Flipping Coins By Telephone

ECE 1762 Algorithms and Data Structures
Spring Semester, 2004 — U Toronto

1 Flipping Coins by Telephone (not a reading assignment)

Alice and Bob discuss on the telephone about their upcoming divorce. They decide to flip a coin to determine who will get possession of their house. Bob decides to take heads; so if the coin comes up heads he will get the house. Alice takes the coin and tosses it.

If the coin comes up tails, Alice tells Bob that she has won. If the coin comes up heads then it all depends on how honest Alice is. But Bob does not trust Alice to tell the truth. Here is how they can flip a coint by telephone.

Assumption. In the following discussion we assume that if p and q are sufficiently large prime numbers, then it is intractable (*i.e.* very hard) to factor their product $n = pq$.

Here are the steps that Bob and Alice follow:

1. Alice picks two very large prime numbers p and q and computes $n = pq$. Alice tells Bob the number n but *not* p or q.

2. Bob picks a random number x smaller than n and computes $z = x^2 \ mod \ n$. Bob sends z to Alice but does not tell her what x is.

3. $z = x^2 \ mod \ n$ has four square roots $mod \ n$, ($\pm \ x \ mod \ n$) and ($\pm \ y \ mod \ n$) (why? see footnote below). These are the numbers which, when squared and taken $mod \ n$, they give the same value z. We will write x to denote the smaller value of $\pm x$ and similarly for y.

4. Since Alice knows the factorization of $n = pq$, she can compute both x and y [1].

   Alice computes x and y, flips a coint, and uses the result to randomly select one of x or y, not knowing which one Bob had originally selected.

5. If Alice sent $\pm y$, then Bob wins. If Alice sent $\pm x$, then Bob loses.

   Informally, the following situation occurs: the square roots x and y represent the values heads and tails. Bob has picked x as the value (heads/tails) for which Alice wins.

   Alice knows both p and q, and therefore, given $z = x^2 \ mod \ n$, she can compute the values x and y in polynomial time as such a procedure uses the Chinese Remainder Theorem but requires knowing the factors of n (p and q) that Alice indeed does. Nevertheless, **Alice does not know** which value (x or y) Bob has selected, but she must guess this value correctly to win.

   On the other hand, **Bob knows** only n and the value x which he has selected. By our assumption on the difficulty of factoring of n, **Bod does not know** p and q. This implies

[1] This is a straightforward application of Corollary 31.28 (old edition 33.28) for the Chinese Remainder Theorem.

that he has no way to know the other square root (y) of $z \ mod \ n$; if he did know both x and y, the he would know the complete factorization of n.

Proof: Let's say Bob knows x and y. We know $x \not\equiv y \ mod \ n$ (by our hypothesis) so $x \pm y \not\equiv 0 \ mod \ n$. But

$$\begin{aligned}(x+y)(x-y) &\equiv x^2 - y^2 \ mod \ n &(1)\\ &\equiv z - z \ mod \ n &(2)\\ &\equiv 0 \ mod \ n &(3)\end{aligned}$$

which just means that n divides $x^2 - y^2$. Since $n = pq$ and p is prime, p divides $x^2 - y^2 = (x+y)(x-y)$, and so either p divides $(x-y)$ or p divides $(x+y)$. The same is true for q.

But p and q cannot both divide the same factor, since if they did then $pq = n$ divides it and either $(x-y) \equiv 0$ or $(x+y) \equiv 0 \ mod \ n$, both of which we know to be false. So p divides one of the factors, say $x+y$, and q the other. This means that we can factor n by taking $p = \gcd(n, x+y)$ and $q = \gcd(n, x-y)$. Euclid's algorithm works here in polynomial time. But this contradicts the intractability of factoring n that we assumed earlier. Therefore, if factorization is intractable, Bob cannot compute both x and y.

As a final step, Alice and Bob will now prove to each other that they behaved honestly:

- **Alice loses.** If Alice does not believe that she has lost, she challenges Bob to prove it. In this case, Bob knows x and Alice sent $y \ mod \ n$. By the argument above, Bob now has enough information to factor n. Bob computes $\gcd(x+y, n)$, which is one of the factors p or q of n, and sends it to Alice.

  Note that if Alice had actually sent $\pm x \ mod \ n$, Bob could not have computed this factor of n, as argued above, since he has recieved no additional information about the factorization of n.

- **Bob loses.** If Bob has lost, he wants to verify that the number n was constructed properly. This can be done in several ways. For example, Alice may send p and q to Bob, who then verifies that p and q are prime using a primality testing routine. This can be done in expected polynomial time using randomization.