MATH-3420 - Assignment 4 - Jonathon Meney - 348074

Jonathon Meney

November 2023

1. You need to decrypt a lengthy cipher text that was sent using an encryption function of the form $E(\alpha) = a\alpha + b \bmod 26$. You know that the letters were converted to numbers as follows: $A \leftrightarrow 0$, $B \leftrightarrow 1, \ldots, Z \leftrightarrow 25$, and that the encryption was done one letter at a time. The problem is that you know neither a nor b.

   You have analyzed the cipher text and observed that the most frequently occurring letter in the cipher text is X and the second most frequently used is U. Since the most frequently used English letters are E and T, in that order, you are going to assume that E has been encrypted as X and T has been encrypted as U.

   (a) Find a and b.

   Since $E = 4$ encrypts to $X = 23$, and $T = 19$ encrypts as $U = 20$ we know:

$$\begin{aligned} 19a + b &\equiv 20 \pmod{26} \\ 4a + b &\equiv 23 \pmod{26} \end{aligned}$$

   Thus subtracting the second equation from the first we get:

$$\begin{aligned} 15a &\equiv -3 \pmod{26} \\ 15a &\equiv 75 \pmod{26} \\ a &\equiv 5 \pmod{26} \end{aligned}$$

   Substituting a back into equation the second equation we get:

$$\begin{aligned} 4a + b &\equiv 23 \pmod{26} \\ 4(5) + b &\equiv 23 \pmod{26} \\ b &\equiv 3 \pmod{26} \end{aligned}$$

   Therefor $a = 5$ and $b = 3$

(b) Find the decryption function $D(\alpha)$.

First we need to find the inverse of a:

$$\begin{aligned} 5x &\equiv 1 \pmod{26} \\ 5x &\equiv 105 \pmod{26} \\ x &\equiv 21 \pmod{26} \end{aligned}$$

Therefore $D(\alpha)$ is:

$$\begin{aligned} D(\alpha) &= a^{-1}(\alpha - b) \bmod 26 \\ D(\alpha) &= 21(\alpha - 3) \bmod 26 \end{aligned}$$

(c) Find the plaintext for the intercepted message HV QVJ.

The ciphertext HV QVJ represented by numerical values is 7,21,16,21,9. Decrypting these values results in 6,14,13,14,22 which results in the plaintext GO NOW.

2. Consider the encryption function $E(x) = x^3 \bmod 2419$. Note that $2419 = 41 \cdot 59$.

   (a) Find the decryption function $D(x)$.
   Firstly, note that:

$$\begin{aligned} \phi(2419) &= \phi(41)\phi(59) \\ &= 40(58) \\ &= 2320 \end{aligned}$$

   We need to find f such that:

$$x^{3f} \equiv x \pmod{2419}$$

   Equivalently:

$$\begin{aligned} 3f &\equiv 1 \pmod{\phi(2419)} \\ 3f &\equiv 1 \pmod{2320} \end{aligned}$$

   Using the euclidean algorithm on $3f + 2320y = 1$ we see:

$$\begin{aligned} 2320 &= 3(773) + 1 \\ 1 &= 2320 + 3(-773) \end{aligned}$$

   Therefore $f = -773 \equiv 1547 \pmod{2320}$. Thus $D(x)$ is:

$$\begin{aligned} D(x) &= x^f \bmod 2419 \\ D(x) &= x^{1547} \bmod 2419 \end{aligned}$$

   (b) Suppose you receive an encrypted number that is 100 digits long. You know that the function $E(x) = x^{13} \bmod 2419$ was used to encrypt the message. How would you go about decrypting the message to find the original 75-digit-long number that was encrypted?

   Since the modulus of encryption is 4 digits we will group the ciphertext into groups of 4 digits that will decrypt into groups of 3 digits, thus decrypting the 100 digit message to 75 digits.

3. Using the fact that 7 is a primitive root of 22, find all integers x such that $5^{11x} \equiv 9 \pmod{22}$.

   Since 7 is a primitive root of 22, 5 and 9 can be written as powers of 7 modulus 22:

$$\begin{aligned} 5 &\equiv 7^2 \pmod{22} \\ 9 &\equiv 7^8 \pmod{22} \end{aligned}$$

   Therefore:

$$\begin{aligned} 5^{11x} &\equiv 9 \pmod{22} \\ (7^2)^{11x} &\equiv 7^8 \pmod{22} \end{aligned}$$

   Also note:

$$\begin{aligned} \phi(22) &= \phi(2)\phi(11) \\ &= 1(10) \\ &= 10 \end{aligned}$$

   Thus:

$$\begin{aligned} 22x &\equiv 8 \pmod{\phi(22)} \\ 22x &\equiv 8 \pmod{10} \\ 22x &\equiv 88 \pmod{10} \\ x &\equiv 4 \pmod{5} \\ x &\equiv 4, 9 \pmod{10} \end{aligned}$$

4. Given that 8 has order 12 modulo 37, find all positive integers less than 37 that that have order 12 modulo 37.

   Since 8 has order 12 modulo 37, we know that 8^h has order $\frac{12}{\gcd(h,12)}$. So, 8^h has order 12 when $\gcd(h, 12) = 1$. Therefore since $0 < h \leq 36$ $h = 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35$.

   Also note that $\phi(12) = \phi(2^2)\phi(3) = 2(2) = 4$, therefore there is 4 positive integers less than 37 that that have order 12 modulo 37.

   Taking $h = 1, 5, 7, 11$ we get:

$$\begin{aligned} 8^1 &= 8 \\ 8^5 &= 23 \\ 8^7 &= 29 \\ 8^{11} &= 14 \end{aligned}$$

   Therefore 8, 23, 29, 14 all have order 12 modulo 37. Taking other valid values of h will result in one the above 4 values above, and we know that since $\phi(12) = 4$ we will only have 4 solutions.