EECS 70 Discrete Mathematics and Probability Theory
Fall 2015 Satish Rao **Discussion 5B**

1. RSA Warm-Up

Consider an RSA scheme modulus $N = pq$, where p and q are prime numbers larger than 3.

Motivation: A simple problem which requires them to know how RSA works. They will be able to walk through the steps and see how encryption and decryption are inverses.

1. Recall that e must be relatively prime to $p-1$ and $q-1$. Find a condition on p and q such that $e = 3$ is a valid exponent.

   Solution: Both p and q must be of the form $3k+2$. $p = 3k+1$ is a problem since then $p-1$ has a factor of 3 in it. $p = 3k$ is a problem because then p is not prime.

2. Now suppose that $p = 5$, $q = 17$, and $e = 3$. What is the public key?

   Solution: $N = p \cdot q = 85$ and $e = 3$ are displayed publically. Make sure to point out that in practice, p and q should be much larger 512-bit numbers. We are only choosing small numbers here to allow manual computation.

3. What is the private key?

   Solution: We must have $ed = 3d \equiv 1 \mod 64$, so $d = 43$. Reminder: we would do this by using extended gcd with $x = 64$ and $y = 3$. We get $gcd(x,y) = 1 = ax + by$, and $a = 1$, $b = -21$.

4. Alice wants to send a message $x = 10$ to Bob. What is the encrypted message she sends using the public key?

   Solution: We have $E(x) = x^3 \mod 85$. $100^3 \equiv 65 \mod 85$, so $E(x) = 65$.

5. Alice receives the message $y = 24$ back from Bob. What equation would she use to decrypt the message?

   Solution: We have $D(y) = y^{43} \mod 85$. $24^{43} \equiv 14 \mod 85$, so $D(y) = 14$.

2. RSA with Multiple Keys

Members of a secret society know a secret word. They transmit this secret word x between each other many times, each time encrypting it with the RSA method. Eve, who is listening to all of their communications, notices that in all of the public keys they use, the exponent e is the same. Therefore the public keys used look like $(e, N_1), \ldots, (e, N_k)$ where no two N_i's are the same. Assume that the message is x such that $0 \leq x < N_i$ for every i.

1. Suppose Eve sees the public keys $(7, 35)$ and $(7, 77)$ as well as the corresponding transmissions. How can Eve use this knowledge to break the encryption?

   Solution: Yes. Note that gcd(77, 35) = 7. She can figure out the gcd of the two numbers using the gcd algorithm, and then divide 35 by 7, getting 5. Then she knows that the p and q corresponding to the first transmission are 7 and 5, and can break the encryption.

2. The secret society has wised up to Eve and changed their choices of N, in addition to changing their word x. Now, Eve sees keys $(3, 5 \times 23)$, $(3, 11 \times 17)$, and $(3, 29 \times 41)$ along with their transmissions. Argue why Eve cannot break the encryption in the same way as above.

   Solution: Since none of the N's have common factors, she cannot find a gcd to divide out of any of the N's. Hence the approach above does not work.

3. Euler's totient function

Euler's totient function is defined as follows:

$$\phi(n) = \mid \{i : 1 \le i \le n, \texttt{gcd}(n,i) = 1\} \mid$$

In other words, $\phi(n)$ is the total number of positive integers less than n which are relatively prime to it. Here is a property of Euler's totient function that you can use without proof:

For m,n such that $\texttt{gcd}(m,n) = 1$, $\phi(mn) = \phi(m) \cdot \phi(n)$.

1. Let p be a prime number. What is $\phi(p)$?

   Solution:

   Since p is prime, all the numbers from 1 to $p-1$ are relatively prime to p.

   So, $\phi(p) = p-1$.

2. Let p be a prime number and k be some positive integer. What is $\phi(p^k)$?

   Solution:

   The only positive integers less than p^k which are not relatively prime to p^k are multiples of p.

   Why is this true? This is so because the only possible prime factor which can be shared with p^k is p. Hence, if any number is not relatively prime to p^k, it has to have a prime factor of p which means that it is a multiple of p.

   The multiples of p which are $\le p^k$ are $1 \cdot p, 2 \cdot p, \ldots, p^{k-1} \cdot p$. There are p^{k-1} of these.

   The total number of positive integers less than or equal to p^k is, obviously, p^k.

   So $\phi(p^k) = p^k - p^{k-1} = p^{k-1} \cdot (p-1)$.

3. Let p be a prime number and a be a positive integer smaller than p. What is $a^{\phi(p)} \pmod{p}$? *(Hint: use Fermat's Little Theorem.)*

   Solution:

   From Fermat's Little Theorem, and part 1,

   $a^{\phi(p)} \equiv a^{p-1} \equiv 1 \pmod{p}$

4. Let b be a number whose prime factors are $p_1, p_2, \ldots, p_k$. We can write $b = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Show that for any a relatively prime to b, the following holds:

   $$\forall i \in \{1,2,\ldots,k\}, \quad a^{\phi(b)} \equiv 1 \pmod{p_i}$$

   Solution: From the property of the totient function and part 3:

   $$\begin{aligned}\phi(b) &= \phi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_k^{\alpha_k}) \\ &= \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \ldots \phi(p_k^{\alpha_k}) \\ &= p_1^{\alpha_1 - 1}(p_1 - 1) \cdot p_2^{\alpha_2 - 1}(p_2 - 1) \ldots p_k^{\alpha_k - 1}(p_k - 1)\end{aligned}$$

   This shows that, for every p_i, which is a prime factor of b, we can write $\phi(b) = c \cdot (p_i - 1)$, where c is some constant. Since a and b are relatively prime, a is also relatively prime with p_i. From Fermat's Little Theorem:

   $a^{\phi(b)} \equiv a^{c \cdot (p_i - 1)} \equiv (a^{(p_i - 1)})^c \equiv 1^c \equiv 1 \mod p_i$

   Since we picked p_i arbitrarily from the set of prime factors of b, this holds for all such p_i.