1035-G1-1259 **Yesem Kurt*** (ykurt@randolphcollege.edu), 2500 Rivermont Ave., Lynchburg, VA. *Lessons from a Course in Cryptography.* Preliminary report.

I taught a course in Cryptography, an upper division course in the Mathematics Department, at Pomona College in the spring semester of 2007. The prerequisite for the course was Linear Algebra. It was a very enjoyable and enriching experience for me. We covered a variety of subjects including symmetric ciphers, their cryptanalysis, public key cryptosystems, RSA encryption method, Diffie-Hellman key agreement protocol, algorithms for factoring integers and for the discrete logarithm problem, knapsack and elliptic curve cryptosystems. In the meantime, we developed the necessary theory in algebra (groups, rings, finite fields, elliptic curves) and number theory (prime numbers, factorization, congruences, quadratic residues). My goal was to show students a variety of topics in cryptography, to discuss real life concerns, and to have them see how beautifully different theories in mathematics can be applied. It was the first time I taught such a course and at the end, I thought several things could be done better. This talk will be about my experince teaching this course; what I found useful, what went wrong, what would I change to make it better. (Received September 20, 2007)