Homework 25, due November 3

(1) Read the following Wikipedia pages, and write something you learned from each one:
   (a) Cryptographic hash function
   (b) Merkle-Damgard construction (the hash functions MD5, SHA-1, and SHA-2 are based on the Merkle-Damgard construction)
   (c) Sponge function (the hash function SHA-3 is based on a sponge construction; NIST wanted a hash which was structurally different from the MD5/SHA-1 family of hashes)

(2) In a family of six, what is the probability that no two people have birthdays in the same month? Assume that all months have equal probabilities.

(3) (a) How many people should there be in a room in order to have a 99 percent chance that at least two have the same birthday?
   (b) How many people should there be in a room in order to have a 100 percent chance that at least two have the same birthday?