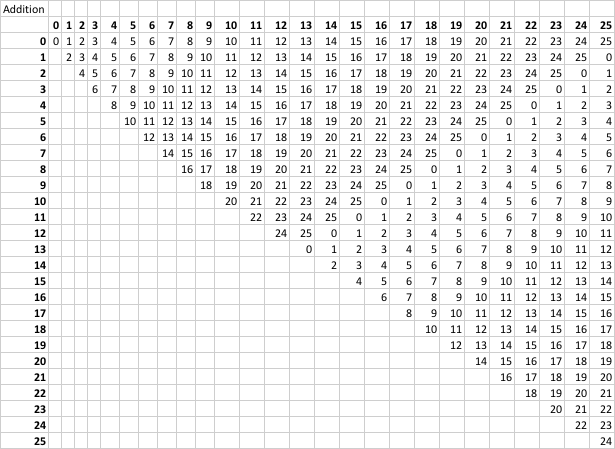
Michael Esposito

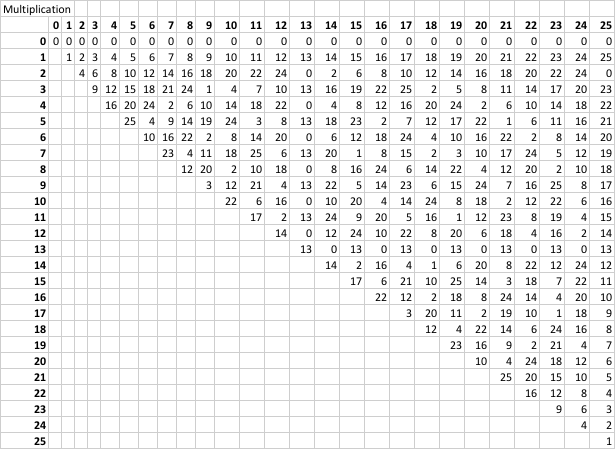
Cryptography

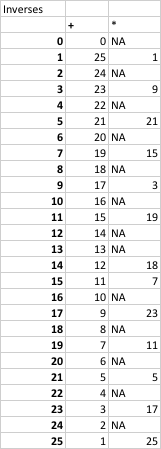
Professor Nelson

Homework 1

1. **(15 points) Write the addition and multiplication tables for** *Z26*, **and find the additive and multiplicative inverses for the elements when they exist.**

****

****

****

1. **(20 points) Decrypt the following substitution cipher. Show all work, including the frequency table and substitution assignments for the letters required to solve the cipher.**

**VLG CJMAFVCJXVG VLUJR XIACV VLUD QAFTP UD VLXV RAAP LXIUVD XFG**

**DA OCYL GXDUGF VA RUZG CW VLXJ IXP AJGD.**

**-Q. DAOGFDGV OXCRLXO**

THE UNFORCTUNATE THING ABOUT THIS WORLD IS THAT GOOD HABITS ARE SO MUCH EASIER TO GIVE UP THAN BAD ONES W SOMERSET MAUGHAM

My reasoning:

1. First, I noticed that VLG was a single word, and the bigram VL occurred many times. I started with the substitution VLG->THE

2. The previous substitution implied that VLXV might either be THAT or THAN

3. The word VA had to be a word on its own that started with the letter T. The second letter had to be a vowel. Out of A, E, I, O, and U, only A E and O make sense. A and E are already defined, therefore I substituted A->O

4. I looked at the two letter word CW. It couldn’t contain any of the letter assigned already. I took a guess that it meant UP, which was a lucky but helpful guess.

5. Some words were almost all filled in. CJMAFVCJXVG looked like UNFORTUNATE, so assigned the rest of the letters in that word.

6. A\_OUT looked like ABOUT, so I->B

7. EA\_\_IER -> EASIER

8. SO\_ERSET->SOMERSET

9. rOOp->GOOD

10. MUyH->MUCH

11. GIzE->GIVE

12. At this point, the only letters I hadn’t used were J, K, L, Q, W, X, and Z. This made me realize that qORtD -> WORLD

14. The final key: O\*US\*RE\*BN\*HF\*MDWG\*LITPACV

1. **Encrypt the message below in three (3) ways:**
   1. **(15 points) Permutation Cipher with**
   2. **(15 points) Affine Cipher with K = (7, 4)**
   3. **(15 points) Vigenere Cipher with K = USETHISKEY**

