USS: Introduction to mathematical cryptography
Friday July 22 problems

1. (This is repeated from yesterday if anyone didn't get to it.) Use the baby steps, giant steps algorithm to solve the problem

$$11^x \equiv 21 \pmod{71}.$$

2. Let $p = 101$, $g = 3$ and $h = 17$. The goal of this problem will be to compute $\log_3 17$ in $(\mathbb{Z}/101\mathbb{Z})^\times$.

   (a) First use the factorization of the least residue of 2^7 modulo 101 to find the value of $\log_3 2$.

   (b) Then compute and factor the least residue of 17^{-1} modulo 101.

   (c) Use the information you have to compute $\log_3 17$.

3. This is problem 3.36 in Section 3.8 from Hoffstein, Pipher and Silverman. You will need a calculator or a computer to solve this problem.
   Let $p = 19079$ and $g = 17$, and your factor base be $\{2, 3, 5\}$.

   (a) Check that the least residue of g^i is divisible only by primes in the factor base for $i = 3030, 6892$, and 18312.

   (b) Use part (a) to compute $\log_g 2$, $\log_g 3$, and $\log_g 5$. For this you will need to work in $\mathbb{Z}/19078\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9539\mathbb{Z}$, where 9539 is prime, so it might be easier to work in the two finite fields and then use Sun Zi's Remainder Theorem to get the solutions modulo 19078.

   (c) Check that the least residue of $19 \cdot 17^{-12400}$ is divisible only by primes in the factor base.

   (d) Finally, compute $\log_g 19$.