Broken RSA

Подготовили: Воробьёв Д. Нецветайлов А., КБ-2

Балтийский Федеральный университет им. Иммануила Канта, Калининград

1 июля 2022

Квадратичный вычет
Символ Лежандра

Квадратичныый вычетом по модулю m называется такое целое число a, для которого выполняется тождество
$x^2 \equiv \ (\text{mod } m)$
Если сравнение не разрешимо, то число a называют квадратичным **невычетом**

Символ Лежандра — функция, используемая в теории чисел. Введён французским математиком А. М. Лежандром.
Пусть a - целое число и p - просто число, отличное от 2 Символ Лежандра $\frac{a}{p}$ определяется следующем образом:

- $\frac{a}{p} = 0$, если a делится на p;
- $\frac{a}{p} = 1$, если a является квадратичным вычетом по модулю p, но при этом a не делится на p;
- $\frac{a}{p} = -1$, если a является квадратичным невычетом по модулю p.

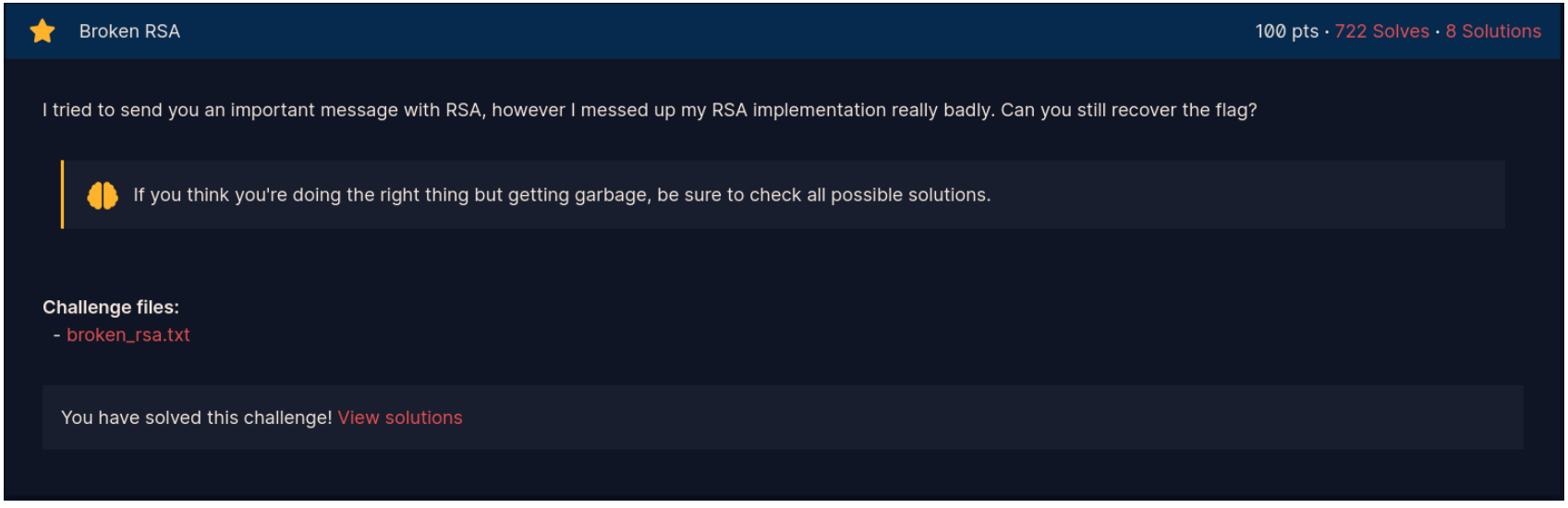
Алгоритм Тонелли-Шенкса

Входные данные: p — нечётное простое число, n — целое число, являющееся квадратичным вычетом по модулю p, другими словами, $n/p = 1$, где ab — символ Лежандра. $x^2 \equiv n \pmod{p}$
Результат работы алгоритма: вычет R, удовлетваряющий сравнению $R^2 \equiv n \pmod{p}$
1. Выделим степени двойки из $p - 1$, то есть пусть $p - 1 = 2^S Q$ где Q нечётно, $S >= 1$. Заметим, что если S=1, то есть $p \equiv 3 \pmod{4}$, тогда решение определяется формулой $R \equiv \pm n^{\frac{p+1}{4}}$. Далее полагаем $S >= 2$
2. Выберем произвольный квадратичный вычет z, то есть символ Лежандра $\frac{z}{p} = -1$, положим $c \equiv z^Q \pmod{p}$
3. Пусть также $R \equiv n^{\frac{Q+1}{2}} \pmod{p}$, $t \equiv n^Q \pmod{p}$, $M = S$
4. Выполняем цикл:

- Если $t \equiv 1 \pmod{p}$, то алгоритм возвращает R
- В проивном случае в цикле находим наименьшее i, $0 < i < M$, такое, что $(t^2)^i \equiv 1 \pmod{p}$ с помощью итерирования возведения в квадрат.
- Пусть $b \equiv (c^2)^{(M - i - 1)} \pmod{p}$, и положим $R :\equiv Rb \pmod{p}$, $t :\equiv tb^2 \pmod{p}$, $c \equiv b^2 \pmod{p}$, $M := i$, возвращаемся к началу цикла

После нахождения решения сравнения R второе рещение сравнение находится как $p - R$

Задача


Broken RSA
100 pts · 722 Solves · 8 Solutions
I tried to send you an important message with RSA, however I messed up my RSA implementation really badly. Can you still recover the flag?
If you think you're doing the right thing but getting garbage, be sure to check all possible solutions.
Challenge files:
- broken_rsa.txt
You have solved this challenge! View solutions