Problem Set 4

This problem set is due *on paper,* on *Thursday, October 16* at the beginning of class. **Note:** You have *two weeks* to complete this problem set!

You are to work on this problem set in groups of three or four people. Problems turned in by individuals, pairs, pentuples, etc. will not be accepted. Be sure that all group members can explain the solutions. See Handout 1 (*Course Information*) for our policy on collaboration. If you do not have a group, seek partners by emailing TA.

Homework must be typed! Each problem answer must appear on separate sheets of paper. Mark the top of each sheet with your names (alphabetically by last name), the course number (6.857), the problem set number and question, and the date. **Homework must be typed and clear.** We have provided templates for LaTeX and Microsoft Word on the course website.

Grading and Late Policy: Each problem is worth 10 points, except where noted. Late homework will not be accepted without prior approval. Homework should not be submitted by email except with prior approval. (*Somebody* from your group should be in class on the day that the homework is due.)

With the authors' permission, we will distribute our favorite solution to each problem as the "official" solution – this is your chance to become famous! If you do not wish for your homework to be used as an official solution, or if you wish that it only be used anonymously, please note this on your homework.

Problem 4-1. Paillier Encryption [20 points]

In this problem, we introduce the *Paillier cryptosystem*, which shares some of the flavors of both RSA and discrete log-based systems, but also enjoys many other desirable properties (and whose security relies upon new assumptions).

For a summary of the relevant mathematics and the definition of the Paillier scheme, read Sections 2.1 through 2.3 (especially Figure 1) on pages 4–5 of "Efficient Public-Key Cryptosystems Provably Secure Against Active Adversaries," by Paillier and Pointcheval (the paper is posted on the 6.857 website). In this problem, we will only be dealing with the so-called "Main Scheme."

(a) Implement key generation, encryption, and decryption algorithms for the Paillier scheme in your favorite programming language. You may use any big-integer libraries you like. Include your code in your write-up, and *make it clean and readable!*

(b) When you are confident in the correctness of your code, generate a public/private key pair n, g, p, q (where n is about 256 bits long), and the encryptions of $m = 2$ and $m = 314159$ under your key.

(c) The Paillier cryptosystem has a nice *homomorphic* property: $E_{n,g}(m_1) \cdot E_{n,g}(m_2) \bmod n^2$ is an encryption of $(m_1 + m_2) \bmod n$. This inspires Ben Bitdiddle to propose the following voting scheme: a Paillier keypair is generated by the election agency, and the public key (n, g) is disseminated to the populace. To vote in favor of a resolution, a voter encrypts a 1; to vote against the resolution, he encrypts a 0. The ciphertext is then submitted to a device which keeps a running product mod n^2 of all the ciphertexts. At the end, the election agency decrypts this cumulative product: if the value of the plaintext exceeds half the number of votes, the resolution passes, otherwise it fails. Ben claims that this scheme protects the voter's anonymity while ensuring correctness. Find one major security flaw in his idea.

Problem 4-2. The MegaSoft Corporation has introduced a new public key cryptosystem, which works as explained throughout the parts of this problem. Please answer all parts.

(a) Each user finds a large prime p of the form $p = 2qr + 1$ where q and r are themselves distinct large primes. Sketch briefly how you would find such a prime p.

(b) What are the possible orders of an element in $\mathbb{Z}_p^*$? How many are there of each type? (Note that there are $\phi(t)$ elements of order t, where ϕ is Euler's totient function.) Explain briefly how you would find a generator g in $\mathbb{Z}_p^*$.

(c) Each user also needs to find two elements, a and b, of respective orders q and r. Explain how, given a generator g of $\mathbb{Z}_p^*$, you could find such elements. (Note: be careful — they are rare!)

(d) A user's public key consists of the quadruple (p, g, a, b). (The generator g isn't really used, but is included anyway.) When another user wants to send an n-bit message m to the first user, he proceeds as follows:

1. Let $m = m_1 \ldots m_n$ denote the message, bit by bit.
2. Each bit is encrypted and transmitted separately, in order.
3. If $m_i = 0$, he generates a random value $k \in \mathbb{Z}_q^*$, and sends $a^k \bmod p$ as the ciphertext for this bit. If $m_i = 1$, he generates a random value $k \in \mathbb{Z}_r^*$, and sends $b^k \bmod p$ as the ciphertext for this bit.

(Note that this encryption is not terribly efficient: each message bit requires a modular exponentiation, and expands to a number as large as p in the ciphertext.) Argue that encryption is unambiguous: the ciphertext for a bit is either the result of encrypting a 0, or the result of encrypting a 1. In other words, no particular ciphertext for a bit can arise in both ways.

(e) Explain how the recipient can decrypt the ciphertext efficiently.

(f) Suppose that the discrete logarithm problem is easy modulo p: i.e., there is an efficient algorithm $\mathcal{A}$ which, given a prime p, a generator g, and a value y, finds an x such that $y = g^x \bmod p$. Show how, by invoking $\mathcal{A}$ *only once*, an adversary can break this cryptosystem entirely.

Problem 4-3. Please read the paper about Sebek, "Know Your Enemy: Sebek2," which is posted on the class web site. This paper was recently posted on the Internet.

(a) Please give a summary of this paper in at most 1/2 page, in your own words. Be careful not to plagiarize or paraphrase the original paper too closely.

(b) On balance do you think it is a good idea for such papers to be posted? Are such postings beneficial to society, or harmful? Please give your opinion, and explain your reasoning. Use at most one page. (For grading purposes, we care less about whether you are pro or con, and more about how well you articulate and justify your chosen position.)