Massachusetts Institute of Technology
6.857: Network and Computer Security
Professor Ronald L. Rivest

Handout 9
October 1, 1998

Problem Set 3

This problem set is due on *Thursday, October 7, 1998* at the end of class. Late homeworks will *not* be accepted. You are to work on this problem set in groups of three to four people. Mark the top of each sheet with your names, 6.857, the problem set number and question, and the date. **Type up your solutions**, and be clear. Points may be deducted if your TA has problems understanding your solution.

Problem 3-1. A pair (p, r) of primes is known as *twin primes* if the equation $r = p + 2$; holds (that is, they differ by two). Examples of twin primes are $(11, 13)$ and $(29, 31)$.

We define an *Oreo cookie* to be a triple (p, q, r) where (p, r) is a pair of twin primes, together with a factorization of the intermediate value $q = p + 1$. (Think of p and r as being the chocolate cookie wafers and q as being the filling.) As an example, $(29, 30 = 2 \cdot 3 \cdot 5, 31)$ is an Oreo cookie. To be an Oreo cookie, the factorization of q *must* be supplied.

(As you might suspect, the term Oreo cookie was made up for this assignment, and is not something you'll find in the literature. Indeed, the concept itself has not appeared before, to our knowledge.)

Your assignment is to find the largest Oreo cookie you can. There are many different possible approaches to this problem. You may not submit any of the above examples as a solution.

The team finding the largest Oreo cookie wins a package of Oreo cookies.

We presume that you will use a computer to assist you. Please turn in as part of the assignment your program. As part of your solution, you should also explain why the TA should believe that p, r, and the factors of q you give really are primes. Also give the number of bits in the binary representation of p (so the TA doesn't have to count them to compare different solutions).

If you are using shared computing resources, be considerate of the other users (e.g. give your job a low scheduling priority and do not abuse the dialups).

You may wish to browse links off of Ron's cryptography homepage for ideas on how to solve this problem:

`http://theory.lcs.mit.edu/~ rivest/crypto-security.html`