MATH 314 Spring 2018 - Class Notes

4/23/2019

Scribe: Abel Tadesse

Summary: Continuation on Diffie Hellman from the last class.

Notes: In the previous lesson we covered the main strategies on how to implement the method and we will starts of from an example.

Diffie - Hellman example

$p = 13$, $\alpha = 2$
Alice picks the secret key of $a = 3$.
Bob picks the secret key of $b = 8$.

Bob computes $B = \alpha^b \equiv 2^8 \equiv 9 \pmod{13}$
and sends this to Alice.
Alice computes
$A = \alpha^a \equiv 2^3 \equiv 8 \pmod{13}$ and sends this to Bob.
Now Alice computes
$k = B^a \equiv 9^3 \equiv 9^2(9) \equiv 3(9) \equiv 1 \mod 13$
And Bob computes
$k = A^b = 8^8 \equiv 1 \pmod{13}$ They both share the key $k = 1$.
Say eve wants to break Diffie Hellman $\pmod{s) heidstosolve}$A $\equiv \alpha \pmod{}$

She can try every possible value of a this requires o(p) time

Baby Step Giant Step
$N = \lceil \sqrt{p} \rceil$
She creates two tables

Eve finds the secret exponential

How many steps we had to create tables in $NoN = o\sqrt{p}$
running time why is there exactly one
$a < p - 1 < p = \sqrt{p}^2 < N^2$ write a/n base N as $a = x + yN$
we can find x and y $\alpha^a \equiv \alpha^{x+yN} \equiv \pmod{} \alpha^l \equiv \alpha^{-yN}$

Trap door function for RSA:

Integer factorization

if we want a new public key
we need a new trapdoor function

Discrete Logarithm Problem

$\ln \alpha = \beta^x \bmod m$

If we knowβ, compute α quickly (mod exp. If we know α β want to find x-this turns out to be hard

Ex. Solve $6 \equiv 2^x \bmod 13$
$x = 5$ works $2^5 = 32 \equiv 6 \bmod 13$ We can find this by brute force attack
try all values of x

If this was calculus, how would you solve $6 = 2^x$
$\log_2 6 = \log_2 2^x \log_2 6 = \ln 6 / \ln 2 = x$

This problem is called the discrete log problem.
Also like factoring we didn't know that there isn't a fast way to compute
discrete logs but so far we haven't found Diffie Hellman key exchange can
be used to send a message but allows Alice and Bob to agree on a shared private key that
can be used for symmetric key cryptosystem

Steps of Diffie - Hellman

1.) Alice picks a large prime p
2.)She finds a primitive root $\alpha \pmod{}$ (recallα is a prime root $\pmod{i} f$ $\alpha \pmod{}$ produces every residu
3.)Alice picks a random b with $2 < b < p - 1$
4.)A and b are secret not to be shared with each other. Alice computes $A = \alpha^a \pmod{}$ bob computes B
5.) Alice computer $k(B)^a \pmod{}$ bob computes $A^b \pmod{}$ why is $A^b \equiv B^a \pmod{}$?
$A^b \equiv \alpha^{ab} \equiv \alpha^{ab} \equiv \alpha^{ba} \equiv B \pmod{}$
secret k which you can use for AES Suppose Eve is tying to break this Eve knows p and
α and A, B her goal is to find k so she has to compute either B^2 or $A^b \pmod{}$ to do this she
needs to finds a or b. To find these she would have to solve $A = \alpha \pmod{}$. for a or $B \equiv \alpha^b$
$\pmod{}$ for b.