Tutorial Week 10

Questions

1. Is the Diffie-Hellman algorithm a public key encryption algorithm? If not, what is it?

   The algorithm is a technique for coming to agreement on a shared secret key across an insecure channel. Although it uses many of the ideas of public key cryptography it is not a public key encryption algorithm.

2. 133 is the product of two primes. What are they?

   19 and 7

3. Calculation of 5^5 mod 23

   5^5 mod 23

   = (5^2 mod 23)(5^2 mod 23)(5 mod 23) mod 23

   = (25 mod 23)(25 mod 23)(5 mod 23) mod 23

   = (2)(2)(5) mod 23

   = 20 mod 23 = 20

4. What key do Alice and Bob agree upon using the Diffie-Hellman algorithm using the following values?

   p = 17 and g = 3. Alice chooses a = 3, Bob chooses b = 4.

   Alice calculates A = g^a mod p = 3^3 mod 17 = 27 mod 17 = 10 and transmits it to Bob.

   Bob calculates B = g^b mod p = 3^4 mod 17 = 81 mod 17 = 13 and transmits it to Alice.

   Alice calculates s = B^a mod p = 13^3 mod 17 = 2197 mod 17 = 4.

   Bob calculates s = A^b mod p = 10^4 mod 17 = 10000 mod 17 = 4.

   So the shared secret value they agree upon is 4.

5. The following is a public/private key pair.

   [33,3] and [33,7]

   Use the keys and RSA to encrypt and decrypt'2'.

   Encryption

   c = 2^3 mod 33 = 8 mod 33 = 8

   Decryption

   m = 8^7 mod 33 = 2097152 mod 33 = 2

   There are two different ways to calculate this. The simplest, if you have a calculator and the number is not too large, is to calculate 8^7 which is 2097152 mod 33, calculate 2097152 / 33 = 63550.0606

   Discard the whole number part leaving 0.060606

Multiply this by 33 to get 2

The other approach (described in question 3) is useful if you do not have a calculator or the number is too large for your calculator, is to make use of modular arithmetic being associative and commutative:

8^7 mod 33 = (8^2 mod 33) * (8^2 mod 33) * (8^2 mod 33) * (8 mod 33) mod 33

= (64 mod 33 * 64 mod 33 * 64 mod 33 * 8) mod 33

= (31 * 31 * 31 * 8) mod 33

= (31 * 31 mod 33) * 31 * 8 mod 33

= 961 mod 33 * 248 mod 33

= 4 * 17 mod 33

= 68 mod 33 = 2

Another example:

8^7 mod 33 = 8^3 mod 33 * 8^3 mod 33 * 8 mod 33

= 512 mod 33 * 512 mod 33 * 8 mod 33

= 17 * 17 mod 33 * 8 mod 33

= 289 mod 33 * 8 mod 33

= 25 * 8 mod 33

= 200 mod 33 = 2

6. Generate a public / private key using the prime numbers 3 and 11.

   n = p*q = 3*11 = 33

   x = (p-1)*(q-1) = 2*10 = 20

   Choose e relatively prime to x. We can choose any number up to n, but for these problems it is wise to choose the smallest value possible. Choose e = 3

   So first key is [33,3]

   We now need to find d such that (d*e) mod x = 1 ie.

   3d mod 20 = 1.

   We can do this by inspection (through trying different values of d) or we can rearrange the equation as follows.

   We want d, such that:

   3d = 20 Q + 1, Q and d need to be an integer

   d = (20Q +1) / 3

   We need an integer value for d. Try successive values of Q until an integer is found:

   Q = 1 gives d = 7 which is the only solution.

   So second key is [33,7]