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 $U(pq)$, $|U(pq)|$?

Solution: There are $pq-1$ potential elements $\{1, 2, \ldots, pq-1\}$. We exclude the elements $\{p, 2p, \ldots, (q-1)p\}$ (there are $q-1$ of these) and the elements $\{q, 2q, \ldots, (p-1)q\}$ (there are $p-1$ of these). Note that these two excluded sets have nothing in common since anything in common is divisible by both p and q. Thus we have in total

$$(pq-1) - (q-1) - (p-1) = pq - q - p + 1 = (p-1)(q-1)$$

elements. It's not hard to see $(p-1)(q-1)$ in other ways either, but this is quite direct.

2. If p and q are still distinct primes, show that the natural map $\mathbb{Z}_{\bmod pq} \to \mathbb{Z}_{\bmod p} \times \mathbb{Z}_{\bmod q}$ is bijective (here the map sends r to $(r \bmod p, r \bmod q)$). (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 $(a, b) \in \mathbb{Z}_{\bmod p} \times \mathbb{Z}_{\bmod q}$. Write $1 = cp + dq$ for some integers c and d (we can do this because p and q are relatively prime), now form $r = (bcp + adq \bmod pq)$. Compute $(r \bmod p)$ and $(r \bmod q)$.

Solution: We use the notation from the hint. Note $(r \bmod p) = ((bcp + adq \bmod pq) \bmod p) = (adq \bmod p)$ (note modding out by pq followed by modding out by p is the same as modding out by p since p divides pq). Now observe that $(adq \bmod p) = (a(dq + cp) \bmod p)$ which itself equals $(a \cdot 1 \bmod p) = (a \bmod p)$. Likewise

$$(r \bmod q) = (bcp \bmod q) = (b(cp + dq) \bmod q) = (b \cdot 1 \bmod q) = b \bmod q.$$

This proves that the function is surjective since r is sent to (a, b).

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

Solution: This is easy, the function, say we call in ϕ, described above is bijective and in particular injective, so if $\phi(n_1 \bmod pq) = \phi(n_2 \bmod pq)$, then $(n_1 \bmod p) = (n_2 \bmod p)$ and also $(n_1 \bmod q) = (n_2 \bmod q)$, we immediately see that $(n_1 \bmod pq) = (n_2 \bmod pq)$ as desired.

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: $3^5 \bmod 35 = (3^2 \bmod 35)(3^3 \bmod 35) \bmod 35$. Similarly, you can find the inverse of $(r \bmod 24)$ by raising r to bigger and bigger powers.

Solution: First note that $3^4 \bmod 35 = 81 \bmod 35 = 11$. Thus $3^5 \bmod 35 = (3 \cdot 3^4 \bmod 35) = (3 \cdot 11 \bmod 35) = 33 = N$. Now we compute the multiplicative inverse of $(r \bmod 24)$. In this case it's really easy, $(5^2 \bmod 24) = (25 \bmod 24) = 1$ so $s = 5$ also (r is its own inverse). Ok, now we are in business, we need to check the inverse, and so to compute $33^5 \bmod 35$. Note that $33 = -2 \bmod 35$ which will make computations much easier. Thus $(-2)^5 \bmod 35 = (-32) \bmod 35 = 3 \bmod 35 = M$ as desired.

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. **Solution:** Simply observe that $M^{rs} = M^{1+tm} = M^1 M^{tm}$. Now, write $tm = (p-1)k$, so that $M^{tm} \bmod p = (M^{(p-1)})^k = 1^k = 1$ by Fermat's little theorem. Likewise $(M^{tm} \bmod q) = 1$. In particular, $(M^{tm} \bmod p) = (1 \bmod p)$ and $(M^{tm} \bmod q) = (1 \bmod q)$ so that $1 = (M^{tm} \bmod pq)$ by a previous exercise. But now,

$$(M^{rs} \bmod pq) = (M^{1+tm} \bmod pq) = (M \bmod pq)(M^{tm} \bmod pq) \bmod pq = (M \bmod pq) = M$$

which completes the proof.