Notes on the RSA Algorithm (a.k.a. "RIZZ")

Exercises for Part D.

For these exercises, you might find the following list of the first 60 primes useful:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281

1. Find gcd(9060, 333000). Hints: $111 = 3 \cdot 37$; $906 = 3 \cdot 302$.

$$\begin{aligned}\gcd(9060, 333000) &= \gcd(906 \cdot 10, 333 \cdot 1000) = \gcd(3 \cdot 302 \cdot 2 \cdot 5, 3 \cdot 111 \cdot 2^3 \cdot 5^3)\\ &= \gcd(3 \cdot 2 \cdot 151 \cdot 2 \cdot 5, 3 \cdot 3 \cdot 37 \cdot 2^3 \cdot 5^3)\\ &= \gcd(2^2 \cdot 3 \cdot 5 \cdot 151, 2^3 \cdot 3^2 \cdot 5^3 \cdot 37) = 2^2 \cdot 3 \cdot 5 = 60.\end{aligned}$$

2. Find gcd(777777,4949). Hints: $777777 = 77 \cdot 10101$; $10101 = 91 \cdot 111$; $4949 = 49 \cdot 101$.

$$\begin{aligned}\gcd(777777, 4949) &= \gcd(77 \cdot 10101, 49 \cdot 101) = \gcd(7 \cdot 11 \cdot 91 \cdot 111, 7^2 \cdot 101)\\ &= \gcd(7 \cdot 11 \cdot 7 \cdot 13 \cdot 3 \cdot 37, 7^2 \cdot 101) = \gcd(3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 37, 7^2 \cdot 101)\\ &= 7^2 = 49.\end{aligned}$$

3. 18 and 55 are coprime; note that

$$18 \cdot (-3) - 55 \cdot (-1) = 1.$$

The problem is that -3 and -1 are not natural numbers. Can you find natural numbers x and y such that $18x - 55y = 1$? Hint: add 55 to -3, and add something to -1 to compensate.

We add 55 to -3 to get 52, and add 18 to -1 to get 17. Then we compute that

$$18 \cdot 52 - 55 \cdot 17 = 1.$$

4. Suppose $a, b \in \mathbb{Z}$ are coprime; let $x = x_0$ and $y = y_0$ be a pair of natural numbers satisfying

$$ax - by = 1.$$

(Such x and y exist by Theorem RSA_1 above.)

(a) Show that the integers

$$x = a - y_0 \quad \text{and} \quad y = b - x_0$$

satisfy the equation

$$bx - ay = 1.$$

We are assuming that

$$ax_0 - by_0 = 1.$$

But then, letting $x = a - y_0$ and $y = b - x_0$, we find that

$$bx - ay = b(a - y_0) - a(b - x_0) = ba - by_0 - ab + ax_0 = ax_0 - by_0 = 1.$$

(b) 41 and 27 are coprime; note that

$$41 \cdot 2 - 27 \cdot 3 = 1.$$

Use part (a) of this exercise, above, to find natural numbers x and y such that

$$27x - 41y = 1.$$

We are given that the numbers $x_0 = 2$ and $y_0 = 3$ satisfy $41x_0 - 27y_0 = 1$. By part (a) of this exercise, we should let $x = a - y_0 = 41 - 3 = 38$, and $y = b - x_0 = 27 - 2 = 25$. Let's try it:

$$27x - 41y = 27 \cdot 38 - 41 \cdot 25 = 1026 - 1025 = 1.$$

5. Let $a = 10$ and $m = 33$.

(a) Check that the hypotheses (that is, the conditions) of Theorem RSA$_2$ are met for this a and m.

$m = 3 \cdot 11$, so m is a product of two distinct primes. Also, $a = 10 = 2 \cdot 5$ is coprime to $m = 33 = 3 \cdot 11$. So the hypotheses of Theorem RSA$_2$ hold.

(b) Compute $a^{\varphi(m)}$ by successive squaring, to confirm that the conclusion of Theorem RSA$_2$ holds in this case.

Step 1: Compute the binary expansion of $\varphi(m) = 20$:

$$20 = 16 + 4.$$

Step 2. Raise $a = 10$ to successive powers of 2 (mod 33).

$$10 \equiv 10 \pmod{33},$$
$$10^2 \equiv 100 \equiv 33 \cdot 3 + 1 \equiv 1 \pmod{33},$$
$$10^4 \equiv (10^2)^2 \equiv 1^2 \equiv 1 \pmod{33},$$
$$10^8 \equiv (10^4)^2 \equiv 1^2 \equiv 1 \pmod{33},$$
$$10^{16} \equiv (10^8)^2 \equiv 1^2 \equiv 1 \pmod{33}.$$

Step 3. Put Steps 1 and 2 together to compute $10^{20} \pmod{33}$:

$$10^{20} \equiv 10^{16+4} \equiv 10^{16} \cdot 10^4 \equiv 1 \cdot 1 \equiv 1 \pmod{33}.$$

Exercises for Part E.

