This is a 50-minute in class closed book exam. All questions are straightforward. Please show all work and write legibly. Grading will take into account the clarity of your answer. If your answer is correct you will get full credit. If your answer is not correct, partial credit will depend on how clearly you explain what you are doing.

1. Given an encoding algorithm \( E \) and a decoding algorithm \( D \) such that \( E(D(m)) = m \) and \( D(E(m)) = m \) how would you set up a public key cryptosystem? In particular, answer the following questions:

   (a) What is made public and what is kept private?
      \[ \text{Solution} \] keep \( D \) private and make \( E \) public.

   (b) How would you send a message, \( m \), so that no one besides the intended recipient can read it? You do not need to explain padding or any sophisticated aspect, just a one sentence explaining the basic method.
      \[ \text{Solution} \] Grab the intended recipient’s public key \( E \) and send the encryption \( E(m) \).

   (c) How does one sign an encrypted message?
      \[ \text{Solution} \] One signs a message by applying your private decoding algorithm to \( m \). To send it you send \( E_{\text{recipient}}(\text{‘Hi Bob, this is Jason’} + D_{\text{Jason}}(m)) \).

2. We wish to detect a rare disease. We design a test such that it returns ‘yes’ or ‘no’ for detecting the disease and:

\[
P(\text{no|disease}) = P(\text{yes|no disease}).
\]

Suppose we know the disease occurs with probability \( P(\text{disease}) \) and would like to set \( P(\text{disease|yes}) \) to a specific value. How good must the test be, or precisely, what is \( P(\text{yes|disease}) \)?

Write out an equation for \( P(\text{yes|disease}) \) in terms of the givens \( P(\text{disease}) \) and \( P(\text{disease|yes}) \). Once you have an equation in terms of \( P(\text{yes|disease}) \), \( P(\text{disease}) \), and \( P(\text{disease|yes}) \) you do not need to simplify.

\[ \text{Solution} \]

\[
P(\text{yes|disease}) = \frac{P(\text{disease|yes})P(\text{yes})}{P(\text{disease})}
= \frac{P(\text{disease|yes})(P(\text{yes|disease})P(\text{disease}) + P(\text{yes|no disease})P(\text{no disease}))}{P(\text{disease})}
= \frac{P(\text{disease|yes})(P(\text{yes|disease})P(\text{disease}) + (1 - P(\text{yes|disease}))(1 - P(\text{disease})))}{P(\text{disease})}
\]

There are three stages one must realize:
(a) Baye’s Rule
(b) What $P(\text{yes})$ is
(c) What $P(\text{yes|no disease})$ is

3. Given 100 boxes some of which have paint spots as listed below how many boxes have no paint spots?

(a) 40 with some red paint
(b) 60 with some blue paint
(c) 10 with some black paint
(d) 30 with some red and some blue
(e) 5 with some red and some black
(f) 5 with some blue and some black
(g) 2 with some of all three colors

Solution By inclusion-exclusion principle:

\[ P(\text{no paint}) = \text{Total Boxes} - \text{Those of at least one color} + \text{Those of at least two colors} - \text{Those of all three colors} \]
\[ = 100 - (40 + 60 + 10) + (30 + 5 + 5) - 2 \]
\[ = 28 \]

4. Consider two operations on a $2 \times 2$ square. The operations $r$ which is a rotation of $180^\circ$ and $f$ which is a flip about the diagonal axes from upper left to lower right.

(a) What are the additional operations that need to be added to form a group?

\[ \{I, r, f, rf\} \]

(b) Write out the group table.

\[ \begin{array}{cccc}
I & r & f & rf \\
I & I & r & f & rf \\
r & r & I & rf & f \\
f & f & rf & I & r \\
r & rf & f & r & I \\
\end{array} \]

OVER FOR FIGURE
\[
\begin{array}{c|c|c|c|c}
1 & 2 & \multicolumn{1}{|c}{r} & 4 & 3 \\
3 & 4 & & 2 & 1 \\
\end{array}
\]

\[
\begin{array}{c|c|c|c|c}
1 & 2 & \multicolumn{1}{|c}{f} & 1 & 3 \\
3 & 4 & & 2 & 4 \\
\end{array}
\]