CHƯƠNG 3

MỘT SỐ BÀI TOÁN SỐ HỌC CƠ SỞ

Tài liệu: Handbook of Applied Cryptography

Katz Jonathan, Menezes Alfred J, Van Oorschot Paul C, Vanstone Scott A

CRC Press

Nội dung

- Phân tích số tự nhiên thành nhân tử
- Bài toán RSA
- Bài toán thặng dư bậc hai
- Tìm căn bậc hai modulo n
- Bài toán Logarit rời rạc
- Bài toán Diffie-Hellman

Bài toán phân tích thành nhân tử

Định nghĩa:

Phân tích số tự nhiên n ra thành nhân tử là tìm các nhân tử nguyên tố p_i đôi một khác nhau sao cho

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$$

Chiến lược chung tìm nhân tử

- Áp dụng phép chia thử để tìm các ước số nhỏ hơn một số nguyên tố giới hạn b_1
- Áp dụng thuật toán của Pollard đề tìm nhân tử trong giới hạn $b_2 \geq b_1$
- Áp dụng thuật toán đường cong Elliptic để tìm nhân tử trong giới hạn $b_3 \geq b_2$
- Áp dụng thuật toán sàng bậc hai để tìm nhân tử

Số tự nhiên trong giới hạn p-nguyên tố

Định nghĩa:

Với p là một số nguyên tố. Số tự nhiên n gọi là p-nguyên tố giới hạn nếu mọi ước số nguyên tố của n đều $\leq p$.

Ví dụ:

- 50 là 5-nguyên tố giới hạn vì $50 = 2^1 5^2$

Thuật toán rho của Pollard tìm nhân tử

INPUT: hợp số n không phải là lũy thừa của một số nguyên tố

OUTPUT: ước số d không tầm thường của $n, (1 < d < n)$

1. $a \leftarrow 2, b \leftarrow 2$
2. *For i = 1,2,... Do*

   $a \leftarrow a^2 + 1 \, mod \, n, b \leftarrow b^2 + 1 \, mod \, n, \, b \leftarrow b^2 + 1 \, mod \, n$

   $d = gcd(a - b, n)$

   Nếu $1 < d < n$ thì thông báo kết quả d

   Nếu $d = n$ thì thông báo thuật toán không tìm được ước của n

Thuật toán sàng bậc hai tìm nhân tử

INPUT: hợp số n không phải là lũy thừa của một số nguyên tố

OUTPUT: ước số d không tầm thường của $n, (1 < d < n)$

1. Chọn t số $S = \{p_1, p_2, \dots, p_t\}$, ở đó $p_1 = -1$, $p_j (j \geq 2)$ là các số đầu tiên theo thứ tự trong dãy số nguyên tố mà n *là thặng dư bậc hai của* p_j
2. Tính $m = [\sqrt{n}]$
3. Lựa chọn $t + 1$ cặp:

   $\{(a_i, b_i) \mid a_i = (x + m)^2 \equiv b_i (mod\ n), x = 0, \pm 1, \pm 2, \dots\}$

   theo các bước sau đây:

Thuật toán sàng bậc hai tìm nhân tử

For $i = 1, \ldots, t+1$

3.1 $b = q(x) = (x+m)^2 - n$, *sử dụng phép chia thử để kiểm tra xem b có là* p_t *- nguyên tố giới hạn không. Nếu không thì chọn lại và lặp lại bước này.*

3.2 nếu b là p_t *- nguyên tố giới hạn, giả sử* $b = \Pi_{j=1}^{t} p_j^{e_{ij}}, a_i \leftarrow (x+m), b_i \leftarrow b, v_i = (v_{i1}, v_{i2}, \ldots, v_{it})$ *với* $v_{ij} = e_{ij} \bmod 2$

4. Tìm tập $\phi \neq T \subseteq \{1,2, \ldots, t+1\}$ sao cho $\sum_{i \in T} v_i = 0$

5. Tính $x = \Pi_{i \in T} a_i \bmod n$

6. For $i=1,\ldots,t$ tính $l_j = {}^{(\sum_{i \in T} e_{ij})}/_{2}$

Thuật toán sàng bậc hai tìm nhân tử

7. Tính $y = \Pi_{j=1}^{t} p_j^{l_j} \; mod \; n$

8. Nếu $x = \pm y \; (mod \; n)$ *thì quay lại bước 4 tìm tập T khác và thực hiện theo các bước.*

9. *Thông báo kết quả* $d = \gcd(x - y, n)$

Bài toán RSA

Định nghĩa:

Bài toán RSA là: Cho trước số tự nhiên n là tích của hai số nguyên tố lẻ khác nhau p và q. Với số tự nhiên e sao cho $gcd\big(e,(p-1)(q-1)\big)=1$ và số c, hãy tìm m thỏa mãn $m^e \equiv c(mod\ n)$.

Chú ý:

- m là một căn bậc e modulo n
- Bài toán RSA tương đương thời gian đa thức với bài toán phân tích thành nhân tử

Bài toán thặng dư bậc hai

Định nghĩa:

Bài toán thặng dư bậc hai (QRP) là cho trước một hợp số lẻ n và $a \in J_n = \{k \in \mathbb{Z}_n^* | \left(\frac{k}{n}\right) = 1\}$. Hỏi a có là thặng dư modulo bậc hai của n hay không?

Nghĩa là có tồn tại x để $x^2 \equiv a \ (mod\ n)$?

Chú ý:

- Nếu p là nguyên tố thì đã có thuật toán hiệu quả tìm các thặng dư bậc hai modulo n
- Bài toán QRP tương đương thời gian đa thức với bài toán phân tích thành nhân tử

Logarit trong $\mathbb{Z}_n^*$

Định nghĩa:

Gọi G là nhóm $\mathbb{Z}_n^*$ cyclic cấp $n-1$ của $\mathbb{Z}_n$ có phần tử sinh α. *Ta gọi logarit của* β cơ số α, ký hiệu $log_\alpha \beta$, là số tự nhiên duy nhất x, $1 \leq x \leq n-1$ sao cho $\beta = \alpha^x$.

Ví dụ:

- $\mathbb{Z}_{23}^*$ là nhóm cyclic cấp 22. Xét phần tử sinh là 5 có $log_5 12 = 20$ trong $\mathbb{Z}_{23}^*$ vì $5^{20} \equiv 12 \ (mod\ 23)$

Bài toàn logarit rời rạc

Định nghĩa:

Bài toán logarit rời rạc (DLP) là: Cho trước số nguyên tố p và phần tử sinh α của $\mathbb{Z}_p^*$. *Với* $\beta \in \mathbb{Z}_n^*$, tìm x, $1 \leq x \leq p-1$ sao cho $\alpha^x \equiv \beta \ (mod\ p)$.

Chú ý:

- Độ khó của bài toàn logarit không phụ thuộc vào cơ số
- Thuật toán cho tìm logarit là tính các lũy thừa của cơ số $\alpha^0, \alpha^1, \alpha^2, \ldots$

Bài toàn Diffie-Hellman

Định nghĩa:

Bài toán Diffie-Hellman (DHP) là:

Cho trước số nguyên tố p, phần tử sinh α của $\mathbb{Z}_p^*$ và các phần tử $\alpha^a \ (mod\ p), \alpha^b \ (mod\ p)$. Hãy tìm $\alpha^{ab} \ (mod\ p)$?

Chú ý:

- $\alpha^{ab} = (\alpha^a)^b$, nên giải bài toán Diffie-Hellman là giải bài toàn logarit rời rạc
- Bài toán DHP tương đương thời gian đa thức với bài toán DLP