IV054 Coding, Cryptography and Cryptographic Protocols
2011 - Exercises X.

1. Suppose you can predict results of coin flips. At least how many coin flips would you need to prove this to your friend without revealing your secret so that he would be at least $n\%$ sure about it?

2. Decide whether the zero-knowledge proof for quadratic residua is perfect zero-knowledge or computationally zero knowledge. Suppose for the sake of simplicity that the protocol consists of only one round. Explain your reasoning.

3. Provide a proof sketch that the protocol below constitutes a zero-knowledge proof for graphs containing Hamiltonian cycles.

   Common Input: an undirected graph $G = (V, E)$ with $|V| = n$.
   Auxiliary Input to Prover: a Hamiltonian cycle C, $C \subseteq E$, in G.

   Steps of the protocol:

   (a) **Prover's first step (P1):** The prover selects a random permutation Π over the vertices V, and commits (using a perfectly-binding commitment scheme) to the entries of the adjacency matrix of the resulting permuted graph. That is, he sends an n-by-n matrix where the $(\Pi(i), \Pi(j))$-th entry is a commitment to 1 if $(i, j) \in E$, and is a commitment to 0 otherwise.

   (b) **Verifier's first step (V1):** The verifier uniformly selects $\sigma \in \{0, 1\}$ and sends it to the prover.

   (c) **Prover's second step (P2):**

      i. If $\sigma = 0$, the prover sends Π to the verifier and opens all of the commitments in the adjacency matrix.

      ii. If $\sigma = 1$, the prover opens the commitments of entries $(\Pi(i), \Pi(j))$ for which $(i, j) \in C$ (and only these commitments).

   (d) **Verifier's second step (V2):**

      i. If $\sigma = 0$, the verifier checks that the revealed graph is isomorphic to G via Π.

      ii. If $\sigma = 1$, the verifier checks that all revealed values are 1 and that the corresponding entries form a Hamiltonian cycle.

4. Let Peggy and Victor share a Sudoku puzzle. How can Peggy prove to Victor that she has a solution to this puzzle, while not giving away any information about the solution. Non-cryptographic (practical) solutions are acceptable.