Final Exam

Practice Test

December 7, 2006

1. (a) Explain how the RSA algorithm works.
   (b) Show an example of RSA using primes $p = 19, q = 11$. This means
      - Choose an encryption key and the corresponding decryption key.
      - Encrypt the plaintext number $P = 2$.
2. (a) What is a group?
   (b) Prove: in a group, if $ab = ac$, then $b = c$.
   (c) Provide an example of arithmetic mod N, where $ab = ac$ but $b \neq c$.
3. (a) Explain the ElGamal encryption algorithm.
   (b) Provide an example using the prime $p = 19$, and generator $g = 2$ That means: generate a public key, and use it to encrypt the plaintext $P = 3$.
4. Write out the elements of the group $\mathbb{Z}_{30}^{\times}$. Name three elements of $\mathbb{Z}_{30}^{\times}$ equal to their own inverses.
5. Compute:
   - $\phi(50)$
   - $\phi(1024)$
   - $\phi(77)$
   - The last 3 digits of $7^{5122005}$

6. Compute the following inverses:

   - $16^{-1} \pmod{31}$
   - $7^{-1} \pmod{100}$

7. (a) Suppose you have a large number $n = pq$. Now suppose I have the job of computing $3^{2^M} \pmod{n}$. That is, I have to start with the number 3, then square it M times.

   This requires M squarings. Explain how I could do it faster if I knew the factorization of n.

   (b) An example: suppose I take the number 3 and square it 15 times. What is this number modulo 100?