MATH 314 Spring 2018 - Class Notes

11/14/2015

Scribe: Cole Bauer

Summary: Diffie Hellman Key Exchange and Decrypting

Notes: Include detailed notes from the lecture or class activities. Format your notes nicely using latex such as

- Diffie Hellman key exchange allows two strangers to share a key but not send a message, this uses a discrete logarithm problem to keep things secure
- The idea behind this is that solving $y = a^x(modp)$ for given (y, a, p) is hard
- We'd like to have a different secure way to send messages if RSA is broken using the discrete log problem. El Gamal cryptosystem (Public key crypto system based on the discrete log problem that allows sending secure messages)

SETUP:

- Alice picks a large prime, "p" (to be secure have at least 100 digits)
- Have a primitive root α (mod p). Powers of this number produce all of the residues (mod p)
- Alice picks a secret number "k" - 1 <k <(p-1)
- Compute $\beta = \alpha^k(modp)$
  - Alice's public key is (p, α, β)

Bob wants to use this public key to send a message 'm' (assume m <p). Bob is going to pick a secret number b - 1 <b <(p-1).

HE COMPUTES:

* $\Gamma = a^b(modp)$ - This masks the secret b
* $t = \beta^b * m(modp)$ - This hides the message m
* He sends both Γ and t to Alice. The cipher text is the pair (Γ, t)

Alice wants to decrypt the original message

* She computes $\Gamma^{-k} * t(modp)$ this should give her m
* Unpack $\Gamma^{-k} * t \equiv (\alpha^l)^b * mequiv\alpha^-(bk + bk) * m \equiv m$

Eve could decrypt the message if she learned either k or b If she finds 'k' she can decrypt the same as Alice if she finds 'b'. Then she could compute: $t * \beta \equiv m * \beta^b * \beta^{-b} \equiv m$

Both require solving the discrete log problem. Alice always uses the same 'k' but Bob needs to pick a different 'b' each time.

NOTICE:

If Bob always uses the same 'b' and Eve manages to figure out one message m then she knows $t = m * \beta^b$ which means she can find $\beta^b \equiv t * m^{-1}(modp)$. If Bob changes 'b' each time this doesnt work.

EXTRA SECURITY:

If Eve can guess possibilities for m, she tries to encrypt then every secret number 'b' produces a different encryption. There is no way for Eve to verify that her guess is correct. Another goal of public key cryptography is authentication.

Suppose Alice receives a message from Bob. How does she know is really Bob? Why couldnt Eve pretend to be Bob?

* The only way we solved this problem was with physical letter seals, signatures which are unique to the person
* Digitally a signature can be perfectly duplicated and so this alone doesnt work
* To make this work we need to create a mathematical connection between a message and the digital signature that somehow only Bob can produce