Senior Math Circles – Cryptography and Number Theory Week 3 Solutions

Dale Brydon

These are not necessarily full solutions, but should convey the idea of how to solve all the problems. Use at your own risk.

1. First we need to figure out d. Since $n = 35 = 5(7)$, we can see that $\varphi(n) = 4(6) = 24$. Then we compute $d = e^{-1} \bmod 24$ to see that $d = 5$. Finally, we compute $c^d \bmod 35 = 8$ and so the message is 8. (This reveals a secondary danger of using very small key sizes: encryption may do nothing.)

2. We verify the signature by computing $r = 39^3 \bmod 55$. Doing this yields $r = 29$. Since $r \neq m$, this is not a valid signature.

3. (a) $\varphi(n) = (p-1)(q-1) = pq-p-q+1 = n-p-q+1$. Hence, $\varphi(n)-(n+1) = -p-q$.

   (b) $(x-p)(x-q) = x^2-(p+q)x+pq = x^2+(\varphi(n)-(n+1))x+n$, by part (a).

   (c) Simply applying the quadratic formula to the polynomial in part (b) will reveal p and q, since they are the roots of this polynomial. Hence we have that the two solutions to

   $$\frac{n+1-\varphi(n) \pm \sqrt{(\varphi(n)-(n+1))^2-4n}}{2}$$

   are p and q.

   (d) We plug in n and $\varphi(n)$ to the equation above to get

   $$\frac{32 \pm \sqrt{(-32)^2-(4)247}}{2} = \frac{32 \pm \sqrt{36}}{2} = 19, 13.$$

   Notice $19(13) = 247$, so we have indeed factored n.

4. The original message is "CONGRATS." There was an error in the original problem as distributed in class: it should have read $c_1 = 593$.

5. (a) To factor $n = pq$ in this case, first assume $p < q$. Then we have $p < \sqrt{n} < q$. Now since there can be no primes between p and q, we know that p must be the prime immediately before $\sqrt{n}$. Since we assume we can find this number, we can then compute $q = n/p$.

   (b) $\sqrt{2491} \approx 49$. The prime immediately before 49 is 47. 2491/47=53. Hence the factors are 47 and 53.

6. It can be shown that $de - 1$ is a multiple of both $p - 1$ and $q - 1$ and so we must have $\text{lcm}(p - 1, q - 1) \mid (de - 1)$, where lcm is the least common multiple function. We will define L to be $\text{lcm}(p - 1, q - 1)$. Given a single exponent pair (e, d) we can compute $de - 1$ to find a multiple, kL, of L. If we were to take many such pairs, subtract 1 from their product, and then take the GCD of these differences, the result would be very likely to be L.

   Once we know L, we can use the facts that $L \mid \varphi(n)$ and $\varphi(n) \approx n$ to compute $\varphi(n)$. Simply round n/L to the nearest integer, since $n/L \approx \varphi(n)/L$, which we know to be an integer. Using this, we can compute $\varphi(n)$ and hence factor n, by problem 3. (It turns out that a single decryption exponent in enough to factor n, although the method in that case is more complicated.)