Cryptology 5

Ryan Kellar

March 2024

1 Problem 1

If E had a factor in common with $(p-1)(q-1)$, then we wouldn't be able to find a corresponding D that is also in $\mathbb{Z}_{(p-1)(q-1)}$, so we wouldn't be able to decode it.

2 Problem 2

D = 3 using the B6 magic provided by Mr. Bailey.

3 Problem 3

M mod pq	1	2	3	4	5	6	7	8	9	10	11	12	13	14
M^E mod pq	1	8	12	4	5	6	13	2	9	10	11	3	7	14
M^{ED} mod pq	1	2	3	4	5	6	7	8	9	10	11	12	13	14

4 Problem 4

M^{ED} will always be equal to M, which makes sense because if M is a number representing the message, then if we apply the encode and decode process, we will get the message back again.

5 Problem 5

$pq = 14,647$
$(p-1)(q-1) = 14,400$
We will solve this as a system of equations:
$pq - p - q + 1 = 14,400$
$pq - p - q = 14,399$
$14,647 - 14,399 = p + q$
$p + \frac{14,647}{p} = 248$
$p^2 - 248p + 14,647$
$p = 97$ or $p = 191$
q will be which ever value p does not take.

6 Problem 6

This is simply an application of Euler's Theorem to the RSA Cryptosystem. We have already defined $\phi(pq) = (p-1)(q-1)$, so by using Euler's Theorem of $a^{\phi(m)} \equiv 1 \bmod m$, we can say that $M^{(p-1)(q-1)} \equiv 1 \bmod pq$.

7 Problem 7

This is the same thing but with coefficients and exponents multiplying the $M^{(p-1)(q-1)}$. We can rewrite the formula $M^{1+k(p-1)(q-1)}$ as $M * (M^{(p-1)(q-1)})^k$. Since we are in mod pq, we can simplify this to $M * (1)^k$. Because it doesn't matter what k is, we can further simplify this into M, assuming we are still in mod pq.

8 Problem 8

$a \bmod b = c$
$ED \bmod b = c$
$a = kb + c$
$ED \bmod b = 1$
$a = kb + 1$
$b = (p-1)(q-1)$
$M^{1+kb} \bmod pq = M$
$M^{1+k(p-1)(q-1)} \bmod pq = M$ (We proved this in the last problem)