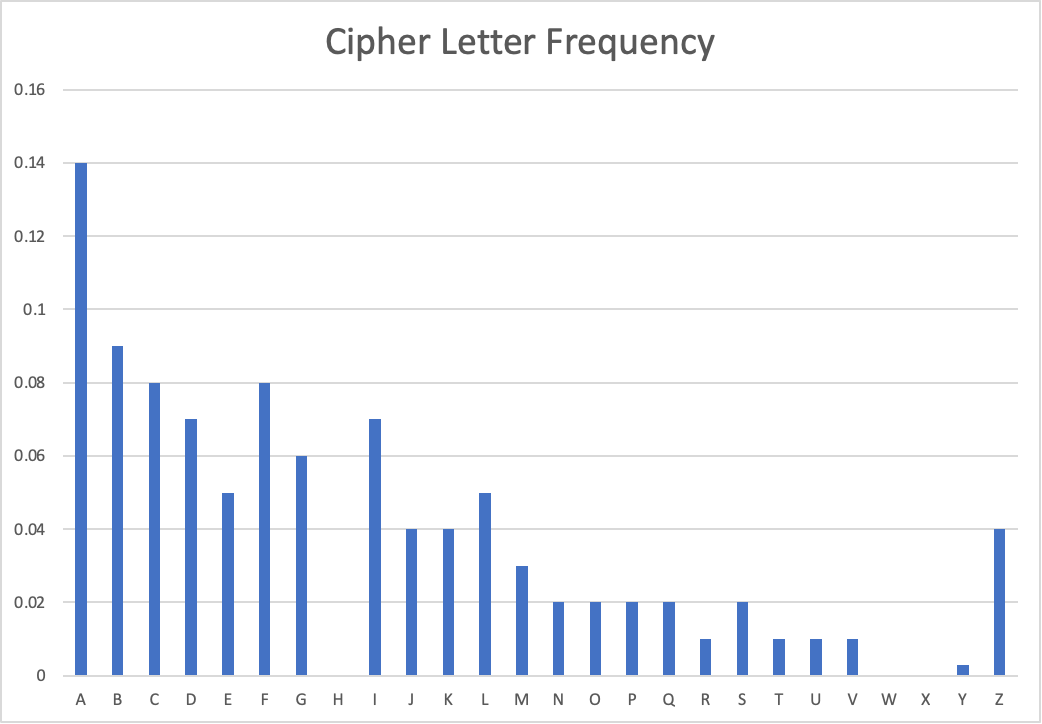
Justin Cabral

ECE/CS 578 Assignment 1

**1.A) Provide the relative frequency of all letters A...Z in the ciphertext.**



|  |  |
| --- | --- |
| **Ciphertext** | **Frequency** |
| A | 150 |
| B | 100 |
| C | 86 |
| D | 76 |
| E | 58 |
| F | 83 |
| G | 70 |
| H | 0 |
| I | 75 |
| J | 40 |
| K | 47 |
| L | 50 |
| M | 37 |
| N | 24 |
| O | 19 |
| P | 19 |
| Q | 23 |
| R | 15 |
| S | 24 |
| T | 9 |
| U | 15 |
| V | 9 |
| W | 0 |
| X | 0 |
| Y | 3 |
| Z | 45 |

**1.B) Decrypt the ciphertext with the help of the relative letter frequency of the English Language.**

Ciphertext DECODED:

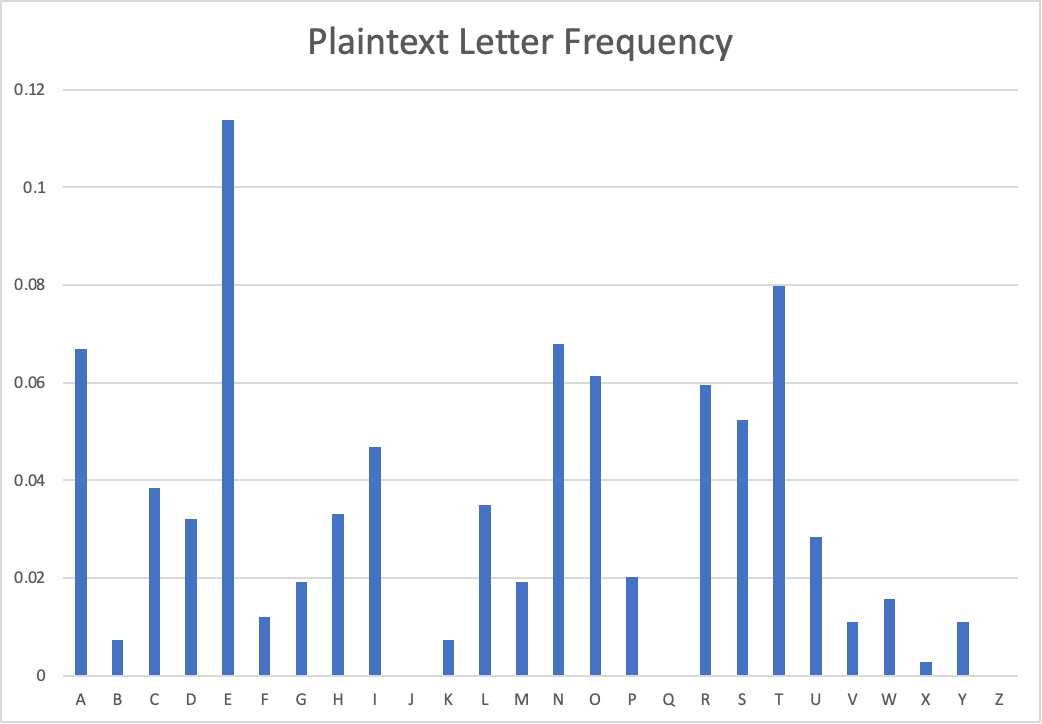
ELECTRICAL AND COMPUTER ENGINEERS DEVELOP AND CREATE PRODUCTS THAT CHANGE THE WORLD AND MAKE OUR LIVES EASIER. THE CELL PHONES WE DEPEND ON THE COMPUTERS USED IN NATIONAL SECURITY AND THE ELECTRICAL SYSTEMS THAT MAKE OUR CARS OPERATE WERE ALL CREATED BY ELECTRICAL AND COMPUTER ENGINEERS. AT WPI WE KEEP THAT PROGRESS MOVING FORWARD WITH OUR INNOVATIVE RESEARCH AND OUT OF THE BOX APPROACHES. THE DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING AT 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 UNDERGRA DUATE MINOR OR A DOCTORATE TO TACKLE SOCIETYS MOST PRESSING PROBLEMS AND UNCOVER NEW WAYS OF SOLVING THEM. WHETHER ITS DEVELOPING SYSTEMS THAT CAN LOCATE FIRE FIGHTERS 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 OURSELV ES 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.

