1047-20-324 **Vladimir Shpilrain*** (shpil@groups.sci.ccny.cuny.edu), Department of Mathematics, The City College of New York, New York, NY 10031. *Search problems in group theory.* Preliminary report.

Decision problems are problems of the following nature: given a property $\mathcal{P}$ and an object $\mathcal{O}$, find out whether or not the object $\mathcal{O}$ has the property $\mathcal{P}$. On the other hand, search problems are of the following nature: given a property $\mathcal{P}$ and an object $\mathcal{O}$ with the property $\mathcal{P}$, find a proof (sometimes called a "witness") of the fact that $\mathcal{O}$ has the property $\mathcal{P}$. This is a substantial shift of paradigm, and in fact, studying search problems often gives rise to new research avenues in mathematics, very different from those prompted by addressing the corresponding decision problems. To give just a couple of examples from different areas of mathematics, we can mention (1) the isoperimetric function that can be used to measure the complexity of a proof that a given word is trivial in a given group; (2) Reidemeister moves that can be used to measure the complexity of a proof that two given knot diagrams are those of two isotopic knots.

In this talk, we are going to discuss various search problems in group theory, some of them motivated by cryptography. (Received February 01, 2009)