Homework 1

This homework is due on *Wednesday, January 22, 2014* by 10:39:00AM. There are **25 possible points**. You must submit your homework on paper in lecture. We do not accept emailed or otherwise electronic submissions (zero points). Late submissions or submissions that do not follow the strict policies from the syllabus will receive a zero. **Students who do not perform well on this homework will be automatically dropped from the course.** Please contact the TA well ahead of the deadline if you have a question about these procedures.

Submit each homework[1] problem stapled separately. We will have five separate boxes at the front of the lecture hall for submitting each problem. Points will be deducted for solutions that do not follow this process. On the front page of **each** stapled problem, the top right corner must provide the following items:

- Print your name
- Print your uniqname
- Print the homework-problem number.

The result for the second problem on this first homework should then look like:

```
Name: John P. Doe
Uniqname: johnpdoe
Problem: 1-2
```

If your solution spans multiple pages for a problem, mark the top of each page with your initials. Some problems contain multiple components. For each component of a problem, write a descriptor of the component. For instance, for the first component of the problem, write "Stinson 1.1." in the text of your solution. Points may be deducted if your TA has problems understanding or reading your solution. In mathematical problems, **show all your work**.

Problem 1-1. Modular arithmetic (5 points)

In these problems, we review number theory introduced by other classes. We also peek at future topics in this course in order to prepare you for the magic of public key cryptography.

Do problems 1.1 and 1.7 from Stinson. **Show all your work**. Problem 1.1 should reintroduce you to modular arithmetic. Problem 1.7 gives you a flavor of key density in a precursor to public key cryptography. We reprint the problems here, in case you do not yet have the book:

Stinson 1.1 (2 points) Evaluate the following and show all your work:
(a) 7503 mod 81, (b) $(-7503) \bmod 81$, (c) 81 mod 7503, (d) $(-81) \bmod 7503$

Stinson 1.7 (3 points) Determine the number of keys in an Affine Cipher over $\mathbb{Z}_m$ for $m = 30, 100,$ and 1225.

[1] We will distribute our favorite solution for each problem to the class as the "official" solution—this is your chance to become famous!

Problem 1-2. Inverses are weird (8 points)

(a) Stinson 1.8 (3 points)
List all the invertible elements in $\mathbb{Z}_m$ for $m = 28, 33,$ and 35.

(b) It's a trick, get an axiom (3 points)
Given a prime p, **compute the set** formed by the set builder notation of $S = \{a^{-1} | a \in Z_p^*\}$ where a^{-1} represents the inverse of $a \bmod p$. In your final answer, use the most concise notation possible to convey this set S. Describe the **size of the set** S. Had the prime p instead been replaced with a composite $n = q * r * s$ where q, r, s are distrinct and unique primes, how large would the set S have been? **Show all your work** as to why you believe your answers are correct. Hint: First play around with specific primes to get an idea for what is happening before solving the general case.

(c) Composites make things more fun (2 points)
Given a composite n that is the product of two primes 2 and 11, create a table of inverses. For each element $a \in Z_n$, write the integer b such that $a * b \equiv 1 \bmod n$. If the inverse does not exist, write "DNE." Write your answer in the form of a table with 22 rows where the first column holds the a's and the second column holds the corresponding b's or the letters "DNE." Begin with $a = 0$.

Problem 1-3. Experience the magic of modular exponentiation (4 points)

When computing a modular exponentiation such as $a^b \bmod m$, we can optimize by first reducing the exponent by $\phi(m)$. Theorem 1.2 in Stinson explains the formula for $\phi(m)$. In the vernacular, we can say that "downstairs" the operations are mod m while "upstairs" the operations are mod $\phi(m)$. Using this technique, compute the 2 rightmost decimal digits of $3^{40000005}$. **Show all your work.** Hint: You shouldn't need a calculator for this.

Problem 1-4. Threat Models (4 points)

In your own words, explain what the notion of brute force guessing a cryptographic key means under the four different attack models from Stinson: ciphertext only attack, known plaintext attack, chosen plaintext attack, chosen ciphertext attack. That is, quantify the difficulty of brute force breaking a cryptosystem under the different attack models given no other information. Limit your answer to one-page of double-spaced text with an 11pt font or greater.

Problem 1-5. Snowed In (4 points)

As part of the first lecture, you were asked to do library work to read up on the Crypto Wars of the 1990s. In the 1970s, distinguished cryptographers alleged that the National Security Agency (NSA) had tampered with the design of the "substitution boxes" or S-boxes to deliberately weaken the Data Encryption Standard (DES), a 56-bit key block cipher operating on 64-bit plaintext messages. Read up on this incident, and in your own words, explain the reasons cryptographers initially had doubts on DES S-boxes, and then explain what happened that mitigated this doubt. Limit your answer to one-page of double-spaced text with an 11pt font or greater. Make use of the library and electronic sources, but **cite all your sources of information.**