**CƠ SỞ TOÁN HỌC CỦA RSA**

**1. Tính chất số nguyên tố và bài toán phân tích thừa số**

Thuật toán RSA dựa trên tính chất rằng việc nhân hai số nguyên tố lớn rất dễ, nhưng phân tích một số lớn thành thừa số nguyên tố rất khó. Điều này tạo nên tính bảo mật của RSA.

Ví dụ: Nếu ta có hai số nguyên tố lớn p và q, tích của chúng là: n = p × q Việc tính n rất dễ, nhưng nếu chỉ biết n mà không biết p, q, việc phân tích n thành p và q rất khó khi n đủ lớn.

**2. Hàm số Euler và định lý Euler**

Hàm số Euler φ(n) của một số nguyên n là số lượng số nguyên dương nhỏ hơn n và nguyên tố cùng nhau với n.

Công thức tính hàm Euler cho số nguyên tố: - Nếu n là số nguyên tố: φ(n) = n - 1 - Nếu n = p × q với p, q là số nguyên tố: φ(n) = (p - 1) × (q - 1)

Định lý Euler:

Định lý Euler phát biểu rằng nếu a và n là hai số nguyên tố cùng nhau, thì: a^φ(n) ≡ 1 (mod n) Nghĩa là khi nâng lũy thừa a lên bậc φ(n), kết quả sẽ đồng dư với 1 theo modulo n.

Ví dụ: Giả sử n = 10, khi đó φ(10) = 4. Nếu chọn a = 3 (số nguyên tố cùng nhau với 10), ta có: 3^4 = 81 ≡ 1 (mod 10) Định lý Euler là nền tảng giúp tính toán nghịch đảo modulo trong RSA, đảm bảo rằng khi chọn số mũ công khai e và số mũ bí mật d, ta có: (M^e)^d ≡ M (mod n) Điều này giúp giải mã thông điệp chính xác.

**3. Định lý số dư Trung Hoa**

Định lý số dư Trung Hoa (Chinese Remainder Theorem - CRT) giúp giải hệ phương trình đồng dư khi các modulo là nguyên tố cùng nhau từng đôi một.

Phát biểu định lý:

Giả sử có hệ phương trình đồng dư: x ≡ a1 (mod m1) x ≡ a2 (mod m2) ... Nếu m1, m2, ..., mk là các số nguyên tố cùng nhau từng đôi một, thì hệ phương trình có nghiệm duy nhất modulo M, trong đó: M = m1 × m2 × ... × mk

Ví dụ:

Tìm x thỏa mãn: x ≡ 2 (mod 3) x ≡ 3 (mod 5) x ≡ 2 (mod 7) Tính M = 3 × 5 × 7 = 105. Tính từng phần: M1 = 105 / 3 = 35 → Nghịch đảo 35 mod 3 là 2. M2 = 105 / 5 = 21 → Nghịch đảo 21 mod 5 là 1. M3 = 105 / 7 = 15 → Nghịch đảo 15 mod 7 là 1. Tính tổng: x = (2 × 35 × 2) + (3 × 21 × 1) + (2 × 15 × 1) mod 105 x = (140 + 63 + 30) mod 105 x = 233 mod 105 x = 23 Vậy x = 23 là nghiệm của hệ phương trình.

Trong RSA, định lý số dư Trung Hoa giúp tối ưu hóa quá trình giải mã bằng cách làm việc với các modulo nhỏ hơn thay vì modulo lớn.

**VÍ DỤ MINH HỌA**

**1. Ví dụ mã hóa và giải mã với số nhỏ**

Giả sử chọn hai số nguyên tố nhỏ: p = 61, q = 53

Tính n: n = p × q = 61 × 53 = 3233

Tính φ(n): φ(n) = (p - 1) × (q - 1) = 60 × 52 = 3120

Chọn e sao cho 1 < e < φ(n) và gcd(e, φ(n)) = 1: e = 17

Tìm d sao cho: d × e ≡ 1 (mod φ(n)) d × 17 ≡ 1 (mod 3120) d = 2753

Khóa công khai: (n = 3233, e = 17) Khóa bí mật: (n = 3233, d = 2753)

Mã hóa thông điệp M = 65: C = M^e mod n = 65^17 mod 3233 = 2790

Giải mã: M = C^d mod n = 2790^2753 mod 3233 = 6