Chapter 4

The Discrete Log

THE D. L. P.

Let a, b, x and n be integers such that $b \equiv a^x \bmod n$. Suppose that we know a, b and n. Can we find x? If n is reasonably small, we could try values for x and after n tries we would have the answer. If n is very big, this is a very difficult problem; so much so that crypto systems depend on how hard it is

Ex. Let $a = 2$ $b = 15$ $n = 17$.
Start with $x = 1, 2, \ldots$ until we find $2^5 \equiv 15 \bmod 17$, hence $x = 5$.

The Diffie Hellman Key Exchange

A key exchange refers to Alice and Bob picking a key to use in a cryptosystem. In a classic paper, Diffie and Hellman were showing a key exchange, a method which had consequences far beyond a key exchange. It led to the beginning of public key cryptography.

DIFFIE HELLMAN

Alice picks a prime p and an integer c with $\gcd(c,p)=1$ and sends (c,p) to Bob

Alice picks an integer a and computes $x \equiv c^a \bmod p$ and sends x to Bob

Bob picks an integer b and computes $z = c^b \bmod p$ and sends z to Alice and also $K = x^b = c^{ab} \bmod p$.

Alice now computes $z^a = c^{ab} \bmod p = K$

Both Alice and Bob have K, the key that they wanted

Eve knows c, p, x and z where $x = c^a \bmod p$ and $z = c^b \bmod p$

She wants $K = c^{ab} \bmod p$

She can find K if she can find a and b which is the D.L.P. Alice and Bob are depending that she can't.

Ex Alice picks $p = 23$ and $c = 5$ and send (p, c) to Bob

Alice picks $a = 6$ and finds $x = c^a = 5^6 \bmod 23 = 8$ which she sends to Bob

Bob picks $b = 15$ and computes $y = c^b = 5^{15} \bmod 23 = 19 \rightarrow$ to Alice

and

$K = x^b = 8^{15} \bmod 23 = 2$

Alice computes $y^a \bmod p = 19^6 \bmod 23 = 2$

4 $\boxed{K = 2}$

Eve knows p ~~a~~ x y

$x = c^a \bmod p$ $y = c^b \bmod p$

Beside the DLP, she can ~~be~~ find k if she can compute $c^{ab} \bmod p$ from her information. This is called the D.H.P (Diffie-Hellman problem). Clearly, if she can solve the DLP, she can solve the DHP. So the DLP is at least as hard as the D.H.P. It is interesting that it is not known if solving the DHP also allows solving the DLP. An open problem.

EL-GAMAL CRYPTOSYSTEM.

Alice picks n and $a < n$ and j. Alice computes $b \equiv a^j \bmod n$ and makes public (a, b, n), her public key.

Bob wants to send message w to Alice. He picks k and computes $y = a^k \bmod n$ and $z = w b^k \bmod n$ and sends (y, z), his cypertext, to Alice.

Alice computes $z y^{-j} = w b^k a^{-kj} = w a^{kj} a^{-kj} = w \bmod n$ to get w.

Eve knows everything except j. To find it she needs to solve the D.L.P. from $y = a^k \bmod n$.

Ex Alice picks $n=7$, $a=3$, $j=5$
and computes $b = a^j \bmod n = 5$
She makes public $(a, b, n) = (3, 5, 7)$

Bob wants to send $w=4$ to
Alice He picks $k=2$ and finds
$y = a^k \bmod n = 3^2 \bmod 7 = 2$
$z = wb^k \bmod n = 4 \cdot 5^2 \bmod 7 = 2$
Bob sends $(y, z) = (2, 2)$ to Alice

Alice computes
$zy^{-j} = 2 \cdot 2^{-5} = 2 \cdot 32^{-1} \bmod 7 =$
$2 \cdot 4^{-1} \bmod 7 = 2 \cdot 2 = 4 = w.$

