**Mã hóa Không Đối Xứng**

**Asymmetric Cryptography – RSA**

**Ý tưởng chính về mã hóa không đối xứng**

Initial data –(key1)-- 🡪 Encoded data ---(key2) 🡪 Initial data

Trong đó: key1 khác key2

**Giới thiệu về mã hoá không đối xứng RSA**

Thuật toán được Ron Rivest, Adi Shamir và Len Adleman mô tả lần đầu tiên vào năm 1977 tại Học viện Công nghệ Massachusetts (MIT). Tên của thuật toán lấy từ 3 chữ cái đầu của tên 3 tác giả.

Trong mật mã học, **RSA** là một thuật toán mật mã hóa khóa công khai. Đây là thuật toán đầu tiên phù hợp với việc tạo ra chữ ký điện tử đồng thời với việc mã hóa. Nó đánh dấu một sự tiến bộ vượt bậc của lĩnh vực mật mã học trong việc sử dụng khóa công cộng. RSA đang được sử dụng phổ biến trong thương mại điện tử và được cho là đảm bảo an toàn với điều kiện độ dài khóa đủ lớn. (Wiki)

**Giải thuật RSA mức đơn giản**

Gọi N là số lượng mã được hỗ trợ mã hóa và giải mã, thường là số không nbguye6n tố (hợp số) thí dụ: N= 77

|  |  |  |
| --- | --- | --- |
| **Bước** | **Tiến hành** | **Nhận xét** |
| 1 | Chọn 2 số nguyên P, Q | Thí dụ P= 7, Q= 11 |
| 2 | Tính N= P\*Q | N là số lượng ký hiệu được hỗ trợ mã hóa/ giải mã (N=77) |
| 3 | Tìm pN = (P-1)\*(Q-1) | pN là hợp số |
| 4 | Chọn E là số nguyên tố < pN. Thí dụ: E = 13 |  |
| 5 | Chọn D sao cho (D\*E) mod pN 🡪 1, thí dụ D=37 |  |

**Công thức Mã hóa và giải mã**

Gọi mã ban đầu là C1, mã đã mã hóa là C2.  C2 = (C1E)mod N , C = (C2’D)mod N

Thí dụ: C1 = 5, C2 = 513 mod 77 = 26 , C1 = 2637 mod 77 = 5

Cặp (E,N) được gọi là public key, cặp (D,N) được gọi là private key.

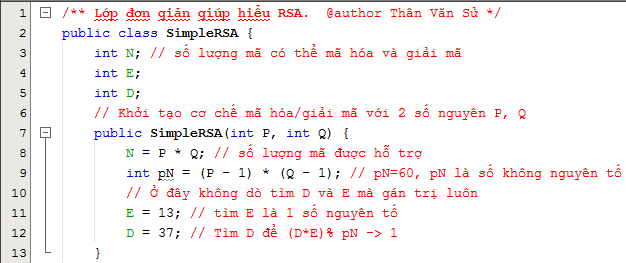
**Nhận xét chung**

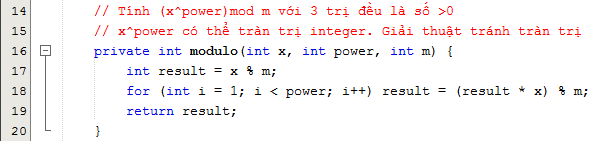
1. Với N= 77, có nhiều cặp số P,Q thỏa P\*Q=N nhưng chỉ có cặp số (7,11) được giới thiệu trong bảng trên mới có được đặc điểm giúp mã hóa và giải mã.
2. Với N nhỏ, người ta có thể dò tìm các trị E vả D 🡪 Bảo mật kém.
3. Thực tế, các trị P, Q, N N là những số cực ký lớn, P, Q có thể là số nguyên hệ 10 dài trên 150 ký số và N dài trên 300 ký số. Vì vậy, việc dò tìm các số E và D trở nên cực kỳ khó khăn cho các hacker.
4. Vì public key và prvate key dài không thể nhớ nên chúng thường được để trong tập tin.

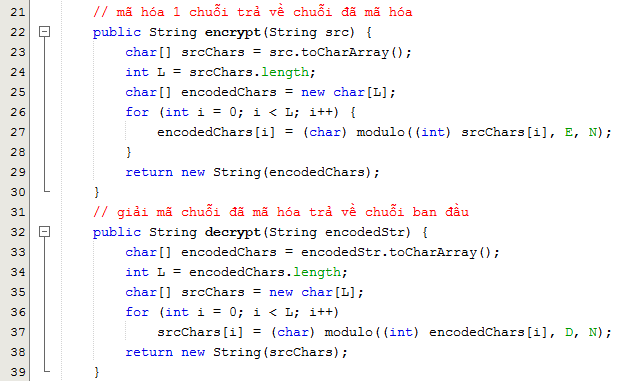
Kiến trúc của bài tập

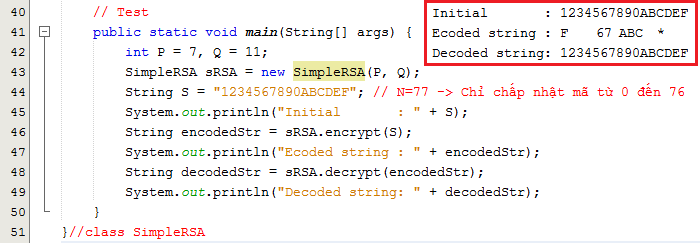
|  |  |
| --- | --- |
|  | Hai file chứa key  Chương trình sinh keys  Lớp có công cụ mã hóa  Lớp giúp tìm hiểu mã hóa RSA |

**Code mẫu cho tình huống N= 77, P=7, Q=11**









**Sử dụng Giải thuật RSA trong thư viện java.security**

