Tutorial Week 10

Questions

1. Is the Diffie-Hellman algorithm a public key encryption algorithm? If not, what is it?
2. 133 is the product of two primes. What are they?
3. RSA and Diffie-Hellman can generate very large numbers that require their modulus to be calculated. Fortunately, modulo arithmetic is associative and commutative. That is:

   $a^{p+q+r} \bmod N = (a^p \bmod N)\ (a^q \bmod N)\ (a^r \bmod N) \bmod N$

   For example

   $3^6 \bmod 5$

   $= (3^2 \bmod 5)\ (3^2 \bmod 5)\ (3^2 \bmod 5) \bmod 5$

   $= (9 \bmod 5)(9 \bmod 5)(9 \bmod 5) \bmod 5$

   $= 4^3 \bmod 5 = 64 \bmod 5 = 4$

   Try this approach with $5^5 \bmod 23$
4. What key do Alice and Bob come to agree upon using the Diffie-Hellman algorithm using the following values?

   Alice chooses a = 3, Bob chooses b = 4, p = 17 and g = 3.
5. The following is a public/private key pair.

   [33,3] and [33,7]

   Use the keys and RSA to encrypt and decrypt‘2’.
6. Generate a public / private key using the prime numbers 3 and 11.
7. Test the following numbers for primality to a confidence level of 0.75.

   9, 11