Introduction to Cryptography

Homework 4

November 14, 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.

   Here $\gcd(e_1, e_2) = 1$, so we compute $t_1 \equiv 11^{-1} \equiv 1 \bmod 5$ and $t_2 = \frac{11t_1-1}{5} = 2$. Then $c_1^{t_1} c_2^{-t_2} \equiv 1514 \cdot 8189^2 \equiv 100 \bmod N$.

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

   Enumeration means we just compute $2^x \bmod 101$ until the result is 6 mod 101. The oneliner

   ```
   for(a=1,100,if(Mod(2^a-6,101),,print(a)))
   ```

   tells us that $x = 70$.

   Baby-step Giant-step: here we compute $6 \cdot 2^{-r} \bmod 101$ for $r = 0, 1, \ldots,$ 11 and store the values; since none of the elements $(2^{-r} \cdot 6 \bmod 101, r)$ has the form $(1, r)$, we compute $d \equiv g^m = 2^{11} \bmod 101$ and the giant steps $d^m \bmod 101$. We find the match $d^6 \equiv 6 \cdot 2^{-4} \bmod 101$, which gives us $x = 6m + 4 = 70$.

   Pollard's ρ method: see the notes.

   Pohlig-Hellman: we want to solve $2^x \equiv 6 \bmod 101$ in the group $(\mathbb{Z}/101\mathbb{Z})^\times$ of order $100 = 2^2 5^2$. To this end we put $n_2 = 25$ and $n_5 = 4$, as well as $g_2 \equiv g^{25} \equiv 10 \bmod 101$, $a_2 \equiv 6^{25} \equiv 100 \bmod 101$ and $g_5 \equiv g^4 \equiv 16 \bmod 101$, $a_5 \equiv 6^4 \equiv 84 \bmod 101$. Then we have to solve $100 \equiv 10^{x(2)} \bmod 101$ and $84 \equiv 16^{x(5)} \bmod 101$.

   In this case we already see that $x(2) = 2$. To find $x(5)$, we raise $84 \equiv 16^{x(5)} \bmod 101$ to the 5th power and find $1 \equiv 95^{5x(5)} \bmod 101$. With $x(5) = x_0 + 5x_1$ this gives $5x(5) \equiv 0 \bmod 25$ or $x_0 = 0$.

Now we have to solve $16^{5x_1} \equiv 84 \bmod 101$; enumeration (this is a DLP in a group of order 5) gives $x_1 = 4$.

Thus $x(2) = 2$, $x(5) = 4 \cdot 5 = 20$, and the system $x \equiv 2 \bmod 4$, $x \equiv 20 \bmod 25$ has the solution $x \equiv 70 \bmod 101$.

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

   If $b_r = f_r(x) = f_s(x) = b_s$, then of course $b_{r+1} = f(b_r) = f(f_r(x)) = f(f_s(x)) = b_{s+1}$.

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.

   This is trivial since $i \geq s$.

   (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.

   We have $b_i = b_{i+c}$ since c is the cyclie length. Thus we only have to show that $i + c \leq 2i$, which is equivalent to $c \leq i$.