Quentin Moore
qrm6ff

Problem Set 2

1) The attacker must be earning more bitcoin through the mining reward than he would by stealing his spent bitcoin. Also, Satoshi is assuming that the attacker only derives utility based on the amount of bitcoin the attacker has at the end of the day, and there are no other motives.

2) If an attacker controls 45% of the bitcoin network, there is less than a 0.1% chance that the attacker can reverse a transaction if 340 blocks have been generated since the transaction happened.

3)

q = 0.10	z = 3
q = 0.15	z = 3
q = 0.20	z = 5
q = 0.25	z = 6
q = 0.30	z = 10
q = 0.35	z = 17
q = 0.40	z = 36
q = 0.45	z = 137

4) (a) You could verify that the data had not been tampered with, but you cannot verify that the data returned is the data you asked for (it could be some other part of your data). (b) This is because the signature and verification of the signature are totally separate operations, and just because the signature is verified, the data could be anything that we wrote (since we signed everything with the same key).

5) (a) To write, we would add data, hash the full set of data, and sign that hash. To read, we would retrieve the data, verify the signature, and unencrypt. (b) This time complexity of this approach scales linearly with n.

6) (b) To write we would add data, hash into the appropriate branch of the Merkle tree, and sign the Merkle hash. To read, we would retrieve the data, verify the signature, and only unencrypt the branch of the tree that we needed. (b) The time complexity of this approach scales with log(n).

7) (a) With 15% of the mining power, a pool expects to find 6 * 24 * 0.15 = 21.6 blocks per day. (b) The general formula is $\alpha*(t/10)$.

8) Seconds where orphaned blocks are possible per day = $(6*24*L)$.
Seconds to find a block = $(600/ \alpha)$

Orphaned blocks per day = $(6*24*L)/(600/ \alpha)$

9) The number of orphaned blocks will always increase by a lot if a pool if mining selfishly. This is because if the selfish pool is only one block ahead of the honest blockchain, and the honest blockchain catches up, then the selfish pool will have an orphaned block. As the relative hashing power of the selfish pool in relation to the rest of the network decreases, the selfish pool will have even more orphaned blocks.

10) Question: It seems like you always have to trust something to make a bitcoin transaction... is it possible to stay truly anonymous with bitcoin (of course, true anonymity would be an absolute pain for lawyers and law enforcement in situations where bitcoin was being used for illicit activities)?

Code to generate table:

```java
package ps2;

import java.util.Scanner;

public class main {
	public static double calc(double q, int z){
		double p = 1.0 - q;
		double lambda = z*(q/p);
		double sum = 1.0;
		int i, k;
		for(k = 0; k <= z; k++){
			double poisson = Math.exp(-lambda);
			for(i = 1; i <= k; i++){
				poisson *= lambda/i;
			}
			sum -= poisson*(1-Math.pow(q/p,z-k));
		}
		return sum;
	}
	public static void main(String[] args){
		Scanner input = new Scanner(System.in);
		double q = input.nextDouble();
		int z = 1;
		double ans = 0;
		while(true){
			ans = calc(q, z);
			if(ans < 0.05){
				System.out.println(z);
				System.exit(0);
			}
			z++;
		}
	}

}
```