MATH/CSCI 408 Name: ________________________________

**CRYPTOGRAPHY MISSION 09 SOLUTIONS**

**Deadline: Thursday, 17 November 2016 at 3:05pm**
This mission covers Sections 6.3, 6.4, and 7.1

## 1. Graded Problems

1. Read through the Miller-Rabin Primality Test (6.3 p. 178). Work through the example, and write a new example here.

$$n = 101$$
$$n - 1 = 100 = 2^2 \cdot 25$$
$$\text{Choose } a = 3.$$
$$b_0 = 3^{25} \equiv 10 \bmod 101$$
$$b_1 = 10^2 \equiv 100 \bmod 100$$

So $n = 101$ is probably prime.

2. Use the Fermat Factoring method to factor 70747.

$$70747 + 1^2 = 70748$$
$$70747 + 2^2 = 70751$$
$$70747 + 3^2 = 70756$$

and $\sqrt{70756} = 266$, so $70756 = (266+3)(266-3) = 269 \cdot 263$.

3. Use the $p - 1$ Factoring Algorithm to factor 4757.

```
n = 4757
for i in range(1,10):
        print gcd(2^(factorial(i))%n-1,n)}
```

We find that when $i = 7$, we get the gcd to be 71, so 71 is a factor and so is $4757/71 = 67$.

4. Use SageMath's `factor()` to check your answers to problems 1 and 2.

```
factor(101)
factor(70747)
```

yields 101 (which is prime) and $263 \cdot 269$.

5. Given $p = 17$. Solve the following discrete logs problems if possible. If not, explain why.
   a. $14 \equiv 3^x \mod 17$

$x = 9$ works.

   b. $5 \equiv 4^x \mod 17$

This is impossible. If we try several $x$ values, we find that we get possible mod17 values of 1, 4, 16, 13. These repeat, so any other value (namely, 5) won't appear.