1026-20-18   **Michal Sramka*** (`sramka@math.fau.edu`). *Generalized Discrete Logarithm and Stickel's Key Exchange Scheme.*

E. Stickel proposed a variation of the Diffie-Hellman key exchange scheme based on finite non-abelian groups, claiming that the underlying problem is more secure than the traditional discrete logarithm problem in cyclic groups. We show that the proposed scheme does not provide a higher level of security in comparison to the traditional Diffie-Hellman scheme. Furthermore, we briefly survey factorization methods for finite groups and investigate the possible cryptographic use of the generalized discrete logarithm $\beta = \alpha_1^{x_1} \cdots \alpha_r^{x_r}$ in finite non-cyclic groups. (Received February 10, 2007)