ElGamal crypto system:

$G = \langle g \rangle$ Alice & Bob picks $\underline{a\ \&\ b}$

& g^a & g^b are made public.

Bob wants to send message M.

He picks k & computes g^k & $(g^a)^k = g^{ak}$ & Mg^{ak} & sends

$(g^k,\ Mg^{ak})$ to Alice.

Alice computes $(g^k)^a = g^{ak}$

& computes $(M g^{ak})\, g^{-ak} = M$.

$\mathbb{F}_q \setminus \{0\} = \mathbb{F}_q^\times$ is a cyclic group.

Example: $G = \mathbb{Z}_{29}^\times$ units of $\mathbb{Z}_{29}$

$= \langle 2 \rangle$

2 is public

$M=12$

$a=3$ & public : $2^3 = 8$

~~$b=5$ & public $2^5=32=3$~~

$k=5$ $\quad (2^k,\ M2^{ak}) = (3,\ 12\times 2^{3\times 5}) = (3,\ 12\times 8^5)$

$2^k = 32 = 3.$ $\quad = (3, 5)$ sent to Alice

Alice computes $(2^k)^a = (2^5)^3 = 3^3 = 27$

$27 \times 14 = 1 \mod 29$

$(-2)\times 14 = -28$

$(M2^{ak})2^{-ak} = 5 \times 27^{-1} =$

$= 5 \times 14$

$= 70$

$= \underline{12}$

For a gp G if $a, b \in G$

Find the smallest non-negative integer x

s.t. $a^x = b$

This eqn may not have a soln.

If there is a soln, then the smallest non negative integer is denoted by $\log_a b$ & it is called the discrete logarithm of b wrt a.

E.g., $\mathbb{Z}_5 = \{0, 1, 2, 3, 4, \cancel{5}\}$

$\mathbb{Z}_5^\times = \{1, 2, 3, 4, \cancel{5}\} = \{2, 2^2 = 4, 2^3 = 3, 2^4 = 1\} = \langle 2 \rangle$

$b \in \mathbb{Z}_5^\times$ $\quad 2^x = b$ has solns.

& $2^x = 4$ then $x = 2, 6, \ldots$

$\underline{\log_2 4 = 2}$ in $\mathbb{Z}_5^\times$

$\underline{3, 3^2 = 4, 3^3 = 2, 1}$ $\quad \underline{3^y = 4}$ $\quad \log_3 4 = 2$

$\log_3 1 = 0$

$\underline{\log_4 2 \text{ in } \mathbb{Z}_5^\times \; ?}$

$2 \notin \langle 4 \rangle = \{4, 1\}$ $\quad 4^x = 2$ has no soln.

$\log_4 2$ does not exist

$G = S_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$

$(1\ 2)^2 = 1 = (1\ 3)^2 = (2\ 3)^2$

$(1\ 2\ 3)^2 = (1\ 3\ 2)$

$(1\ 2\ 3)^3 = 1$

$(1\ 3\ 2)^2 = (1\ 2\ 3)$

$(1\ 3\ 2)^3 = 1$

$\log_{(1,3\,2)} (1\ 2\ 3) = 2$

$\log_{(1\ 2)} (1\ 2\ 3)$ does not exist

Observe in a cyclic group ~~of~~ with respect to a generator of the gp, discrete log exists for every element. (Since any $b \in \langle g \rangle$, $\exists\, x$ s.t. $g^x = b$

To find a, we can find $g, g^2, g^3, \ldots, g^{n-1}$ & compare b with each of them. (n = order of g)

Can we find $\log_g b$ with lesser operations

Shank's Baby-step Giant-step algorithm

$G = \langle g \rangle$ order g is n.

Have to find $\log_g a$ (i.e. finding x s.t. $g^x = a$

$m = \lceil \sqrt{n} \rceil$ least integer larger ~~than~~ or equal to $\sqrt{n}$.

$x = mq + r$ where $0 \le r \le m-1$

$0 \le q \le m-1$

as
$(m(m-1) + m - 1$
$= m^2 - \cancel{m} + \cancel{m} - 1$
$= m^2 - 1 \simeq n$

$a = g^x = g^{mq+r}$

$$\boxed{g^{mq} = a g^{-r}}$$

Baby-step Compute

$$B = \{ (a g^{-r}, r) \mid 0 \le r \le m-1 \} \subset G \times \{0, 1, \ldots, m-1\}.$$

Suppose $\boxed{a g^{-s} = 1}$ for $r = s$

Then $a = g^s$ so that $\log_g a = s$.

Suppose $a g^{-r} \neq 1$ for $r \in \{0, 1, \ldots, m-1\}$

Then go to the giant step.

Compute g^m, $g^{2m} = (g^m)^2$, g^{3m}, ...

Find q (smallest) s.t. $g^{mq} = a g^{-s}$ for some $s \in \{0, 1, \ldots, m-1\}$

Then $a = g^{mq+s}$

so that $\log_g a = mq + s$.

$$\boxed{2\sqrt{n} + \sqrt{n} \times \sqrt{n} = 2\sqrt{n} + n\ ?}$$

$n = 61$ $\quad G = \mathbb{Z}_{61}^{\times} = \{1, \ldots, 60\}$ mod 61.

$= \langle 2 \rangle = \{2, 4, 8, 16, 32, 3, 6, 12, 24,$
$48, 35$

$g = 2$, $g^{-1} = 31$

$m = \lceil \sqrt{61} \rceil = 8$, $a_1 = 6$, $a_2 = 7$ $\quad \log_2 7$, $\log_2 6$

$a g^{-r} \to (6, 0)$ $(6 \times 31, 1)$, $(6 \times 31^2, 2)$

$$\overset{\shortparallel}{3 \times (2\times 31)}$$
$$(3,1) \qquad (3\times 31,\ 2) = (32, 2),$$
$$\overset{\shortparallel}{(1+2)31}$$
$$31+1 = 32$$

$$(32\times 31,\ 3) = (16,3), \quad (16\times 31,\ 4) = (8,4), \quad (8\times 31,\ 5)$$
$$\overset{\shortparallel}{16\times \underline{2\times 31}} \qquad (4,5),$$

$$(4\times 31,\ 6) = (2,6), \quad (2\times 31,\ 7) = (1,7)$$

$$ag^{-7} = 1 \text{ so } a = g^7 \quad \therefore \quad \log_g a = 7$$

$$\boxed{\log_2 6 = 7}$$

Next, $\log_2 7 = ?$

$$(7,0), \ (7\times 31, 1) = ((1+4)\times 31, 1) = (31+2, 1) = (33,1)$$
$$(33\times 31, 2) = (1+2\times 16)\times 31,\ 2) = (31+16, 2) = (57, 2),$$