Ü5

1. DH KE

a)

$\mathbb{Z}_{23}^* = \{1, 2, \ldots, 22\}$, $g = 5$

	mod23		mod23		mo
1	$5^0 = 1 \Rightarrow 1$	11	5^9	21	5^{13}
2	$5^2 = 25 \Rightarrow 2$	12	5^{20}	22	5^{11}
3	$5^{16} \Rightarrow 3$	13	5^{14}		
4	$5^4 \Rightarrow 4$	14	5^{21}		
5	$5^1 \Rightarrow 5$	15	5^{17}		
6	$5^{18} \Rightarrow 6$	16	5^8		
7	$5^{19} \Rightarrow 7$	17	5^7		
8	$5^6 \Rightarrow 8$	18	5^{12}		
9	$5^{10} \Rightarrow 9$	19	5^{15}		
10	$5^3 \Rightarrow 10$	20	5^5		

b)

Alice: $x = 17 \Rightarrow X = g^x = 5^{17} \bmod 23 = \underline{15}$

Bob: $y = 3 \Rightarrow Y = g^y = 5^3 \bmod 23 = \underline{10}$

c)

gemeinsamer Schlüssel:

Alice: $Y^x = g^{xy} = 10^{17} \bmod 23 = \boxed{17}$

Bob: $X^y = g^{xy} = 15^3 \bmod 23 = \boxed{17}$