Algorithms Exercises Answers and Notes

exceedhl@gmail.com

May 4, 2012

1 Chapter 1

1.1 RSA algorithm

p, q are primes, $N = pq$, $N' = (p-1)(q-1)$, e is relatively prime to N'. x is the plain text and $x \in 0, 1, \ldots, N-1$.

N and e are public, the encrypted text is:

$$x' = x^e \ rem\ N, \quad x' \in 0, 1, \ldots, N-1 \tag{1}$$

Let

$$de \equiv 1 \ modulo\ N', \tag{2}$$

d can be calculated using extended Euclid algorithm.

Then

$$de - 1 = kN' \tag{3}$$
$$de = kN' + 1 \tag{4}$$
$$x'^d - x = x^{ed} - x = x^{1+k(p-1)(q-1)} - x \tag{5}$$

Because p, q are primes and $x < N$, so according to Fermat's little theorem:

$$x^{p-1} \equiv 1 \ modulo\ p \tag{6}$$
$$\Rightarrow x^{(p-1)k(q-1)} \equiv 1 \ modulo\ p \tag{7}$$
$$x^{q-1} \equiv 1 \ modulo\ q \tag{8}$$
$$\Rightarrow x^{(q-1)k(p-1)} \equiv 1 \ modulo\ q \tag{9}$$
$$\Rightarrow x^{(q-1)k(p-1)} - 1 \ rem\ pq = 0 \tag{10}$$
$$\Rightarrow x^{(q-1)k(p-1)} \equiv 1 \ modulo\ pq \tag{11}$$
$$\Rightarrow x'^d - x = x^{ed} - x = x^{1+k(p-1)(q-1)} - x \ rem\ pq = 0 \tag{12}$$
$$\Rightarrow x'^d \equiv 1 \ modulo\ N \tag{13}$$

Because $x^{ed} \equiv x$ *modulo* N and $x < N$, we can get x by calculating x'^d *rem* N.

So if we make N, e public, keep d, p, q secret, then we can encrypt and decrypt messages using power and rem operations.

Finally, since x^e *rem* $N = x'$, and x'^d *rem* $N = x$, it is obvious that they are bijection functions.

1.2 Exercises

1.2.1 1.1

Consider the biggest possible value of adding three digits in base b: $3(b-1)$. The biggest value of two digits in base b is: $b^2 - 1$. Now we just need to prove $b^2 - 1 \geq 3(b-1)$.

$$
\begin{aligned}
b^2 - 1 - 3(b-1) &= b^2 - 3b + 2 && (14)\\
&= (b-1)(b-2) && (15)\\
&\geq 0 \quad (\forall\ b \geq 2) && (16)
\end{aligned}
$$