Abel Marin

Prof Joe

Cryptology

May 31, 2020

Assignment 4

1. Problem 1
   1. Greatest common denominator for 26 and 7 is 1. We need to find (7)-1 mod 26 or 7d = 1mod26. 1 = 15(7)mod26. 7d = 1 mod 26 or 7(15) = 1 mod 26 Thus the multiplicative inverse is 15.
   2. Greatest common denominator for 19 and 999 is 1. We need to find (19)-1 mod 999 or 19d = 1mod999. 1 = 631(19)mod999. 19d = 1 mod 999 or 19(631) = 1 mod 999 Thus the multiplicative inverse is 631.
2. Problem 2
   1. φ(p) = (p1−p0) =p−1
   2. φ(p\*q) = (p-1) \* (q-1)
3. Problem 3
   1. e = 3 and y = 26
   2. d = 27 and y = 14
4. Problem 4
   1. Encryption formula: y = xe mod n. We can’t solve the equation because xe is a part of a finite integer ring. There are no efficient algorithms for computing the roots.
   2. The formula is φ(n) = p\*q. We can’t use this formula because we do not know p and
   3. The results of the factoring: q = 61 and p = 43. Φ(n) = 42 · 60 = 2520. d ≡ e^{-1} mod 2520 ≡ 191. Thus x = 1088. For larger number of length 1024 bits or more this process would become very time consuming since the complexity is exponential. Thus this would not be suitable for these larger numbers.