Geoffrey Parker - grp352
HW 27: 5.6 - 5.7
M328K
May 3rd, 2012

5.6 Exercise. *Describe an RSA Public Key Code System based on the primes* 11 *and* 17*. Encode and decode several messages.*

Solution. Let $p = 11$ and $q = 17$. To generate our keys, $n = pq = 187$ and $\phi(n) = 10 \cdot 16 = 160$. Then let $e = 3$ and note that $(3, 160) = 1$. Now we need to use the Extended Euclidean Algorithm to find d such that $3d + (-160)y = 1$.

$$\begin{aligned}
3 &= 1 \cdot -160 + 163 \\
-160 &= -1 \cdot 163 + 3 \\
163 &= 54 \cdot 3 + 1 \\
1 &= (-54)3 + 163 \\
163 &= 3 - (-160) \\
1 &= (-54)3 + 3 + (-1)(-160) \\
1 &= (-53)3 + (-1)(-160)
\end{aligned}$$

So $d \equiv -53 \pmod{160}$, and we can add 160 to get $d = 107$. So now we have our public key: $3, 187$ and our private key: $107, 187$. Time to encrypt some messages.

Let's encrypt the string "RSA". Since we have such a small modulus, we will encrypt each character separately. Encoded as a null terminated UTF-8 string, "RSA" is represented by the numbers $82, 83, 65, 0$. Now we calculate each of these numbers raised to the 3 modulo 187 giving $92, 128, 109, 0$, our cyphertext. We can then raise each of these to the 107 modulo 187 to recover $82, 83, 65, 0$ □

5.7 Exercise. *You are a secret agent. An evil spy with shallow number theory skills uses the RSA Public Key Coding System in which the public modulus is* $n = 1537$, *and the encoding exponent is* $E = 47$. *You intercept one of the encoded secret messages being sent to the evil spy, namely the number* 570. *Using your superior number theory skills, decode this message, thereby saving countless people from the fiendish plot of the evil spy.*

Solution. To begin, factor $n = 1537 = 29 \cdot 53$. Then we use this p, q and e to generate d. We find $\phi(n) = 28 * 52 = 1456$, so we know that $47d + (-1456)y = 1$. Then we preform the Extended Euclidean Algorithm:

$$\begin{aligned} 47 &= 1 \cdot -1456 + 1503 & 1503 &= 47 - 1 \cdot (-1456) \\ -1456 &= (-1) \cdot 1503 + 47 & & \\ 1503 &= 31 \cdot 47 + 46 & 46 &= 1503 - 31 \cdot 47 \\ 47 &= 1 \cdot 46 + 1 & 1 &= 47 - 1 \cdot 46 \end{aligned}$$

So we can now back substitute to see that:

$$\begin{aligned} &1 = 47 - 1 \cdot 46 & & \\ &1 = 47 - 1 \cdot (1503 - 31 \cdot 47) & &1 = 32 \cdot 47 - 1503 \\ &1 = 32 \cdot 47 - (47 - 1 \cdot (-1456)) & &1 = 31 \cdot 47 + -1 \cdot -1456 \end{aligned}$$

So the decrypting exponent d is 31. If our cyphertext is 570, we can recover the original message $m = 570^{31} \pmod{1537}$. So the original message is 131. □