PROGRAMMING AND DISCRETE MATHEMATICS (XX10190)
SEMESTER 2 MATHEMATICS: PROBLEM SHEET 5 – SOLUTIONS

All the large numbers in this sheet are assigned to MatLab variables in the MatLab script GKS5nums.m, to be found on Moodle.

1. Alice and Bob are getting better at this now. They are using a cryptosystem based on exponentiation in $(\mathbb{F}_q^*)^2$, with q a safe prime. That is, they use the subgroup G of index 2 and order $p = \frac{q-1}{2}$, generated by the square of any element of $\mathbb{F}_q^*$ other than ± 1. The Sophie Germain prime p is $10^{20} + 1243$.
Alice wishes to send Bob the secret message m, which is actually 10^{20} (and therefore a square by construction and hence a square mod q). Her key is $a = 5610810599101$ and Bob's key is $b = 6611198$.
Find the three messages they send during their Diffie-Hellman exchange.
You have to use `myExptMod` *(see the sheet on the symbolic toolbox), or an equivalent. Then the following will do.*

```
>> a2b1=myExptMod(m,a,q)
a2b1 =
30161234124124881209
>> b2a=myExptMod(a2b1,b,q)
b2a =
155779382343220026630
>> a2b2=myExptMod(b2a,mod(1/a,p),q)
a2b2 =
178541749312017537128
>> mrecover=myExptMod(a2b2,mod(1/b,p),q)
mrecover =
100000000000000000000
```

2. Later on, Alice sends Bob a second message m', using the same system and the same keys as in Question 1. Eve has by now found out (from Fred, who is Bob's security manager) that Bob's key b is 6611198, and she hears what is sent: Alice sends x, Bob sends back y and Alice sends $z = 18505096680418679204$. Find m'.
You need to compute an inverse c to b mod p and then compute z^c mod q:

```
>> b=6611198
b =
6611198
```

```
>> z=18505096680418679204
z =
18505096680418679204
>> mdashrecover=myExptMod(z,mod(1/b,p),q)
mdashrecover =
625
```

3. Finally, Alice and Bob practise setting up a shared secret by a symmetric Diffie-Hellman process. They work in $\mathbb{F}_{47}^*$ (not bothering about squares). Alice's key is 5 and Bob's is 9. They take $m = 11$. What messages do they send and what shared secret do they end up with?
Alice sends $11^5 \bmod 47 = 29 = -18$*; Bob sends* $11^9 \bmod 47 = 38 = -9$*; the shared secret is* $29^9 = 38^5 = 11^{45} = 30 = -17 \bmod 47$*.*

GKS, 4/4/17