Cryptography Homework

1.0 RSA

Using the prime numbers p=13 q=3

Compute an RSA public and private key pair of (n,e) and (n,d) respectively.

Using the last two digits of your Poly student ID, XY calculate XYmod38 as the message m. Encrypt the message, m using RSA. $c = m^e \bmod n$

So for example if the last two digits of your Poly ID are 99 then 99mod38=23 and you would use 23 as the message m.

Now using the RSA cipher output (c) decrypt using your private key (n,d). $m = c^d \bmod n$

Show all steps in the computation. Be verbose. When calculating large exponents in a modulus be sure to use the binary expansion technique. Show all steps of this binary expansion.

2.0 Diffie-Helman

Use the last two digits XY of your student ID number to form the secrets chosen by Alice and Bob respectively as 1X and 1Y. So if your student ID number is 21 you will use 12 and 11 as the secrets chosen by Alice and Bob respectively. If the last two digits are 40 and you will use 14 and 10 respectively and so on.

Compute the shared secret that is arrived at by Alice and Bob using Diffle Hellman. Show all steps in your computation.

Type up your solutions and submit electronically in either Word or PDF format.