CIS 3362 Test #3: Public Key Encryption

Date: 11/17/2017

Name: _____
Note: For questions with numeric answers, put a box around your final answer.
Aids: You may use a calculator and 2 sheets of notes

1) (8 pts) What is the prime factorization of 419325984?

2) (8 pts) What is φ(419325984)?

3) (12 pts) Using Fermat's Theorem, determine 2536^{42841} mod 6121. (Note: 6121 is a prime number.

4) (12 pts) Using Euler's Theorem, determine $638^{15363} \bmod 5525$.

5) (12 pts) In an RSA scheme, p = 11, q = 41 and e = 189. What is d?

6) (10 pts) Alice's Public El Gamal keys are q = 31, and $\alpha = 11$. Alice's secret key $X_A = 9$. Bob has sent a message to Alice. The ciphertext he has sent to Alice is $C_1 = 3$, $C_2 = 18$. What is the plaintext?

7) (12 pts) Write a short brute force function in C below so that it returns 1 if its input parameter g is a generator mod p, and returns 0 otherwise. You may assume that p is a prime, $p < 10^4$ and that $1 < g < p-1$.

```
// Returns 1 if g is a generator mod p, 0 otherwise.
int isGenerator(int g, int p) {

}
```

8) (12 pts) Consider the Elliptic Curve $E_{31}(5,2)$. Let the point P on this curve be (23, 16) and the point Q be (5, 11). What is P + Q?

9) (12 pts) Consider the Elliptic Curve $E_{31}(5,2)$. Let the point P on this curve be (23, 16). What is 2P?

9) (2 pts) What were the hours that 7-11 (when it first opened) was open? _____

Scratch Page - Please clearly label any work on this page you would like graded.