EE 465: Cryptocurrency and Blockchain Technologies (Autumn 2018)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Assignment 1: 20 points Date: July 31, 2018

---

1. [5 points] Find two distinct inputs such that the corresponding SHA-256 hash function outputs coincide in the initial 28 bits.

2. [5 points] Show that the discrete logarithm problem can be solved in polynomial time in $\mathbb{Z}_n$, i.e. given a generator i of $\mathbb{Z}_n$ and any $j \in \mathbb{Z}_n$ there is a polynomial-time algorithm to find $k \in \mathbb{Z}_n$ such that
$$\underbrace{i + i + \cdots + i}_{k \text{ times}} = j.$$
Note that i is not necessarily equal to 1. *Hint: Extended Euclidean algorithm, multiplication, and addition in $\mathbb{Z}_n$ are polynomial-time algorithms.*

3. [5 points] Suppose G is a cyclic group of order q with generator g. Let $x \in \mathbb{Z}_q$ and $h = g^x$. Show that (I, r, s) and (I', r', s') have the same distribution where
   - $k \leftarrow \mathbb{Z}_q$, $I = g^k$, $r \leftarrow \mathbb{Z}_q$, and $s = rx + k \bmod q$
   - $r' \leftarrow \mathbb{Z}_q, s' \leftarrow \mathbb{Z}_q, I' = g^{s'} h^{-r'}$

   Recall that the notation $a \leftarrow A$ implies that the element a is randomly picked from the set A.

4. [5 points] Enumerate all the points of the elliptic curve $Y^2 = X^3 + 9X + 5$ over $\mathbb{F}_{13}$. You are allowed to use the software package of your choice.