**Speaker:** Maggie Habeeb  
**Title:** Aspects of Nonabelian Group Based Cryptography  
**Abstract:**  
Most common public key cryptosystems and public key exchange protocols presently in use, such as the RSA algorithm, Die-Hellman, and elliptic curve methods are number theory based and hence depend on the structure of abelian groups. The strength of computing machinery has made these techniques theoretically susceptible to attack and hence recently there has been an active line of research to develop cryptosystems and key exchange protocols using noncommutative cryptographic platforms. This line of investigation has been given the broad title of noncommutative algebraic cryptography. This was initiated by two public key protocols that used the braid groups, one by Ko, Lee et al., and one by Anshel, Anshel and Goldfeld. The study of these protocols and the group theory surrounding them has had a large effect on research in group theory. In this talk I survey some of these noncommutative group based methods and discuss several ideas in abstract infinite group theory that have arisen from them. I will mention about some new results.