Homework 3: Public-Key Cryptography
DUE Wednesday, October 10

William Stein

Math 124 Harvard University **Fall 2001**

Cite sources of help, work with other students, and come see me during office hours (WF at 2pm). Feel free to make unrestricted use of PARI in problems 1–7.

1. (3 points) You and Nikita wish to agree on a secret key using the Diffie-Hellman protocol. Nikita announces that $p = 3793$ and $g = 7$. Nikita secretely chooses a number $n < p$ and tells you that $g^n \equiv 454 \pmod{p}$. You choose the random number $m = 1208$. Tell me what the secret key is!

2. (4 points) This problem concerns encoding phrases using numbers.

   (a) Find the number that corresponds to `VE␣RI␣TAS`, where we view this string as a number in base 27 using the encoding of Section 2 of Lecture 9. (Note that the left-most "digit", `V`, is the least significant digit, and ␣ denotes a blank space.)

   (b) What is the longest sequence of letters (and space) that can be stored using a number that is less than 10^{20}?

3. (4 points) You see Michael and Nikita agree on a secret key using the Diffie-Hellman key exchange protocol. Michael and Nikita choose $p = 97$ and $g = 5$. Nikita chooses a random number n and tells Michael that $g^n \equiv 3 \pmod{97}$, and Michael chooses a random number m and tells Nikita that $g^m \equiv 7 \pmod{97}$. Crack their code: What is the secret key that Nikita and Michael agree upon? What is n? What is m?

4. (2 points) Using the RSA public key is $(n, e) = (441484567519, 238402465195)$, encrypt the year that you will graduate from Harvard.

5. (6 points) In this problem, you will "crack" an RSA cryptosystem.

   (a) What is the secret decoding number d for the RSA cryptosystem with public key $(n, e) = (5352381469067, 4240501142039)$?

   (b) The number 3539014000459 encrypts an important question using the RSA cryptosystem from part (a). What is the question? (After decoding, you'll get a number. To find the corresponding word, see Section 2 of Lecture 9.)

6. (4 points) Suppose Michael creates an RSA cryptosystem with a very large modulus N for which the factorization of N cannot be found in a reasonable amount of time. Suppose that Nikita sends messages to Michael by representing each alphabetic character as an integer between 0 and 26 (`A` corresponds to 1, `B` to 2, etc., and a space $\sqcup$ to 0), then encrypts each number *separately* using Michael's RSA cryptosystem. Is this method secure? Explain your answer.

7. (6 points) Nikita creates an RSA cryptosystem with public key

$$(n, e) = (1433811615146881, 329222149569169).$$

In the following two problems, show the steps you take. Don't simply factor n directly using the `factor` function in PARI.

(a) Somehow you discover that $d = 116439879930113$. Show how to use the probabilistic algorithm of Lecture 10 to use d to factor n.

(b) In part (a) you found that the factors p and q of n are very close. Show how to use the "Fermat Factorization" method of Lecture 10 to factor n.