# Solutions to Assignment #4

#3 Suppose $3 \equiv 5^x \bmod 1223$. Then $1 \equiv 3^{611} \equiv 5^{611x}$.

Since 5 is a generator, $611x \equiv 0 \bmod 1222$ and so $x$ is even.

#4 To employ Pohlig-Hellman, we factor $p-1 = 19-1 = 2 \cdot 3^2$. We then determine $x = L_2(14)$ by figuring out $x \bmod 2$ and $x \bmod 9$.

We preprocess $2^0$ and $2^9 \bmod 19$ which are $1$ and $-1$ and we also compute $2^0, 2^6$ and $2^{18} \bmod 19$ which are $1, 7$ and $11$.

Now for the factor 2, we compute $14^9 \equiv -1 \bmod 19$ so $x \equiv 1 \bmod 2$.

For the factor 3, we write $x \equiv x_0 + x_1 3 \bmod 9$ and determine $x_0$ by computing $14^6 \equiv 7 \bmod 19$ which gives $x_0 \equiv 1 \bmod 3$.

Now $b_1 \equiv 14 \cdot 2^{-1} \equiv 7 \bmod 19$ and $7^2 \equiv 11 \bmod 19$ so $x_1 \equiv 2 \bmod 3$. Altogether then $x \equiv 1 + 2 \cdot 3 \bmod 9$
$\equiv 7 \bmod 9$

So from $x \equiv 1 \bmod 2$ and $x \equiv 7 \bmod 9$ we get $x \equiv 7 \bmod 18$ and $L_2(14) = 7$.

#7 $3^6 \equiv 44 \mod 137$ and $3^{10} \equiv 2 \mod 137$ so

$$11 = 44 \cdot 2^{-2} \equiv 3^6 \cdot 3^{-20} \mod 137$$

$$\equiv 3^{136-14} \mod 137$$

$$= 3^{122} \mod 137 \quad \text{so } x = 122.$$

#8 a) Given that the prime is random and 500 digits long, there is no reason to believe that any discrete log attack on the password file will take less than order $10^{250}$ time steps. which is currently infeasible.

b) If p is only 5 digits long then a brute force attack like baby step - giant step will discover the passwords.

Finite field questions:

1. If g is a generator of $F_q$ then $g^{\frac{q-1}{p_i}} \neq 1$ for all i since the order of g is q-1.
In the other direction, if d = the order of g then d divides q-1. If $d < q-1$ then d divides $\frac{q-1}{p_i}$ for some i. So then $g^{\frac{d-1}{p_i}} = 1$ which is not true. So $d = q-1$ and g is a generator.

2. $40 = 2^3 \cdot 5$ so we need to compute $x^{\frac{40}{p_i}}$ and $x^8$ in $IF_{11}$. for $x = 2, 3, 5$ and 7.

Computing $x^r$ in the following table.

| r \ x | 2 | 3 | 5 | 7 |
|---|---|---|---|---|
| 20 | 21 | -1 | 1 | -1 |
| 8 | 10 | 1 | 18 | 37 |

So only $x = 7$ is a generator from this list.

3. If $g^i$ is a generator for $F_q$ then for some $k$ $(g^i)^k \equiv g$ in $F_q$. Since $g$ is also a generator we then have $ik \equiv 1 \bmod q-1$ which means $\gcd(i, q-1) = 1$.

On the otherhand, if $\gcd(i, q-1) = 1$, choose $x$ and $y$ s.t. $ix + (q-1)y = 1$. Then

$$(g^i)^x = g^{ix+(q-1)y} = g \text{ in } F_q.$$ Since $g^i$ can generate $g$, it can then generate all non-zero elements of $F_q$.

4. $$L_2(60) = L_2(2^2 \cdot 3 \cdot 5) = 2 + L_2(3) + L_2(5)$$
$$= 2 + 69 + 24$$
$$= 95.$$

so $2^{95} \equiv 60 \bmod 101$.