COMS10003 Workshop Sheet 9, outline solutions.

Julian Gough 2014-11-27

Work sheet

1. Use Euler's theorem to calculate

$$3^{81} \pmod{100} \tag{1}$$

Solution: So $100 = 2 \cdot 2 \cdot 5 \cdot 5$ so

$$\phi(100) = 100 \cdot \frac{1}{2}\frac{4}{5} = 40 \tag{2}$$

Now $(3, 100) = 1$ so we can apply Euler's theorem and get

$$3^{40} \equiv 1 \pmod{100} \tag{3}$$

and so

$$3^{81} \equiv 3 \pmod{100} \tag{4}$$

2. An enemy organization has encrypted a message with the public key $n = 111$ and $e = 5$; since n is three digits long the message blocks are all taken to be two digits, that is one character, long, with the simple translation of the alphabet into numbers from zero to 25 we have been using. The message is 001101000081025032000109000021000 where each three digits corresponds to one letter. However, by choosing a public key n with less the 2048 bits the enemy organization has made itself vulnerable to a brute force decryption attack, that's your job. **Solution:** So first of all let's factorize $n = 111$, it is $3 \cdot 37$ so $\phi(111) = 72$. Next we need to find the inverse of $e = 5$, well

$$\begin{aligned} 72 &= 14 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned} \tag{5}$$

so $1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (72 - 5 \cdot 14) = 29 \cdot 5 - 2 \cdot 72$ or $5^{-1} \equiv 29 \pmod{72}$. Now

$$1^{29} \equiv 1 \pmod{111} \tag{6}$$

so the first letter is 'b',

$$101^{29} \equiv 11 \pmod{111} \tag{7}$$

so the second letter is 'l', the third letter is 'a' and the fourth is

$$101^{29} \equiv 12 \pmod{111} \tag{8}$$

or 'm'. In fact, the message is 'blamecanada'.

3. This is about encoding rather than decoding, choose two primes that multiply to give a three digit number, chose a exponent 'e' and a short message to encode and encode it. Ideally you should decode it again afterwards. **Solution:** Obviously this depends on the primes and so on. Lets do a quick example, say $n = 11 \cdot 17 = 187$. Now $\phi(187) = 10 \cdot 16 = 160$ so $e = 7$ works as an exponent since $(7, 160) = 1$. Now, say the message is 'waxon' which in numbers is 2200231413. Now

$$\begin{aligned} c(22) &\equiv 22^7 \equiv 44 \pmod{187} \\ c(00) &\equiv 0^7 \equiv 0 \pmod{187} \\ c(23) &\equiv 23^7 \equiv 133 \pmod{187} \\ c(14) &\equiv 14^7 \equiv 108 \pmod{187} \\ c(13) &\equiv 23^7 \equiv 106 \pmod{187} \end{aligned} \tag{9}$$

so the cipher text is 044000133108106. To decode you would have to find $d \equiv 7^{-1} \pmod{160}$. In fact $160 = 7 \cdot 22 + 6$ and $7 = 6 + 1$ so $1 = 7 - 6 = 7 - (160 - 7 \cdot 22)$ or

$$1 = 23 \cdot 7 - 160 \tag{10}$$

or $7^{-1} \equiv 23 \pmod{160}$ hence the decoding exponent is 23. Applying it to the stuff above

$$44^{23} \equiv 22 \pmod{187} \tag{11}$$

and so on.

4. Suppose the $n = 10088821$ is the product of two primes and $\phi(n) = 10082272$. What are the prime factors of n? **Solution:** Use the totient function rule for two primes to find the sum of the two primes.

$$\begin{aligned} \phi(n) = 10082272 &= (p-1)(q-1) \\ pq - p - q + 1 &= 10082272 \\ 10088821 - p - q + 1 &= 10082272 \\ p + q &= 6550 \end{aligned} \tag{12}$$

Use the quadratic formula on $pq = 10088821$ substituting from (12) above, or: just find the primes that multiply to give n by starting with two mubers of similar size that add up to $p+q = 6550$ you multiply them and see it is greater than n. Iteratively try different values of p and q until you find two that multiply to give n.

$$\begin{aligned} 3273 + 3277 &= 6550 \\ 3273 * 3277 &= 10725621 \\ 2273 * 4277 &= 9721621 \\ 2473 * 4077 &= 10082421 \\ 2477 * 4073 &= 10088821 = n \\ p &= 2477 \\ q &= 4073 \end{aligned} \tag{13}$$