MATH 314 Fall 2023 - Class Notes

11/9/2023

Scribe: Name Courtney Pelkey

Summary: Learning RSA, Diffie Hellman, El Gamal Cryptosystem.

Notes:
RSA- Public-key-crypto-system-Hard-problem-factoring
Discrete Log problem:

- If $y = x^k \pmod{p}$ and y, x, and p are known

Solving for k is hard.
Over the real numbers this is easy:

- $\log(y) = \log(x^k) = K\log(x)$
- $K = \log(y)/\log(x)$

Diffie-Hellman

- Key Exchsnge can't send message
- Alice and Bob agree on a secret random number (Key for AES)
- Alice picks a large prime P and a primative root α(We get all residues $\pmod{p}$ as powers of α)
- Alice and Bob both pick secret exponents $a, b1 < a < p-1, 1 < b < p-1$
- Alice computes $A = \alpha^a \pmod{p}$ Sends to Bob
- Bob computes $B = \alpha^b \pmod{p}$
- Alice computes $K = B^a \pmod{p}$
- Bob computes $K = A^b \pmod{p}$

  El Gamal Cryptosystem

  - Way to send a secret message using the discrete log problem
  - Alice picks a large prime P and a primitive root α and a secret exponent a
  - $\beta = \alpha^a \pmod{p}$. key $= (p, \alpha, \beta)$ $Bobwantstosendamessagem toAlice.Firsthepicksanephemeral$
    $b < p-1$
  - Bob computes $r = \alpha^b \pmod{p}$
  - $t = m\beta^b \pmod{p}$ To decrypt Alice
  - $r^{-a} * t = m \pmod{p}$