# CS6823 - NEWORK SECURITY - CRYPTO

Diffie-Hellman

Use the last two digits XY of your NYU Net ID to form the secrets chosen by Alice and Bob respectively as 1X and 1Y. So if your NET ID ends with 21, then 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 Diffie Hellman. Choose an appropriate base *g* and modulus *n*. Show all steps in your computation.

# What to Submit

[20 pts] Choose *g* and *n* appropriately

[60 pts] Compute the shared secret *K* correctly

[20 pts] Write out all steps in all calculations involving modulo mathematics for your RSA and DH calculations.

## 

**My Net ID is dh2487 so a = 18, b = 17**

**g = 5**

**n = 23**

**A = ga mod n**

**= 518 mod 23**

**51 mod 23 = 5**

**52 mod 23 = 5 \* 5 mod 23 = 2**

**54 mod 23 = 2 \* 2 mod 23 = 4**

**58 mod 23 = 4 \* 4 mod 23 = 16**

**516 mod 23 = 16 \* 16 mod 23 = 256 mod 23 = 3**

**518 mod 23 = 3 \* 2 mod 23 = 6**

**A = 6**

**B = gb mod n**

**= 517 mod 23 = 3\*5 mod 23 = 15**

**B = 15**

**K = Ba mod n**

**= 1518 mod 23**

**15 mod 23 = 15**

**152 mod 23 = 15 \* 15 mod 23 = 225 mod 23 = 18**

**154 mod 23 = 18 \* 18 mod 23 = 324 mod 23 = 2**

**158 mod 23 = 2 \* 2 mod 23 = 4**

**1516 mod 23 = 4 \* 4 mod 23 = 16**

**1518 mod 23 = 16 \* 18 mod 23 = 288 mod 23 = 12**

**K = 12**

**K = Ab mod n**

**= 617 mod 23**

**6 mod 23 = 6**

**62 mod 23 = 6 \* 6 mod 23 = 36 mod 23 = 13**

**64 mod 23 = 13 \* 13 mod 23 = 169 mod 23 = 8**

**68 mod 23 = 8 \* 8 mod 23 = 64 mod 23 = 18**

**616 mod 23 = 18 \* 18 mod 23 = 324 mod 23 = 2**

**617 mod 23 = 2 \* 6 mod 23 = 12**

**K = 12**