Math 335 – CS 480	**Homework 10**	May 9, 2004

The homework was graded out of 40, as follow: I=4.1: 15; II=4.6: 5; III=6.7 a,b): 10; IV=6.12: 5; V=7.1: 5.

Mean was 31.2.

I (André) graded I, II and IV; Jeff graded III and V. See him (Jeff Mermin) during his Math632 office hours fridays 11.30 to 1pm in Malott if you have questions.

Exercise 1: 4.1 from text

Most of the mistakes have occured in part a).

A hash function is *not* injective, as some of you think. It is almost impossible to find $x \neq x'$ such that $h(x) = h(x')$. But it's not because it is impossible practically speaking to do so that those don't exist.

And in fact, since the target domain is (usually much) smaller than the source domain, hash functions cannot be injective. They can be surjective, and they usually are, though they are not required to be.

Many people stated that

$$\sum_{y \in \mathcal{Y}} |h^{-1}(y)| = |\mathcal{X}|$$

without justification. Why couldn't the same $x \in \mathcal{X}$ be counted multiple times? Or some not be present? [Note: I took some points of since almsot all the people who tried to justify it did so incorrectly.]

But of course this cannot be. h is a function in the mathematical meaning of function, that is, every $x \in \mathcal{X}$ has one unique image $y \in \mathcal{Y}$. Therefore the sets $h^{-1}(y)$ for $y \in \mathcal{Y}$) forms a partition of $\mathcal{X}$.

In part d), the text asks to show thta the equality is attainted if and only if when $s_y = N/M$ for every $y \in \mathcal{Y}$. You really have to prove both the *if* and the *only if* part. You cannot skip the *only if* part.

Exercise 3: 6.7a) b) from text

It was rather pathetic.

For the first part, proving that x is a common multiple of y and z is not the same as proving that x is the *least* common multiple of y and z. I would estimate that a little over half the class made this error.

For the second part, many people had the mistaken notion that (Z/n)* has a primitive element. This is false, false, false! Part (a) is pretty much a proof that it's false! (Z/p)* has a primitive element if p is prime, but (Z/n)* almost never does when n is composite. In particular, if n=pq with p and q both not 2, (Z/n)* has no primitive element. Almost everybody who didn't make this mistake said something like: "There exists an alpha primitive mod p and an alpha primitive mod q, so alpha has the right order mod n." But there's no reason to think those alpha are in fact the same - you need to get primitive elements mod each prime and use the Chinese Remainder Theorem to put them together. Something like four people got the second half right.

Exercise 4: 6.12 from text

Some of you rightly pointed out that the text only asked to *show* how to decrypted the message. To the 90% of you who actually decrypted it, I would have done the same, and hopefully found `Galois Field`. Mathematica can do everything for you since it does formal calculus. However, if you don't have such a tool, you can either look for the inverse of the polynomials one by one each time you see a new one, or, since the field is small, compute all α^k for $k = 1 : 26$ and work from there to have the inverse.

Exercise 5: 7.1 from text

I graded pretty much all-or-nothing, since the algorithm is given in the book, and it's inexcusable not to check your answers in this situation.

Specifically, if you're the army and planning to spoof enemy communications during an operation, people DIE when you screw up. So you check your answers (i.e. plug in your a and k to the known messages and see if they work.)

There are two correct answers for k=1165;