1014-E1-383 **Yana Kortsarts*** (`ykortsarts@mail.widener.edu`), Widener University, Computer Science Department, One University Place, Chester, PA 19013. *Applications of Number Theory in Computer Science Curriculum.* Preliminary report.

In classical symmetric or private-key cryptosystems the encryption and decryption keys are either the same or can be easily found from each other. A new type of cryptosystem, call a public-key cryptosystem was invented in the 1970s. In a public key cryptosystem the fact that one knows how to encrypt the message does not mean that it can be easily decrypted. One of the earliest public-key cryptosystem was proposed by R.C. Merkle and M.E. Hellman in 1978. The Merkle-Hellman cryptosystem is based on the subset sum problem, a special case of the knapsack problem. There have been many variants of knapsack cryptosystems and the history of their development and the history of the development of their cryptanalysis are very important. We present a way to integrate knapsack cryptosystems into introductory cryptology courses and into introductory core computer science courses. Ideas for the undergraduate student projects are proposed and discussed. (Received September 13, 2005)