Problem 4- El Gamal attack with same k

April 26, 2020

[17]:
```
import sys
sys.path.append('../')
import crypto_utils as utils
%load_ext autoreload
%autoreload 2
```

```
The autoreload extension is already loaded. To reload it, use:
  %reload_ext autoreload
```

[18]:
```
c1 = (1430, 697)
c2 = (1430, 1113)
p = 2357
m1 = 2035
```

[19]:
```
# first calculate delta1_modp
delta1_modp = c1[1] % p
print(delta1_modp)
```

```
697
```

[20]:
```
# Use y_modp*(delta1_modp) = m1 and get y_modp = m1*delta1_inv modp
y_modp = m1*utils.mod_inverse(delta1_modp, p) % p
print(y_modp)
```

```
872
```

[21]:
```
# y*(delta2_modp) = m2
m2 = y_modp*(c2[1] % p) % p
print(m2)
```

```
1809
```