MATH 314 - Class Notes

11/3/2016

Scribe: Josh Millford

Public Key Cryptography:

- First and most used form of Public Key Cryptography is RSA (1977)
- Steps for RSA
  - Bob creates a public key
  - he takes two different prime numbers (p and q)
  - Multiplies: n = p * q
  - Chooses an exponent **e**
  - we need GCD(e, (p-1)(q-1)) to equal 1
- Bob publishes the encryption key (n and e)
- Bob secretly computes $d = e^-1(mod(p-1)(q-1))$
- so d, p and q are all secret

- Suppose Alice has to send a message "m" to Bob:
  - Assume $m < n$, if not break the message into pieces
  - Alice computes $c \equiv m^e mod(n)$
  - sends c to Bob
  - Remember: computing m^e is fast because we can use modular exponentiation
- To decrypt:
  - Bob computes $c^d(modn)$ which is equal to $m(modn)$
  - recovers the original message

EXAMPLE:

- $p = 11, q = 5, n = 55, (11-1)(5-1) = 40$
- $e = 7$; note GCD(7,40) = 1
- Need $7^{-1}(mod40)$
- Bob uses Euclidean Algorithm:
  1. $40 = 5(7) + 5$
  2. $7 = 1(5) + 2$

3. $5 = 2(2) + 1$

- So then we go to the second Step of Euclids:

1. $1 = 5 - 2(2)$
2. $2 = 5 - 2(7 - 5)$
3. $5 = 3(5) - 2(7)$
4. $1 = 3(40 - 5(7) - 2(7))$
5. $= 3(40) - 17(7)$

- So $7^{-1} = -17(mod40)$ which is $23(mod40)$
- So $d = 23$

- So, Alice wants to send $m = 13$ to Bob, and she computes c which is $13^7(mod55)$, which is 111 in binary
- Start repeated squaring:
  - $13^1 = 13(mod55)$
  - $13^2 = 4(mod55)$
  - $13^4 = 16(mod55)$
- And we want to compute 13^7:
  - $c = 13^7 = 13^4 + 13^2 + 13^1$
  - which equals $16 * 4 * 13$
  - $16 * 52(mod55)$
  - $16 * -3(mod55)$
  - which equals $-48(mod55)$
  - $= 7(mod55)$
- So $c = 7$
- Sends this to Bob
- Bob wants to decrypt c
- Computes $c^{23}(mod55)$
- 23 is 10111 in binary so Repeated Squaring again:

1. $7 = 7(mod55)$
2. $7^2 = 49(mod55)$
3. $7^4 = 36(mod55)$
4. $7^8 = 31(mod55)$

5. $7^{16} = 26 (mod 55)$

- So $7^{23} = 7^{16} * 7^4 * 7^2 * 7^1$
- which is $26 * 36 * 49 * 9 = 13 (mod 55)$
- And there, Bob decrypted the message
- Currently it is recommended that p and q have around 120 digits
- n has around 240 digits
- better if p and q have slightly different lengths