CS 4801: Assignment 1

Adam Camilli (aocamilli@wpi.edu)

Wednesday 7th November, 2018

1. The ciphertext was encrypted using a substitution cipher. The objective is to decrypt the ciphertext without knowledge of the key.

   (a) Provide the relative frequency of all letters [A-Z] in the ciphertext

Letter	**Appearances**	**Relative Frequency**
C	150	13.93%
B	100	9.29%
D	86	7.99%
G	83	7.71%
F	76	7.06%
A	75	6.96%
I	70	6.5%
E	58	5.39%
L	50	4.64%
K	47	4.36%
H	45	4.18%
J	40	3.71%
M	37	3.44%
S	24	2.23%
N	24	2.23%
Q	23	2.14%
O	19	1.76%
P	19	1.76%
U	15	1.39%
R	15	1.39%
V	9	0.84%
T	9	0.84%
Y	3	0.28%
W	0	0.0%
X	0	0.0%
Z	0	0.0%

(b) Decrypt the ciphertext with help of the relative letter frequency of the English language (e.g., search Wikipedia for letter frequency analysis). Note that the text is relatively short and might not completely fulfill the given frequencies from the table.

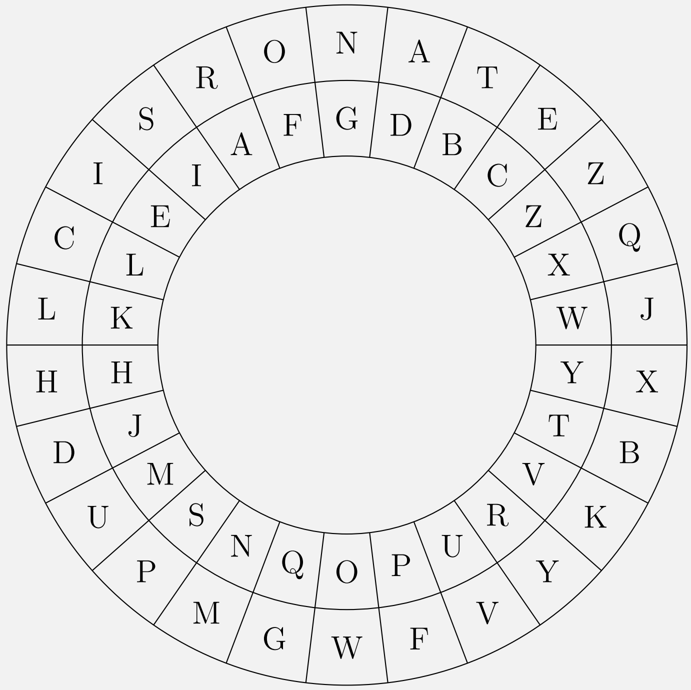
> By comparing the letter frequencies in the above table to those of the English language, and then some of the most common bigrams and trigrams within the text to common English words such as “THE”, “BE”, “AND”, “IN”, etc., I was able to decrypt the ciphertext::

(c) Find the key and provide letter frequency for the given text.

> The letter frequency of the resulting plaintext is:

Letter	**Appearances**	**Relative Frequency**
E	150	13.93%
T	100	9.29%
A	86	7.99%
N	83	7.71%
O	76	7.06%
R	75	6.96%
S	70	6.5%
I	58	5.39%
C	50	4.64%
L	47	4.36%
H	45	4.18%
D	40	3.71%
U	37	3.44%
P	24	2.23%
M	24	2.23%
G	23	2.14%
W	19	1.76%
F	19	1.76%
V	15	1.39%
Y	15	1.39%
K	9	0.84%
B	9	0.84%
X	3	0.28%
J	0	0.0%
Q	0	0.0%
Z	0	0.0%

and the key is:



2. Modular arithmetic is the basis of many cryptosystems. As a consequence, we will address this topic with several problems in this and upcoming chapters.

