11/11 CS 458 Homework 3

Q1: **Part 1:**

1) $7^{13} \bmod 23$

$13 = 1101_2 = 2^3 + 2^2 + 2^0$

$(13)_2$	
1	$c_1 \equiv 1^2 \cdot 7^1 \equiv 7 \bmod 23 = 7$
1	$c_2 \equiv 7^2 \cdot 7^1 = 49 \cdot 7 \equiv 343 \bmod 23 = 21$
0	$c_3 \equiv 21^2 \cdot 7^0 = 441 \cdot 1 \equiv 441 \bmod 23 = 4$
1	$c_4 \equiv 4^2 \cdot 7^1 = 16 \cdot 7 \equiv 112 \bmod 23 = 20$

$7^{13} \bmod 23 = 20$

Part 2:

3) $5^{13} \bmod 23 = 21$

$12^{17} \bmod 29 = 12$

$10^{25} \bmod 37 = 10$

4) c) $5^{13} \bmod 23$

$(13)_2$	
1	$c_1 \equiv 1^2 \cdot 5^1 = 1 \times 5 \equiv 5 \bmod 23 = 5$
1	$c_2 = 5^2 \cdot 5^1 = 25 \times 5 \equiv 125 \bmod 23 = 10$
0	$c_3 = 10^2 \cdot 5^0 = 100 \times 1 \equiv 100 \bmod 23 = 8$
1	$c_4 = 8^2 \cdot 5^1 = 64 \times 5 \equiv 320 \bmod 23 = 21$

$5^{13} \bmod 23 = 21$ ✓

b) Explain why the square and multiply algorithm is more efficient than directly calculating x^y before taking modulus.

This is more efficient because computing x^y would result in a very large numbers which would be computationally expensive and would require a lot of memory.
By breaking the calculation down into these smaller steps it allows the intermediate results to be manageable.
It also reduces the number of operations exponentially.

Q2: $p = 23$

$\alpha = 5$

Alice : $a = 6$

Bob : $b = 15$

Alice public key: $A = \alpha^a \bmod p$

$= 5^6 \bmod 23$

$= 8$

Bob public key: $B = \alpha^b \bmod p$

$= 5^{15} \bmod 23$

$= 19$

Exchange Public keys =

Alice gets $B = 19$

Bob gets $A = 8$

Common secret key K_{AB}:

Alice = $K_{AB} = B^a \bmod p$

$= K_{AB} = 19^6 \bmod 23 = 2$

Bob = $K_{AB} = A^b \bmod p$

$= K_{AB} = 8^{15} \bmod 23 = 2$

Both values of K_{AB} are equal.

It is the same because of the properties of modullar exponentiation

$$K_{AB} = (B^a \bmod p) = (A^b \bmod p)$$

$$B = \alpha^b \bmod p \qquad A = \alpha^a \bmod p$$

$$B^a \bmod p = (\alpha^b)^a \bmod p = \alpha^{ba} \bmod p$$
$$A^b \bmod p = (\alpha^a)^b \bmod p = \alpha^{ab} \bmod p$$

$ab = ba$, so K_{AB} will be equal.