Cryptology Packet Ch 5.1

ID: 1747

March 2023

1. At this point, you should stop and do the Google Sheets activity, "Modular Inverses". Try to answer this question: Why must E be relatively prime to $(p-1)(q-1)$?

   From Packet: If E has factors in common with $(p-1)(q-1)$, then it will not have a multiplicative inverse in $\mathbb{Z}_{(p-1)(q-1)}$. That is, we wouldn't be able to find the corresponding decoding number, D.

2. Let $p = 3$ and let $q = 5$. Then $(p-1)(q-1) = 8$ and $pq = 15$. Suppose that we choose E to be 3. Find D. Remember that $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$.

   D is defined as the multiplicative inverse of E in $\mathbb{Z}_{(p-1)(q-1)}$. So if $E = 3$, then we can find the multiplicative inverse of E while being in $\mathbb{Z}_8$.
   $3 * D \equiv 1 \mod 8$
   $3 * 3 \equiv 1 \mod 8$
   Therefore, D will be 3.

3. Sticking with the same p, q, and E (and therefore the same D), complete the table below using the rules of $\mathbb{Z}_{15}$. Remember that you don't simplify exponents according to the rules of mod numbers: exponents are regular integers. What do you notice about the entries of the last row?

$M \mod pq$	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. At this point, you should stop and do the Google Sheets activity, "RSA Cryptosystem Crux Theorem". State a conjecture based on your observations from the activity

   From the google sheet activity, I found that $M \equiv M^{ED} \mod pq$ where M is a number in $\mathbb{Z}_{pq}$

5. Find the primes p and q if $pq = 14,647$ and $\phi(pq) = 14400$

   $\phi(pq) = \phi(p) * \phi(q) = (p-1)(q-1) = pq - q - p + 1$

$14400 = 14647 - q - p + 1$
$-248 = -q - p$
$p + q = 248$
$q = 248 - p$
$pq = 14647$
$p(248 - p) = 14647$
$248p - p^2 = 14647$
$p^2 - 248p + 14647 = 0$
$(p - 97)(p - 151) = 0$
$p = 97, 151$
$p = 97, q = 151$

6. Prove Theorem 5.2 based on what you have already learned (perhaps in a previous section).

   $M^{\phi(pq)} \equiv 1 \mod pq$(Euler's theorem)
   $\phi(pq) = \phi(p) * \phi(q) = (p - 1)(q - 1)$
   $M^{\phi(pq)} = M^{(p-1)(q-1)}$
   $M^{(p-1)(q-1)} \equiv 1 \mod pq$

7. Prove Theorem 5.3 based on what you have already learned.

   $M^{(p-1)(q-1)} \equiv 1 \mod pq$
   $M^{k(p-1)(q-1)} \equiv 1^k \mod pq$
   $M^{1+k(p-1)(q-1))} \equiv 1^k * M \mod pq$
   $M^{1+k(p-1)(q-1))} \equiv M \mod pq$

8. Prove Theorem 5.1 (RSA Cryptosystem Crux) based on what you have already learned.

   From theorem 5.4, $D * E \equiv 1 \mod (p - 1)(q - 1)$ which is also $D * E \equiv 1 + k(p - 1)(q - 1)$ where k is a positive integer.

   If M is a number in $\mathbb{Z}_{pq}$ then $M^{ED} = M^{1+k(p-1)(q-1)}$.

   From theorem 5.3, $M^{1+k(p-1)(q-1)} \equiv M \mod pq$ so $M^{ED} \equiv M \mod pq$