   (a) Compute the results:

      i. $27 \cdot 13 \bmod 23$

      $$27 \cdot 13 \equiv 351 \bmod 23$$
      $$= \mathbf{6} \qquad \left(351 - 23 \cdot \left\lfloor \frac{351}{23} \right\rfloor = 6\right)$$

      ii. $17 \cdot 13 \bmod 23$

      $$17 \cdot 13 \equiv 221 \bmod 23$$
      $$= \mathbf{14} \qquad \left(221 - 23 \cdot \left\lfloor \frac{221}{23} \right\rfloor = 14\right)$$

iii. $28 \cdot 15 \bmod 12$

$$\begin{aligned} 28 \cdot 15 &\equiv 420 \bmod 12 \\ &= \mathbf{0} && (12 \cdot 35 = 420) \end{aligned}$$

iv. $15 \cdot 29 + 11 \cdot 15 \bmod 23$

$$\begin{aligned} &15 \cdot 29 + 11 \cdot 15 \bmod 23 \\ &\qquad = 40 \cdot 15 \bmod 23 \\ &\qquad \equiv 600 \bmod 23 \\ &\qquad = \mathbf{2} && \left(600 - 26 \cdot \left\lfloor \frac{600}{23} \right\rfloor = 2\right) \end{aligned}$$

(b) Find the inverses in the given modular spaces:

i. $4^{-1} \bmod 17$

$$\begin{aligned} &\texttt{gcd}(4, 17) = 1 && \text{(Solution exists)} \\ &4 \bmod 17 = 4 && (17 \cdot 0 + 4 = 4) \\ &4 \cdot 0 \equiv 0 \pmod{17} \\ &\ldots && \text{(Run Euclid's algorithm)} \\ &4 \cdot 13 \equiv 68 \pmod{17} \equiv 1 \pmod{17} \\ &4 \cdot 13 = 1 + 17 \cdot 3 && \text{Modular inverse is } \mathbf{13} \end{aligned}$$

ii. $5^{-1} \bmod 37$

$$\begin{aligned} &\texttt{gcd}(5, 37) = 1 && \text{(Solution exists)} \\ &5 \bmod 37 = 5 && (37 \cdot 0 + 5 = 5) \\ &5 \cdot 0 \equiv 0 \pmod{37} \\ &\ldots && \text{(Run Euclid's algorithm)} \\ &5 \cdot 15 \equiv 75 \pmod{37} \equiv 1 \pmod{37} \\ &5 \cdot 15 = 1 + 37 \cdot 2 && \text{Modular inverse is } \mathbf{15} \end{aligned}$$

iii. $7^{-1} \bmod 17$

$\texttt{gcd}(7, 17) = 1$ (Solution exists)

$7 \bmod 17 = 7$ $(17 \cdot 0 + 7 = 7)$

$7 \cdot 0 \equiv 0 \mod 17$

$\ldots$ (Run Euclid's algorithm)

$7 \cdot 5 \equiv 35 \pmod{17} \equiv 1 \pmod{17}$

$7 \cdot 5 = 1 + 17 \cdot 2$ Modular inverse is **5**

iv. $10^{-1} \bmod 15$

$\texttt{gcd}(10, 15) = 5$ **(Solution does not exist)**

3. List all elements of modulo 36 with no multiplicative inverse.

The elements of a modulo n are defined as

$$\bmod n \equiv \mathbb{Z}_n = \{0, 1, \ldots, n-1\}$$

By the existence property of the modular multiplicative inverse,

$$\exists\ a^{-1} \mid aa^{-1} \equiv 1 \pmod{n} \iff a \perp n$$

i.e. an element a of modulo n will have a multiplicative inverse mod n if and only if it is coprime to n.

