Problem Set 5–Security of RSA

CSCI3381-Cryptography

Solutions to the Written Problems

1. *Square roots modulo n; 10 points.*

(a) $9493^2 \bmod 11413 = 1$. Check it if you don't believe me! Why does this prove that 11413 is composite?

Solution. The equation can be rewritten

$$\begin{aligned} 11413 &\mid 9493^2 - 1 \\ &= (9493 - 1) \cdot (9493 + 1) \\ &= 9492 \cdot 9494 \end{aligned}$$

A prime number p has the property that if p divides a product mn, then p divides either m or n. But clearly 11413 cannot be a divisor of either of these numbers that are smaller than it, so 11413 is not prime.

(b) Use the equation in (a) to factor 11413. It is possible to do this with a computer by trial division because the numbers are relatively small, but I want you to show the steps of a computation that can be carried out by hand, or that could be done if the numbers given in (a) were many, many times larger.

Solution. To continue with the above argument, this means that the factors of 11413 are divided between 9492 and 9494. Thus 11413 has factors in common with each of these numbers, which we can recover by using Euclid's Algorithm. Let's use 9492. The quotients and remainders for the successive divisions are given below:

```
>>> divmod(11413,9492)
(1, 1921)
>>> divmod(9492,1921)
(4, 1808)
>>> divmod(1921,1808)
(1, 113)
>>> divmod(1808,113)
(16, 0)
```

So the gcd is 113. A spot check (division by 3,5,7) shows that 113 is prime, and one more division gives

$$11413 = 113 \times 101.$$

If we had applied Euclid's Algorithm using 9494 instead of 9492 we would have found the factor 101 first.

(c) Similarly, carry out a calculation that will find the other square roots of 1 modulo 11413. Of course, two of these square roots are 1 and 11412; find another one.

Solution. You can obtain the four square roots are obtained by using the Chinese Remainder Theorem to solve the four systems of congruences

$$\begin{aligned} x &\equiv \pm 1 \pmod{113} \\ x &\equiv \pm 1 \pmod{101} \end{aligned}$$

When the two remainders are both 1 we get 1 as the solution, and when they are both -1 we get $-1 \equiv 11412$. You can perform the calculation with the CRT to find out the solution when one of the remainders is 1 and the other -1. But I already gave you one of these answers in (a)! It's 9493. The fourth square root is

$$-9493 \bmod 11413 = 1920.$$

2. *Easy factorization if p, q are too close together: 20 points* This problem forms the theoretical basis for one of the computer problems below. (You do not need to prove the result here in order to tackle the computer problem, you can just accept it and apply the given algorithm.)

Suppose Alice decides to use primes of more than 200 decimal digits (*i.e.,* greater than 10^{200}) to generate her RSA modulus. She picks a prime p at random, and then chooses q to agree with p in all but the last 100 digits. Her reasoning is that p and q have effectively been randomly sampled from a set of size 10^{100}, and that it will be just as hard for an adversary to factor $N = pq$ as it would be to factor the product of two random 100-digit primes.

But Alice is in for a nasty surprise: If we have a factorization $n = pq$, then we can write the two primes as $A - x$ and $A + x$, where $A = (p+q)/2$ is the average of p and q. Thus

$$N = pq = (A-x)(A+x) = A^2 - x^2,$$

so

$$x = \sqrt{A^2 - N}.$$

If we knew what A was, then since computing exact square roots is easy, we could determine x and hence the factors p and q. But how can we determine A without knowing p and q in the first place? Prove that in the circumstances described above, $A = \lceil \sqrt{N} \rceil$, *the smallest integer greater than* $\sqrt{N}$. Thus we can factor N by solving the easy problem of computing the square root, which gives us A, and then x and the prime factors $A \pm x$.

HINT. The 'circumstances described above' are that p and q differ by less than $\sqrt[4]{N}$. You need to prove that in this case

$$\sqrt{N} = \sqrt{pq} < A = \frac{p+q}{2} < \sqrt{N} + 1.$$

It's easiest to do this if you look at what you get by squaring all parts of the inequality.

Solution.

We get $\sqrt{N} < A$ by definition, so we really only need to show that $A < \sqrt{N} + 1$, or equivalently, that

$$A^2 < (\sqrt{N} + 1)^2 = N + 2\sqrt{N} + 1.$$

We have

$$\begin{aligned} A^2 &= \left(\frac{p+q}{2}\right)^2 \\ &= \frac{p^2 + 2pq + q^2}{4} \\ &= \frac{p^2 - 2pq + q^2}{4} + \frac{4pq}{4} \\ &= \left(\frac{p-q}{2}\right)^2 + N \\ &= N + \left(\frac{\sqrt[4]{N}}{2}\right)^2 \\ &= N + \sqrt{N}/4 \\ &< N + 2\sqrt{N} + 1. \end{aligned}$$

In the specific instance described in the problem, $|p-q| < 10^{100}$ and $N = pq > 10^{400}$, so we do indeed have $|p - q| < \sqrt[4]{N}$. As you can see from the proof, we have a lot of room to maneuver here; it would have been enough to have p and q differ by less than $8 \cdot \sqrt[4]{N}$.