Assignment 2

Samantha Vu SID 861291195

Ashu Singh SID 861167389

CS 111 ASSIGNMENT 2

due Friday, February 9

Problem 1: Prove the following statement: Let x, y be two non-negative integers. Then $9|(x^2 + y^2)$ if and only if $3|x$ and $3|y$. (Note: notation $a|b$ means that a is a divisor of b.)

Hint: What are all possible remainders of x^2 modulo 9?

Solution 1:

Prove that if $3|x$ and $3|y$, then $9|(x^2 + y^2)$.

We prove its contrapositive: If $x rem 3 \neq 0$ or $y rem 3 \neq 0$ then $(x^2 + y^2) rem 9 \neq 0$.

For any $x1, y1$ such that $x1 \equiv x (mod 3)$ and $y1 \equiv y (mod 3)$ we have $(x^2 + y^2) rem 9 = (x1^2 + y1^2) rem 9$.

If $x, y \in 0, 1, ..., 8$ and both x, y are not multiples of 3, then $(x^2 + y^2) rem 9 \neq 0$:

$x, y : 0, 1, 2, 3, 4, 5, 6, 7, 8$

$x^2 rem 9, y^2 rem 9 : 0, 1, 4, 0, 7, 7, 0, 4, 1$

Then, we prove that if $9|(x^2 + y^2)$, then $3|x$ and $3|y$.

We prove its contrapositive: If $(x^2 + y^2) rem 9 \neq 0$, then $x rem 3 \neq 0$ and $y rem 3 \neq 0$.

For any $x1, y1$ such that $(x^2 + y^2) rem 9 = (x1^2 + y1^2) rem 9$, we have $x1 \equiv x (mod 3)$ and $y1 \equiv y (mod 3)$.

If $(x^2 + y^2) rem 9 \neq 0$, then both x, y are not a multiple of 3:

$x^2 rem 9, y^2 rem 9 : 0, 1, 4, 0, 7, 7, 0, 4, 1$

$x, y : 0, 1, 2, 3, 4, 5, 6, 7, 8$

Then, $9|(x^2 + y^2)$ if and only if $3|x$ and $3|y$.

Problem 2:

Alice's RSA public key is $P = (e, n) = (31, 95)$. Bob sends Alice the message by encoding it as follows. First he assigns numbers to characters: blank is 2, comma is 3, period is 4, colon is 5, semicolon is 6, dash is 7, then A is 8, B is 9, ..., Y is 32, and Z is 33. Then he uses RSA to encode each number separately.

Bob's encoded message is: Decode Bob's message. Notice that you don't have Alice's secret key, so you need to "break" RSA to decrypt Bob's message.

For the solution, you need to provide the following:

- Describe step by step how you arrived at the solution:
  - Show how you determined p, q, $\phi(n)$, and d;
  - Show the calculation that determines the first letter in the message.
- Give Bob's message in plaintext. The message is a quote. Who said it?
- If you wrote a program, attach your code to the hard copy. If you solved it by hand (not recommended), attach your scratch paper with calculations for at least 5 first letters.

88	11	82	70	27	8
81	33	41	3	81	26
3	30	10	27	8	3
80	88	20	27	81	41
26	3	27	72	8	88
80	3	33	41	88	3
10	27	26	3	72	33
80	59	33	8	8	88
41	3	30	10	27	8
3	33	41	88	3	10
27	26	3	19	88	27
80	41	88	11	3	81
41	3	26	70	10	33
33	19	9			

Solution 2:

Alice's secret key: $n = 95 = pq$

$p = 19, q = 5$

$\phi(n) = (p-1)(q-1) = 18 * 4 = 72$

$d = e^{-1} mod \phi(n) = 31^{-1} mod 72$

$31\alpha + 72\beta = 1$

Multiples of $31\alpha = 31, 62, 93, 124, 155, 186, 217$

Multiples of $72\beta + 1 = 73, 145, 217$

$\alpha = 31^{-1} mod 72 = d = 7$

First letter: $88^7 mod 95$

$= 88 * 88^6 = 88 * (88^2)^3 = 88 * 7744^3 = 88 * 49^3$

$= 88 * 49 * 49^2 = 4312 * 49^2 = 37 * 49^2 = 37 * 2401$

$= 37 * 26 = 962 = 12$

$\rightarrow$ 'E '

Bob's message: EDUCATION IS WHAT REMAINS AFTER ONE HAS FORGOTTEN WHAT ONE HAS LEARNED IN SCHOOL.

