Honors Homework 1

Discrete Structures, CS 173, Spring 2016

Due March 7, 2016

Honors homeworks must be formatted using the LaTeX document formatting package. (Not just the equation mode found in Piazza and Moodle.)

For this homework, you will write a simple latex document that mimics some mathematical text as well as write a description of the Diffie-Hellman protocol and solve a small exercise.

First, see the look through the Latex start-up materials on the CS 173 honors web page. In particular, the web page has a sample latex document that you can use as the starting point for your submission. Install a copy of Latex on your machine. (EWS lab machines have it installed.) Then write and format your document.

Your homework should be submitted as hardcopy in the CS 173 honors dropbox in the basement of Siebel. Please submit a hardcopy of your LaTeX document, including **both source code and formatted output**. The dropboxes are located just east of the lounge area with the big windows. If you get to the candy/soda machines, you've gone too far east.

Your document should use 12pt font and start with the title and author (see the sample document for how to do this). Then write a brief paragraph about yourself (e.g. class year, major). Use intelligent formatting features (e.g. numbered lists) as much as you can, rather than faking their effects by hand.

1 Crazy about Foundations

Reproduce this section (both titles and contents) in LaTeX.

In logic, we learned that $\neg(p \to \neg q) \equiv (p \wedge q)$.

We also saw why the following statement is true:

$\forall x \in \mathbb{N}$, if $x < 0$, then $x > 2^{10000}$

And we saw that

1. $A \cap B \subseteq A$
2. $\{\emptyset\} \neq \emptyset$.
3. $\sqrt{5}$ is not rational.

and that

- $\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}$
- $x - 1 < \lfloor x \rfloor \leq x$
- $p \mid q$ and $q \mid p$ implies $p = \pm q$.

2 Diffie-Hellman Protocol

Read and understand the Diffie-Hellman protocol. You can use the following sources:

- The Wikipedia page on Diffie-Hellman key exchange:
  `https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange`
- The original paper by Diffie and Hellman: New Directions in Cryptography.:
  `https://ee.stanford.edu/~hellman/publications/24.pdf`

  Read the introduction and in Section III, the "new public key distribution system" on Page 649.
- Read the Diffie-Hellman Notes by Silverman, Section 2.3:
  `https://www.math.brown.edu/~jhs/MathCrypto/SampleSections.pdf`

- Read from other sources on the internet.

Write, *in your own words*, a description of the Diffie-Helmann protocol, with the following sections:

1. A description of what the requirements of the protocol are. What problem is the protocol trying to solve?

2. An algorithmic description of the protocol. Make sure you format the protocol well in LaTeX. Use p to denote the prime that is used for modular arithmetic and g the base which exponents are raised to.

3. Why is the protocol hard to break for an eavesdropper?

4. Give an example of the key-exchange, with prime $p = 10007$ and base $g = 1234$ (note that they are relatively prime). Clearly describe the random values chosen by Alice and Bob, the private computation they perform, the messages exchanged, and the final key they agree upon.

5. Solve the following exercise. In a Diffie-Hellman exchange with $p = 23$ and $g = 5$, you as an eavesdropper see the message 11 from Alice to Bob and 13 from Bob to Alice. Find out the actual key they agree upon by decrypting the exchange. Tabulate the values Alice/Bob would send depending on the various values they choose randomly (and draw them as a clean table in LaTeX) and from this decipher the random values they chose, and hence calculate the key they agree upon.