TITLE: Discrete logs and Diffie-Hellman problems in generic groups

ABSTRACT: Many current cryptosystems are based on the discrete logarithm problem, the Diffie-Hellman problem, or some variation. I will discuss a few of these, as well as what is known about their security using the "generic group" model. In particular, I'll focus on the 1-strong Diffie-Hellman problem, its security, and the implications this has.