The 5 questions on this exam had respective point values 7, 6, 4, 7 and 6. The total point value was thus 30 (same as on first midterm).

1. Consider the miniature cryptosystem in which \( \mathcal{M} = \{ a, b \} \), \( \mathcal{K} = \{ K_1, K_2, K_3 \} \), \( \mathcal{C} = \{ 1, 2, 3, 4 \} \) and the encryption functions are given by:

\[
\begin{align*}
 e_{K_1} : a &\mapsto 1, b \mapsto 2, \\
 e_{K_2} : a &\mapsto 2, b \mapsto 3, \\
 e_{K_3} : a &\mapsto 3, b \mapsto 4.
\end{align*}
\]

Further, assume that the probability distributions for the plaintexts and keys are as follows:

\[
\Pr(a) = \frac{1}{4}, \quad \Pr(b) = \frac{3}{4} ; \quad \Pr(K_1) = \frac{1}{2}, \quad \Pr(K_2) = \Pr(K_3) = \frac{1}{4}.
\]

a. Compute the probability distribution on \( \mathcal{C} = \{ 1, 2, 3, 4 \} \).

For \( c \in \mathcal{C} \), the probability \( \Pr(c) \) is the sum of all terms \( \Pr(m) \Pr(k) \) (\( m \in \mathcal{M}, k \in \mathcal{K} \)) for which \( e_k(m) = c \).

Thus, for example, \( \Pr(2) = \Pr(k_1) \Pr(b) + \Pr(k_2) \Pr(a) = 7/16 \). The other values that I got were \( \Pr(1) = 2/16, \Pr(3) = 4/16, \Pr(4) = 3/16 \). Thankfully, \( 7 + 2 + 4 + 3 = 16 \), which serves as a sort of check; it would have been disheartening if the sum of the probabilities had been different from 1!

b. Compute the conditional probabilities \( \Pr(a|3) \) and \( \Pr(b|3) \).

\[
\Pr(a|3) = \frac{\Pr(a,3)}{\Pr(3)} = \frac{\Pr(a) \Pr(k_3)}{\Pr(3)} = \frac{1/4 \cdot 1/4}{1} = 1/4.
\]

This is also the probability \( \Pr(a) \).

Similarly, \( \Pr(b|3) = \frac{\Pr(b,3)}{\Pr(3)} = \frac{\Pr(b) \Pr(k_3)}{\Pr(3)} = \frac{3/4}{4} = 3/4 \), which also happens to be \( \Pr(b) \). These are two of the necessary conditions for perfect secrecy, though it turns out that this cryptosystem does not possess perfect secrecy.

2. Suppose that \( N \) is a composite number for which we have found the four mod \( N \) congruences

\[
\begin{align*}
399^2 &\equiv 2^5 \cdot 3 \cdot 5, \\
763^2 &\equiv 2^6 \cdot 3, \\
773^2 &\equiv 2^6 \cdot 3^5, \\
976^2 &\equiv 2^6 \cdot 5^3.
\end{align*}
\]

a. Show that we can multiply two or more of these congruences together so as to obtain a congruence whose right-hand term is a perfect square. (The congruence then reads \( a^2 \equiv b^2 \), where \( a \) and \( b \) are numbers mod \( N \).)

In case you were wondering, \( N = 52907 \). We could multiply the second and third congruences together to get

\[
763^2 \cdot 773^2 \equiv (2^6 \cdot 3^3)^2.
\]
b. Assume that the congruence \( a^2 \equiv b^2 \mod N \) in part (a) satisfies \( a \neq \pm b \mod N \). Explain how we can then find a non-trivial factor of \( N \).

As you know, it’s enough to consider \( \gcd(a \pm b, N) \), and you get non-trivial factors. For example, \( 763 \cdot 773 \equiv 7822 \mod 52907 \), while \( 26^2 \cdot 3^2 = 12^3 = 1728 \) (which is the number of units in a great gross). We have \( 1728^2 \equiv 7822^2 \equiv 23192 \). We find \( \gcd(7822 - 1728, N) = 277 \), \( \gcd(7822 + 1728, N) = 191 \). Note also that \( 277 \cdot 191 = 52907 \).

