Prof. Sunar, EE-673. Spring 2014

Assignment #2

Advanced Cryptography

1. Develop a program in the language/platform of your choice to implement the Hellman time-memory trade-off (using the distinguished point method) for a simplified version of DES. You can use an existing DES implementation. You are encouraged to (but not required to) build a **Rainbow table** rather than the standard Hellman tables.

   For the following cases, report how long it took for the precomputation and storage as well as the time it takes for online key recovery.

   (a) (30-bits) Fix the first 26-bits of the DES key to zeroes.

   (b) (36-bits) Fix the first 20-bits of the DES key to zeroes.

   (c) (42-bits) Fix the first 14-bits of the DES key to zeroes.