$y^2 = x^3 - 17x + 31, p = 52981, P = (107,391)$

$encrypted\ message$: 77066213

Received four symbol message with last two symbols unreadable: f l _ _

Step 1:

Run readable symbols, f l, through Encode.java and get: 7177

Step 2:

Instructions say to reduce mod 100

Last two digits of x value in point come from shift in first character: $77 - 71 = 06$

Previous two digits of x come from shift in second character: $06 - 77 = -71$

Need positive value in Z_{100} so add 100: $-71 + 100 = 29$

So, last four digits of x are: 2906

Step 3:

Need all points on elliptic curve where last four digits of x are 2906, so run PointECC.java with:

$p = 52981, a = -17, b = 31, x = 107, y = 391$

Get 17,608 results. Need only points with last four digits of x equal to 2906:

2604P= (32906,21402)

7099P= (2906,28589)

10509P= (2906,24392)

15004P= (32906,31579)

Step 4:

For each point result, subtract last two digits of y from third character in encrypted message (62) and subtract previous two digits in y from fourth character in encrypted message (13)

$2604P \rightarrow 62 - 02 = 60, 13 - 14 = -1 + 100 = 99$, Result: 71776099

$7099P \rightarrow 62 - 89 = -27 + 100 = 73, 13 - 85 = -72 + 100 = 28$, Result: 71777328

$10509P \rightarrow 62 - 92 = -30 + 100 = 70, 13 - 43 = -30 + 100 = 70$, Result: 71777070

$15004P \rightarrow 62 - 79 = -17 + 100 = 83, 13 - 15 = -2 + 100 = 98$, Result: 71778398

Step 5:

Run results through Decode.java

$71776099 = fl$[?

$71777328 = flh$;

$71777070 = flee$

$71778398 = flr$?

So, the message is “flee” and the point is $10509P$