At the end of the exam, some students came up to ask why the gcd’s are non-trivial. Here’s the most elementary possible explanation: If \( a^2 \equiv b^2 \mod N \), then \( N \) divides the product \( rs \), where \( r = a + b \), \( s = a - b \). A general principle is that if \( N \) divides \( rs \) and \( \gcd(N, r) = 1 \), then \( N \) divides \( s \). To see this general principle, use the hypothesis \( \gcd(N, r) = 1 \) to write \( 1 = xr + yN \), where \( x \) and \( y \) are integers. Multiply by \( s \) to get \( s = x(rs) + ys(N) \); in this sum, both summands are divisible by \( N \), and therefore the left-hand term \( s \) is divisible by \( N \). In our situation, \( N \) cannot divide either \( r = a + b \) or \( s = a - b \) because of the hypothesis \( a \neq \pm b \mod N \). Accordingly, we certainly can’t have \( \gcd(r, N) = N \) or \( \gcd(s, N) = N \). Also, because of the general principle, we can’t have \( \gcd(r, N) = 1 \) or \( \gcd(s, N) = 1 \). Thus both gcd’s are strictly intermediate between 1 and \( N \) and therefore are “non-trivial.”

3. Pokerhontas drops the King of ♣, the King of ♥ and the Ace of ♠ into an urn. She then removes two of the cards without looking at them. (a) If it is known that one of the two cards is a king, what is the probability that both cards are kings? (b) If it is known that one of the two cards is the King of ♥, what is the probability that both cards are kings?

The answers are (a) 1/3 and (b) 1/2. See http://math.berkeley.edu/~ribet/Math55/old_final_sols.ps for details.

4. a. Determine whether or not \(-6\) is a square modulo the prime number 456767. (Note that 456767 \( \equiv 7 \mod 8.\))

Type “kronecker(-6,456767)” into gp, and the answer -1 comes back. So I expect that \(-6\) is not a square. Note that \(-6 = -1 \cdot 2 \cdot 3\). Because \( p := 456767 \equiv -1 \mod 4 \), \(-1\) is not a square mod \( p \). Since \( p \equiv 7 \mod 8 \), \( 2 \) is a square mod \( p \). As far as \( 3 \) goes, we have \( \left( \frac{3}{p} \right) = -\left( \frac{p}{3} \right) \) by quadratic reciprocity; note that both \( p \) and \( 3 \) are \( 3 \) mod 4. But \( p \equiv 2 \mod 3 \), so \( p \) isn’t a square mod 3. Thus \( 3 \) is a square mod \( p \), so that \(-6\) is the product of a non-square and two squares. Thus it’s a non-square, i.e., it isn’t a square.

b. Suppose that the prime number \( p \) is written as \( a^2 + b^2 \), with \( a \) odd and \( b \) even. Using quadratic reciprocity for the Jacobi symbol, show that \( a \) is a square mod \( p \). (For example, \( 109 = 3^2 + 10^2 \); you are showing that \( 3 \) is a square mod 109.)

This is presumably going to be a hard problem. On the other hand, I did it in class! First of all, squares are all either 0 or 1 mod 4. Thus \( p \equiv 1 \mod 4 \). So by quadratic reciprocity for the Jacobi symbol, \( \left( \frac{a}{p} \right) = \left( \frac{p}{a} \right) \).

On the other hand, mod \( a \) we have \( p = a^2 + b^2 \equiv b^2 \). Thus \( \left( \frac{a}{p} \right) = \left( \frac{b}{a} \right)^2 = +1. \)
5. When $p = 227$ and $g = 2$, we have the mod $p$ congruences

\[
\begin{align*}
g^{20} &\equiv 3^2 \cdot 7, \\
g^{57} &\equiv 3 \cdot 5, \\
g^{128} &\equiv 3 \cdot 7^2.
\end{align*}
\]

Use this information to find the discrete logarithms $\log_g 3$, $\log_g 5$, $\log_g 7$. (It may help to know that the inverse of 3 mod $p - 1$ is 151.)

Let $x = \log_g 2$, $y = \log_g 3$, $z = \log_g 7$; these are numbers mod $p - 1$. We have three equations for $x$, $y$ and $z$:

\[
\begin{align*}
2x + z &= 20, \\
x + 2z &= 128, \\
x + y &= 57.
\end{align*}
\]

I wrote the last equation last because we can use it to find $y$ once we have the value of $x$. The first two equations together can be used to find $x$ and $z$ by Gaussian elimination à la Math 54. The only pitfall to avoid is that you can’t cleanly divide by 2; for example, if you have figured out that $x \equiv 46$ mod 226 and glean from this that $2z \equiv 128 - 46 = 82$, dividing by 2 will tell you only that $z \equiv 41$ mod 113. In fact, the correct value of $z$ is $41 + 113 = 154$ (mod $p - 1$). The other values are $x = 46$, as I said, and $y = 11$. (Again, both of these are mod 226.) As announced in class, I’ll be perfectly happy with answers like $20 - 2 \cdot 46$ for $z$. On the other hand, I will balk at answers that are written as fractions, for example “$x = -88/3$.” Fortunately, to make your lives easier, I told you in the problem that $151 = 1/3$.  
