

1. Let  $G$  be a group, and suppose that we have an algorithm to solve the discrete logarithm problem in  $G$  for any element whose order is a power of a prime. To be concrete, if  $g \in G$  has order  $q^e$ , then we can solve  $g^x = h$  in  $O(S_{q^e})$  steps.

Now let  $g \in G$  be an element of order  $n$ , and suppose that  $n$  factors into a product of prime powers as follows  $n = q_1^{e_1} \cdots q_t^{e_t}$ . Then show that the discrete logarithm problem  $g^x = h$  can be solved in

$$O\left(\sum_{i=1}^t S_{q_i^{e_i}} + \log n\right)$$

steps, using the following procedure:

- (a) For each  $i \in \{1, 2, \dots, t\}$  let  $g_i = g^{n/q_i^{e_i}}$  and  $h_i = h^{n/q_i^{e_i}}$ . Notice that  $g_i$  has prime power order  $q_i^{e_i}$ , so use the given algorithm to solve the discrete logarithm problem  $g_i^y = h_i$ ; let  $y = y_i$  be a solution to this.
- (b) Use the Chinese remainder theorem to solve

$$\begin{aligned} x &\equiv y_1 \pmod{q_1^{e_1}} \\ x &\equiv y_2 \pmod{q_2^{e_2}} \\ &\vdots \\ x &\equiv y_t \pmod{q_t^{e_t}} \end{aligned}$$

2. Let  $G$  be a group and suppose that  $q$  is prime, and that we know an algorithm that takes  $S_q$  steps to solve the discrete logarithm problem  $g^x = h$  in  $G$  whenever  $g$  has order  $q$ . Now let  $g \in G$  be an element of order  $q^e$  with  $e \geq 1$ . Then show that we can solve the discrete logarithm problem  $g^x = h$  in  $O(eS_q)$  steps.
3. Conclude that the discrete logarithm problem in a group  $G$  is not secure if the order of the group is a product of powers of small primes.