Bài tập lập trình 4

Mục đích của bài tập này là phá hệ mã RSA khi modun N được sinh không đúng.

Thông thường, các số nguyên tố trong modun RSA được sinh một cách độc lập. Tuy nhiên, giả sử một lập trình viên quyết định sinh số nguyên tố đầu tiên p bằng cách chọn số ngẫu nhiên R và tìm số nguyên tố gần số ngẫu nhiên này. Số nguyên tố thứ hai q được sinh bằng cách tìm số ngẫu nhiên nguyên tố cũng gần với R. Ta chỉ ra rằng modun RSA $N = p \cdot q$ dễ phân tích thành thừa số nguyên tố trong trường hợp này.

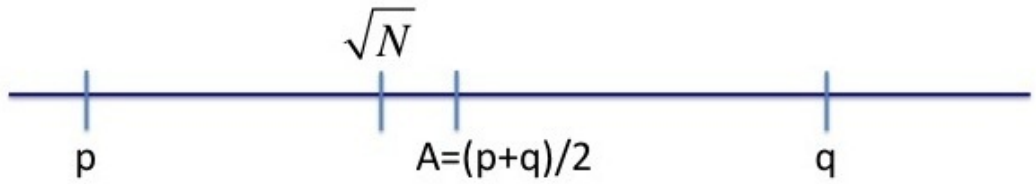
Giả sử bạn có hợp số N và biết rằng N là tích của hai số nguyên tố p và q khá gần nhau. Cụ thể, p và q thoả mãn

$$|p-q| < 2 \cdot N^{1/4} \tag{1}$$

Mục đích của bạn là phân tích thừa số cho N.

Xét A là giá trị trung bình của hai số nguyên tố, tức là $A = (p+q)/2$. Do p và q là lẻ, ta biết rằng $p+q$ chẵn và do đó A là một số nguyên.

Để có thừa số của N, đầu tiên ta quan sát rằng với điều kiện (1), giá trị $\sqrt{N}$ rất gần với A. Đặc biệt, $A - \sqrt{N} < 1$ như chỉ ra trong Câu hỏi 3 dưới đây. Nhưng vì A là số nguyên, làm tròn $\sqrt{N}$ tới giá trị nguyên gần nhất sẽ cho ta giá trị của A; cụ thể, $A = \lceil \sqrt{N} \rfloor$. Về mặt hình ảnh, các số $p, q, \sqrt{N}$ và A có thứ tự như sau:



Do A là điểm chính giữa p và q, có một số nguyên x thoả mãn $p = A - x$ và $q = A + x$. Nhưng vậy thì

$$N = p \cdot q = (A-x)(A+x) = A^2 - x^2$$

và ta có $x = \sqrt{A^2 - N}$. Bây giờ, cho x và A ta có thể phân tích thừa số của p và q vì $p = A - x$ và $q = A + x$.

Trong các thử thách trong các câu hỏi sau đây, bạn sẽ phân tích modun đưa ra dùng phương pháp mô tả ở trên. Bạn nên dùng thư viện có hỗ trợ tính toán số học với độ chính xác lớn và hỗ trợ tính căn bậc hai. Trong Python bạn có thể dùng thư viện gmpy2. Trong C bạn có thể dùng GMP.

1 Câu hỏi 1

Thử thách phân tích thừa số #1: Modun N dưới đây là tích của hai số nguyên tố p và q trong đó $|p-q| < 2 \cdot N^{1/4}$. Hãy phân tích thừa số nguyên tố của N.

```
N = 179769313486231590772930519078902473361797697894230657273430081157 \
    732675805505620686985379449212982959585501387537164015710139858647 \
    478337786069255834975410851965916151280575759407526350074759352887 \
    710823649949940771895617054361149474865046711015101563940680527547 \
    007158456087857766374304008634074285527854909258l
```

2 Câu hỏi 2

Thử thách phân tích thừa số #2: Modun N dưới đây là tích của hai số nguyên tố p và q ở đó $|p-q| < 2^{11} \cdot N^{1/4}$. Hãy phân tích thừa số nguyên tố của N.

