COMPSCI 4CR3 - Assignment 4

1. Given an element $g \in \mathbb{Z}_p^\times$, and the prime factorization $p - 1 = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, the following algorithm determines whether g is a generator or not.

```
for $i = 1$ to $k$ do
    if $g^{(p-1)/p_i} = 1 \pmod{p}$, return False
end for
return True
```

   (a) (20 points) Show that the algorithm is correct; that is, it returns True if and only if g is a generator.

   (b) (10 points) What is the complexity of the algorithm in terms of the number of multiplications? Express your answer using Big-O notation.

   (c) (5 points) What is the output of the algorithm for
   $p = 899009829279928687167847647253$,
   $g = 425044249325748129860331117047$?

2. Let G be a group of order 3^n, i.e., $|G| = 3^n$, and suppose $g \in G$ is a generator of G. Recall that $g^{3^n} = g^{|G|} = 1$. Due to the specific structure of G, the discrete logarithm problem (DLP) is computationally easy in G.

   (a) (15 points) Design an efficient algorithm for DLP in G. Hint. Given $g^x = h$, you can compute one "digit" of x at a time. If

   $$x = 3^{n-1}x_{n-1} + 3^{n-2}x_{n-2} + \cdots + 3x_1 + x_0$$

   is the base-3 expansion of x, you can determine x_0 by computing $h^{3^{n-1}}$. Include the pseudocode of your algorithm here.

   (b) (10 points) Analyze the running time complexity of your algorithm. Express your answer using Big-O notation.

   (c) (15 points) Consider the following values for p and g:
   $p = 206021029217550749079470945356 87$
   $g = 1507469283585031963549937769853 8$.
   For these values, g is a generator of a subgroup $G < \mathbb{Z}_p^\times$ of order 3^{65}. That means the numbers $g^0 \bmod p, g^1 \bmod p, \ldots, g^k \bmod p$, where $k = 3^{65} - 1$, form a group of order 3^{65}. Use your algorithm to find the discrete logarithm $x = \log_g h$ for $h = 193412779505532697608485690260 15$.

3. To prevent the existential forgery attack, we discussed in the class how the RSA signature scheme uses a padding algorithm called EMSA. Suppose that instead of padding, we use just a hash function H.

   (a) (10 points) Write down the algorithms Gen, Sig and Ver for the new signature scheme that employs only H.

   (b) (10 points) Justify why the existential forgery attack is not applicable to the new scheme.

   (c) (5 points) Does using only H have a drawbacks compared to EMSA? Explain.