Abstract

The absence of an efficient algorithm to solve the Discrete Logarithm Problem is often exploited in cryptography. While exponentiation with a modulus, $b^x \equiv a \pmod{m}$, is extremely fast with a modern computer, the inverse is decidedly not. At the present time, the best algorithms assume that the inverse mapping is completely random. Yet there is at least some structure, such as the fact that $b^1 \equiv b \pmod{m}$. To uncover additional structure that may be useful in constructing or refining algorithms, statistical methods are employed to compare mappings, $x \mapsto b^x \pmod{m}$, to random mappings. More concretely, structure will be defined by representing the mappings as functional graphs and using parameters from graph theory such as cycle length. Since the literature for random permutations is more extensive than other types of functional graphs, only permutations produced from the experimental mappings are considered.