Discrete Logarithms:

Discrete logarithms are fundamental to a number of public key algorithms, including Deffie-Hellman key exchange and the digital signature algorithms.

Logarithms for Modular Arithmetic:

With ordinary positive real numbers, the logarithm function is the inverse of exponentiation.

The properties of logarithms include,

$$\log_x(1) = 0$$

$$\log_x(x) = 1$$

$$\log_x(yz) = \log_x(y) + \log_x(z)$$

$$\log_x(y^r) = r \times \log_x(y)$$

Consider a primitive root 'a' for some prime number 'p', then we know that the powers of 'a' from 1 through (p-1) produces each integer from 1 through (p-1) exactly once.

By definition of modular arithmatic we also know that any integer 'b' satisfies

$$b \equiv r \pmod{p} \text{ for some } r \; [0 \leq r \leq (p-1)]$$

We can also say that for any integer 'b' and a primitive root 'a' of a prime number 'p' we can find an unique exponent 'i' such that,

$$b \equiv a^i \pmod{p} \text{ where } 0 \leq i \leq (p-1)$$

This exponent 'i' is refferred to as the discrete Logarithm, of the number b for the base a (mod P).

We denote this as, $dlog_{a,p}(b)$

Note :

$$dlog_{a,p}(1) = 0 \quad \text{because } a^0 \bmod P = 1$$

$$dlog_{a,p}(a) = 1 \quad \text{because } a^1 \bmod P = a$$

Now consider

$$x = a^{dlog_{a,p}(x)} \bmod P \qquad y = a^{dlog_{a,p}(y)} \bmod P$$

$$xy = \boxed{a^{dlog_{a,p}(xy)} \bmod p} \quad \text{———} \quad ①$$

Using the rules of modular multiplication in eqⁿ ① we get

$$\cancel{a^{dlog_{a,p}(x,y)} \bmod P = \left[\left(a^{dlog_{a,p}(x)} \bmod P\right)\left(a^{dlog_{a,p}(y)} \bmod P\right)\right]}$$

$$\boxed{a^{\boxed{dlog_{a,p}(x,y)}} \bmod p} = \left[\left(a^{dlog_{a,p}(x)} \bmod p\right)\left(a^{dlog_{a,p}(y)} \bmod p\right)\right] \bmod P$$

$$= \left(a^{dlog_{a,p}(x) + dlog_{a,p}(y)}\right) \bmod p \quad \text{———} \quad ②$$

But now consider Euler's theorem, which states that, for every a and n that are relatively prime

$$a^{\phi(n)} \equiv 1 \pmod n$$

Any positive integer z can be expressed in the form $z = q + K\phi(n)$ with $0 \leq q < \phi(n)$

Therefore by Euler's theorem,

$$a^z \equiv a^q \pmod{n} \quad \text{if } z \equiv q \bmod \phi(n)$$

Applying this to the foregoing equality we have, (i.e from eq^n 2)

$$\boxed{\text{dlog}_{a,p}(x,y)} \equiv \left[\text{dlog}_{a,p}(x) + \text{dlog}_{a,p}(y)\right] \pmod{\phi(P)}$$

and generalizing,

$$\text{dlog}_{a,p}(y^r) \equiv \left[r \times \text{dlog}_{a,p}(y)\right] \pmod{\phi(P)}$$

This represents the analogy (relation) between true logarithms and discrete logarithms.

<u>Note</u>: Keep in mind that unique discrete logarithms mod 'n' to some base 'a' exists only if 'a' is a primitive root of 'n'.