ECS 227 — Modern Cryptography — Fall 96
Problem Set 1

Phillip Rogaway
Out: 3 October 1996. Due: 17 October 1996.

1. **The birthday problem.** Suppose you throw $q \geq 2$ balls into $N \geq 1$ bins. One by one, each ball is tossed into a random bin—the bin it falls in is independently of the outcome of all the other tosses. We say there is a *collision* if, at the end of the game, there is some bin with at least two balls in it. Let $C(N, q)$ denote the probability that there is a collision.

   Show that there are constants $c_1, c_2 > 0$ so that
   $$c_1 \cdot \frac{q^2}{N} \;\leq\; C(N,q) \;\leq\; c_2 \cdot \frac{q^2}{N} \qquad \text{whenever } q \leq \sqrt{N}\ .$$
   Compute the least number of students which need to be in a room such that the probablity that some two will have the same birthday is at least 1/2. Assume birthdays are uniform in $[1 \ldots 365]$.

   In general, how large does q have to be, as a function of N, before $C(N, q)$ is at least 1/2?

   Hints. You may find the following inequalities useful: for any real number $x \in [0, 1]$—
   $$\left(1 - \frac{1}{e}\right) \cdot x \;\leq\; 1 - e^{-x} \;\leq\; x\ .$$
   The upper bound is easy. For the lower bound first write an expression for $1 - C(N, q)$ *and then make use of the above inequalities.*

   What is the probablity that your protocol *fails*?

2. **DES key-complementation property.** Explain why DES satisfies the following relation:
   $$\mathrm{DES}_k(x) \quad = \quad \overline{DES_{\overline{k}}(\overline{x})}$$
   Can you use this property to recover the key from a (plaintext, ciphertext) pair of your choice in worst-case 2^{55} encryptions? From a couple of chosen (plaintext, ciphertext) pairs?

3. Keyed hash functions. We say that the compression function $h : \{0,1\}^\ell \times \{0,1\}^L \to \{0,1\}^\ell$ is *announced-key target-collision intractable* if for any adversary A who chooses a message block $x \in \{0,1\}^L$ and then is given a random chaining value $k \in \{0,1\}^\ell$, A has almost no chance to find a second message block $x' \in \{0,1\}^L$, $x' \neq x$, such that $h(k,x) = h(k,x')$. (This is a much *weaker* requirement than collision-intractability, as now we are taking away the adversary's ability to choose the k, k' which "work" for x, x'.)

Similarly, $H : \{0,1\}^\ell \times \{0,1\}^* \to \{0,1\}^\ell$ is *announced-key target-collision intractable* if for any adversary B who chooses a message $M \in \{0,1\}^*$ and then is given a random chaining value $k \in \{0,1\}^\ell$, B has almost no chance to find a message $M' \in \{0,1\}^*$, $M' \neq M$ such that $H(k,M) = H(k,M')$.

Assume that h is announced-key target-collision intractable. Let H be obtained from h according to the Merkle construction (ie., the exact same manner that SHA is obtained from sha).

Is H necessarily announced-key collision intractable? Prove your answer.

Construct a hash function $H^* : \{0,1\}^\ell \times \{0,1\}^* \to \{0,1\}^\ell$ out of h and prove that H^* *is* announced-key target-collision intractable.