Zachary Sells SID 861013217

CS 111 ASSIGNMENT 2

due Thursday, February 7

CS/MATH111 ASSIGNMENT 2

due Thursday, February 7 (8AM)

Individual assignment: Problems 1 and 2.
Group assignment: Problems 1,2 and 3.

Problem 1: Let $n = p_1 p_2 ... p_k$ where $p_1, p_2, ..., p_k$ are different primes. Prove that n has exactly 2^k different divisors. Give a complete argument.

For example, if $n = 105$ then $n = 3 \cdot 5 \cdot 7$, so $k = 3$ and thus n has $2^3 = 8$ divisors. These divisors are $1, 3, 5, 7, 15, 21, 35, 105$.

Hint: You can reduce the problem to counting other objects, that we already know how to count. Alternatively, this can be proved by induction on k.

Problem 1 Solution Given: $n = p_1 * p_2 * ....p_k$

By the Fundamental Theorem of Arithmetic, any integer, n is made up of the product of a unique combination of primes: $(p_1, p_2, p_3, ...p_k)$

Since $p_1 ... p_k$ are divisors of n, we can infer that $p_1 * (p_2 \dot{p_3} .... \dot{p_k})$ is also a divisor of n.

It is also true that **any** combination(product) of the primes $p_1, ...p_k$ will also be a unique divisor of n.

We can think of the product of a unique combination of primes as a set, $A_n = p_1, p_2, p_3, ...p_k$

The power set of A_n is all possible combinations(products) of the primes.

The cardinality of a set with k elements is 2^k

Therefore for any given $n = p_1 * p_2 * ....p_k$, there are exactly 2^k divisors of n.

Problem 2: Alice's RSA public key is $P = (e, n) = (11, 65)$. Bob sends Alice the message by encoding it as follows. First he assigns numbers to characters: A is 2, B is 3, ..., Z is 27, and blank is 28. Then he uses RSA to encode each number separately.

Bob's encoded message is:

31	29	11	7	60	30
28	28	11	24	11	20
49	11	7	22	11	31
19	11	11	20	7	15
31	3	23	30	60	30
31	26	7	33	20	60
7	57	11	20	30	3
15	7	30	15	7	31
29	33	31	7	57	11
20	30	3	15	7	29
33	15	7	30	31	15
7	52	30	14	30	31
15					

Decode Bob's message. Notice that you don't have Bob's secrete key, so you need to "break" RSA to decrypt his message.

For the solution, give Bob's message in plaintext. (Also, who said it?) You also need to describe step by step how you arrived at the solution.

Suggestion: this can be solved by hand, but it could get tedious. It may be faster to write a short program.

Problem 2 Solution Knowns: $e = 11$ and $n = 65$. From this we can compute P and Q by factoring $n(65)$
Prime factorization of 65 gives $P = 5$ and $Q = 13$
Now that we have P and Q we can find φ
$\varphi = (5-1) * (13-1) = 12 * 4 = 48$. With this we can find d, Bob's secret key.
$d = e^{-1} \pmod{(\varphi)}$
$d = 35$
Now we can decrypt all of the number codes using the forumla, $M = C^d \pmod{n}$ where C is the encrypted number and M is the decrypted number.

I wrote a program that did this for me and then stored the result in a vector. I then ran another function on that vector that converted all of the numbers into letters according to Bob's assignment of numbers to characters.

The final decrypted message is, "THE DIFFERENCE BETWEEN STUPIDITY AND GENIUS IS THAT GENIUS HAS ITS LIMITS" -Albert Einstein

Problem 3: (a) Compute $8^{-1} \pmod{19}$ by enumerating multiples of the number and the modulus. Show your work.

(b) Compute $8^{-1} \pmod{19}$ using Fermat's theorem. Show your work.

(c) Compute $20^{-1} \pmod{31}$ by enumerating multiples of the number and the modulus. Show your work.

(d) Compute $20^{-1} \pmod{31}$ using Fermat's theorem. Show your work.

(e) Find an integer x, $0 \leq x \leq 36$, that satisfies $17x = 8 \pmod{37}$. Show your work.

Submission. To submit the homework, you need to upload the pdf file into ilearn by 8AM on Thursday, February 7, and turn-in a paper copy in class.