Cryptography W4261
Professor Michael Rabin

Problem Set 2

Due: Thursday, Feb. 8 2007

1. **(More roots than degree.)** Give a ring R and a polynomial $f(x)$ over that ring with a leading coefficient of 1 and degree n, such that $f(x)$ has more than n roots in R. Can f have degree 1, or must the degree of f be greater than 1?

2. **(Generalizing Fermat's Little Thereom.)** Let $n = pq$ for primes p and q. Prove that if $\gcd(a, n) = 1$, then $a^{(p-1)(q-1)} \equiv 1 \pmod{n}$.

3. **(Getting the right answer all of the time.)** Assume we have an algorithm $\mathcal{A}$ that runs in 5 seconds and can decrypt RSA ciphertexts 1% of the time. More precisely: fix RSA modulus N and public exponent e. Let $S \subseteq \mathbb{Z}_N^*$ be the subset of $\mathbb{Z}_N^*$ such that $\mathcal{A}(C) = m$ and $m^e = C$ (i.e., $\mathcal{A}$ gets the right answer for ciphertexts in S). Then since $\mathcal{A}$ is correct 1% of the time, we have $|S| = \frac{|\mathbb{Z}_N^*|}{100}$.

   (a) Show that if one can decrypt ciphertext C_1 and can also decrypt the product C_1C_2, then one can also decrypt C_2.

   (b) Suggest how to use $\mathcal{A}$ to decrypt *any* ciphertext in $\mathbb{Z}_N^*$ in a reasonable amount of time. Use randomization.

4. **(Product of Three Primes.)**

   - let $n = pqr$ be the product of three *distinct* primes. Let $y \in E_n$ be a *quadratic residue* mod n. How many square roots does y have in E_n (E_n was defined in class.)
   - Prove that if there exists an efficient algorithm A which for a given $n = pqr$ and any *quadratic residue* y mod n, finds a square root for y mod n, then there exists an efficient algorithm B that completely factors n. (i.e., B finds p, q and r.)

5. **(Google Challenge - Spider on the wall.)** In the midst of political turmoil, the emperor is designing a new palace. In the past, political dissidents and other enemies of the state have sought to assassinate the emperor by releasing venomous spiders in his bedroom as he slept. To protect against such attacks, the emperor has called together his best engineers to design a spider-proof bedroom. Having discovered that spiders cannot travel across water, the engineers propose to install the bed so that each foot is resting in one of four buckets of water; however, while this protects against attacks from spiders on the ground, it does not protect against spiders who may climb to the ceiling and lower themselves vertically (along a spun thread) onto the bed. To thwart such attacks, one clever engineer proposes suspending a large basin of water above the bed, but this is rejected because a spider could simply climb to the ceiling,

lower itself to the edge of the basin and then climb around to the underside and attack the emperor as before.

How can the emperor be protected from spider attacks? You should assume that the adversaries can release spiders onto the floor, ceiling or any of the walls of the bedroom, but only after the emperor is in bed.