Evan Smith

CIS 628

Section M400

Midterm Exam

**Problem 28**

I used dcode.fr’s XOR cipher tool:

**Graphical user interface, text

Description automatically generated**

**Graphical user interface, application

Description automatically generated**

**Problem 29:**

I used dcode.fr’s shift cipher tool:

**Graphical user interface, text, application

Description automatically generated**

**Problem 30:**

I used dcode.fr’s mono-alphabetic substitution cipher tool:

Text

Description automatically generated

**Problem 31:**

I used the following table to calculate the pattern:

|  |  |  |
| --- | --- | --- |
| FF1 | FF0 | Out |
| 1 | 1 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

Past the highlighted section, the pattern repeats.

**Problem 32:**

My work for this problem was as follows-

350 mod 3 ≡ 35 \* 10 mod 3 ≡ 7 \* 5 \* 10 mod 3 ≡ 1 \* 2 \* 1 mod 3 ≡ **2**

**Problem 33:**

First, we confirm that the question is valid, that is, does the modular multiplicative inverse exist for 7 mod 31? Since 7 and 31 are both prime, they are therefore also coprime, so the inverse does exist. Then, we can just try brute forcing the problem, since the modulo is small and the inverse must be less than the modulo. We can skip any potential values of the inverse where 7x <= 31, which speeds this up, and then just calculate the value of 7x mod 31, looking for a result of 1:

|  |  |  |
| --- | --- | --- |
| **X** | **7x** | **7x mod 31** |
| 5 | 35 | 4 |
| 6 | 42 | 11 |
| 7 | 49 | 18 |
| 8 | 56 | 25 |
| 9 | 63 | 1 |

We see that the answer is 9.