**BÀI TẬP MÔN**

**CƠ SỞ AN TOÀN THÔNG TIN**

**Chủ đề:** Thuật toán mã hóa Rabin

**Giảng viên:** Đỗ Xuân Chợ

**Sinh viên:** Trần Văn Khải

**Mã SV :** B14DCAT241

**Tổ Thực Hành:** 1

**Nhóm:** 2

**Câu 1**: Trình bày mã hóa, giải mã của thuật toán Rabin.

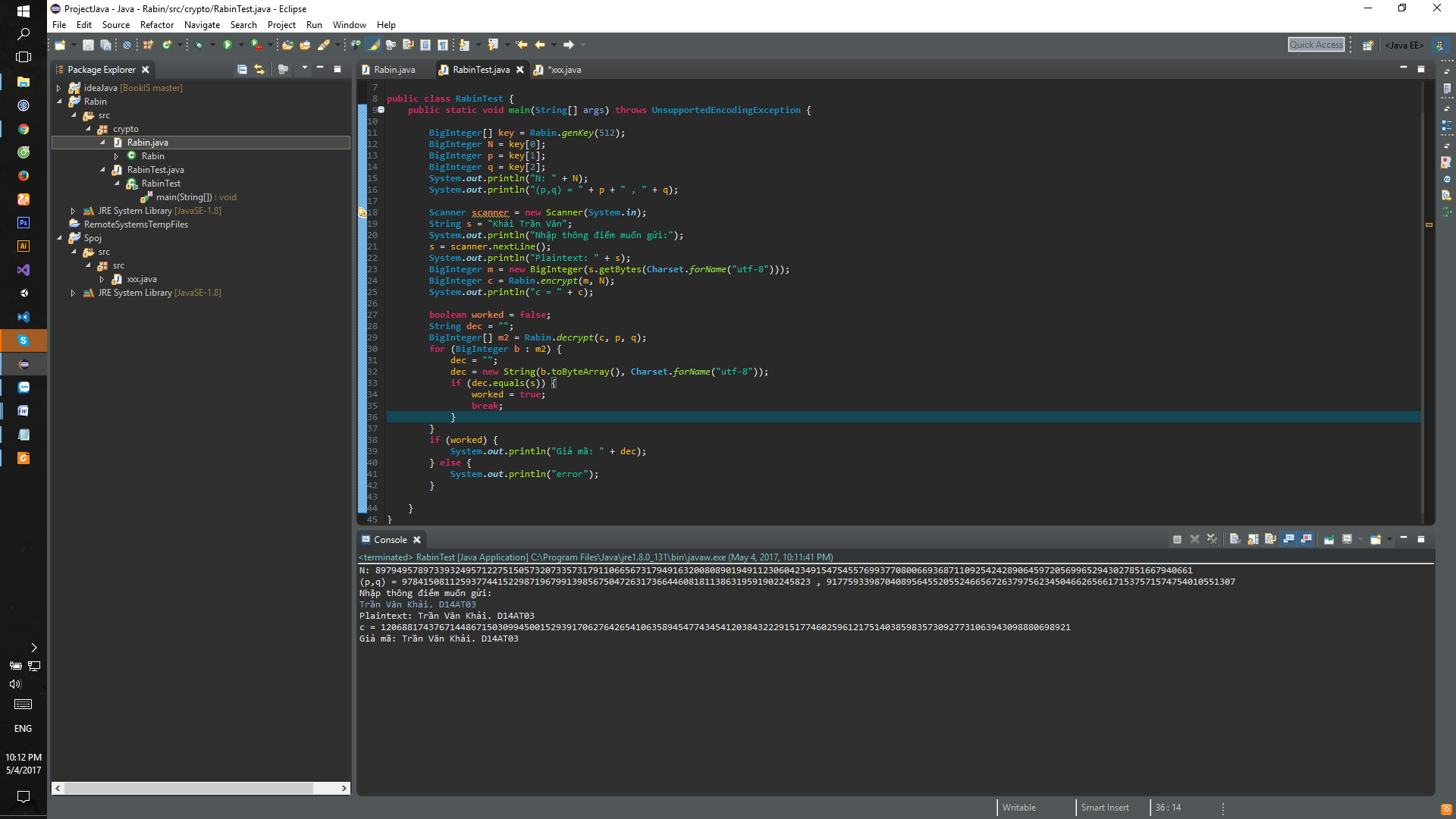
* Tạo khóa:
  + Mỗi bên tạo 1 khóa công khai và 1 khóa bí mật tương ứng.
    - Tạo 2 số nguyên tố ngẫu nhiên lớn khác nhau p và q. p gần bằng q.(p ≡ q ≡ 3 mod 4)
    - Tính n = p\*q
    - Ta có khóa công khai là n và khóa bí mật là (p,q).
* Mã hóa:
  + Nhận khóa công khai đã được xác thực của bên A là: n.
  + Ta gọi thông điểp mà bên B muốn gửi cho A là: m
  + Tính c = m^2 mod n
  + Gửi c cho A.
    - Pp
* Giải mã: Sau khi A nhân được thông điệp đã được mã hóa của B. A có khóa bí mật (p,q). Chúng ta thực hiện tính lần lượt:
  + M1’ = C(p + 1)/4 mod p
  + M2’ = (*p* - *C*(*p*+ 1)/4) mod *p*
  + M3’ = C(q + 1)/4 mod q
  + M4’ = (*q* - *C*(*q* + 1)/4) mod *q*
    - * Sau đó chọn số a,b sao cho:
        + a = *q*(*q*-1 mod *p*)
        + b = *p*(*p*-1 mod *q*)
      * Ta được 4 phương trình tương ứng:
  + M1 = (am1 + bm3) mod n
  + M2= (am1 + bm4) mod n
  + M3= (am2 + bm3) mod n
  + M4= (am2 + bm4) mod n
    - * Chúng ta sẽ được 4 kết quả sau khi giải mã. Nhưng chỉ có M1,M2,M3, hoặc M4 là bản rõ. Bằng cách quan sát chúng ta có thể nhận ra đâu là thông điệp ban đầu khá đơn giản.

**Câu 2**: Ưu điểm và nhược điểm của thuật toán.

* Ưu điểm:
  + Tính bảo mật cao. Đã được chứng minh.
  + Rabin nhanh hơn nhiều so với RSA.
* Nhược điểm:
  + Vì khi giả mã cần thực hiển cả 4 phương trình nên sẽ cho nhiều hơn 1 kết quả về bản rõ. Gây khó khăn cho người nhận.

**Câu 3:**

Demo:



GitHub: <https://github.com/khaitranvan96kt/RabinKTVJava.git>

Google Drive: <https://drive.google.com/drive/folders/0BzCm-V8P3tr9NGIwYl9RYkwycjg?usp=sharing>