Cryptography 4/29

Reagan Shirk

April 29, 2020

Sample Final

- We need to know the good/bad of each type of cipher
  - i.e. caesar chiper can be broken by brute force
- We need to know different methods of encryption and attack as well
  - i.e. symmetric key encryption, signature, key exchange, man in the middle, cipher text only, known plain text, etc
- We can use our book, notes, and sage. We're just not allowed to communicate with other people
- Multiple choice
  - integer factorization is believed to be hard for classical computers but it's not proved
  - integer multiplication is easy
  - gauss reduction with vectors (1, 4) and (2, 5) is (1, 1)
  - To find the center lift of 2/3 in the ring $Z/101Z$, you need to find a number that when multiplied by 3 and mod101 gives you 2. It is -33
- We'll have 10 multiple choice questions
- Describe NTRU key generation, encryption, and decryption algorithm. We can use Sage code in the description
  - We have our book so we can look this up and just type it
  - You can copy/paste your homework if it has been a homework question
- What is a permutation cipher and why is it not safe?
  - It's a linear cipher and easy to break with linear analysis
- How can a no message atack be done on a signature after finding the inverse hash function?

$$S = H(m)^d \bmod nS^e = H(m)m = H^{-1}(S^e)$$

- In a diffie hellman key exchange, we first need to find a large finite field F_p and its multiplicative generator g
  - Describe the rest of the procedure
  - If g is an element with a small order, what is the risk?
    - Easy problem that can be found in the book
- Let I be your OU ID number as a decimal number. Let $p =$ giagantic number. Calculate $I^{I^I} \bmod p$

$$x = I^I \bmod p - 1y = I^x \bmod p$$