LESSON 15

EL GAMAL

Collision Algorithm

POLLARD λ (OR KANGAROO)

The Discrete Log Problem
(D. L. P.)

Let a, b, x and n be integers such that $b \equiv a^x \bmod n$. Suppose a, b and n are known. Can x be found? If n is reasonably small, trial and error could be used. (Let $x = 1, 2, \ldots$) However, if n is big, this is a very difficult problem, one which can be used in cryptography

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 is Alice and Bob constructing a key to use in cryptography. In a classic 1976 paper, Diffie and Hellman were showing a key exchange and the ideas led to public key cryptography although that was not their intention

D-FFIE-Hellman

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

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

13

Bob picks an integer b, computes $z = c^{b} \bmod p$ and sends z and $K = x^{b} = c^{ab} \bmod p$ which he keeps. Alice computes $z^{a} \equiv c^{ab} \bmod p = K$.

Now Bob has $K = x^{b} \equiv c^{ab} \bmod p$

and Alice has

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

The common value they have K also gives them a public key to use.

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. But finding a or b is the hard D.L.P Alice and Bob are depending that Eve can not find them.

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

Alice picks $a = 6$ and finds

$$x = c^a \bmod p = 5^6 \bmod 23 = 8$$

which she send to Bob

Bob picks $b = 15$ and finds both

$$y = c^b = 5^{15} \bmod 23 = 19$$

and

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

Bob sends y to Alice who computes

$$y^a = c^{ab} \bmod 23$$

Both y^a and x^b equal

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

K is the key they will use

Notice Eve knows

$p = 23$, $c = 5$, $x = 8$, $y = 19$

How can Eve find K?

Summarizing, Eve knows p, c, x, y where

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

She can find $K = c^{cb} \bmod p$ if she can solve the DLP for a and b.

She can also find K if she can compute c^{ab} from her information. This is called the Diffie-Hellmen problem (or DHP). If she can solve the DLP then she can solve the DHP. So the DLP is at least as hard as the DHP. It is not known if solving the DHP will allow a solution to the DLP. Again the DHP is

Given $x \equiv c^a \bmod p$, $y = c^b \bmod p$, find

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

Problem. Let $c = 5$, $p = 23$

If $c^a \bmod p = 4$

$c^b \bmod p = 17$

Find $c^{cb} \bmod p$

The EL-GAMAL

Alice picks n and $a < n$ and j. She computes $b = a^j \bmod n$. Her public key is (a, b, n). Her private key is j.

Bob uses this to send Alice a message w. He picks k and computes

$y = a^k \bmod n$ and $z = wb^k \bmod n$.

(y, z) is the ciphertext that Bob sends to Alice

Alice computes

$$zy^{-j} = wb^k a^{-kj} = wa^{kj} a^{-kj} = w \bmod n = w$$

Eve knows a, b, n, y and z. She needs s. She can get it from $b \equiv a^s \bmod n$, but this is the D.L.P.

Ex. Alice picks $p = 31$, $a = 2$, $s = 3$

She finds $b = 2^3 \bmod p = 8$

She makes public

$$(a, b, p) = (2, 8, 31)$$

Bob sends

ALISON KRAUSS

w: 0 11 8 18 14 13 10 12 0 20 18 18

by picking $k = 2$ and computing

$$y = a^k = 4 \bmod 31 = 4$$

and values for z:

$$z = w b^k = w\, 8^2 \bmod 31 = 2w:$$

9

$z = 2w \bmod 31$

w	$z \bmod 31$
0	$2 \cdot 0 = 0$
11	$11 \cdot 2 = 22$
8	$8 \cdot 2 = 16$
18	$18 \cdot 2 = 5$
14	$14 \cdot 2 = 28$
13	$13 \cdot 2 = 26$
10	$10 \cdot 2 = 20$
17	$17 \cdot 2 = 3$
0	$0 \cdot 2 = 0$
20	$20 \cdot 2 = 9$
18	$18 \cdot 2 = 5$
18	$18 \cdot 2 = 5$

