Discrete Logs

Given:

$$x \text{ , } n \text{ and } (x^a \bmod n)$$

it is difficult to work out a.

Needs about $\sqrt{n}$ operations if n chosen carefully. Typically $n \approx 10^{300}$.

At 10^{10} operations per second that is 10^{140} seconds. That is about

31688087814028950237026896848936547772961188430045377341749689456739422515287677136410880421831824980353385555302050853043323953659

centuries.

Diffie-Hellman

1. Alice and Bob agree on x and n in public.
2. Alice and Bob choose large random numbers a and b.
3. Alice tells Bob $x^a \mathrm{mod}\ n$.
4. Bob tells Alice $x^b \mathrm{mod}\ n$.
5. Alice works out $(x^b \mathrm{mod}\ n)^a = x^{ab} \mathrm{mod}\ n$.
6. Bob works out $(x^a \mathrm{mod}\ n)^b = x^{ba} \mathrm{mod}\ n$.

Alice	**Crowded Room**	**Bob**
Agree: x, n		Agree: x, n
	x , n	
Choose: a		Choose: b
Shout:		Shout:
$x^a \mathrm{mod}\ n$		$x^b \mathrm{mod}\ n$
	$x^a \mathrm{mod}\ n$	
	$x^b \mathrm{mod}\ n$	
Calculate:		Calculate:
$x^{ab} \mathrm{mod}\ n$		$x^{ba} \mathrm{mod}\ n$

Binary

17_{10}	10001_2
23_{10}	10111_2
40_{10}	101000_2

In n binary digits (*bits*) you can count from 0 to $2^n - 1$. That is 2^n different possibilities. We'll need that later.

Monte Carlo Integration

If you want to integrate a function f over some area A then pick random points x_i in A and:

$$\int_A f(x)\,dx \approx |A| \frac{\sum_{n=1}^{N} f(x_n)}{N}$$

The more points the better (hopefully). Good for odd shaped A and hard to integrate f.

Sample C Generator

```
unsigned long next = 1;

int rand(void)
{
   next = next * 1103515245 + 12345;
   return (next/65536)%32768;
}

void srand(unsigned int seed)
{
   next = seed;
}
```

Working mod 2

+	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

Note that $+1 = -1$. This means if $x^3 + x + 1 = 0$ then $x^3 = x + 1$.

Primitive Polynomials

Max length sequence for $x^3 + x + 1 = 0$.

x^0	1					1
x^1	x			x		
x^2	x^2	x^2				
x^3	$x+1$			x	$+$	1
x^4	x^2+x	x^2	$+$	x		
x^5	$x+1+x^2$	x^2	$+$	x	$+$	1
x^6	$x+1+x^2+1$	x^2		$+$		1
x^7	$x+1+x$					1

Look at coefficient of x^2:

$$\underbrace{0010111}\,\underbrace{0010111}\ldots$$

Max Length Sequences

$$\underbrace{0010111}\underbrace{0010111}\ldots$$

How often does each pattern occur?

0	1	00	01	10	11	000
3	4	1	2	2	2	0
001	010	100	011	110	101	111
1	1	1	1	1	1	1

Looks good from a statistical point of view.

0,1,2,3

If we use:

$$x^8 + x^4 + x^3 + x^2 + 1 = 0$$

we get the sequence:

$$11111110111000111011010001111110011011011001\underbrace{00011011}_{0,1,2,3}111$$

