CS 2 Computational Thinking for Scientists
Winter Term 2015

(The Last) Homework Assignment 07:

1. What is a networking protocol? Briefly describe two protocols you learned in class.
2. IPv4 has 32-bit destination and 32-bit source addresses. How many different computers can be addressed in IPv4? How many bits are the destination and source addresses in IPv6? How many different computers can be addressed in IPv6?
3. Encrypt the plaintext

   `the heart has its reasons which reason does not know`

   using Shift Cipher with key 13.
4. The following ciphertext is obtained using Shift Cipher:

   `huqbyjo yi cuhubo qd ybbkiyed qbruyj q luho fuhiyijudj edu`

   Discover the key using frequency analysis.
5. Show the steps of the Diffie-Hellman key exchange algorithm for $p = 9973$ and $g = 11$, between two parties A and B such that the secret quantities are $a = 2015$ and $b = 7654$.
6. Given the two primes $p = 9973$ and $q = 10007$, setup an RSA key, determining $n, \phi(n), e, d$. Encrypt the plaintext $m = 9876543$ to obtain the ciphertext c, and then decrypt c to obtain m back.
7. Let an RSA public key be given as $(n, e) = (999919, 113)$. Also, we capture the ciphertext $c = 597486$. Compute the plaintext m by factoring the modulus $n = p \cdot q$, and thus, discovering p and q, and then computing the private exponent using

   $$d = e^{-1} \bmod \phi(n)$$

   and finally computing $m = c^d \bmod n$. Also, note that,

   $$\phi(n) = \phi(p \cdot q) = (p - 1) \cdot (q - 1)$$

Note: Questions 5, 6, and 7 may require access to Python or Mathematica.
$\longrightarrow\longrightarrow$ The due date of this homework is Friday (not Wednesday). $\longleftarrow\longleftarrow$

Due 5pm Friday, March 13
Either, email an electronic copy to the Instructor (koc@cs.ucsb.edu) or the TA (zhijing@cs.ucsb.edu). Or, deliver a paper copy to the HW Box in HFH 2108. Electronic copy of your homework or lab report can be in Text, PDF or MS Word, or Open Office format. You could also scan/pdf your handwritten work; however, do not send phone-camera images under any circumstances!