Cryptography

Lab 3

Problem 1 Implement Merkle-Hellman [1] cryptosystem (use gmp-like library to support large numbers). Implement $\langle \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec} \rangle$ functions.

Problem 2 Implement Shamir's attack [2] on the system.

References

[1] Ralph Merkle and Martin E Hellman. Hiding information and signatures in trapdoor knapsacks. *Information Theory, IEEE Transactions on*, 24(5):525–530, 1978.

[2] Adi Shamir. A polynomial time algorithm for breaking the basic merkle-hellman cryptosystem. In *Advances in Cryptology*, pages 279–288. Springer, 1983.