y and all the z's are sent

to Alice

#0

Alice computes

$$z y^{-1} = z \cdot 4^{-3} = z^{\cancel{(31-1)-3}}$$

$$= z\, 4^{(31-1)-3} = z\, 4^{27} \bmod 31$$

To compute

$$4^{27} = 4^{(16+8+2+1)}$$

$$= 4^{16} 4^{8} 4^{2} 4^{1}$$

By repeated squaring

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

So we find $z y^{27} \bmod 31$

z	$z y^{27} = z \cdot 16 \bmod 31$	
0	$0 \cdot 16 = 0$	A
22	$22 \cdot 16 = 11$	L
16	$16 \cdot 16 = 8$	I
5	$5 \cdot 16 = 18$	S
28	$28 \cdot 16 = 14$	O
26	$26 \cdot 16 = 13$	N
20	$20 \cdot 16 = 10$	K
3	$3 \cdot 16 = 17$	R
0	$0 \cdot 16 = 0$	A
9	$9 \cdot 16 = 20$	U
5	$5 \cdot 16 = 18$	S
5	$5 \cdot 16 = 18$	S

We used a computational fact: If the mod is a prime p, then

$$y^{-s} \equiv y^{(n-1)-s} \bmod p$$

n-1-s is positive so we do not have to find inverses.

ATTACK ON THE DLP

Given $b = a^x \bmod n$, and given a, b, n, find x.

We are going to look at Pollard's λ-method, or Kangaroo method as it is sometimes called. It is a collision algorithm, which we discuss first

Collesion Algorithm's

Given a set S, $|S| = s$

and τ distinguished elements in S, what is the probability of picking r elements, with replacement, and getting a distinguished one?

$Pr(\text{getting one or more}) = 1 - Pr(\text{getting none})$

TABLE

TRIES r	$Pr(\text{getting none})$	$Pr(\text{one or more})$
1	$\frac{s-\tau}{s}$	$1 - \frac{s-\tau}{s}$
2	$\left(\frac{s-\tau}{s}\right)^2$	$1 - \left(\frac{s-\tau}{s}\right)^2$
$\vdots$		
r	$\left(\frac{s-\tau}{s}\right)^r$	$1 - \left(\frac{s-\tau}{s}\right)^r$

Recall

$$e^x = 1 + x + \frac{x^2}{2!} + \cdots \frac{x^n}{n!}$$

1. $$e^{-x} = 1 - x + \frac{x^2}{2!} \cdots (-1)^n \frac{x^n}{n!}$$

Let $x = \tau/s$

$$e^{-\tau/s} \to e^{-\tau/s} \geq 1 - \tau/s \quad \text{from 1.}$$

So

$$e^{-(\tau/s)r} \geq (1 - \tau/s)^r$$

AND

$$1 - \left(\frac{s-\tau}{s}\right)^r \geq 1 - e^{-\tau r/s}$$

Ex An urn has 10 red and 8 blue balls. What is the probability of getting a red ball on 6 tries

$$1 - \left(1 - \frac{10}{18}\right)^6 \geq 1 - e^{-60/18} = 1 - e^{-4} \approx 1 - \frac{1}{54}$$

$$= \frac{53}{54} \approx .98$$

Ex 8 cards are dealt face up from a second deck, 8 cards are drawn with replacement. What is the probability of getting a match?

$$\Pr(\text{match}) = 1 - \Pr(\text{no match})$$
$$= 1 - \left(1 - \frac{8}{52}\right)^8 \geq 1 - e^{-\frac{64}{52}} \approx 73.7$$

Ex Let $|S| = n$. k elements are choosen and a list is made of which ones were picked. (with replacement). How large should k be to have at least 50% chance of a match?