1. Decode the message $b = 22$, with $k = 19$ and $m = 51$, using successive squaring. Hint:

$$19 \cdot 27 - 32 \cdot 16 = 1.$$

The RSA decoding algorithm says that we should compute $22^{27} \pmod{51}$, so let's.

Step 1: Compute the binary expansion of $k = 27$:

$$27 = 16 + 8 + 2 + 1.$$

Step 2. Raise $b = 22$ to successive powers of $2 \pmod{51}$.

$$\begin{aligned}
22 &\equiv 22 \pmod{51},\\
22^2 &\equiv 484 \equiv 51 \cdot 9 + 25 \equiv 25 \pmod{51},\\
22^4 &\equiv (22^2)^2 \equiv 25^2 \equiv 625 \equiv 51 \cdot 12 + 13 \equiv 13 \pmod{51},\\
22^8 &\equiv (22^4)^2 \equiv 13^2 \equiv 169 \equiv 51 \cdot 3 + 16 \pmod{51},\\
22^{16} &\equiv (22^8)^2 \equiv 16^2 \equiv 256 \equiv 51 \cdot 5 + 1 \equiv 1 \pmod{51}.
\end{aligned}$$

Step 3. Put Steps 1 and 2 together to compute $22^{27} \pmod{51}$:

$$\begin{aligned}
22^{27} &\equiv 22^{16+8+2+1} \equiv 22^{16} \cdot 22^8 \cdot 22^2 \cdot 22\\
&\equiv 1 \cdot 16 \cdot 25 \cdot 22\\
&\equiv 400 \cdot 22\\
&\equiv (51 \cdot 7 + 43) \cdot 22 \equiv 43 \cdot 22 \equiv 946 \equiv 51 \cdot 18 + 28 \equiv 28 \pmod{51}.
\end{aligned}$$

2. (a) Encode the message "A," with $k = 35$ and $m = 65$, using numerization and successive squaring.

A$\longrightarrow$ 11.

Step 1: Compute the binary expansion of 35:

$$35 = 32 + 2 + 1.$$

Step 2. Raise 11 to successive powers of 2 (mod 65).

$$\begin{aligned}
11 &\equiv 11 \pmod{65},\\
11^2 &\equiv 121 \equiv 56 \pmod{65},\\
11^4 &\equiv (11^2)^2 \equiv 56^2 \equiv 3136 \equiv 65\cdot 48 + 16 \equiv 16 \pmod{65},\\
11^8 &\equiv (11^4)^2 \equiv 16^2 \equiv 256 \equiv 65\cdot 3 + 61 \equiv 61 \pmod{65},\\
11^{16} &\equiv (11^8)^2 \equiv 61^2 \equiv 3721 \equiv 65\cdot 57 + 16 \equiv 16 \pmod{65},\\
11^{32} &\equiv (11^{16})^2 \equiv 16^2 \equiv 61 \pmod{65}.
\end{aligned}$$

Step 3. Put Steps 1 and 2 together to compute $11^{35} \pmod{65}$:

$$\begin{aligned}
11^{35} &\equiv 11^{32+2+1} \equiv 11^{32}\cdot 11^2 \cdot 11\\
&\equiv 61\cdot 56\cdot 11 \equiv 3416\cdot 11 \equiv 36\cdot 11 \equiv 396 \equiv 6 \pmod{65}.
\end{aligned}$$

(b) Suppose your answer to part (a) of this problem is b. Pretending that you don't know where b came from, decode b to get the original message n. Make sure you get what you should. Hint:

$$35\cdot 11 - 48\cdot 8 = 1.$$

We need to compute $6^{11} \pmod{65}$. DIY: you get 11, which *was* our original message (numerized).

3. (a) Encode the message "V," with $k = 23$ and $m = 77$, using numerization and successive squaring.

The numerization of V is 32. DIY: we compute, by successive squaring, that $32^{23} \equiv 65 \pmod{77}$.

(b) Suppose your answer to part (a) of this problem is b. Pretending that you don't know where b came from, decode b to get the original message n. Make sure you get what you should. Hint:

$$23\cdot 47 - 60\cdot 18 = 1.$$

We need to compute $65^{47} \pmod{77}$. DIY: you get 32, which *was* our original message (numerized).