EECS 70 Discrete Mathematics and Probability Theory
Fall 2014 Anant Sahai

Discussion 6M

1. Bijections

Are the following functions bijective?

(a) $f(x) = 2x \mod 5, \quad \text{where } f : \mathbb{N}_5 \to \mathbb{N}_5$

(b) $f(x) = (3x+1) \mod 12, \quad \text{where } f : \mathbb{N}_{12} \to \mathbb{N}_{12}$

2. RSA Warm-Up

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

(a) 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.

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

(c) What is the private key?

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

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

3. RSA Reasoning

In RSA, if Alice wants to send a confidential message to Bob, she uses Bob's public key to encode it. Then Bob uses his private key to decode the message. Suppose that Bob chose $N = 77$. And then Bob chose $e = 3$ so his public key is $(3,77)$.And then Bob chose $d = 26$ so his private key is $(26,77)$.

Will this work for encoding and decoding messages? If not, where did Bob <u>first</u> go wrong in the above sequence of steps and what is the consequence of that error? If it does work, then show that it works.

4. 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 $(e,N_1),\dots,(e,N_k)$ where no two N_i's are the same. Assume that the message is x such that $0 \le x < N_i$ for every i.

(a) 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?

(b) 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.