Computing the Discrete Log with Baby/Giant Step method

May 20, 2009

The security of both the ElGamal and Diffie-Hellman systems relies on the difference in computational complexity of computing $a^b \ (mod\ m)$ versus computing the discrete logarithm mod m. The problem of computing the discrete logarithm can be summarized as follows:

"Given a primitive root a of the modulus n and an integer b such that $1 \leq b < n$, find a value x such that $a^x \equiv b \ (mod\ n)$."

Both ElGamal and Diffie-Hellman use the modulus n is a prime number p. What I will describe here is a deterministic algorithm for computing the discrete log problem within a number of multiplications and exponentiations proportional to $\sqrt{\phi(n)}$. Since the 'encryption' procedure of ElGamal and Diffie-Hellman requires just a few multiplication and exponentiation operations, the security of these systems is dependent on the large difference in complexity of these operations.

It is recommended that when choosing a prime modulus for the ElGamal and Diffie-Hellman system that $p-1$ have at least one large prime factor. If this is not the case then $\phi(n)$ may be small and this algorithm (and similar deterministic and non-deterministic algorithms for computing the discrete log) will run much faster than expected and perhaps make these systems vulnerable to attack.

In the Baby step/Giant step algorithm we let $m = \lceil \sqrt{\phi(n)} \rceil$. If n is not prime then we may need to estimate m and we will see that our algorithm might need to run a little longer than expected, but will still determine the discrete log.

To compute the discrete log, we exploit the fact that our value x that we are looking for is less than or equal to $\phi(n)$ and therefore can be expressed as $qm + r$ for some $0 \leq r < m$ and q will be less than or equal to $\phi(n)/m \approx m$.

Now given a which we assume to be a primitive root and b which is an integer less than or equal to b we compute the m values $a^r \ (mod\ n)$ and $ba^{-mq} \ (mod\ n)$ where $1 \leq r < m$ and $1 \leq q < m$.

Since x is going to be equal to $mq + r$ for some q and r values we will find that

$$a^r \equiv ba^{mq} \ (mod\ n)$$

by consequence

$$a^r \cdot a^{mq} \equiv b \ (mod\ n)$$

and we have determine that $qm + r$ is equal to our x.

The values $a^r \ (mod\ n)$ are what the words 'baby steps' are referring to because they are the simple powers of a and the values $ba^{-qm} \ (mod\ n)$ are the 'giant steps' since each value differs from the next by multiplication by $a^{-m} \ (mod\ n)$.

For example, say that we choose our public modulus to be 53 and $a = 3$ and we wish to solve for x in the equation

$$3^x \equiv 41 \ (mod\ 53).$$

We set $m = \lceil \sqrt{52} \rceil = 8$ and then compute that $3^{-8} \equiv 24 \ (mod\ 53)$.

We compute the table

k	$3^k \ (mod\ 53)$	$41 \cdot 24^k \ (mod\ 53)$
0	1	41
1	3	30
2	9	31
3	27	2
4	28	48
5	31	39
6	40	35
7	14	45

It is not really necessary to compute the whole table, we need only compute just enough that we find one value in the second column and one value in the third column which are equal. Indeed, we find that $3^5 \equiv 31 \ (mod\ 53)$ and $41 \cdot 24^2 \equiv 41 \cdot (3^{-8})^2 \equiv 31 \ (mod\ 53)$ are two values which are equal.

We conclude that $3^{2 \cdot 8 + 5} \equiv 3^{21} \equiv 41 \ (mod\ 53)$ and that our value of x is 21.

Exercises:

1. Alice and Bob agree to communicate by the ElGamal crypto system. They agree on a public modulus of 307 and a primitive root 208. Alice then sends to Bob her public key of 98 (found by raising 208 to Alice's secret key mod 307). To find Alice's secret key, an attacker who

intercepts these exchanges calculates the following table.

i	$208^i \pmod{307}$	$98 \cdot 208^{-18i} \pmod{307}$
0	1	98
1	208	172
2	284	45
3	128	292
4	222	5
5	126	203
6	113	137
7	172	159
8	164	254
9	35	120
10	219	267
11	116	218
12	182	132
13	95	263
14	112	117
15	271	268
16	187	13
17	214	98

Next, Bob sends to Alice the pair $(Y, Z) = (133, 285)$.

(a) Find Alice's secret key.

(b) Find the message that Bob sends to Alice. Hint: $133^{-1} \equiv 277 \pmod{307}$