Name: Solutions

Directions: Show all work. No credit for answers without work.

1. **[2 points]** Let $p = 13$ and $g = 7$. Find $\log_g(11)$ in $\mathbb{F}_p$.

13, 26, 39, 52, 65, 78

n	0	1	2	3	4	5
g^n	1	7	10	5	9	11

$\cdot 7$ $\cdot 7$

So $\log_7(11) = \boxed{5}$

2. **[2 points]** Let $p = 3167$ and $g = 7$; note that p is prime. Given that in $\mathbb{F}_p$, we have $\log_g(2) = 786$ and $\log_g(3) = 953$, find $\log_g(12)$.

Given: $g^{786} = 2$ and $g^{953} = 3$, we have that

$$12 = 2^2 \cdot 3 = (g^{786})^2 \cdot g^{953} = g^{(2\cdot 786)+953}.$$

So $\log_g(12) = 2\cdot 786 + 953 = \boxed{2525}$.

3. **[2 parts, 3 points each]** Alice and Bob use the Diffie-Hellman key exchange protocol with $p = 179$ and $g = 2$.

   (a) Alice picks $a = 33$ as her private number. What should she send to Bob?

Need $A = g^a = 2^{33}$

$2^2 = 4$

$2^4 = 4\cdot 4 = 16$

$2^8 = 16\cdot 16 = 256 = 77$

$2^{16} = 77\cdot 77 = 22$

$2^{32} = 22\cdot 22 = 126$.

So $A = 2^{33} = 2^{32}\cdot 2$

$= (126)\cdot 2 = 252 = \boxed{73}$

   (b) Alice receives $B = 145$ from Bob. What is their shared secret?

The shared secret is $B^a = (145)^{33}$.

$(145)^2 = 82$

$(145)^4 = 82\cdot 82 = 101$

$(145)^8 = 101\cdot 101 = 177$

$(145)^{16} = 177\cdot 177 = 4$

$(145)^{32} = 4\cdot 4 = 16$

So $B^a = (145)^{33}$

$= (145)^{32}\cdot 145$

$= 16\cdot 145$

$= \boxed{172}$.