Since zero has no real reciprocals, it and any element of $\mathbb{Z}_{36}$ which shares a non-trivial factor with 36 should be listed. We can take the prime factorization of 36

$$36 = 2^2 \cdot 3^2$$

and simply list all elements of $\mathbb{Z}_{36}$ which share one of these factors:

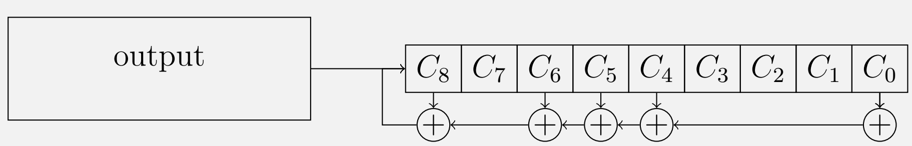
$$\begin{aligned} \{\} &: \{0\} \\ \{2\} &: \{2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34\} \\ \{3\} &: \{3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33\} \end{aligned}$$

$$\mathbf{\{0, 2, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18,}$$
$$\mathbf{20, 21, 22, 24, 26, 27, 28, 30, 32, 33, 34\}}$$

4. An LFSR is given by

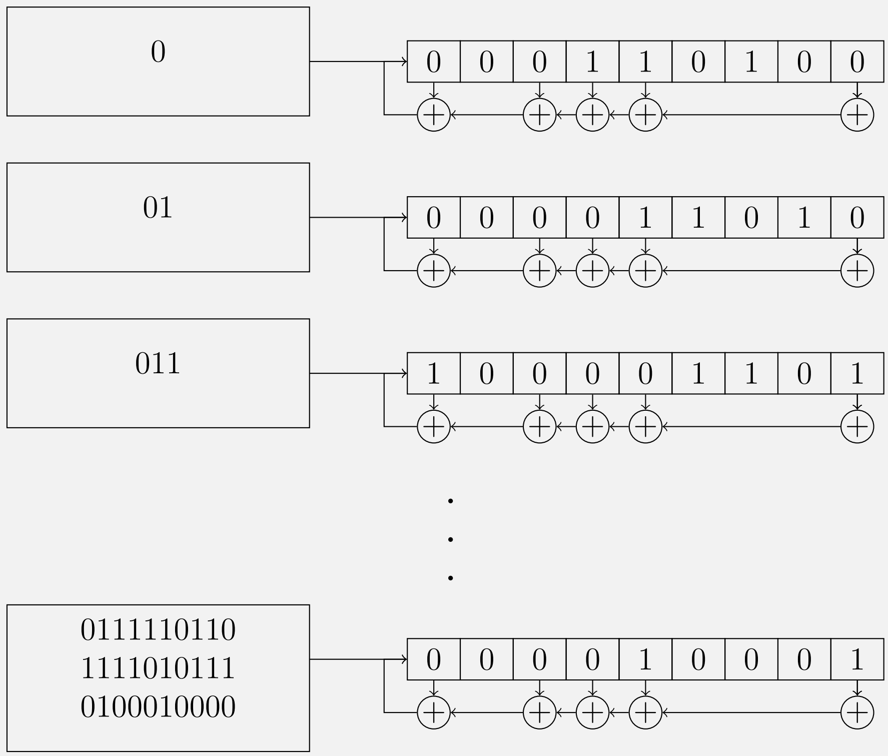
$$(9, (C_0, C_1, \ldots, C_8), (Z_0, Z_1, \ldots, Z_8)) = (9, x^8 + x^6 + x^5 + x^4 + 1, (0, 0, 0, 1, 1, 0, 1, 0, 0)).*$$

(a) Draw a circuit diagram for the given LFSR.



(b) Compute first 30 bits of the output bit stream

The output bit at each run can be simplified: Since XOR-gates are the function in use for this LFSR, one can determine the output of a given input by counting the odd bits that have on gates. An odd number means an output of 1, and an even number an output of 0.



(c) Use Vernam Cipher to encrypt the following plaintext using the bit stream generated in part b. P='111011000001101110110100111110'

111011000001101110110100111110

$\oplus$

011111011011110101110100010000

100100011010011011000000101110

100100011010011011000000101110