Introduction to mathematical cryptography
Homework problems
Week 7

13. Assume p is a prime number and $1 \leqslant g, h \leqslant p-1$ are primitive roots modulo p. Show that if there is an algorithm which solves the DLP with base g in polynomial time, then there is an algorithm which solves the DLP with base h in polynomial time.

14. Let $\mathscr{K}$ be a finite set of positive rational numbers. Define the function $R : \mathscr{K} \times \mathbf{N} \to \{0,1\}$ as follows: for $k \in \mathscr{K}$ and $n \in \mathbf{N}$, let $R(k,n)$ be the nth binary digit of k after the decimal point, i.e.

$$k = \text{integer} + \sum_{n=1}^{\infty} R(k,n) 2^{-n}.$$

Prove that $R(k,n)$ is not a pseudorandom number generator. (Note that the binary digits of any k are well-defined unless k is a rational number whose denominator is a power of 2, e.g.

$$\frac{3}{8} = 0.0110000\underbrace{\ldots}_{\text{all 0's}} = 0.0101111\underbrace{\ldots}_{\text{all 1's}}.$$

In such exceptional cases, we use that form of k which contains infinitely many zeros.)

Note: Please provide complete arguments everywhere.