WORKSHEET # 3 (RSA CRYPTOGRAPHY)

MATH 435 SPRING 2011

Consider the group $U(n)$, the set of integers between 1 and $n-1$ relatively prime to n, under multiplication mod n.
1. Suppose that p and q are distinct primes. What is the order of $U(pq)$, $|U(pq)|$?

2. If p and q are still distinct primes, show that the natural map $\mathbb{Z}_{\text{mod } pq} \to \mathbb{Z}_{\text{mod } p} \times \mathbb{Z}_{\text{mod } q}$ is bijective (here the map sends r to $(r \text{ mod } p, r \text{ mod } q)$). (This is basically the Chinese Remainder Theorem)
Hint: To show it is bijective, it is enough to show it is surjective since the sets are the same size. Fix $(a, b) \in \mathbb{Z}_{\text{mod } p} \times \mathbb{Z}_{\text{mod } q}$. Write $1 = cp + dq$ for some integers c and d (we can do this because p and q are relatively prime), now form $r = (bcp + adq \text{ mod } pq)$. Compute $(r \text{ mod } p)$ and $(r \text{ mod } q)$.

3. Suppose that p and q are distinct primes and that n_1 and n_2 are arbitrary integers such that $(n_1 \text{ mod } p) = (n_2 \text{ mod } p)$ and $(n_1 \text{ mod } q) = (n_2 \text{ mod } q)$. Use the previous exercise to conclude that $(n_1 \text{ mod } pq) = (n_2 \text{ mod } pq)$.

Now we get to some cryptography. As before, fix p and q to be distinct primes and set $n = pq$, $m = (p-1)(q-1)$ (alternately, take m to be the lcm of $(p-1)$ and $(q-1)$), and finally fix r to be any integer relatively prime to m.

In RSA (Rivest, Shamir, Adleman) encryption, suppose there are two people, (A) and (B). (A) knows p, q and r. He then publishes n and r. If person (B) wants to send (A) an encrypted message, in the form of an integer M between 1 and n, person (B) merely computes:

$$N = M^r \bmod n.$$

He can even make this public! Anyone who knows how to factor n (for example person (A)) can decrypt this message as follows. Find the s such that $1 = rs \bmod m$ (in other words, find the multiplicative inverse of r modulo m). We will show that

$$M = N^s \bmod n.$$

The reason that this is secure, is that very large numbers are very hard to factor! In particular, we don't have a good way to factor n.

4. Fix the following numbers $p = 5, q = 7$, and $r = 5$. Encrypt the number 3 and then decrypt what you got and verify that you get 3 back.
Hint: $3^5 \bmod 35 = (3^2 \bmod 35)(3^3 \bmod 35)$. Similarly, you can find the inverse of $(r \bmod 24)$ by raising r to bigger and bigger powers.

We need to prove that the algorithm works. In particular, we need to prove that

$$(N^s \bmod pq) = (M^{rs} \bmod pq) = (M \bmod pq) = M.$$

This is very similar to Fermat's little theorem $((a^{p-1} \bmod p) = 1)$ and we will use it during the proof.

5. Prove that $(N^s \bmod pq) = (M \bmod pq)$.
Hint: Write $rs = 1 + tm$ for some integer t and compute M^{rs} mod both p and q. Then use the work from the first page.