

Cryptography

Lab 2

1. Implement Merkle-Puzzle cryptosystem [1] (read the story behind: <http://www.merkle.com/1974/>). Run your system for $N = 2^n$, where $n = 24, 32, 40$ and compute and/or estimate space and time requirements. You need to prepare a presentation of the system with $n = 24$ (at least).

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.