

## Homework 1            ICS 247 Security Algorithms

Due: Wednesday, January 15, 2003, in class

Please answer the following questions, each of which is worth 10 points.

1. Construct a table showing an example of the RSA cryptosystem with parameters  $p = 17$ ,  $q = 19$ , and  $e = 5$ . The table should have two rows, one for the plaintext  $M$  and the other for the ciphertext  $C$ . The columns should correspond to integer values in the range  $[10, 20]$  for  $M$ . Hint: Write a small Java program or use a spreadsheet.
2. In a public-key system using RSA, you intercept the ciphertext  $C = 10$ , sent to a user whose public key is  $e = 5$ ,  $n = 35$ . What is the plaintext  $M$ ?
3. In a public-key system using RSA, the public key of a certain user is  $e = 31$ ,  $n = 3599$ . What is the plaintext  $M$ ? Hint: you may use the Unix program **factor**.
4. In a public-key system using RSA, the public key of a certain user with public key  $e, n$  leaks his private key  $d$ . Being lazy, he recomputes a new  $e$  and  $d$  using the same  $n$ . Is this safe? Why or why not?
5. Let  $p$  be a prime. Give an efficient alternative algorithm for computing the multiplicative inverse of an element of  $Z_p$  that is not based on the extended Euclid's algorithm. What is the running time of your algorithm? Hint: Use Fermat's Little Theorem.