Class Notes 2-28-2017

Richard Truitt

March 28, 2017

Notes: Eulers Phi Function

- Phi(n) is going to count the number of residues mon N that are coprime to N
- Phi(N) = $1 <= a <= N | gcd(a, N) = 1$
- Phi(26) = 12
- Phi(27) = 27/3 = 9, 2*9=18
- If Phi is prime, then we can say Phi(p) is always p-1.
- $Phi(p^k) = (p-1)/p * p^k or [(p-1) * p^k - 1)]$
- $Phi(27) = Phi(3^3) = ((2)/3) * 3^3 = 18.$
- $TocalculatePhiforageneralcompositenumber$
- If N and M have gcd(m, n)=1, then Phi(m*n) = Phi(M)*Phi(N). this is referred to as a multiplicative function
- Phi(26) = Phi(2) * phi(13) = 1 * 12 = 12
- Phi(100) = $Phi(2^2) * Phi(5^2) = ((2-1)/2) * 2^2 * ((5-1)/5) * 5^2 = 2 * 20 = 40$

Notes: Eulers THM

- Says that if the gcd(a, n) = 1, then if we take a, and raise it to Phi(n) === 1(mod n
- Note, that n=p is prime, then Phi(p) = p-1. This just says that $a^p - 1 === 1 mod(p)$
- Basic principal is to compute $a^s(modm)$, we work (mod phi(m)) into the exponent

Notes: Special Case

- If R is === to $s^-1(mod(phi(m))$ and the $gcd(1, m) = 1$, then $(a^s)^r isa^(s * r)(modm)$

- This is known as the 3 pass protocol here is the idea:

    1. Alice wants to send a letter to Bob, but wants to make sure nobody in-between can read the message. So she is going to place the message in the box, and lock the box with her padlock.
    2. She sends this locked box to Bob, but he can't open the box because he doesn't have the key. Bob will then lock the box again using his padlock then send it back to alice
    3. Alice has the key to the box, and she's going to unlock her lock, but that still leaves Bobs padlock on it, and sends it back to him.
    4. Now since it's only locked by Bobs padlock, bob can unlock the box and get the letter.

- and this is how it is mathematically performed:

    1. Alice is going to pick a large prime number P, she can announcer her large rime number because it doesn't matter if everyone knows it or not. Now she needs to figure out how she's going to encrypt her message. So she is going to pick a residue 'a' that is larger than one and less than p-1, and will also computer $a^-1(modp-1)$.
    2. She takes her message, and encodes it as an integer 'm $<$ p'. and wants to send this number across to Bob.
    3. To encrypt (locking her message), she computes her message raised to the a power ($C1 = m^a(modp)$))
    4. She sends c1 over to Bob
    5. Bob is going to pick another number, B, that is 1 $<$ B $<$ p-1, and computes the inverse $b^-1(modp-1)$ ($C2 = c1^b(modp)$)
    6. Bob sends back to Alice, and she computes c3 ($C3 = c2^{a^-}1(modp)$)
    7. Alice sends this back to bob, and computes c3 and raises to to the b^-1
    8. **NOTE* Alice and Bobs keys need to be coprime to P-1**