Cryptology Packet Ch 5.2

ID: 1747

April 2023

1. Suppose that Alice's secret message is the number $M = 2$. What number does she send Bob? Describe in your own words how you found this number.

   $M^E \mod 291$
   $2^5 \mod 291$
   $32 \mod 291$
   32

   Using the description from the problem, we know that Alice encodes her message by doing M^E and then modding it by 291 as the answer is to be computed in $\mathbb{Z}_{291}$. Therefore, we can use $M^E \mod 291$ to find the number that Alice sent to Bob, which is 32.

2. Suppose that Alice's secret message is the number $M = 150$. What number does she send Bob? If you try to do this directly, your calculator might overflow, but there is a way to avoid this problem (and these sorts of computational shortcuts are important in practical implementations of RSA). Describe how you found the number in your own words.

   $M^E \mod 291$
   $150^5 \mod 291$
   $150^2 * 150^2 * 150^1 \mod 291$
   $93 * 93 * 150 \mod 291$
   $1297350 \mod 291$
   72

   I followed the same encryption method as the previous problem but separated the 150^5 into $150^2 * 150^2 * 150^1$. Then, I found $150^2 \mod 291$ to be 93 and found that $93 * 93 * 150 \mod 291$ is 72.

3. Bob can now decode Alice's message:

   (a) Verify that 77 is indeed the multiplicative inverse of 5 in $\mathbb{Z}_{192}$. Explain in your own words how you know that you are correct.

$77 * 5 \mod 192$
$385 \mod 192$
$1 \mod 192$

First, we know that a multiplicative inverse for $5 \mod 192$ exists because they are relatively prime. Modulo multiplicative inverse of two numbers, x and y, will be $x * y \equiv 1 \mod m$. 77 is the multiplicative inverse of 5 because we get $1 \mod 192$ when we do $77 * 5 \mod 192$.

(b) Using the RSA Cryptosystem Crux Theorem, explain how Bob can use the number D to decode Alice's encoded message M^E and recover her original message M.

$M^{E^D} \equiv M \mod pq$

Therefore, Bob can decode Alice's encoded message M^E and recover her message M by finding $M^{E^D} \mod pq$.

For example, using $M = 2$, $E = 5$, $D = 77$, $pq = 291$, $(p-1)(q-1) = 192$
$M^{E^D} \equiv M \mod pq$
$2^{5^{77}} \mod pq$
$2^{5^{77}} \mod 291$
$2^{5*77} \mod 291$
$2^{385} \mod 291$
$2^1 * 2^{384} \mod 291$
$2^1 * 2^{192*2} \mod 291$
$2^{1+2(192)} \mod 291$
$2 \mod 291$ (Using theorem 5.3)