# *Quiz 4*

EECS 203

Spring 2016

**Name (Print):** _____

**uniqname (Print):** _____

**Instructions**. You have ***25*** minutes to complete this quiz. You may not use any sources of information, including electronic devices, textbooks, or notes. Leave at least one seat between yourself and other students. Please write clearly. If we cannot read your writing, it will not be graded.

**Honor Code**. This course operates under the rules of the College of Engineering Honor Code. Your signature endorses the pledge below. After you finish your exam, please sign on the line below:

*I have neither given nor received aid on this examination, nor have I concealed any violations of the Honor Code.*

_____

1. Recall the following from our text: **[10 points]**

## RSA Decryption

The plaintext message can be quickly recovered from a ciphertext message when the decryption key $d$, an inverse of $e$ modulo $(p-1)(q-1)$, is known. [Such an inverse exists because $\gcd(e,(p-1)(q-1))=1$.] To see this, note that if $de \equiv 1 \pmod{(p-1)(q-1)}$, there is an integer $k$ such that $de = 1 + k(p-1)(q-1)$. It follows that

$$C^d \equiv (M^e)^d = M^{de} = M^{1+k(p-1)(q-1)} \pmod{n}.$$

By Fermat's little theorem [assuming that $\gcd(M,p)=\gcd(M,q)=1$, which holds except in rare cases, which we cover in Exercise 28], it follows that $M^{p-1} \equiv 1 \pmod{p}$ and $M^{q-1} \equiv 1 \pmod{q}$. Consequently,

$$C^d \equiv M \cdot (M^{p-1})^{k(q-1)} \equiv M \cdot 1 = M \pmod{p}$$

and

$$C^d \equiv M \cdot (M^{q-1})^{k(p-1)} \equiv M \cdot 1 = M \pmod{q}.$$

Because $\gcd(p,q)=1$, it follows by the Chinese remainder theorem that

$$C^d \equiv M \pmod{pq}.$$

a. If e=3, p=2 and q=5, what is the decryption key, "d"? Briefly explain/justify your answer. **[5]**

$d = e^{-1} \bmod (p-1)(q-1) = 3^{-1} \bmod 4$. This is small enough to find by trial and error.

$3 * 3 = 9 \equiv 1 \bmod 4$, so $3 = 3^{-1} \bmod 4$, making $d = 3$

b. If the cyphertext is 6, what is the plaintext? Use your answer from "a" above—you will get credit if you do this part correctly even if your value of "d" is incorrect. Again, you must briefly show your work. **[5]**

$M \equiv C^d \equiv 6^3 \bmod 10$. $6 * 6 = 36 \equiv 6 \bmod 10$. $6^3 = 6^2 * 6 = 6 * 6 = 36 \equiv 6 \bmod 10$

2) How many bit strings of length 6 have *<u>at least</u>* one of the following properties:
   - Start "010"
   - Start with "11"
   - End in a "00"

   You are to give your answer as a number and show your work. To have a chance at partial credit, it must be clear exactly what you did. **[8 points]**

Let A=strings that start with 010, B=strings that start with 11, and C=strings that end with 00. We want to find $|A \cup B \cup C|$, which we can find via the inclusion-exclusion principle. Note that $A \cap B = \varnothing$, as will $A \cap B \cap C$. Otherwise, we simply note that each unspecified bit has 2 options, so each term will just be $2^n$, where n is the number of unbound bits.

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap C| - |B \cap C| = 2^3 + 2^4 + 2^4 - 2^1 - 2^2 = 8 + 16 + 16 - 2 - 4 = 34$$

3) How many ***<u>6</u>***-card poker hands consist of exactly 2 pairs? That is two of one rank of card, two of another rank of card, one of a third rank, and one of a forth rank of card? Recall that a deck of cards consists of 4 suits each with one card of each of the 13 ranks. <u>You should leave your answer as an equation.</u> *Again, notice we are talking about a* ***<u>six</u>****-card poker hand*. **[8 points]**

First, we choose the ranks of the 2 pairs, noting that the order we pick these two ranks doesn't matter, so there are $\binom{13}{2}$ options here. Next, we pick the 2 suits for the first pair, $\binom{4}{2}$ and the suits for the second pair $\binom{4}{2}$. Then we decide which 2 ranks of the remaining 11 to use for the other cards, $\binom{11}{2}$, and finally choose each of their suits $\binom{4}{1}\binom{4}{1}$. Altogether this gives $\binom{13}{2}\binom{4}{2}\binom{4}{2}\binom{11}{2}\binom{4}{1}\binom{4}{1}$ hands.

4) How many bit strings of length 19 contain at least 9 1's and at least 9 0's? You may leave your answer as an equation. Briefly justify your answer. **[4 points]**

This requirement leaves only 1 bit undecided, so there are 2 cases to deal with: the case with nine 1s and ten 0s, and the case with ten 1s and nine 0s. In each case, we simply choose which 9 or 10 of the 19 places to make 1s, giving $\binom{19}{9} + \binom{19}{10} = 2\binom{19}{9}$