01010010010100110100111100000010010000101000101110111100

1001110000110001100111010010110111010110101011000100010

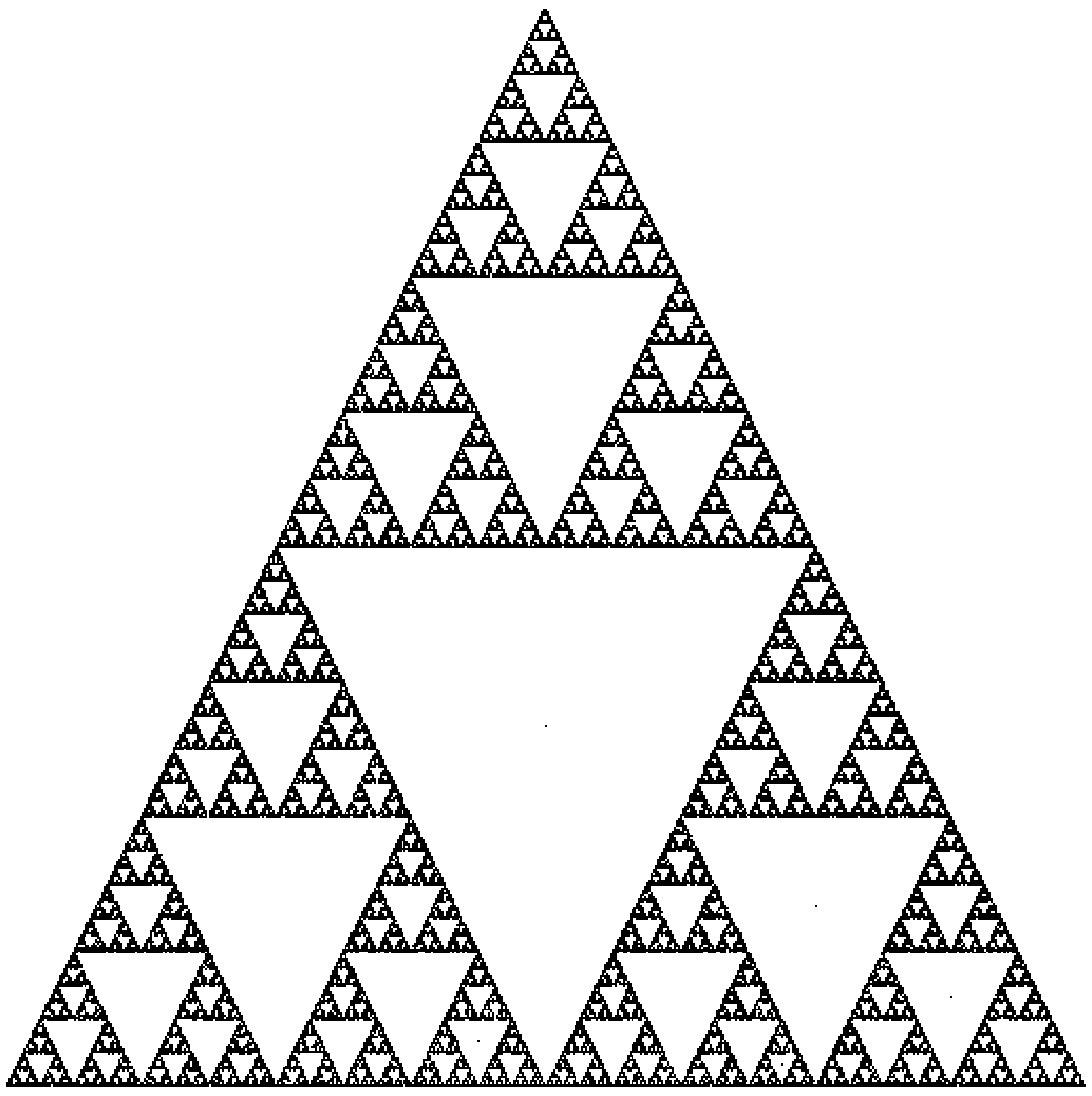
0110000100000010110011001010111001111100010101010000011

010111101100000000011110100001110010

Random Points in a triangle?

1. Set $i = 0$ and
$$\vec{P}_i = \frac{\vec{c}_0 + \vec{c}_1 + \vec{c}_2}{3}.$$
2. Let $i = i + 1$ and $n = rand() \mathrm{mod}\ 3$.
3. Get your new P_i by:
$$\vec{P}_i = \frac{\vec{c}_n + \vec{P}_{i-1}}{2}.$$
4. Go to Step 2.

If you plot the points they actually looks like this:



Measures

Mathematical way of looking at probability. We have a probability function p so that:

$$p : \text{Sets} \to [0, 1].$$

$p(E)$ is the probability of something in set E "happening". Given some sets $E_1, E_2, E_3, \ldots$ we want to be able to work out:

$$p(E_1')$$

$$p(E_1 \cup E_2 \cup E_3 \cdots)$$

$$p(E_1 \cap E_2 \cap E_3 \cdots)$$

We would also like these to make sense as probabilities. So we want things like:

$$p(\text{Whole set}) = 1$$

$$p(\text{Empty set}) = 0$$

$$p(E_1 \cup E_2 \cup \cdots) = p(E_1) + p(E_2) + \ldots$$

providing the E_n don't overlap.

