

Homework 2 ICS 247 Security Algorithms

Due: Friday, January 24, 2003, in class

Please answer the following questions, each of which is worth 10 points.

1. Let π be a permutation of the integers $0, 1, 2, \dots, 2^n - 1$ such that $\pi(m)$ gives the permuted value of m , $0 \leq m < 2^n$. That is, π maps the set of n -bit integers into itself in a one-to-one fashion (that is, it is a *bijection*). The encryption scheme DES is one such permutation for 64-bit integers. We say that such a permutation π has a *fixed point* if there is an m such that $\pi(m) = m$. In other words, for any π that is a permutation encryption scheme, if π has a fixed point, then there is an input m such that the encryption of m is m itself (which is clearly not desirable). Show the somewhat surprising fact that if π is chosen at random, then it has a 60% chance of having a fixed point.
2. Prove that Euclid's algorithm for computing $\gcd(a, b)$ uses $O(\log \max\{a, b\})$ arithmetic operations.
3. Suppose a hash function f randomly maps n integers into the range $[0, 2n - 1]$.
 - (a) Give a good bound on the probability that two integers collide.
 - (b) Show that with probability at least $1 - 1/n$, the number of integers colliding for any given output value is $O(\log n)$.
4. Describe a dynamic authenticated dictionary scheme, which can process insertions and deletions of items without completely reconstructing the data structure used to maintain the set. What is the running time of your update methods?
5. Use Fermat's little theorem to compute $3^{201} \bmod 11$. Show your work.