Suggested Answers to Homework 3.1

1. Prob(no collision after first person announced) = 1.
2. Prob(no collision after second person) = $\frac{364}{365}$.
3. Prob(no collision after third person) = $\frac{364}{365} \times \frac{363}{365}$.
4. Prob(no collision after k persons) = $\frac{365}{365} \times \ldots \times \frac{365-k+1}{365}$.
6. Rewrite the formula in Q4 as $\prod_{i=0}^{i=k-1}(1 - \frac{i}{365})$.
7. $e^0 \times \ldots \times e^{-\frac{k-1}{365}}$ = exp $(\sum_{i=0}^{i=k-1} \frac{-i}{365})$= $e^{-k(k-1)/730}$.
8. It is easy to verify that if k > 23, then $e^{-k(k-1)/730}$ < 0.5.

9. Trudy can trick Bob into signing a malicious contract. She creates a fair contract, and finds many variations of it without changing its meaning (inserting whitespace, punctuations, etc). She also creates many similar variations of the malicious contract. She then applies the hash function to all the variations of the contracts, and finds a version of the fair contract, say F, that hashes to the same digest as a version of the malicious contract, say M. Trudy presents F to Bob and asks him to sign its digest. She then attaches the signed digest to M and uses it to "prove" that Bob signed M.