

DISCRETE LOGARITHMS

Definition : -----

for integer a relatively prime with n , and let $M = \{k \in \mathbb{Z}, a^k \equiv 1 \pmod{n}\}$ we define the

general expression $a^m \equiv 1 \pmod{n}$ with $m = \min M$

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 length 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 $0 \leq q < \phi(n)$

Proof :

we divide z by $\phi(n)$ in the euclidian sense we get the desired result.

Property :

if a is primitive root for n , then $a^p = a^q \pmod{n}$ if and only if $p \equiv q \pmod{\phi(n)}$.

Proof :

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

we introduce the discrete logarithm as $d\log_{n,a}(b) = i$ with a is a primitive root of n , that verify the equation $b \equiv a^i \pmod{n}$, if $x \equiv a^{d\log_{n,a}(x)} \pmod{n}$, $y \equiv a^{d\log_{n,a}(y)} \pmod{n}$ and $xy \equiv a^{d\log_{n,a}(xy)} \pmod{n}$ then $xy \equiv (x \pmod{n} \times y \pmod{n}) \pmod{n}$, hence $a^{d\log_{n,a}(xy)} \equiv a^{d\log_{n,a}(x) + d\log_{n,a}(y)} \pmod{n}$, and by the previous property $d\log_{n,a}(xy) \equiv (d\log_{n,a}(x) + d\log_{n,a}(y)) \pmod{\phi(n)}$ we can generalize this to $d\log_{n,a}(x^y) \equiv y \times d\log_{n,a}(x) \pmod{\phi(n)}$
