Solutions to Homework Assignment # 8

1. (a) Z_5^*:

a	1	2	3	4
ord(a)	1	4	4	2

   (b) Z_{13}^*:

a	1	2	3	4	5	6	7	8	9	10	11	12
ord(a)	1	12	3	6	4	12	12	4	3	6	12	2

2. (a) $|Z_5^*| = 4$ $|Z_{13}^*| = 12$
   (b) yes
   (c) $Z_5^* : 2, 3$ $Z_{13}^* : 2, 6, 7, 11$
   (d) $\phi(4) = 2$ $\phi(12) = 4$
   (e) $1^6 = 2^6 = 3^6 = 4^6 = 5^6 = 6^6 \equiv 1 \bmod 7$

3. (a) $|Z_5^*| = 4 = 2 \cdot 2$ one subgroup with 2 elements
   $|Z_{13}^*| = 12 = 6 \cdot 2 = 2 \cdot 2 \cdot 3$ four subgroups with 6, 4, 3 and 2 elements, respectively
   (b) Z_5^*: subgroup $H = \{1, 4\}$

$\times$ mod 5	1	4
1	1	4
4	4	1

   Z_{13}^*: subgroup $H_1 = \{1, 3, 4, 9, 10, 12\}$

$\times$ mod 13	1	3	4	9	10	12
1	1	3	4	9	10	12
3	3	9	12	1	4	10
4	4	12	3	10	1	9
9	9	1	10	3	12	4
10	10	4	1	12	9	2
12	12	10	9	4	3	1

   subgroup $H_2 = \{1, 5, 8, 12\}$

$\times$ mod 13	1	5	8	12
1	1	5	8	12
5	5	12	1	8
8	8	1	12	5
12	12	8	5	1

subgroup $H_3 = \{1, 9, 3\}$

$\times \bmod 13$	1	9	3
1	1	9	3
9	9	3	1
3	3	1	9

subgroup $H_4 = \{1, 12\}$

$\times \bmod 13$	1	12
1	1	12
12	12	1

(c) Z_5^* : $H = \{1, 4\}$ $\rightarrow$ 4 is primitive element
Z_{13}^* : $H_1 = \{1, 3, 4, 9, 10, 12\}$ $\rightarrow$ 4 and 10 are primitive elements
$H_2 = \{1, 5, 8, 12\}$ $\rightarrow$ 5 and 8 are primitive elements
$H_3 = \{1, 9, 3\}$ $\rightarrow$ 9 and 3 are primitive elements
$H_4 = \{1, 12\}$ $\rightarrow$ 12 is a primitive element

If a subgroup (or any cyclic group) has a prime cardinality, i.e., the number of elements is a prime, all elements are primitive.

4. (a) $ord(2) = 3570 \bmod 3571$ primitive
$ord(4) = 1785 \bmod 3571$
$ord(2048) = 3570 \bmod 3571$ primitive

(b) $ord(2) = 3138 \bmod 12553$
$ord(5) = 12552 \bmod 12553$ primitive
$ord(5300) = 12552 \bmod 12553$ primitive

5. (a) One needs about p steps for finding a primitive element if one computes

$$a \stackrel{?}{\equiv} 1 \bmod p, \quad a^2 \stackrel{?}{\equiv} 1 \bmod p, \quad a^3 \stackrel{?}{\equiv} 1 \bmod p \ldots$$

Note that each step requires a multiplication with a.
$\Rightarrow$ since $p \geq 2^{1024}$, this test is not feasible in real–size DL systems.

(b) We know à priori that not all orders are possible but only those that divide $p-1$. Hence it is sufficient to raise a given element "a" to these possible orders using the square & multiply algorithm and to check whether the result is equal to one. Since the square & multiply algorithm has logarithmic complexity and there are only "a few" orders to check, this approach is very feasible.

6. (a) $K_{pub_A} = 8 \qquad K_{pub_B} = 32 \qquad K_{AB} = 78$

   (b) $K_{pub_A} = 137 \qquad K_{pub_B} = 84 \qquad K_{AB} = 90$

   (c) $K_{pub_A} = 394 \qquad K_{pub_B} = 313 \qquad K_{AB} = 206$

7. (a) $K_{pr_A} = \alpha^{a_A} = 4^{400} \equiv 89 \bmod 467$
   $K_{pr_B} = \alpha^{a_B} = 4^{134} \equiv 51 \bmod 467$
   $K_{AB} = K_{pr_B}^{(a_A)} = K_{pr_A}^{(a_B)} \equiv 161 \bmod 467$

   (b) $K_{pr_A} = \alpha^{a_A} = 4^{167} \equiv 89 \bmod 467$
   $K_{pr_B} = \alpha^{a_B} = 4^{134} \equiv 51 \bmod 467$
   $K_{AB} = K_{pr_B}^{(a_A)} = K_{pr_A}^{(a_B)} \equiv 161 \bmod 467$
   4 has order 233 in Z_{467}^*, i.e., $4^{233} \equiv 1 \bmod 467$. Alice computes in a)

$$K_{pr_A} = b_A = \alpha^{a_A} = 4^{400} = 4^{233+167} = 1 \cdot 4^{167} \equiv 4^{167} \bmod 467$$

   Which is the same private key that she computes in b).
   Note also that you can write:

$$4^{400} = 4^{400 \bmod 233} = 4^{167}$$

   In general, if you have an element a of order n it doesn't make any sense to compute a^j if $j > n$. Instead one can immediately compute $a^j = a^{j \bmod n}$.

8. Alice / Oscar / Bob

Alice		Oscar		Bob
$\alpha^{a_A} = b_A$	$\xrightarrow{b_A}$	$\alpha^{a_o} = b_o$	$\xrightarrow{b_o}$	
	$\xleftarrow{b_o}$		$\xleftarrow{b_B}$	$\alpha^{a_B} = b_B$
$b_o^{a_A} = \alpha^{a_A \cdot a_o} = K_{Ao}$		$b_A^{a_o} = \alpha^{a_A \cdot a_o} = K_{Ao}$ $b_B^{a_o} = \alpha^{a_B \cdot a_o} = K_{Bo}$		$b_o^{a_B} = \alpha^{a_B \cdot a_o} = K_{Bo}$

   Oscar shares now a "secret" key with Alice and Bob. Alice and Bob both don't know about it and think they share a key with with each other. Oscar can now decrypt, read and encrypt any messages between Alice and Bob without them learning about it if he continues to intercept all encrypted messages.

   This is the infamous "man-in-the-middle" attack. We will talk a lot about it in the key distribution lecture. This attack is, in essence, responsible for things such as certificates, public-key infrastructures, etc.