Evan Smith

CIS 628

Section M400

HW 3

Problems from Chapter 1

**Problem 1.1**

1. Letter frequency in the text is shown in this table:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| r | b | m | k | j | w | i | p | u | d | h | v | x | y | n | s | t | l | q | o | e | a | c | f | g | r |
| 84 | 68 | 62 | 49 | 48 | 47 | 41 | 30 | 24 | 23 | 23 | 22 | 20 | 19 | 17 | 17 | 13 | 8 | 7 | 7 | 5 | 5 | 5 | 1 | 1 | 84 |

1. The decrypted text is:

*because the practice of the basic movements of kata is the focus and mastery of self is the essence of matsubayashi ryu karate do i shall try to elucidate the movements of the kata according to my interpretation based on forty years of study it is not an easy task to explain each movement and its significance and some must remain unexplained to give a complete explanation one would have to be qualified and inspired to such an extent that he could reach the state of enlightened mind capable of recognizing soundless sound and shapeless shape i do not deem myself the final authority but my experience with kata has left no doubt that the following is the proper application and interpretation i offer my theories in the hope that the essence of okinawan karate will remain intact*

1. This text is by Shoshin Nagamine in the book *Essence of of Okinawan Karate-Do*

**Problem 1.2**

1. Once one letter is found using the frequency analysis, the rest of the cypher is trivial, because the shift is consistent over the whole cypher. The cleartext is *IF WE ALL UNITE WE WILL CAUSE THE RIVERS TO STAIN THE GREAT WATERS WITH THEIR BLOOD*
2. It was written by Chief Tecumseh.

**Problem 1.4**

1. The size of the key space would be 8\*128 = 1024 characters.
2. The key length in bits would be 8\*7 = 56 bits
3. Using only 26 characters, we would need to use log(26) = 4.7, rounded up to 5 bits per character. The key length is then 8\*5 = 40 bits
4. The minimum characters for a password to be 128bits given different character lengths:
   1. 7-bit : 128/7 = 18.29, rounded to 19 characters.
   2. 5-bit: 128/5 = 25.6. rounded to 26 characters.

**Problem 1.5**

1. 15\*29 = 435 mod 13 ≡ 6
2. 2\*29 = 58 mod 13 ≡ 6
3. 2\*3 = 6 mod 13 ≡ 6
4. -11\*3 = -33 mod 13 ≡ 6

We see that all these calculations are the same in mod 13!

**Problem 1.6**

1. 1/5 mod 13 ≡ 0.2
2. 1/5 mod 7 ≡ 0.2
3. 3\*2/5 = 6/5 mod 7 ≡ 1.2

**Problem 1.7**

1. Multiplication Table for Z4:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **X** | **0** | **1** | **2** | **3** |
| **0** | 0 | 0 | 0 | 0 |
| **1** | 0 | 1 | 2 | 3 |
| **2** | 0 | 2 | 0 | 2 |
| **3** | 0 | 3 | 2 | 1 |

1. Addition Table for Z5:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **X** | **0** | **1** | **2** | **3** | **4** |
| **0** | 0 | 1 | 2 | 3 | 4 |
| **1** | 1 | 2 | 3 | 4 | 0 |
| **2** | 2 | 3 | 4 | 0 | 1 |
| **3** | 3 | 4 | 0 | 1 | 2 |
| **4** | 4 | 0 | 1 | 2 | 3 |

Multiplication Table for Z5:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **X** | **0** | **1** | **2** | **3** | **4** |
| **0** | 0 | 0 | 0 | 0 | 0 |
| **1** | 0 | 1 | 2 | 3 | 4 |
| **2** | 0 | 2 | 4 | 1 | 3 |
| **3** | 0 | 3 | 1 | 4 | 2 |
| **4** | 0 | 4 | 3 | 2 | 1 |

1. Addition Table for Z6:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **X** | **0** | **1** | **2** | **3** | **4** | **5** |
| **0** | 0 | 1 | 2 | 3 | 4 | 5 |
| **1** | 1 | 2 | 3 | 4 | 5 | 0 |
| **2** | 2 | 3 | 4 | 5 | 0 | 1 |
| **3** | 3 | 4 | 5 | 0 | 1 | 2 |
| **4** | 4 | 5 | 0 | 1 | 2 | 3 |
| **5** | 5 | 0 | 1 | 2 | 3 | 4 |

Multiplication Table for Z6:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **X** | **0** | **1** | **2** | **3** | **4** | **5** |
| **0** | 0 | 0 | 0 | 0 | 0 | 0 |
| **1** | 0 | 1 | 2 | 3 | 4 | 5 |
| **2** | 0 | 2 | 4 | 0 | 2 | 4 |
| **3** | 0 | 3 | 0 | 3 | 0 | 3 |
| **4** | 0 | 4 | 2 | 0 | 4 | 2 |
| **5** | 0 | 5 | 4 | 3 | 2 | 1 |

1. The elements in Z4 without a multiplicative inverse are 0 and 2. In Z6 they are 0, 2, 3, and 4. A multiplicative inverse exists for all elements in Z5 because 5 is prime.

**Problem 1.8**

1. The multiplicative inverse of 5 in:
   1. Z11 = 9 (5\*9 = 45 mod 11 ≡ 1)
   2. Z12 = 5 (5\*5 = 25 mod 12 ≡ 1)
   3. Z13 = 8 (5\*8 = 40 mod 13 ≡ 1)

**Problem 1.9**

1. 3^2 mod 13 = 9 mod 13 ≡ 9
2. 7^2 mod 13 = 49 mod 13 ≡ 10
3. 3^10 mod 13 = 3^2 \* 3^2 \*3^2 mod 13 = 9 \* 9 \* 9 mod 13 = 81\*9 mod 13 = 3\*9 mod 13 = 18 mod 13 ≡ 5
4. 7^100 mod 13 = 7^2 \* 7^2 \*… mod 13 = 10\*10… mod 13 = 10^50 mod 13 = 10^2\*10^2… mod 13 = 9\*9… mod 13 = 9^25 mod 13 = 9\*9^2\*9^2… mod 13 = 9\*3\*3… mod 13 = 3^2\*3^12 mod 13 = 3^14 mod 13 = 3^3\*3^3\*3^2 mod 13 = 1\*1\*9 mod 13 ≡ 9
5. Not sure how to approach this one!

**Problem 1.11**

1. The decrypted text is *first the sentence and then the evidence said the queen*
2. Lewis Carroll wrote this quote.

**Problem 1.12**

1. The encryption equation for this cipher is ek(x) = y ≡ a\*x +b mod 30, and the decryption equation is dk(y) = x ≡ a^-1 (y-b) mod 30
2. Since there are only 8 coprime values less than 30 (1,7,11,13,17,19,23,29), the key space for this cypher is 8\*30 = 240.
3. 23\*(26-1) mod 30 = 23\*25 = 575 mod 30 ≡ 5 (‘F’),

23\*(20-1) mod 30 = 23\*19 = 437 mod 30 ≡ 17 (‘R’),

23\*(29-1) mod 30 = 23\*28 = 644 mod 30 ≡ 14 (‘O’),

23\*(22-1) mod 30 = 23\*21 = 483 mod 30 ≡ 3 (‘D’)

The plaintext is *FRODO*, and he comes from the village of Hobbiton!