1125-20-1236 **Randall D. Helmstutler*** (rhelmstu@umw.edu), Department of Mathematics, 1301 College Avenue, Fredericksburg, VA 22401. *Generalized dihedral groups in non-commutative cryptographic protocols.* Preliminary report.

Given an abelian group A, we may construct the associated dihedral group $D(A)$ by allowing the group of order two to act on A by inversion. When not all elements of A have order two, the group $D(A)$ is non-abelian. This gives a convenient taxonomy to many unnamed non-abelian groups, these groups being amenable to analysis under several key exchange protocols in non-commutative cryptology. We will provide an overview of the most commonly studied non-commutative protocols, showing how these protocols behave under generalized dihedral groups. In particular, we highlight an example of a recently completed undergraduate research project, wherein Ko-Lee key exchange was shown to be susceptible to a quadratic-time attack. By studying these protocols using different classes of platform groups, similar open problems arise that are within reach of the undergraduate student with a solid course in group theory. (Received September 15, 2016)