DISCRETE LOGARITHM

$Definition: --$

$for\ integer\ a\ relativly\ prime\ with\ n,\ and\ let\ M = \left\{k \in \mathbb{Z},\ a^k \equiv 1 \pmod n\right\}\ we\ define\ the$ $general\ expression\ \ a^m \equiv 1 \pmod n\ \ with\ m = minM$
$the\ existence\ of\ such\ m\ is\ always\ true,\ and\ the\ set\ M\ is\ non\ empty\ for\ \phi(n) \in M,\ and\ we\ say\ that$ $m\ is\ the\ legth\ of\ the\ period\ generated\ by\ a,\ and\ if\ m = \phi(n)\ for\ an\ a\ we\ say\ that\ a\ is\ primitive$ $root\ of\ n.$

$Property:$
$any\ integer\ z\ can\ be\ represented\ as\ z = q + k\phi(n)\ with\ 0 \leqslant q < \phi(n)$

$Proof:$
$we\ devid\ z\ by\ \phi(n)\ in\ the\ euclidian\ sence\ we\ get\ the\ desired\ result.$

$Property:$
$if\ a\ is\ primitive\ root\ for\ n,\ then\ a^p = a^q \bmod n\ if\ and\ only\ if\ p \equiv q \bmod \phi(n).$

$Proof:$
$for\ a\ is\ primitive\ root\ for\ n\ we\ take\ p = q + k\phi(n)\ we\ notice\ that\ if\ p \equiv q \bmod \phi(n),$ $a^p \equiv a^q \times a^{k\phi(n)} \equiv a^q \bmod n, if\ a^p = a^q \bmod n,\ then\ a^{p-q} = 1 \bmod n, meaning\ that$ $p - q =\ k\phi(n),\ hence\ p \equiv q \bmod \phi(n).$

$we\ introduce\ the\ discret\ logarithm\ as\ dlog_{n,a}(b) = i\ with\ a\ is\ a\ primitive\ root\ of\ n,\ that\ verify\ the$ $equation\ b \equiv a^i \bmod n,\ if\ x \equiv a^{dlog_{n,a}(x)} \bmod n,\ y \equiv a^{dlog_{n,a}(y)} \bmod n\ and\ xy \equiv a^{dlog_{n,a}(xy)} \bmod n$ $then\ xy \equiv (x \bmod n \times\ y \bmod n) \bmod n,\ hence\ a^{dlog_{n,a}(xy)} \equiv a^{dlog_{n,a}(x) + dlog_{n,a}(y)} \bmod n,\ and\ by\ the$ $previous\ property\ dlog_{n,a}(xy) \equiv (dlog_{n,a}(x)\ +\ dlog_{n,a}(y)) \bmod \phi(n)\ we\ can\ generaliz\ this\ to$ $dlog_{n,a}\left(x^y\right) \equiv y \times dlog_{n,a}(x) \bmod \phi(n)$

$--$