# Breaking RSA

### Breaking RSA

The weak point of the RSA algorithm lies in the key generation: specifically, the difficulty of factoring $N$ into its prime components. This factorisation is only possible through trial and error, and the algorithm remains secure until someone discovers a heuristic method to do it efficiently.

You wouldn't believe how tricky it is to find $p$ and $q$ when $N = 77$. Once you've figured it out, think about how you did it. What was the process? How did you come up with the solution?

The RSA Labs used to offer $200,000 for the factorization of 2048-bit numbers. However, they removed the prize because more recent research has shown that the method can be broken if the primes $p$ and $q$ have a special relationship.

The RSA Labs previously offered a $100,000 prize to anyone who could submit the prime factors of the following integer $N$, that is, the two primes whose product is $N$:

```
N = p x q = 25195908475657893494027183240048398571429282126204
03202777713783604366202070759555626401852588078440
69182906412495150821892985591491761845028084891200
72844992687392807287776735971418347270261896375014
97182469116507761337985909570009733045974880842840
17974291006424586918171951187461215151726546322822
16869987549182422433637259085141865462043576798423
38718477444792073993423658482382428119816381501067
48104516603773060562016196762561338441436038339044
14952634432190114657544454178424020924616515723350
77870774981712577246796292638635637328991215483143
81678998850404453640235273819513786365643912120103
97122822120720357
```

You can sense how difficult this task is: we are dealing with 617 digits, and unfortunately, the last digit is not even.