Gợi ý: trong trường hợp này $A - \sqrt{N} < 2^{20}$ bởi vậy hãy thử tìm A bắt đầu từ $\sqrt{N}$ trở đi, cho đến khi phân tích được thừa số nguyên tố cho N.

```
N = 648455842808071669662824265346772278726343720706976263060439070378 \
    973086180811164627140152760614175691955873218402545206554249067198 \
    242884484183935328197298853131051173864896596258282150250499026445 \
    100885281673303711142296421027840289307657458645233683357077834689 \
    158386460882396402368662522117900857878l
```

3 Câu hỏi 3

Thử thách phân tích thừa số #3: Modun N dưới đây là tích của hai số nguyên tố p và q ở đó $|3p-2q| < N^{1/4}$. Hãy phân tích thừa số của N.

Gợi ý: dùng tính toán dưới đây để chỉ ra rằng $\sqrt{6N}$ là gần với $(3p+2q)/2$ và sau đó dùng phương pháp tương tự ở trên để phân tích thừa số N.

```
N = 720062263747350425279564435525583738338084451473999841826653057981 \
    635569018833779042340866418766393848517526499401789708352407913568 \
    774411551320151882793318123090919962463618968365736431191740949613 \
    524639707885238799396839230364676670221627018353299443241192173812 \
    927614753074859730219275137573938792l
```

Bây giờ ta xem xét xem tại sao $A - \sqrt{N} < 1$. Điều này được chỉ ra bởi các tính toán đơn giản sau đây. Đầu tiên, quan sát rằng

$$A^2 - N = \left(\frac{p+q}{2}\right)^2 - N = \frac{p^2+2N+q^2}{4} - N = \frac{p^2-2N+q^2}{4} = (p-q)^2/4$$

Bây giờ, bởi vì với mọi x, y : $(x-y)(x+y) = x^2 - y^2$ ta đạt được

$$A - \sqrt{N} = (A-\sqrt{N})\frac{A+\sqrt{N}}{A+\sqrt{N}} = \frac{A^2-N}{A+\sqrt{N}} = \frac{(p-q)^2/4}{A+\sqrt{N}}$$

và bởi vì $\sqrt{N} \leq A$ ta có

$$A - \sqrt{N} \leq \frac{(p-q)^2/4}{2\sqrt{N}} = \frac{(p-q)^2}{8\sqrt{N}}$$

Do giả sử (1) ta biết rằng $(p-q)^2 < 4\sqrt{N}$ và do đó ta có

$$A - \sqrt{N} \leq \frac{4\sqrt{N}}{8\sqrt{N}} = 1/2.$$

4 Câu hỏi 4

Bản mã thử thách dưới đây là kết quả của việc mã hoá một thông điệp bí mật viết ở ASCII dùng RSA modun đưa ra trong thử thách đầu tiên (Câu hỏi 1). Số mũ mã hoá là $e = 65537$. Bản rõ ASCII được padding với PKCS v1.5 trước khi được mã hoá.

Hãy dùng phân tích thừa số nguyên tố của RSA modun để giải mã bản mã thử thách này. Nhắc lại rằng dùng các thừa số nguyên tố này bạn có thể tính được $\phi(N)$ và do đó lấy được số mũ giải mã d của RSA.

Bản mã giải mã (viết ở dạng cơ số 10) như sau:

```
220964518674103817763065611348834180174100697878928310717318391436761356001 20 \
538004282329650473509424343946219751512256465839967942889460764542040581564 74 \
898801373486412045232522932017648791666640299750918872997169052608322206777 16 \
000193292608700095799937240774589677736978175712672299511486629596279347915 40
```

Sau khi dùng số mũ d để giải mã bản mã thử thách, bạn có được bản rõ ở với padding ở dạng PKCS1. Để có được bản rõ cần tìm, cách tốt nhất là viết các số ở dạng hexa. Bạn quan sát thấy rằng số bắt đầu với '0x02' theo sau bởi nhiều giá trị ngẫu nhiên khác không. Tìm '0x00' là giá trị ngăn cách; và giá trị số sau giá trị ngăn cách này là các chữ cái ASCII của bản rõ (*chú ý:* ký hiệu ngăn cách được dùng ở đây là '0x00' chứ không phải '0xFF' như trong slides.)