Anand Mahadevan - SID 862132182
Husam Chekfa - SID 862184675

CS111 Homework 2

due Friday, Apr 30th 11:59 PM

Problem 1.

Suppose $3|x$ and $3|y$.
When x and y are squared, their factors of 3 each will become 9.
For example, $6 = 2 * 3$
$6^2 = 2 * 3 * 2 * 3 = 2 * 2 * 9$
Summing two multiples of 9 will result in a number that is divisible of 9.
Thus, $9|x^2$ and $9|y^2$.

Suppose either $3 \nmid x$ OR $3 \nmid y$.
Since the factorization of 9 is $3 * 3$, there doesn't exist the 3 factor necessary in either x or y that becomes 9 in x^2 or y^2. Thus, $9 \nmid x^2$ OR $9 \nmid y^2$.
Since the sum of $x^2 + y^2$ needs to have both terms be multiples of 9 in order to be divisible by 9, $9 \nmid (x^2 + y^2)$.

So with x, y being two non-negative integers. $9|(x^2 + y^2)$ if and only if $3|x$ and $3|y$.
Q.E.D.

Problem 2.

(a)
p and q were found by factoring 187, the known value for n. p is chosen to be less than q. $\phi(n)$ was found with the formula $(p-1)*(q-1)$. d was found through $e^{-1}(mod\phi(n))$
$p = 11$
$q = 17$
$\phi(n) = 160$
$d = 9^{-1}(mod 160)$
Multiples of 9: 9, 18, ... , 801; = **89** * 9
Multiples of 160: 9, 18, ... , 800; = 5 * 9
Thus, $d = 89$.

(b)
$D(C) = C^d$ rem n
The following is a decryption of $C = 21$
21^{89} rem 187
$21^{89} \equiv 21 * (21^2)^{44} (\text{mod } 187)$
$\equiv 21 * 441^{44} (\text{mod } 187)$
$\equiv 21 * 67^{44} (\text{mod } 187)$
$\equiv 21 * (67^2)^{22} (\text{mod } 187)$
$\equiv 21 * 4489^{22} (\text{mod } 187)$
$\equiv 21 * 1^{22} (\text{mod } 187)$

$\equiv 21 * 1 (\bmod 187)$
$\equiv 21 (\bmod 187)$

The letters in this RSA range from values 3 to 28 (A = 3, ...). 21 falls in this range. Since the letters are shifted two to the right (A is 3 instead of the standard of 1), we can subtract 2 from 21 and convert that to the 19th letter of the alphabet. 21 - 2 = 19. The 19th letter of the alphabet is S. Thus, the value C = 21 represents the letter S.

(c)

This is the decoded message as a list of integers:
30 7 3 22 29 3 29 14 11 24 7 29 8 20 17 9 29 8 11 20 21 22 29 22 10 11 16 9 29 11 16 29 22 10 7 29 15 17 20 16 11 16 9 29 3 16 6 29 16 17 22 10 11 16 9 29 25 17 20 21 7 29 25 11 14 14 29 10 3 18 18 7 16 29 22 17 29 27 17 23 29 22 10 7 29 20 7 21 22 29 17 8 29 22 10 7 29 6 3 27 30 31

(d)

This is the decoded message in plain-text and its origin:
"EAT A LIVE FROG FIRST THING IN THE MORNING AND NOTHING WORSE WILL HAPPEN TO YOU THE REST OF THE DAY".
This is a quote by Mark Twain about getting tasks done on time. If someone completes a task in the morning, they will have an easy rest of the day. This quote is about procrastination.

(e)

```
#include <iostream>
#include <vector>
#include <cmath>
using namespace std;

int decrypt(int C, int d, int n){
    int ans = 1;

    do {
        if(d % 2 != 0){
            ans = (ans*C) % n;
        }
        d /= 2;
        C = (C*C) % n;
    }while(d > 0);
    return ans;
}

char decode_char(int num){
    char c;
    if(num == 29)  return ' ';
    else if(num == 30) return '"';
    else if(num == 31) return '.';
    else {
        return char(num+62);
    }
```

```
    return c;
}

int main(){
    int numbers[]={183,129,48,165,107,48,107,37,176,61,129,107,161,82,
68,60,107,161,176,82,21,
165,107,165,109,176,152,60,
107,176,152,107,165,109,129,
107,168,68,82,152,176,152,
60,107,48,152,79,107,152,
68,165,109,176,152,60,107,
59,68,82,21,129,107,59,
176,37,37,107,109,48,52,
52,129,152,107,165,68,107,
75,68,45,107,165,109,129,
107,82,129,21,165,107,68,
161,107,165,109,129,107,79,
48,75,183,71};

    vector<int> decrypt_ints;
    vector<char> decrypt_chars;
    for(unsigned i = 0; i < sizeof(numbers)/sizeof(int); i++){
            decrypt_ints.push_back(decrypt(numbers[i], 89, 187));
            decrypt_chars.push_back(decode_char(decrypt_ints.at(decrypt_ints.size()-1)));
    }
    for(unsigned i = 0; i < sizeof(numbers)/sizeof(int); i++){
        printf("%d ", decrypt_ints.at(i));
    }
    for(unsigned i = 0; i < sizeof(numbers)/sizeof(int); i++){
        printf("%c", decrypt_chars.at(i));
    }

    return 0;
}
```

Problem 3.

(a)

$$\begin{aligned} 7^{234673} &\equiv (7^{16})^{14667} * 7^1 (mod 17) \\ &\equiv 1 * 7 (mod 17) \\ &\equiv 7 (mod 17) \end{aligned}$$

(b)

$$32x + 52 \equiv 4(mod 37)$$

32 factors: 32, 64, ... , 704; 704 = **22** * 32

37 factors: 37, 74, ... , 703; 703 = 19 * 37

$$So, 32^{-1} \equiv 22(mod 37)$$

$$32x + 52 \equiv 4(mod 37)$$

$$32x \equiv -48(mod 37)$$

$$32x \equiv 26(mod 37)$$

$$22 * 32x \equiv 22 * 26(mod 37)$$

$$x \equiv 572$$

$$x = 17$$

(c)

All values with inverses modulo 256 are relatively prime to 256. That is, their gcd is 1.
The prime factorization of 256 is 2^8.
If a number is relatively prime to an even number, it must be odd. Since the prime factorization of 256 only involves the number 2, any odd number in the range of $\{1, 2, ..., 256\}$ is relatively prime to 256.
Thus, there are **128** relatively prime numbers in this set: {1, 3, 5, ..., 255}.
So there are **128** integers in the range $\{1, 2, ..., 256\}$ that have inverse modulo 256.

Academic integrity declaration.
Anand Mahadevan and Husam Chekfa completed this assignment together, and did not use external websites.