ECS 227: Modern Cryptography
Homework 2

Phillip Rogaway

Out: 23 January 1996. Due: Thursday, 1 February 1996

4. With reference to to the structure of DES described in the handout distributed in class, explain why DES has the following *key complementation property*

$$\mathrm{DES}_k(x) \quad = \quad \overline{DES_{\overline{k}}(\overline{x})}$$

Under what assumptions can you use this property to reduce the time of exhaustive key search?

5. Complete the proof (do "Case 3") for showing how to find collisions in sha given collisions in SHA. That is, you are assuming $\mathrm{SHA}(M) \neq \mathrm{SHA}(M')$, where M has n blocks and M' has $n' \neq n$ blocks; and you should show how to efficiently find a $(k, x) \neq (k', x')$ such that $\mathrm{sha}(k, x) = \mathrm{sha}(k', x')$.

6. Formalize, under the asymptotic approach, what it means for H to be a collision-intractable hash function with respect to uniform polynomial-time adversaries. (Hint: let $H = \{H_n : \{0,1\}^* \to \{0,1\}^n\}$ be a family of functions.) Can you find a non-uniform notion for H to be collision-intractable?