MATH 314 Spring 2018 - Class Notes

10/31/2018

Scribe: Braeden Dorsey

Summary: Today we analyzed the steps involved in encrypting a message using the RSA Public Key Cryptosystem

- RSA revolves around the key idea that factorization is **hard**
- If you have 2 prime numbers p and q, multiplying them together is easy
- n = pq
- However, if youre just given n and must find prime p and q, it is much harder
- Remember **Euler's Theorem**, that if n=pq, then Phi(n) = (p-1)(q-1)

Steps to Encrypt using RSA:

Step 1: Alice picks p and q, finds n
Alice picks 2 prime integers p and q. For our example, lets use
p = 11, q = 13
n = p*q
our n = 11*13 = 143

Step 2:Find Phi(n)
By Euler's Theorem, Phi(n) = (p-1)*(q-1)
Our Phi(n) = (11-1)*(13-1) = 10*12 = 120

Step 3: Find encryption exponent e and decrption exponent d
Encryption exponent **e** is an integer where **gcd(e,Phi(n))=1**
We make our e = 7 because gcd(7,120) = 1
Decryption exponent **d** is the result of e^{-1}(mod Phi(n))
IN our example, 7^{-1}(mod 120) equals 103.
d = 103

Step 4: Alice sends out the public key
The public key is (n,e), which others will use to send Alice a message
Alice's private key is d, which she tells **no one**
In our example, the public key she sends out is (143,7)

Step 5: Bob uses the public key for his message
Bob picks his message **m**, where m ¡ n
m CAN be larger than n, but in this case it must be broken into blocks.
In our example, let m = 9.
to encrypt, Bob finds **ciphertext =** m^e **(mod n)**
In our example, 9^7 (mod 143) = 48 = c
Bob sends the message "48" to Alice

Step 6: Alice decrypts c
This where d being a secret comes into play
To find the message m, Alice computes c^d (mod n)
IN our example, this is 48^{103} (mod 143) = 9.
The message m is 9, so decryption is successful.

- But how is Eve supposed to crack this RSA system?
- to crack, Eve must find the decryption exponent d
- notice, Eve already knows e and n thanks to the public key.
- since d = e^{-1} (mod Phi(n)), Eve must factor n so that she can find Phi(n) and thus d.
- a way to do this will be discussed in later notes