This is a quote from Albert Einstein.

Algorithm:

```
#include <iostream>
#include <string>
#include <math.h>
using namespace std;

int mod(string , int );
char convert(int );
```

```
int main() {
    //Declare and fill array with Bob's encrypted message
    const int SIZE = 81;
    int encrypted_message [SIZE] = { 88, 11, 82, 70, 27, 8,
                                     81, 33, 41, 3, 81, 26,
                                     3, 30, 10, 27, 8, 3,
                                     80, 88, 20, 27, 81, 41,
                                     26, 3, 27, 72, 8, 88,
                                     80, 3, 33, 41, 88, 3,
                                     10, 27, 26, 3, 72, 33,
                                     80, 59, 33, 8, 8, 88,
                                     41, 3, 30, 10, 27, 8,
                                     3, 33, 41, 88, 3, 10,
                                     27, 26, 3, 19, 88, 27,
                                     80, 41, 88, 11, 3, 81,
                                     41, 3, 26, 70, 10, 33,
                                     33, 19, 9 };

    cout << "Bob's decrypted message: ";
    for(int i = 0; i < SIZE; i++) {
        cout << convert(mod(to_string(pow(encrypted_message[i], 7)), 95));
    }
    cout << endl;

    return 0;
}

int mod(string num, int a) {
    int res = 0;
    for (int i = 0; i < num.find('.'); i++) {
         res = (res * 10 + (int)num[i] - '0') % a;
    }
    return res;
}

char convert(int number) {
    if(number == 2) { return number + 30; } //' '
    else if(number == 3) { return number + 41; } //','
    else if(number == 4) { return number + 42; } //'.'
    else if (number == 5) { return number + 53; } //';'
    else if (number == 6) { return number + 38; } //'-''
    else { return number + 57; } //'A'-'Z'
}
```

Problem 3: (a) Compute $15^{-1}(mod 17)$ by enumerating multiples of the number and the modulus. Show your work.

(b) Compute $15^{-1}(mod 17)$ using Fermat's theorem. Show your work.

(c) Find a number $x \in 1, 2, ..., 36$ such that $7x \equiv 11(mod 37)$. Show your work. (You need to follow the method covered in class; brute-force checking all values of x will not be accepted.)

Solution 3:

(a) $15^{-1}(mod 17)$

$15\alpha + 17\beta = 1$

Multiples of $15\alpha = 15, 30, 45, 60, 75, 90, 105, 120$

Multiples of $17\beta + 1 = 18, 35, 52, 69, 86, 103, 120$

$\alpha = 15^{-1} mod 17 = 8$

(b) $15^{-1}(mod 17)$

$15^{-1} = 15^{15}$

$= 15 * 15^{14} = 15 * (15^2)^7 = 15 * 225^7 = 15 * 4^7$

$= 15 * 4 * 4^6 = 60 * 4^6 = 9 * 4^6 = 9 * (4^2)^3$

$= 9 * 16^3 = 9 * 16 * 16^2 = 144 * 16^2 = 8 * 16^2$

$= 8 * 256 = 8 * 1 = 8$

(c) $7x \equiv 11(mod 37)$

$7^{-1} mod 37$

$7\alpha + 37\beta = 1$

Multiples of $7\alpha =, 14, 21, 28, 35, 42, 49, 56, 63, 70, 77, 84, 91, 98, 105, 112$

Multiples of $37\beta + 1 = 38, 75, 112$

$\alpha = 7^{-1} mod 37 = 16$

So, $7^{-1}(7x) = 11(7^{-1}) mod 37$

$x = 11 * 16(rem 37) = 176 mod 37 = 28$