Class Notes, 11-15-2016

Dalton Watts

November 22, 2016

Discrete Logarithm
If $\beta = \alpha^x \pmod{p}$
Given α, β its hard to solve for x
Basis for Diffie-Hellman Key Exchange
Not a way to send messages, so it's not a public key cryptosystem.

ElGamal Cryptosystem
Based on the difficulty of discrete logs.
Like RSA it can be used to send messages.
Bob chooses a prime p and a primitive root mod p. Secret integer a: $1ap-1$
Compute $\beta \equiv \alpha^a \pmod{p}$
Public key is (p, α, β)
Alice wants to send Bob a message m, so she picks a secret integer k: $1kp-1$
She computes $r = \alpha^k \pmod{p}$ and $t = m * \beta^k \pmod{p}$
This respectively masks k and m.
She sends (r,t) to Bob. Encryption is $E_{p,\alpha,\beta,k}(m)$ =$(\alpha^k, m * \beta^k)$
To Decrypt, Bob computes $D_{p,\alpha}(r,t) = tr^{-a}$
Now, why is $tr^{-a} \equiv m \pmod{p}$?

$$tr^{-a} \equiv (m\beta^k)(\alpha^k)^{-a} \pmod{p}$$

$$\equiv m(\alpha^a)^k(\alpha^k)^{-a} \pmod{p}$$

$$\equiv m\alpha^{ak-ak} \pmod{p}$$

$$\equiv m \pmod{p}$$

If Eve wants to decrypt (r, t) She needs to know a where $\beta = \alpha^a \pmod{p}$
Therefore, she needs to solve the discrete log.

Note: It is important that Alice use a different value of k for every message
Suppose Alice sends m1 and m2 using the same k
Encryption results in the same r, which makes it easier for Eve to crack k.

Baby Example: p = 17, Primitive Root $\alpha = 3$
Bob picks a = 7 (secret)
Compute $\beta \equiv \alpha^a \equiv 3^7 \pmod{17} \equiv 11 \pmod{17}$
Public Key $(p, \alpha, \beta) = (17, 3, 11)$
Alice wants to send m = 10
She picks k = 15 (secret)
Alice computes $r \equiv a^k \equiv 3^15 \equiv 6 \pmod{17}$
$t \equiv m * \beta^k \equiv 10 * 11^15 \equiv 4 \pmod{17}$
Encrypted message (r, t) = (6, 4)
Bob computes tr$^{-a} Soheneedsinverseofrwhichinthiscase, r^{-1} \equiv 6^-1 \equiv 3$ (mod 17)
$4 * 3^7 \equiv 10 \pmod{17}$
Then another example on Sage Math Cloud.

For ElGamal if Eve claims to have decrypted (r, t) and god m there is no way to verify that she is right without knowing Alice's secret k. Some message m encrypts to different ciphertexts for different values of k.
How could Eve attack Discrete Logarithm Problem?
Solve $\beta = \alpha^a \pmod{p}$ for a
Method 1: Just try values of a = 2, 3, ... p-1 until we find one that works. On average, this takes p/2 steps, which is way too slow.
Method 2: Baby Step Giant Step
Eve wants to solve $= \alpha^a \pmod{p}$ for a
Let $N = floor(\sqrt{p}) + 1$
$N^2 pp - 1$
She makes 2 lists:
First Baby Steps list contains $\alpha^j \pmod{p}$ for $0jN$
Second Giant Steps list contains $\beta\alpha^{-Nk} \pmod{p}$ for $0kN$
If we find something in both lists:
$\alpha^j \equiv \beta\alpha^{-Nk} \pmod{p}$
$\alpha^{j+Nk} \equiv \beta \pmod{p}$
So, $a = j + Nk$
Why should a number show up in both lists, you might ask?
Know that $1ap - 1N^2$
Write a in "Base N" as $a = a_0 + a_1 N$ where $a_0, a_1 N$
Take $j = a_0, k = a_1$ such that Entries in the tales agree for these values.
Baby Step Giant Step requires O($\sqrt{p}) Steps$

Method 3?: Index Calculus, which is similar to Dickson's Factoring Method, only use numbers with small prime factors (Less than B for some upper bound B)
Solve DLP for lots of random numbers and look for small primes
Because of. this to be secure you need primes with at least 200 digits.
Piece together to get a solution. running time is $O(e^{\sqrt{ln(x)(ln(ln(x)))}})$