Solutions to Test 3

1a) $L_2(3925 \cdot 1046) = L_2(3925) + L_2(1046) \mod 3988$

$= 2000 + 300$

$= 1022$

b) $5^2 \equiv 8 \mod 17$ so $L_5(5^2) = L_5(8) \mod 16$

and $2 = 3L_5(2) \mod 16$. $10 = 15L_5(2) \mod 16$

$= -L_5(2)$

so $L_5(2) = -10 = 6 \mod 16$.

2. Even if Eve can compute the discrete log $L_g(g^{3a})$, she will only obtain $3a$. But since $3 \mid 15$ (gcd$(3,15) \neq 1$), she will be unable to determine a.

3. $b^4 = 1$ so $L_2(b^4) = L_2(2^0) \mod 36$ This gives

$4L_2(b) = 0 \mod 36$. So $L_2(b)$ could be $0, 9, 18$ or 27.

4. a) The squares in F_7 are as follows:

y	0	1	2	3	-3	-2	-1
y^2	0	1	4	2	2	4	1

and the values of $x^3 - x + 1$ are

x	0	1	2	3	-3	-2	-1
x^3-x+1	1	1	0	4	5	2	1

This means that the points on the elliptic curve are

$(0,\pm 1)$, $(1,\pm 1)$, $(2,0)$, $(3,\pm 2)$, $(5,\pm 3)$, $(6,\pm 1)$ and O. 12 points.

b) The tangent line at (x,y) has slope $\frac{3x^2-1}{2y}$. So at $(1,1)$, this is $\frac{2}{2}=1$. The tangent line is then $y=x$ and so the third point on this line is $(-1,-1)$ which means

$(1,1)+(1,1)=(-1,1)$ (the reflection of $(-1,-1)$).

The slope between $(1,1)$ and $(0,-1)$ is $2/1=2$ and so the line between them is $y=2x-1$. The third point is then $(3,-2)$. The reflection is then $(3,2)$ so

$(1,1)+(0,-1)=(3,2)$.

5. a) g is a generator of F_{601} if $g^{600}\equiv 1 \bmod 601$ but no smaller power will work. If a smaller power works it must be a divisor of 600 and so a maximal divisor will also yield 1. Since $600=2^3\cdot 3\cdot 5^2$, the maximal divisors are 120, 200 and 300. Since 7 raised to any of these powers is <u>not</u> $\equiv 1 \bmod 601$, 7 is a generator.

b) In general, if $g^u \not\equiv 1 \bmod p$ for any maximal divisor of $p-1$ then g is a generator of F_p.