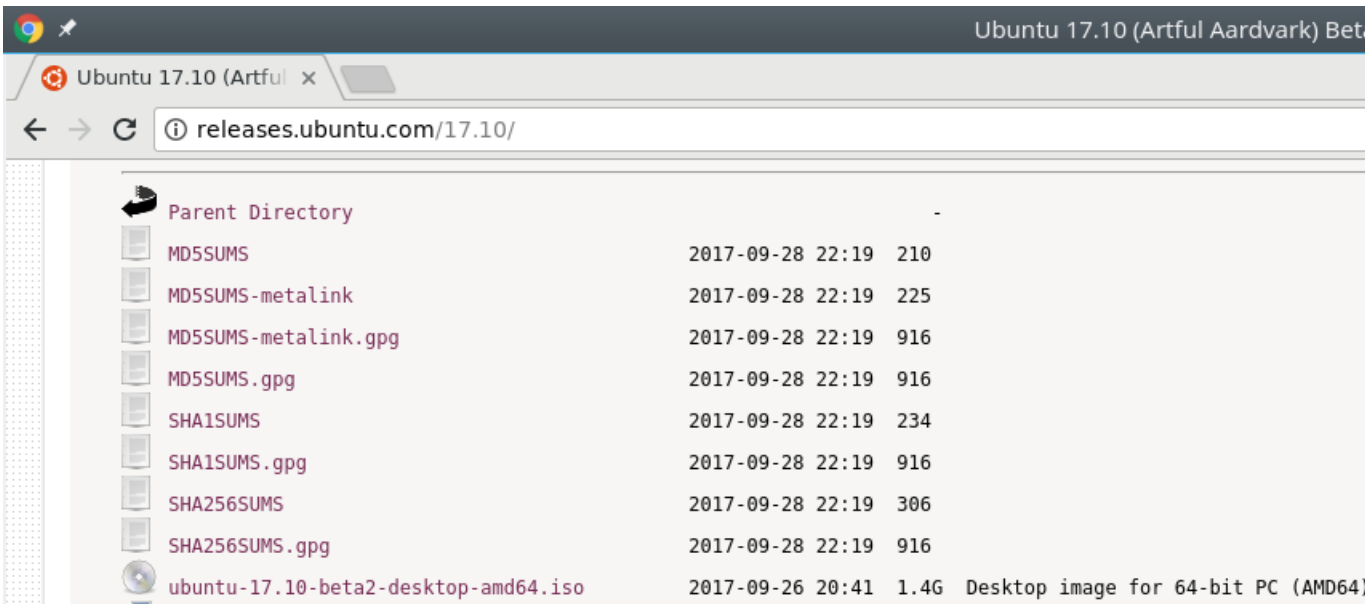
Your Name Goes Here

Math 25

Homework 5

1. Below is a screen shot of the web page `http://releases.ubuntu.com/17.10/` which happens to be a release page for the Linux distribution Ubuntu. Any other vendor that releases software has a similar page, see `https://ftp.mozilla.org/pub/firefox/releases/55.0.3/` for example.



   The file listed at the bottom of the image (`ubuntu-17.10-beta2-desktop-amd64.iso`) is a 1.4G file (in iso format meaning could be burned to a DVD). Mounting the file, or burning it to a DVD and inserting in a computer would offer to install a new operating system on your computer. **I am not suggesting you do this!**

   Visit this site, and look at the files MD5SUMS, SHA1SUMS, SHA256SUMS. Each contain hash values for the file `ubuntu-17.10-beta2-desktop-amd64.iso`.

   (a) Go online, poke around, and tell me a little about the differences about MD5SUMS, SHA1SUMS, and SHA256SUMS. Detail at least the length of the hash, and the relative security of each algorithm.

   (b) Explain the purpose of the presence of the hash values on the download page. What is a downloader supposed to do with them?

   (c) More interestingly, there are three other files also listed on that page: MD5SUMS.gpg, SHA1SUMS.gpg and SHA256SUMS.gpg. They are Ubnutu's official digital signatures of the files MD5SUMS, etc., analogous to the signatures we talked about in class.

   Give an explanation of why it is important for such files to be on a download site, given that you as the downloader will almost never access them.

2. Set up public and private keys for an RSA system using the primes 17 and 23.

3. Show that for each $k \geq 1$, there are at most a finite number of positive integers n for which $\phi(n) = k$.

4. Prove that for all $n \geq 1$, $\phi(n^2) = n\phi(n)$.

5. Let $\sigma(n) = \sum_{d|n} d$ be the usual sum of the positive divisors of n. We have shown that σ is multiplicative, but not completely multiplicative. Verify, that for a prime p and integer $k \geq 1$,
$$\sigma(p^{k+1}) = \sigma(p)\sigma(p^k) - p\sigma(p^{k-1}).$$

6. For a prime p, consider the power series
$$\sum_{k=0}^{\infty} \sigma(p^k)x^k.$$
   (a) Find the radius of convergence of the series. Eeek! Calculus!
   (b) For x in the interval of convergence, verify the identity
$$\sum_{k=0}^{\infty} \sigma(p^k)x^k = \frac{1}{1 - \sigma(p)x + px^2}.$$