Math 565, Problem Set 6: *due Friday, February 16*

1. Prove that the three parts of the quadratic reciprocity theorem are equivalent to the following three concise formulas, where p and q are odd primes:

   a) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

   b) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

   c) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

2. Suppose that the plaintext space $\mathcal{M}$ of a cryptosystem is the set of bit strings of length $2b$. Let e_k and d_k be the encryption and decryption functions associated with a key $k \in \mathcal{K}$. The problem describes a method of turning the original deterministic cryptosystem into a probabilistic cryptosystem. Alice sends Bob an encrypted message by performing the following steps:

   - Alice chooses a b-bit message m' to encrypt.
   - Alice chooses a string r consisting of b random bits.
   - Alice sets $m = r||(r \oplus m')$, where $||$ denotes concatenation of strings and $\oplus$ denotes bitwise addition in $\mathbb{F}_2^b$. Notice that m is a string of length $2b$.
   - Alice computes $c = e_k(m)$ and sends the ciphertext c to Bob.

   Just to be clear, here is an example of the computation of m from m' in the case $b = 3$: suppose $m' = 011$ and $r = 101$. Then $r \oplus m' = 110$, so $m = 101||110 = 101110$.

   a) Explain how Bob decrypts Alice's message and recovers the plaintext m'. We assume, of course, that Bob knkows the decryption function d_k.

   b) If the plaintexts and the ciphertexts of the original cryptosystem have the same length, what is the message expansion ratio of the new probabilistic cryptosystem?

   c) More generally, if the original cryptosystem has a message expansion ratio of μ, what is the message expansion ratio of the new probabilistic cryptosystem?