Introduction to Cryptography

Homework 4

October 16, 2006

1. Assume that Alice uses the shared modulus $N = 18923$ and the encryption exponents $e_1 = 11$ and $e_2 = 5$. Suppose Alice encrypts the same message m twice, as $c_1 = 1514$ and $c_2 = 8189$. Show how to compute the plaintext m.

2. Solve the DLP $6 \equiv 2^x \bmod 101$ using enumeration, bsgs, Pollard's rho method, and Pohlig-Hellman.

3. Show that the sequence of b_i in Pollard's ρ method is periodic after a match has occurred.

4. This exercise explains why Floyd's cycle finding method works. Let s and $s + c$ denote the smallest indices with $b_s = b_{s+c}$; then the preperiod (the tail of the ρ) has length s, and the cycle has length c.

   (a) Let $i = 2^j$ be the smallest power of 2 with $2^j \geq s$. Show that b_i is inside the cycle.

   (b) If $i = 2^j \geq c$, show that one of the elements $b_{i+1}, b_{i+2}, \ldots, b_{2i}$ is equal to b_i.