Computation fact. If $n=p$ a prime
Then $y^{-j} = y^{(n-1)-j}$ ~~and~~ mod n
and $n-1-j$ is positive so we
do not need to compute
an inverse

Ex. Alice picks $p = 31$, $a = 2$, $j = 3$
She finds $b = 2^3 \bmod 31 = 8$ and
makes public $(a, b, n) = (2, 8, 31)$

Bob wants to send

A	L	I	S	O	N	K	R	A	U	S	S
0	11	8	18	14	13	10	12	0	20	18	18

to Alice

Bob picks $k = 2$ and computes
$y = a^k = 2^2 \bmod 31 = 4$
$z = w b^k = w\, 8^2 = w\, 64 \bmod 31 = 2w$
Then

$z = 0 \cdot 2 = 0$
$z = 11 \cdot 2 = 22$
$z = 8 \cdot 2 = 16$
$z = 18 \cdot 2 = 5 \bmod 31$
$z = 14 \cdot 2 = 28$
$z = 13 \cdot 2 = 26$
$z = 10 \cdot 2 = 20$
$z = 12 \cdot 2 = 34 = 3 \bmod 31$
$z = 0 \cdot 2 = 0$
$z = 20 \cdot 2 = 40 = 9 \bmod 31$
$z = 18 \cdot 2 = 36 = 5 \bmod 31$
$z = 18 \cdot 2 = 36 = 5 \bmod 31$
y and all the z's are sent
to Alice

8

Alice computes $z y^{-j} = z \cdot 4^{-3} = z\, 4^{(31-1)-3}$

$= 2 \cdot 4^{27} \bmod 31$

To compute 4^{27}

$27 = 16 + 8 + 2 + 1$

$y = 4 \quad y^2 = 16 \quad y^4 = 8 \quad y^8 = 2 \quad y^{16} = 4$

(all mod 31)

$y^{27} = y^1 y^2 y^8 y^{16} = 4 \cdot 16 \cdot 2 \cdot 4 = 16 \bmod 31$

So $\quad z\, y^{27} \bmod 31$

$0 \cdot 16$	$= 0$	A
$22 \cdot 16$	$= 11$	L
$16 \cdot 16$	$= 8$	I
$5 \cdot 16$	$= 18$	S
$28 \cdot 16$	$= 14$	O
$26 \cdot 16$	$= 13$	N
$20 \cdot 16$	$= 16$	K
$3 \cdot 16$	$= 17$	R
$0 \cdot 16$	$= 0$	A
$9 \cdot 16$	$= 26$	U
$5 \cdot 16$	$= 18$	S
$5 \cdot 16$	$= 18$	S

9

ATTACK ON THE DLP
POLLARD λ (KANGAROO METHOD)

Problem. For integers n, $a<n$, b with $b = a^x \bmod n$, find x.

SET UP A HASH FUNCTION

: Let S be a set where S has about $\sqrt{n}$ elements

A hash function is a function $h: \mathbb{Z}_n \to S$ where $\mathbb{Z}_n$ is the integers mod n

Ex $n = 29$ $\sqrt{29} \sim 5$ $S = \{1, 2, 3, 4, 5\}$

Define h.

z	1	2	3	4	5	6	7	8	9	10	11	12
$h(z)$	1	2	3	4	5	4	3	2	1	2	3	4

z	13	14	15	16	17	18	19	20	21	22	23	24
$h(z)$	5	4	3	2	1	2	3	4	5	4	3	2

z	25	26	27	28	29
$h(z)$	1	2	3	4	5

10 METHOD:
MAKE TWO LISTS

$a_0 = a$
$a_1 = a_0 a^{h(a_0)}$
$a_2 = a_1 a^{h(a_1)}$
$a_3 = a_2 a^{h(a_2)}$
$\vdots$

$$a_{m+1} = a_m a^{h(a_m)} = a_{m-1} a^{h(a_{m-1})} a^{h(a_m)}$$
$$= a_{m-2} a^{h(a_{m-2})} a^{h(a_{m-1})} a^{h(a_m)} \ldots$$
$$= a^{1 + h(a_0) + \cdots + h(a_m)}$$