$$\Pr(\text{match}) = 1 - \Pr(\text{no match}) = 1 - (1 - k/n)^k$$
$$\geq 1 - e^{-k^2/n} \overset{?}{=} 1/2$$
$$\rightarrow e^{-k^2/n} = 1/2$$
$$-k^2/n = \ln \tfrac{1}{2} = -\ln 2$$
$$k^2 = n \ln 2$$
$$k = \sqrt{n \ln 2} \approx .83\sqrt{n}$$

k is a little smaller than $\sqrt{n}$

Collision Algorithm

Prop Let G be a group and $g \in G$, $|g| = N$. If $g^x = h$ has a solution in G, then a solution can be found in $O(\sqrt{n})$ steps. (Each step is exponentiation in G)

Proof Let $x = y - z$

$$g^y = g^x g^z = h g^z$$

Pick $y_1, \ldots y_n$ integers

Compute $g^{y_1}, \ldots g^{y_n} \in \{1, \ldots, g^{N-1}\} = S$

Pick $z_1, \ldots z_n \in \mathbb{Z}$ (integers)

Compute $hg^{z_1}, \ldots hg^{z_n}$

$$\Pr(\text{at least one match}) = 1 - \Pr(\text{no match})$$

$$= 1 - \left(1 - \frac{n}{N}\right)^n \approx 1 - e^{-n^2/N}$$

If $n = 3\sqrt{N}$, $1 - e^{-n^2/N} = 1 - e^{-9} \approx 99.98$

If $n = 5\sqrt{N}$, $1 - e^{-n^2/N} = 1 - e^{-25} \approx 1 - 10^{-10}$

17

POLLARD λ or Kangaroo Method

Problem. For integers n, $a<n$, b with $b \equiv a^x \bmod n$, find x (D.L.P.)

Use a HASH FUCTION h

Let S be a set with about $\sqrt{n}$ elements. $\mathbb{Z}_n$ stands for the integers mod n. Let $h: \mathbb{Z}_n \to S$, a function from $\mathbb{Z}_n$ to S. h is called a hash function.

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

Define h as

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

13	14	15	16	17	18	19	20	21	22
5	4	3	2	1	2	3	4	5	4

23	24	25	26	27	28	29
3	2	1	2	3	4	5

METHOD: MAKE TWO LISTS

$$a_0 \equiv a$$
$$a_1 = a_0\, a^{h(a_0)}$$
$$a_2 = a_1\, a^{h(a_1)}$$
$$a_3 = a_2\, a^{h(a_2)}$$
$$\vdots$$
$$a_{m+1} = a_m\, a^{h(a_m)} = a_{m-1}\, a^{h(a_{m-1})}\, a^{h(a_m)}$$
$$= a_{m-2}\, a^{h(a_{m-2})}\, a^{h(a_{m-1})}\, a^{h(a_m)}$$
$$= \cdots$$
$$= a^{1+h(a_0)+\cdots+h(a_m)}$$

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

When

$$b_{n+1} = a_{m+1}$$
$$b\, a^{h(b_0)+\cdots+h(b_n)} = a^{1+h(a_0)+\cdots+h(a_m)}$$
$$\rightarrow \quad b = a^{1+h(a_0)+\cdots+h(a_m)-(h(b_0)+\cdots+h(b_n))}$$

which gives x to be the last exponent

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

$a_0 = a = 3$

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

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

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

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

$a_5 = a_4\, a^{h(a_4)} = 3^{14}\, a^{h(28)} = 3^{14}\, 3^4 = 3^{18} = 6$

$a_6 = a_5\, a^{h(a_5)} = 3^{18}\, a^{h(6)} = a^{18}\, 3^4 = 3^{22} = 22$

$b_0 = 2$

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

$b_2 = b_1\, a^{h(b_1)} = 2 \cdot 3^2\, 3^{h(18)} = 2 \cdot 3^2 \cdot 3^2 = 17$

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

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

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