***“LOVE IS THE ONLY MEDICINE FOR A BROKEN HEART”***

a. Permutation Cipher with π = (2 5 1 4 6 3)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| L | O | V | E | I | S | T | H | E | O | N | L | Y | M | E | D | I | C |
| 2 | 5 | 1 | 4 | 6 | 3 | 2 | 5 | 1 | 4 | 6 | 3 | 2 | 5 | 1 | 4 | 6 | 3 |
| **V** | **L** | **S** | **E** | **O** | **I** | **E** | **T** | **L** | **O** | **H** | **N** | **E** | **Y** | **C** | **D** | **M** | **I** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| I | N | E | F | O | R | A | B | R | O | K | E | N | H | E | A | R | T |
| 2 | 5 | 1 | 4 | 6 | 3 | 2 | 5 | 1 | 4 | 6 | 3 | 2 | 5 | 1 | 4 | 6 | 3 |
| **E** | **I** | **R** | **F** | **N** | **O** | **R** | **A** | **E** | **O** | **B** | **K** | **E** | **N** | **T** | **A** | **H** | **R** |

b. Affine Cipher

Ciphertext = (7x + 4) mod 26

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| L | O | V | E | I | S | T | H | E | O | N | L | Y | M | E | D | I | C |
| 11 | 14 | 20 | 4 | 8 | 18 | 19 | 7 | 4 | 14 | 13 | 11 | 24 | 12 | 4 | 3 | 8 | 2 |
| 3 | 24 | 21 | 6 | 8 | 0 | 7 | 1 | 6 | 24 | 17 | 3 | 16 | 10 | 6 | 25 | 8 | 18 |
| **D** | **Y** | **V** | **G** | **I** | **A** | **H** | **B** | **G** | **Y** | **R** | **D** | **Q** | **K** | **G** | **Z** | **I** | **S** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| I | N | E | F | O | R | A | B | R | O | K | E | N | H | E | A | R | T |
| 8 | 13 | 4 | 5 | 14 | 17 | 0 | 1 | 17 | 14 | 10 | 4 | 13 | 7 | 4 | 0 | 17 | 19 |
| 8 | 17 | 6 | 13 | 24 | 19 | 4 | 11 | 19 | 24 | 22 | 6 | 17 | 1 | 6 | 4 | 19 | 7 |
| **I** | **R** | **G** | **N** | **Y** | **T** | **E** | **L** | **T** | **Y** | **W** | **G** | **R** | **B** | **G** | **E** | **T** | **H** |

c. Vigenere Cipher

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| L | O | V | E | I | S | T | H | E | O | N | L | Y | M | E | D | I | C |
| 11 | 14 | 20 | 4 | 8 | 18 | 19 | 7 | 4 | 14 | 13 | 11 | 24 | 12 | 4 | 3 | 8 | 2 |
| 5 | 6 | 25 | 23 | 15 | 0 | 11 | 17 | 8 | 12 | 7 | 3 | 2 | 5 | 11 | 11 | 0 | 12 |
| **F** | **G** | **Z** | **X** | **P** | **A** | **L** | **R** | **I** | **M** | **H** | **D** | **C** | **F** | **L** | **L** | **A** | **M** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| I | N | E | F | O | R | A | B | R | O | K | E | N | H | E | A | R | T |
| 8 | 13 | 4 | 5 | 14 | 17 | 0 | 1 | 17 | 14 | 10 | 4 | 13 | 7 | 4 | 0 | 17 | 19 |
| 12 | 11 | 24 | 23 | 18 | 10 | 7 | 9 | 9 | 24 | 14 | 2 | 7 | 25 | 8 | 19 | 24 | 1 |
| **M** | **L** | **Y** | **X** | **S** | **K** | **H** | **J** | **J** | **Y** | **O** | **C** | **H** | **Z** | **I** | **T** | **Y** | **B** |

1. **(20 points) Decrypt the following Affine Cipher, showing all work to find the key (a, b) with b = 8.**

**A F Q N X I V I D Q O C O E B X T S I B B C V S A C N T S F A I V R S W G C X S C V X S F S O X C V K**

After a considerable amount of time attempting to try various different substitutions, because that’s what an affine cipher ultimately ends up being, I decided to focus on the double letter B. In the ciphertext, there is a BB followed by a C. I figured that B was a consonant, therefore C would have to be a vowel. A frequency analysis showed that C had the highest frequency of occurrence in the ciphertext, so I began my decryption based on the assumption that an E in the plaintext produced a C in the ciphertext. Given that we know b in the ciphertext must be 8, and the encryption formula is now , I needed to see what vales for A produced 2 (equivalent to C). I wrote a short Python script to do this, shown below:

for a in range (0,26):

y = mod(4\*a+8, 26)

print "a= ", a, " y= ", y

None of the outputted A values made any sense when transformed into a key and applied to the ciphertext. Therefore, I backtracked and applied the same logic, except assuming that I in the plaintext produced a C in the plaintext. I was still pretty sure that this C had to be a vowel, and I was my next choice. I then ran this Python script:

for a in range (0,26):

y = mod(8\*a+8, 26)

print "a= ", a, " y= ", y

and discovered that y was equal to 2 when a was either 9 or 22. This meant that the Affine cipher used was either or . I started decrypting the ciphertext using the key (9, 22). This meant I could perform the following substitutions:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M |
| I | V | A | J | S | B | K | T | C | L | U | D | M |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| V | E | N | W | F | O | X | G | P | Y | H | Q | Z |

The above substitution produced this plaintext:

CRYPTANALYSIS OF THE AFFINE CIPHER CAN BE QUITE INTERESTING