X^3 + 324X + 1287, P = (920, 303) \in E(\mathbb{F}_{3851}). \tag{1}$$

Alice và Bob chọn $n_A = 1194$ và $n_B = 1759$

$$\begin{array}{ll} \text{Alice computes} & Q_A = 1194P = (2067, 2178) \in E(\mathbb{F}_{3851}), \\ \text{Bob computes} & Q_B = 1759P = (3684, 3125) \in E(\mathbb{F}_{3851}). \end{array}$$

Alice gửi Q_A cho Bob và ngược lại:

$$\begin{array}{ll} \text{Alice computes} & n_A Q_B = 1194(3684, 3125) = (3347, 1242) \in E(\mathbb{F}_{3851}), \\ \text{Alice computes} & n_B Q_A = 1759(2067, 2178) = (3347, 1242) \in E(\mathbb{F}_{3851}). \end{array}$$

Bob và Alice đã trao đổi điểm bí mật $(3347, 1242)$. Như sẽ được giải thích trong Chú thích 5.20, họ nên loại bỏ tọa độ y và chỉ coi giá trị $x = 3347$ là giá trị được chia sẻ bí mật.

Một cách để Eve phát hiện ra bí mật của Alice và Bob là giải bài toán logarit rời rạc trên đường cong eliiptic $nP = Q_A$, vì nếu Eve có thể giải được bài toán này, thì cô ấy biết n_A và có thể sử dụng nó để tính $n_A Q_B$. Tuy nhiên để giải bài toán này rất khó và tốn thời gian.

Định nghĩa: Gọi $E(F_p)$ là một đường cong elliptic trên trường hữu hạn và $P \in E(Fp)$. Bài toán trao đổi khoá Elliptic Diffie–Hellman là bài toán tính giá trị $n_1 n_2 P$ từ các giá trị $n_1 P$ và $n_2 P$.

Ghi chú: Trao đổi khoá Elliptic Diffie–Hellman yêu cầu Alice và Bob trao đổi điểm trên một đường cong elliptic, nghĩa là trao đổi cả hai toạ độ$Q = (x_Q, y_Q)$ trong đó $x_Q, y_Q \in F_Q$. Tuy nhiên, vì hai người biết giá trị của A, B trong phương trình đường cong elliptic$Y^2 = X^3 + AX + B$ nên ta chỉ cần trao đổi giá trị của x_Q.

Khi đó, hai người sẽ giải ra được 2 nghiệm của y rồi sẽ chọn 1 trong hai giá trị. Người thực hiện là Bob

+ Nếu chọn đúng, đó là giá trị đang sử dụng là Q_A

+ Nếu chọn sai, đó là giá trị đang sử dụng là $-Q_A$

$\Longrightarrow$ Trong mọi trường hợp: Alice và Bod đang sử dụng

$$\pm n_A \times Q_B = \pm(n_A n_B) \times P = \pm n_B Q_A$$

3. Hệ thống mã khoá công khai Elliptic ElGamal

Cách tạo, mã hóa và giải mã khóa Elliptic ElGamal được định nghĩa như sau:

• Một bên tin cậy chọn và đưa ra một số nguyên tố p (lớn), một đường cong elliptic E trên F_p và một điểm P trong $E(F_p)$.

• Alice chọn một khoá riêng tư n_A và tính $Q_A = n_A P$. Q_A là khoá công khai của Alice.

• Bob chọn bản rõ $M \in E(F_q)$. Anh ta chọn một số nguyên k làm khóa tạm thời của mình và tính:

$$C_1 = kP \qquad \text{and} \qquad C_2 = M + kQ_A$$

Bob gửi hai điểm (C_1, C_2) cho Alice

• Alice tính:

$$C_2 - n_A C_1 = (M + kQ_A) - n_A(kP) = M + k(n_A P) - n_A(kP) = M$$

0.2 Thuật toán phân tích nhân tử đường cong elliptic của Lenstra

0.2.1 Phương pháp phân tích nhân tử $p - 1$ của Pollard

Đầu vào: Số nguyên N có thể phân tích thành các thừa số

1. Đặt $a = 2$ (Hoặc bất kì số nào thuận tiện cho việc tính toán)
2. Vòng lặp $j = 2, 3, 4...$ lên đến một giới hạn nhất định
3. Đặt $a = a^j \mathrm{mod} N$
4. Tính $d = \gcd(a - 1, N)$ (gcd là ước chung lớn nhất)
5. Nếu $1 < d < N$ thì trả về d là một thừa số của N
6. Nếu không thì tăng j và thực hiện lại bước 2

Sau khi thực hiện thuật toán ta có được số $d, N = d * a$. ta đã phân tích được số N.

Phương pháp của Pollard chứng minh rằng có những mô-đun RSA không an toàn mà thoạt nhìn có vẻ là an toàn. Chúng ta được trình bày với một số $N = pq$ và nhiệm vụ của chúng ta là xác định các thừa số nguyên tố p và q.

Thuật toán phân tích nhân tử đường cong elliptic của Lenstra

Đầu vào: Số nguyên N có thể phân tích thành các thừa số

1. Chọn các giá trị ngẫu nhiên A, a, b modulo N
2. Đặt $P = (a, b)$ và$B \equiv b^{2\backsim} a^3 - a.A(\mathrm{mod} N)$

Gọi E là đường cong elliptic $E : Y^2 = X^3 + AX + B$

3. Vòng lặp $j = 2, 3, 4, ...$ lên đến một giới hạn nhất định
4. Đặt $Q \equiv jP(\mathrm{mod} N)$ và $P = Q$
5. Nếu bước 4 không tính được, ta tìm được$d > 1$ với d là thừa số của N
6. Nếu $d < N$, trả về d
7. Nếu $d = N$, quay về bước 1 chọn các điểm và đường cong mới
8. Nếu không thì tăng j và thực hiện lại bước 2