Problem 5- El Gamal how to find k efficiently

April 26, 2020

[14]:
```
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
```

[15]:
```
p = 31847
g = 5
beta = 25703
```

[16]:
```
m1 = 8990
sig1 = (23972, 31396)
m2 = 31415
sig2 = (23972, 20481)
```

[17]:
```
# no hash function, therefore, for m, s = k^-1(m-ar) mod(p-1)
# from handwritten notes we know: k = (s1-s2)^-1*(h(m1)-h(m2)) mod(p-1)
# simplify h(m1) -> m1 and h(m2) -> m2
s1_s2 = sig1[1]-sig2[1]
s1_s2_inv = utils.mod_inverse(s1_s2, p-1)
m1_m2 = m1 - m2
k = (s1_s2_inv*m1_m2) % (p-1)
print(k)
```

```
1165
```