Cryptology 5.2

Ryan Kellar

April 2024

1 Problem 1

To find the product of $(p-1)(q-1)$, we need to find two prime numbers p and q which multiply to get 21.
The only combination of prime numbers which satisfy this condition is $p = 7$ and $q = 3$ (or $p = 3$ and $q = 7$, but the order/configuration of these numbers does not matter).
Then, we know that the product of $(p-1)(q-1) = 6 * 2 = 12$.
Next, to find the decoding number, D, we need to find the modular inverse of the encoding number, $E = 5(in) \mod \mathbb{Z}_{(p-1)(q-1)} = \mathbb{Z}_{18}$, which is 5 since $(5 * 5) mod \mathbb{Z}_{12} = 25 mod \mathbb{Z}_{12} = 1$.
This means that our decoding number $D = 5$.

2 Problem 2

$p = 29$
$q = 53$
$570^{31} \mod (28 * 52)$
$570^{31} \mod (1537)$
$P = 131$

3 Problem 3

As long as the public key isn't shared then it's impossible to decode the message being sent because you don't know what the number is being modulated in so there is essentially infinitely many possibilities.

4 Problem 4

If just some of the data is published/leaked to someone potentially trying to decrypt the message then it's pretty easy to decrypt the message.