Xi Liu, Assignment 3

1
if it is easy to find a $s2$ such that $H(s1) = H(s2)$, then it is possible to carry out a classical collision attack. since bitcoins are rewarded to the public key when the hash value satisfies proof of work requirement (k bits are 0), then if $H(s1)$ meets proof of work requirement, then $H(s2)$ also meets proof of work requirement, then 2 mining rewards are given to the same hash value

2
1) no, it can be detected, since all transactions are recorded in block chain which is a shared public ledger
2) suppose pk_i is the public key of victim, pk_j is public key of receiver
adversary can steal bitcoins by using the forged signature to send money from pk_i to pk_j in the form $sign(pk_i \underrightarrow{x\ coins}\ pk_j)$. the transaction succeeds since the validity of the transaction is checked through 2 criteria: 1. valid signature, 2. pk_i would not overdrawn after send. then the bitcoins cannot be retrieved to the victim since transactions are irreversible due to the append only nature of block chain public ledger

3
it is not secure if the who mines the current block pick a very easy DNA sequencing problem for the next miner to solve, then the next miner can obtain the bitcoin rewards in a very short time

4
it is possible but very unlikely for the forks to remain to be equally long, since people have different computing power and the probability that mining in a single attempt for a hash output that have k bits of 0 is approximately

$1/2^k$
when 1 of the branches is merely 1 block longer than the other, people tend to continue to mine on the slightly longer block since it is less likely to be erased

5
let cdh be the given algorithm that solves the computational Diffie Hellman problem such that $g^{ab} \leftarrow cdh(g, g^a, g^b)$
construction of Elgamal scheme:
let G_p be a group that satisfies decisional Diffie Hellman assumption, $g \in G_q$ be a generator

$gen(n)$
{
    sample random element x from $\mathbb{Z}_q^*$
    return $(pk = g^x, sk = x)$
}
$enc(pk, m)$
{
    sample random element r from $\mathbb{Z}_q^*$
    return $(c_1 = g^r, c_2 = pk^r \cdot m)$
}

to break Elgamal encryption, adversary need to find message m without knowing the secret key sk. assumes adversary only knows $pk = g^x$, $c_1 = g^r$, and $c_2 = pk^r \cdot m$

$$pk^r = (g^x)^r = g^{xr}$$

use the $cdh()$ algorithm: $g^{xr} \leftarrow cdh(g, g^x, g^r)$

now adversary knows $pk^r = g^{xr}$ and c_2

$$c_2 = pk^r \cdot m$$
$$m = c_2 \cdot pk^{-r}$$

6

suppose m is Bob's bid (i.e., $m = 100$), since Trudy knows $(c_1 = g^r, c_2 = pk^r \cdot m) \leftarrow enc(pk, m)$, Trudy can produce a ciphertext c_2' such that $c_2' = 2 \cdot c_2 = 2(pk^r \cdot m) = pk^r \cdot (2m)$