# Exercise Set Part 5
# Public Key Cryptography

Hans Georg Schaathun

12th November 2015

**Exercise 0.1** *Calculate*

*1.* $6^3 \mod 11$

**Solution:**

1. $6^3 \mod 11 = 7$

**Problem 0.1** *Show how to calculate the following powers:* $5^{17} \mod 9$ *How many multiplications do you need?*

**Solution:** We can use the square-and-multiply algorithm.

$$5^{17} \mod 9 = (((5^2)^2)^2)^2 \cdot 5 \mod 9. \tag{1}$$

Thus we can calculate

$$\begin{aligned} 5^2 &\mod 9 = 25 \mod 9 = 7, && (2)\\ (5^2)^2 &\mod 9 = 7^2 \mod 9 = 4, && (3)\\ ((5^2)^2)^2 &\mod 9 = 4^2 \mod 9 = 7, && (4)\\ (((5^2)^2)^2)^2 &\mod 9 = 7^2 \mod 9 = 4, && (5) \end{aligned}$$

and finally

$$5^{17} \mod 9 = 4 \cdot 5 \mod 9 = 2.$$

We needed four squarings and one extra multiplication, for a total of five multiplications.

**Problem 0.2** *What does the encryption function for RSA look like?*

**Solution:** The RSA encryption function is

$$e_{e,n}(x) = x^e \mod n$$

where $n = pq$ is a product of two large primes $p, q$ and $e$ is invertible modulo $(p-1)(q-1)$.

**Problem 0.3** *Show how to calculate the following powers:* $5^{17} \mod 9$ *How many multiplications do you need?*

**Solution:** We can use the square-and-multiply algorithm.

$$5^{17} \mod 9 = (((5^2)^2)^2)^2 \cdot 5 \mod 9. \tag{6}$$

Thus we can calculate

$$\begin{aligned} 5^2 &\mod 9 = 25 \mod 9 = 7, & (7)\\ (5^2)^2 &\mod 9 = 7^2 \mod 9 = 4, & (8)\\ ((5^2)^2)^2 &\mod 9 = 4^2 \mod 9 = 7, & (9)\\ (((5^2)^2)^2)^2 &\mod 9 = 7^2 \mod 9 = 4, & (10) \end{aligned}$$

and finally

$$5^{17} \mod 9 = 4 \cdot 5 \mod 9 = 2.$$

We needed four squarings and one extra multiplication, for a total of five multiplications.