Cyber Defense Club @ UI

Date: 11/08/16

Start Time: 7:00 PM

End Time: 8:10 PM

1. Happenings
   1. Anton gives presentation on Cryptography
   2. Find code on: <https://ghostbin.com/paste/cbzph>
   3. RSA:
      1. Pick two large prime numbers ‘p’ and ‘q’
      2. Let n = pq \*Note that n is difficult to factor
      3. φ(n) = (p-1)(q-1)
      4. Choose another prime ‘e’, such that GCD(e, φ(n)) = 1
         1. Import gcd function from fractions
         2. ***from fractions import gcd***
         3. Check that the GCD is 1
      5. d\*e ≡ 1 (mod φ(n))
         1. d ≡ 1\*e-1(mod φ(n))
         2. Use wolfram alpha to compute ‘d’
      6. Your public key is (e, n)
      7. Your private key is (d, n)