Cryptography

Programming 4

Ex 1 Implement Merkle-Hellman (*Hiding Information and Signatures in Trapdoor Knapsacks*) cryptosystem (use gmp-like library).

Ex 2 Implement Shamir's attack on the system (*A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem*).