Cryptography

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 NYU N-number, 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 NYU N-number is 21, then 21mod38=21 and you would use 21 as the message *m*.

Now decrypt your resulting ciphertext *c* using your private key (n,d), showing that you obtain the original message *m*. $m = c^d \bmod n$

Show all steps in the computation. Be verbose. When calculating large exponents with a modulus be sure to use a manual technique such as the binary expansion method shown in class. Write out all steps for any modulo math.

2.0 Diffie-Helman

Use the last two digits XY of your NYU N-number to form the secrets chosen by Alice and Bob respectively as 1X and 1Y. So if your N-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 then you will use 14 and 10 respectively and so on.

Compute the shared secret *K* that is arrived at by Alice and Bob using Diffle Hellman. Choose an appropriate base *g* and modulus *n*. Show all steps in your computation.

3.0 What to Submit

Type up your solutions and submit electronically. Show all computational steps.

RSA: [5 pts] Choosing a correct *e*
[5 pts] Choosing a correct *d*
[15 pts] Encrypting message *m* correctly
[15 pts] decrypting ciphertext correctly

DH: [10 pts] Choose *g* and *n* appropriately
[30 pts] Compute the shared secret *K* correctly

[20 pts] Write out all steps in all calculations involving modulo mathematics