$b_0 = b$
$b_1 = b_0 a^{h(b_0)}$
$b_2 = b_1 a^{h(b_1)}$
$\vdots$
$b_{m+1} = b_n a^{h(b_n)} = b a^{h(b_0) + \cdots + h(b_n)}$

If (when)
$b_{n+1} = a_{m+1}$

$$x a^{h(b_0) + \cdots + h(b_n)} = a^{1 + h(a_0) + \cdots + h(a_m)}$$

$\rightarrow x = a^{(1 + \cdots h(a_m)) - (h(b_0) + \cdots + h(b_n))}$
which finds the exponent

Ex Let $a = 3$ $b = 2$ $n = 29$

$a_0 = a = 3$

$a_1 = a_0 a^{h(a_0)} = 3 \cdot 3^{h(3)} = 3 \cdot 3^9 = 3^4 = 23$

$a_2 = a_1 a^{h(a_1)} = 3^4 3^{h(23)} = 3^4 3^3 = 3^7 = 12$

$a_3 = a_2 a^{h(a_2)} = 3^7 3^{h(12)} = 3^7 3^4 = 3^{11} = 15$

$a_4 = a_3 a^{h(a_3)} = 3^{11} 3^{h(15)} = 3^{11} 3^3 = 3^{14} = 28$

$a_5 = a_4 a^{h(a_4)} = 3^{14} 3^4 = 3^{18} = 6$

$a_6 = a_5 a^{h(a_5)} = 3^{18} 3^4 = 3^{22} = 22$

$b_0 = 2$

$b_1 = b_0 a^{h(b_0)} = 2 \cdot 3^2 = 18$

$b_2 = b_1 a^{h(b_1)} = 2 \cdot 3^2 \cdot 3^2 = 2 \cdot 3^{14} = 17$

$b_3 = b_2 a^{h(b_2)} = 2 \cdot 3^4 3^{h(17)} = 2 \cdot 3^4 \cdot 3 = 2 \cdot 3^5 = 22$

$3^{22} = 22 = 2 \cdot 3^5 \mod 29$

$3^{17} = 2 \mod 29$

Mischief On The Key Exchange

Alice picks p and c, $\gcd(c, p) = 1$ and make (c, p) public.

Alice picks integer a, computes $x = c^a \bmod p$ and sends x to Bob

Bob picks an integer b and computes $z = c^b \bmod p$ and sends z to Alice.

Eve has p, c, x and z

Eve picks d and computes $y = c^d \bmod p$ and send y to Both Bob and Alice telling Bob it came from Alice and telling ~~Bob~~ Alice it came from Bob

Eve $c^{da} \bmod p$ as does Alice (Eve compute $c^{da} = (c^a)^d \bmod p$)

Now Eve pretends she is Bob using $c^{da} \bmod p$ as their key.

Eve computes $c^{db} \bmod p$ as does Bob and can exchange messages in Alice's name

HIERACHY

Given g and prime p

we have 3 protcols

I DLP Given $g^a \bmod p$, find a

II DHP Given $g^a \bmod p$, $g^b \bmod p$,

find $g^{ab} \bmod p$

III EL GAMAL. Review it

Alice picks a and sends

$(g, g^a \bmod p)$

She gets back $(g^b, g^{ab} m \bmod p)$

She can find $(g^b)^{-a} g^{ab} m \bmod p = m$

since she knows a.

