1 Tutorial 8

Questions 1 and 2 are due the week of October 14, while questions 3, 4 and 5 are due the week of October 7th.

1. Consider $n = p \times q$ where both p, q are (probable) primes. Let

   $$p = 4703713376517472005806418066555779293457873398157752389958 09$$

   and let

   $$q = 4499844734117731401670236904640172639714995487317761872083826 1$$

   Find

   ```
   659798681212804331928725342070000524862635920743474257017255732454895236384572 62\
   351946261146698247560345
   ```

   raised to itself (mod n) using (a) modular exponentiation and (b) the Chinese Remainder Theorem. You must implement both of them yourself. Time both measurements by running your program 10 times and reporting the average and standard deviation in both instances.

   You may use a big integer package and use its multiplication, division, inverse, and other operations except for its modular exponentiation and chinese remainder theorem implementations.

2. Consider a 512 bit Diffie-Hellman system in which

   ```
   p = 0x00B074C48A962CDF1EB3895DA6DBE20A7AFBADE32ED9AF48CC7FFE378BBCE063848ECD57CCF\
         90D4184E0E91836F156D0D2C8063B948EC179CE54B179C7DADD8B45
   q = 0x00A612AB9B9E27938F402C38BF6464BA1BFCA8C1B3
   g = 0x373CBDEAFF2C44FE1EA25B500E112383F7E41F6278DA39E9347A640E9C95702A65E6BA2BD15\
         4DA6ABDFCB8E73107EB5CA9118DA79406EE2E7DEDC7B4157D15B7
   ```

   If Alice uses the random integer 6325782345 and Bob uses the random integer 629851207 for key exchange and use the least significant 64 bits of the resulting shared secret as a DES key for encrypting traffic, what is the key they agree on?

3. Given that the Lamport hash value is sent in the clear over the network, why is it more secure than a password?

4. Is the Lamport hash protocol vulnerable to disctionary attack by an eavesdropper? Can someone impersonating the server do a dictionary attack?

5. As described in the text, the mental poker protocol has a flaw. If there are only ten cards, as soon as Alice sees her hand, she knows from set difference what cards Bob must have. Suggest an alternative protocol