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.

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.

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

3. What is the private key?

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

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

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?

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.

3. Euler's totient function

Euler's totient function is defined as follows:

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

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 $\phi(p)$?

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

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.)*

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:

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