Probability for a 6 sided die

$p(\{\}) = \frac{0}{6}$,

$p(\{1\}) = \frac{1}{6}, p(\{2\}) = \frac{1}{6}, p(\{3\}) = \frac{1}{6}, p(\{4\}) = \frac{1}{6}, p(\{5\}) = \frac{1}{6}$,
$p(\{6\}) = \frac{1}{6}$,

$p(\{1,2\}) = \frac{2}{6}, p(\{1,3\}) = \frac{2}{6}, p(\{1,4\}) = \frac{2}{6}, p(\{1,5\}) = \frac{2}{6}$,
$p(\{1,6\}) = \frac{2}{6}, p(\{2,3\}) = \frac{2}{6}, p(\{2,4\}) = \frac{2}{6}, p(\{2,5\}) = \frac{2}{6}$,
$p(\{2,6\}) = \frac{2}{6}, p(\{3,4\}) = \frac{2}{6}, p(\{3,5\}) = \frac{2}{6}, p(\{3,6\}) = \frac{2}{6}$,
$p(\{4,5\}) = \frac{2}{6}, p(\{4,6\}) = \frac{2}{6}, p(\{5,6\}) = \frac{2}{6}$,

$p(\{1,2,3\}) = \frac{3}{6}, p(\{1,2,4\}) = \frac{3}{6}, p(\{1,2,5\}) = \frac{3}{6}$,
$p(\{1,2,6\}) = \frac{3}{6}, p(\{1,3,4\}) = \frac{3}{6}, p(\{1,3,5\}) = \frac{3}{6}$,
$p(\{1,3,6\}) = \frac{3}{6}, p(\{1,4,5\}) = \frac{3}{6}, p(\{1,4,6\}) = \frac{3}{6}$,
$p(\{1,5,6\}) = \frac{3}{6}, p(\{2,3,4\}) = \frac{3}{6}, p(\{2,3,5\}) = \frac{3}{6}$,
$p(\{2,3,6\}) = \frac{3}{6}, p(\{2,4,5\}) = \frac{3}{6}, p(\{2,4,6\}) = \frac{3}{6}$,
$p(\{2,5,6\}) = \frac{3}{6}, p(\{3,4,5\}) = \frac{3}{6}, p(\{3,4,6\}) = \frac{3}{6}$,
$p(\{3,5,6\}) = \frac{3}{6}, p(\{4,5,6\}) = \frac{3}{6}$,

$p(\{1,2,3,4\}) = \frac{4}{6}, p(\{1,2,3,5\}) = \frac{4}{6}, p(\{1,2,3,6\}) = \frac{4}{6}$,
$p(\{1,2,4,5\}) = \frac{4}{6}, p(\{1,2,4,6\}) = \frac{4}{6}, p(\{1,2,5,6\}) = \frac{4}{6}$,
$p(\{1,3,4,5\}) = \frac{4}{6}, p(\{1,3,4,6\}) = \frac{4}{6}, p(\{1,3,5,6\}) = \frac{4}{6}$,
$p(\{1,4,5,6\}) = \frac{4}{6}, p(\{2,3,4,5\}) = \frac{4}{6}, p(\{2,3,4,6\}) = \frac{4}{6}$,
$p(\{2,3,5,6\}) = \frac{4}{6}, p(\{2,4,5,6\}) = \frac{4}{6}, p(\{3,4,5,6\}) = \frac{4}{6}$,

$p(\{1,2,3,4,5\}) = \frac{5}{6}, p(\{1,2,3,4,6\}) = \frac{5}{6}, p(\{1,2,3,5,6\}) = \frac{5}{6}$,
$p(\{1,2,4,5,6\}) = \frac{5}{6}, p(\{1,3,4,5,6\}) = \frac{5}{6}, p(\{2,3,4,5,6\}) = \frac{5}{6}$,

$p(\{1,2,3,4,5,6\}) = \frac{6}{6}$.

Bits of State

If your number generator has only n bits of state then your program can have at most 2^n different ways it can run.

Lotto Quick Pick:

$$\frac{42!}{6!36!} = 5245786$$

Requires $\log_2(5245786) \approx 23$ bits.

Shuffling Cards:

$$52! = 8.0658\ldots \times 10^{67}$$

Requires about $\log_2(52!) \approx 226$ bits (29 bytes).

Shuffling Election votes: For n votes we need about this many bits:

$$\begin{aligned}\log_2(n!) &= \sum_{m=1}^{n} \log_2(m) \\ &\approx \int_1^n \log_2(m)\, dm \\ &\approx n \log_2(n)\end{aligned}$$

For 1,000,000 votes that is about 20 million bits - or about 1.25MB!