**1.C) Find the plaintext/ciphertext letter pairs, alphabetized by plaintext.**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Plain Text** | | | | | | | | | | | | | | | | | | | | | | | | | |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |

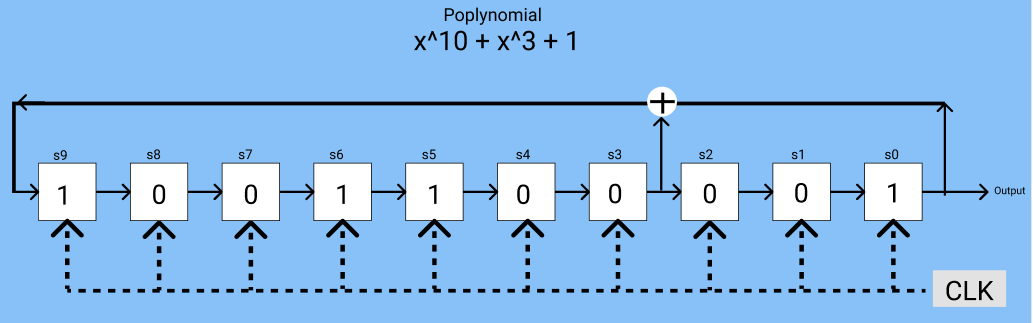
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| C | T | L | J | A | P | Q | Z | E | H | V | K | N | F | D | S | W | I | G | B | M | U | O | Y | R | X |
| **Cipher Text** | | | | | | | | | | | | | | | | | | | | | | | | | |

**1.D) Provide letter frequency for the given plaintext.**



|  |  |
| --- | --- |
| **Plaintext** | **Frequency** |
| A | 73 |
| B | 8 |
| C | 42 |
| D | 35 |
| E | 124 |
| F | 13 |
| G | 21 |
| H | 36 |
| I | 51 |
| J | 0 |
| K | 8 |
| L | 38 |
| M | 21 |
| N | 74 |
| O | 67 |
| P | 22 |
| Q | 0 |
| R | 65 |
| S | 57 |
| T | 87 |
| U | 31 |
| V | 12 |
| W | 17 |
| X | 3 |
| Y | 12 |
| Z | 0 |

**2.A) Draw a circuit diagram for the given LFSR - (x10 + x3 + 1)**



**2.B) Compute the first 512 bits of the output bit stream. You can use any program of your choice.**

10000110011011010100000111010011110100110101001001110000011111001110011011110100010101011011111000010011101000111010111110110100100001000010100101011000111001111111011000010001101001110010011110000110111011000110001111011111010010010100000011010001100101110100101101000100010110011010010100100011000011101101111000001011100101011100111011101110011001110101011101111011001010001001101100010000111001011111001010011001100101010100111111001100011010111100110101101001100010010111000010111101010101011111111010000010

**2.C) What is the period of the output stream?**

Since the polynomial I chose is considered a primitive polynomial, the period is 2n – 1.

Therefore, in my use case the period of the output stream is 210 – 1 = 1023

**2.D) Encrypt the following 32-bit plaintext using the first 32 bits of the key stream generated above. P=`11101100000110111011010011111010`**

P **= 11101100 00011011 10110100 11111010**

**⊕**

K **= 10000110 01101101 01000001 11010011**

**=**

C **= 01101010 01110110 11110101 00101001**

**2.E) Decrypt the ciphertext you found in part D using the same bit key stream generated above.**

C **= 01101010 01110110 11110101 00101001**

**⊕**

K **= 10000110 01101101 01000001 11010011**

**=**

P= **11101100 00011011 10110100 11111010**

Message = ì ß´ú