Andrew Robbertz alrobbertz@wpi.edu
CS 4801 Cryptography
November 7, 2018

Assignment 1

1. Substitution Cipher
    a. Cipher Text Letter Frequency

'C'	0.116913484
'B'	0.077942323
'D'	0.067030398
'G'	0.064692128
'F'	0.059236165
'A'	0.058456742
'I'	0.054559626
'E'	0.045206547
'L'	0.038971161
'K'	0.036632892
'H'	0.035074045
'J'	0.031176929
'M'	0.028838659
'N'	0.018706157
'S'	0.018706157
'Q'	0.017926734
'O'	0.014809041
'P'	0.014809041
'R'	0.011691348
'U'	0.011691348
'T'	0.007014809
'V'	0.007014809
'Y'	0.00233827
'W'	0
'X'	0
'Z'	0

b. Message Text

ELECTRICAL AND COMPUTER ENGINEERS DEVELOP AND CREATE PRODUCTS THAT CHANGE THE WORLD AND MAKE OUR LIVES EASIER THE CELL PHONES WE DEPEND ON THE COMPUTERS USED IN NATIONAL SECURITY AND THE ELECTRICAL SYSTEMS THAT MAKE OUR CARS OPERATE WERE ALL CREATED BY ELECTRICAL AND COMPUTER ENGINEERS AT WPI WE KEEP THAT PROGRESS MOVING FORWARD WITH OUR INNOVATIVE RESEARCH AND OUT-OF-THE BOX APPROACHES THE DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERINGAT WPI CHALLENGES STUDENTS TO PUSH THEMSELVES TO UNDERSTAND SOCIETYS AND TECHNOLOGYS COMPLEX ISSUES IN A BROADER CONTEXT THAN WHATS IN FRONT OF THEM WE WANT OUR STUDENTS WHETHER THEY ARE EARNING AN UNDERGRADUATE MINOR OR A DOCTORATE TO TACKLE SOCIETYS MOST PRESSING PROBLEMS AND UNCOVER NEW WAYS OF SOLVING THEM WHETHER ITS DEVELOPING SYSTEMS THAT CAN LOCATE FIREFIGHTERS IN THE MIDDLE OF A BURNING BUILDING OR CREATING NEUROPROSTHETICS THAT LOOK AND FUNCTION LIKE NATURAL LIMBS OUR FACULTY AND STUDENTS ARE AT THE FRONT EDGE OF REMARKABLE INNOVATION WHILE ADVANCING TECHNOLOGIES IS AT OUR CORE WE ALSO TAKE HUMAN CONNECTIONS VERY SERIOUSLY IN ECE WE PRIDE OURSELVES ON THE FAMILY-LIKE ATMOSPHERE WE CULTIVATE; FACULTY STUDENTS AND STAFF ENCOURAGE EACH OTHERS EVERY SUCCESS AND ARE THERE FOR THE CHALLENGES BOTH IN THE CLASSROOM AND IN LIFE

c. Mapping

Within the dictionary, the first character is the cipher text value, and the second character is the message text value. For example, an ‘A’ in the cipher text maps to a ‘R’ in the message text.

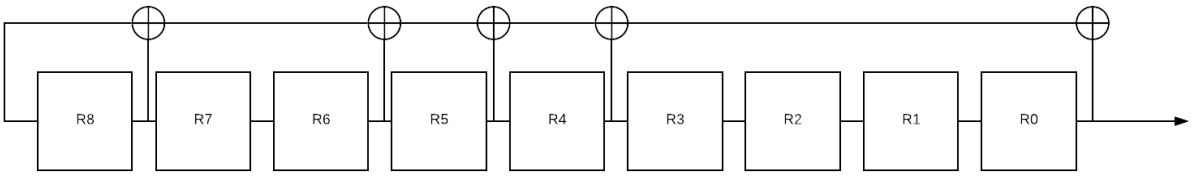
mapping = {'A': 'R','C': 'E','B': 'T','E': 'I','D': 'A','G': 'N','F': 'O','I': 'S','H': 'H','K': 'L','J': 'D','M': 'U','L': 'C','O': 'W','N': 'M','Q': 'G','P': 'F','S': 'P','R': 'Y','U': 'V','T': 'B','W': 'J','V': 'K','Y': 'X','X': 'Q','Z': 'Z'}

2. Modular Arithmetic
   a. Multiplication and Addition
      i. 27 * 13 mod 23 = 6 mod 23
      ii. 17 * 13 mod 23 = 14 mod 23
      iii. 28 * 15 mod 12 = 6 mod 12
      iv. 15 * 29 + 11 * 15 mod 23 = 2 mod 23
   b. Multiplicative Inverses
      i. 4^{-1} mod 17 = 13
      ii. 7^{-1} mod 17 = 5
      iii. 5^{-1} mod 37 = 15
      iv. 10^{-1} mod 15 = Does Not Exist

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

   {2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 26, 27, 28, 30, 32, 33, 34}

4. LFSR
    a. Circuit Diagram



    b. Output Stream

[0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0]

    c. Vernam Encryption Cipher text

[1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0]