1016-11-263 **Daniel R Cloutier*** (Daniel.R.Cloutier@alumni.rose-hulman.edu) and **Joshua R Holden** (holden@rose-hulman.edu), Rose-Hulman Institute of Technology, CM #125, 5500 Wabash Ave., Terre Haute, IN 47803-3999. *Mapping the Discrete Logarithm.*

The discrete logarithm is a problem that surfaces frequently in the field of cryptography as a result of using the transformation $g^a \bmod n$. This paper focuses on a prime modulus, p, for which it is shown that the basic structure of the functional graph is largely dependent on an interaction between g and $p-1$. In fact, there are precisely as many different functional graph structures as there are divisors of $p-1$. This paper extracts two of these structures, permutations and binary functional graphs. Estimates exist for the shape of a random permutation, but similar estimates must be created for the binary functional graphs. Experimental data suggests that both the permutations and binary functional graphs correspond well to the theoretical data which provides motivation to extend this to larger divisors of $p-1$ and study the impact this forced structure has on the many cryptographic algorithms that rely on the discrete logarithm for their security. This is especially applicable to those algorithms that require a "safe" prime ($p = 2q + 1$, where q is prime) modulus since all non-trivial functional graphs generated using a safe prime modulus can be analyzed by the framework presented here. (Received February 13, 2006)