Khoa Khoa học & Kỹ thuật máy tính
Trường ĐH Bách Khoa TP.HCM

Cryptography and Network Security
Tóm tắt giải thuật RSA

Hieu Nguyen

Ngày 18 tháng 9 năm 2016

Thuật toán RSA được đề xuất bởi Rivest, Shamir và Adleman.

Gọi p và q là hai số nguyên tố lớn ngẫu nhiên phân biệt.

Modun n là tích của hai số nguyên tố này:

$$n = pq$$

Hàm phi Euler (Euler's totient function) của n cho bởi:

$$\phi(n) = (p-1)(q-1)$$

Chọn một số 1<e<$\phi(n)$ sao cho:

$$gcd(e, \phi(n)) = 1$$

và tính d với công thức:

$$d = e^{-1} mod\, \phi(n)$$

Việc mã hóa được thực hiện bằng cách tính:

$$C = M^e \, (mod\, n)$$

với M là plaintext, C là ciphertext tương ứng của M.
Từ C, M được tính bằng công thức:

$$M = C^d \, (mod \, n)$$

Ví dụ:
Chúng ta xây dựng một hệ thống mã hóa RSA như sau: Cho p = 11, q = 13, và tính

$n = pq = 11.13 = 143$

$\phi(n) = (p-1)(q-1) = 10.12 = 120$

Số mũ công khai e được chọn thỏa $1 < e < \phi(n)$ và $gcd(e, \phi(n)) = 1$

Chọn $e = 17$ thỏa ràng buộc. Tính d sử dụng công thức:

$d = e^{-1} mod \, \phi(n) = 17^{-1} mod \, 120 = 113$

(Sử dụng thuật toán Euclid mở rộng hay bất cứ thuật toán nào khác để tính phần tử nghịch đảo modun)

Người dùng công bố số mũ công khai e và modun n: (e,n) = (13,143), và giữ bí mật các giá trị sau: d = 113, p = 11, q = 13.

Tiến trình mã hóa/giải mã tiêu biểu được thực hiện như sau:

Mã hóa: $M = 50$

$C = M^e \, (mod \, n)$

$C = 50^{17} \, (mod \, 143) = 85$

Giải mã: $C = 85$

$M = C^d \, (mod \, n)$

$M = 85^{113} \, (mod \, 143) = 50$