Problem 1- Decrypt RSA Text

April 12, 2020

[165]:
```
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
```

[166]:
```
n = 18923
b = 1261
unit1 = 12423
unit2 = 11524
unit3 = 7243
```

[167]:
```
utils.factor(n)
```

[167]:
```
[1, 127, 149, 18923]
```

[168]:
```
phi_of_n = (127-1)*(149-1)
print(phi_of_n)
# len(utils.compute_phi(n)) # gets same answer yay
```

```
18648
```

[169]:
```
a = utils.mod_inverse(b, phi_of_n)
print(a)
```

```
5797
```

[170]:
```
val1 = utils.ModExp(unit1, a, n, debug=False)
val2 = utils.ModExp(unit2, a, n, debug=False)
val3 = utils.ModExp(unit3, a, n, debug=False)
```

[171]:
```
# does the same thing as above
# post_exp = unit3**a
# post_mod = post_exp % n
# print(post_mod)
```

[172]:
```
def word_2_base26ish(word):
    total = 0
    d = len(word)
    for i in range(d):
        total = total + (utils.let_to_num(word[i])*(26**(d-i-1)))

    return total

# print(word_2_base26ish("DOG"))
# print(word_2_base26ish("CAT"))
# print(word_2_base26ish("ZZZ"))
# This is the wrong way, now reverse it
```

[173]:
```
def base26ish_2_word(value):
    total = 0
    word = ['','','']
    for i in range(2,-1,-1):
        letter = value // (26**i)
        word[2-i] = (utils.num_to_let(letter))
        value = value - (letter*(26**i))

    return word
```

[174]:
```
full_text = base26ish_2_word(val1) + base26ish_2_word(val2) +␣
 ↪base26ish_2_word(val3)
print(' '.join(let[0] for let in full_text))
```

```
I B E C A M E I N
```