**Tìm hiểu về giải thuật mã hóa khóa công khai RSA**

1. Phòng chống:

+ Độ an toàn của hệ thống RSA dựa trên 2 vấn đề của toán học:

* Bài toán phân tích số nguyên tố các số nguyên lớn
* Bài toán RSA.

+ Nếu 2 bài toán trên là khó thì không thể thực hiện được việc phá mã toàn bộ đối với RSA. Phá mã một phần phải được ngăn chặn bằng các phương pháp chuyển đổi bản rõ an toàn. Bài toán RSA là bài toán tính căn bậc e moddun n: tìm số m sao cho pow(m,e) = c mod n, trong đó (e,n) chính là khóa công khai và c là bản mã.

+ Hiện nay phương pháp triển vọng nhất giải bài toán này là phân tích n ra thừa số nguyên tố. Khi thực hiện điều này, kẻ tấn công sẽ tìm ra số mũ bí mật d từ khóa công khai và có thể giải mã theo đúng quy định của thuật toán. Nếu kẻ tấn công tìm được 2 số nguyên tố p và q sao cho n=p.q thì có thể dễ dàng tìm được giá trị (p-1)(q-1) và qua đó xác định d và e.

+ Vì vậy: Ta cần có các biện pháp phòng chống:

* Kích thước khóa của RSA:
* Kích thước nhỏ hơn 1024 bit được coi là không an toàn do tốc độ các hệ thông máy tính tăng nhanh.
* Khuyến nghị dung khóa >= 2048 bits với các ứng dụng mật mã dân sự hiện nay.
* Tương lai nên dùng khóa >= 3072 bits
* Yêu cầu với các tham số sinh khóa p và q:
* Các số nguyên tố p và q phải được chọn sao cho việc phân tích n (n=pq) là không khả thi về mặt tính toán.
* p và q nên có cùng độ lớn và phải là các số đủ lớn
* Hiệu số p-q không nên quá nhỏ, do nếu quá nhỏ tức p~q và p ~ sqrt(n) -> chọn các số nguyên tố ở gần sqrt(n) và thử nhiều lần
* Nếu p và q được chọn ngẫu nhiên và p-q đủ lớn, khả năng hai số này bị phân tích từ n giảm đi
* Sử dụng số mũ mã hóa (e):
* Khi sử dụng số mũ mã hóa ( e ) nhỏ, chẳng hạn e=3 có thể tăng tốc độ mã hóa
* Kẻ tấn công có thể nghe trộm và lấy được bản mã, từ đó phân tích bản mã để khôi phục bản rõ. Do số mũ nhỏ nên chi phí cho phân tích/vét cạn không quá lớn
* Vì vậy: Sử dụng số mũ e lớn. Và Thêm chuỗi ngẫu nhiên vào khối rõ trước khi mã hóa.
* Sử dụng số mũ giải mã (d ):
* Khi sử dụng số mũ giải mã (d) nhỏ, có thể tăng tốc độ giải mã
* Nếu d nhỏ và gcd(p-1, q-1) cũng nhỏ thì d có thể tính được tương đối dễ dàng từ khóa công khai (n,e)
* Vì vậy: Sử dụng số mũ d đủ lớn