Problem 3- Protocol Failure w Algorithm Exploit

April 15, 2020

[10]:
```
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
```

[11]:
```
# Part a is in handwritten notes
```

[12]:
```
n = 18721
b1 = 43
b2 = 7717
y1 = 12677
y2 = 14702
```

[13]:
```
c1 = utils.mod_inverse(b1, b2)  # c1 = b1^-1 mod b2
c2 = (c1*b1 - 1)/b2  # c2 = (c1*b1 - 1)/b2
```

[14]:
```
y1_c1 = utils.ModExp(y1,c1,n, False);
y2_c2 = utils.ModExp(y2,int(c2),n, False);
y2_c2_inv = utils.mod_inverse(y2_c2,n);
print(y2_c2_inv)
print(y2_c2_inv*y2_c2 % n)
```

```
5668
1
```

[15]:
```
x1 = (y1_c1*y2_c2_inv) % n
print(x1)

# verify answer, should get y1 = 12677
test_y1 = x1**b1 % n
print(test_y1)
print(y1)
print(test_y1==y1)
```

```
15001
12677
12677
True
```