Problem 1- Decrypt ElGamal ciphertext

April 26, 2020

[12]:
```
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
```

[13]:
```
# Exercise 7.9 of Stinson
# parameters of system
p = 31847
alpha = 5
a = 7899
beta = 18074
```

[14]:
```
c1 = (3781, 14409)
c2 = (31552, 3930)
c3 = (27214, 15442)
```

[15]:
```
# First compute y = lambda^(p-1-a) (mod p)
exp_part = p - 1 - a
print(exp_part)
y1 = utils.ModExp(c1[0], exp_part, p, False)
y2 = utils.ModExp(c2[0], exp_part, p, False)
y3 = utils.ModExp(c3[0], exp_part, p, False)
print(y1)
print(y2)
print(y3)
```

```
23947
6479
25886
4876
```

[16]:
```
# Next compute y*symbol (mod p) = m (plaintext)
m1 = y1*c1[1] % p
m2 = y2*c2[1] % p
```

```
m3 = y3*c3[1] % p
print(m1)
print(m2)
print(m3)
```

```
12354
12662
8884
```

[17]:
```
full_text = utils.base26ish_2_word(m1) + \
utils.base26ish_2_word(m2) + \
utils.base26ish_2_word(m3)
print(' '.join(let[0] for let in full_text))
```

```
S H E S T A N D S
```