Eve can not do that step

Abstracting, it is said that one

can solve the EL-GAMAL if given

(C_1, C_2) one can find $C_1^{-a} C_2 \bmod p$

In the real EL-GAMAL

$C_1 = g^b \quad C_2 = g^{ab} m$, all mod p

Suppose we can do this, solve

the abstract EL GAMAL

In the DHP we know $g^a, g^b \bmod p$

Let $C_1 = g^b \quad C_2 = 1$

$C_1^{-a} C_2 = g^{-ab} \cdot 1 \bmod p$ which we

Say we can solve because it is the EL-GAMAL PROBLEM. Hence we can then find $g^{ab} \bmod p$ and we have solved the DHP. Conclusion: If we can solve the EL-GAMAL, then we can solve the DHP

Conversely, in the EL-GAMAL we know $g^a \bmod p$ and $g^b \bmod p$ and $m g^{ab} \bmod p$. Knowing how to solve the DHP, we get $g^{ab} \bmod p$

Then $(g^b)^{-a} m g^{ab} \bmod p = m \bmod p$

(we know $(g^b)^{-a} = g^{-ab} \bmod p$ since we know $g^{ab} \bmod p$

So, if we can solve the DHP, we can solve the EL-GAMAL

CONCLUSION

The DHP and EL-GAMAL are equally hard. The DLP, as we have seen, is at least as hard as the DHP, so it could be the hardest. Could be because we don't know if solving one of the others will solve the DLP

Digital Signatures

Alice picks primes p and q with $p \equiv 1 \bmod q$ and $q < p$

Let g be an element of the multiplicative group of integers mod p. To find g pick a generator g_1 for Z_p^* and compute $g = g_1^{\left(\frac{p-1}{q}\right)}$

Then $g^q \equiv 1 \bmod (p-1)$

Alice picks a and computes $A = g^a \bmod p$. Alice sets out her verification key (p, q, g, A) for all to use

Alice has message D that she sends and wants to sign it

She picks K, $1 < K < q$

She computes

$$S_1 = (g^K \bmod p) \bmod q$$

$$S_2 = (D + aS_1)K^{-1} \bmod q$$

She signs the document: (S_1, S_2) (her signature)

Bob computes $V_1 = D S_2^{-1}$

$V_2 = S_1 S_2^{-1} \bmod q$

The check is does

$$g^{V_1} A^{V_2} \bmod p \bmod q = S_1$$

Proof

$$g^{V_1} A^{V_2} \bmod p \bmod q =$$

$$g^{D S_2^{-1}} A^{S_1 S_2^{-1}} \bmod p \bmod q =$$

$$g^{D S_2^{-1}} g^{a S_1 S_2^{-1}} \bmod p \bmod q =$$

$$g^{D S_2^{-1} + a S_1 S_2^{-1}} \bmod p \bmod q =$$

$$g^{(D + a S_1) S_2^{-1}} \bmod p \bmod q =$$

$$g^{k} \bmod p \bmod q = S_1$$

Ex Alice picks $p = 23$ $q = 11$ $g = 2$ $|g| = 11$

and $a = 5$

She finds $A = g^a \bmod 23 =$

$2^5 \bmod 23 = 9$

Her verification key:

$(p, q, g, A) = (23, 11, 2, 9)$

Suppose her message is $D = 3$

She picks $k = 2$, $k^{-1} \bmod 11 = 6$

Then $S_1 = g^k = 2^2 = 4$

$$S_2 = (D + aS_1)k^{-1} \bmod 11$$
$$= (3 + 5 \cdot 4)6 \bmod 11$$
$$= 6$$

Her signature $(S_1, S_2) = (4, 6)$

Bob finds $V_1 = D S_2^{-1} = 3 \cdot 6^{-1} = 3 \cdot 2 \bmod 11 = 6$

$V_2 = S_1 S_2^{-1} \bmod q = 4 \cdot 6^{-1} \bmod 11 = 8$

THEN

$g^{V_1} A^{V_2} = 2^6 \cdot 9^8 \bmod 23 \bmod 11 =$

$= 8 \cdot 12 \bmod 23 \bmod 11 = 4 = S_1$

Chapter 5

Lattices