1. (0 points) What is your name? Write it clearly. Staple your HW.

2. (20 points) Alice and Bob want to use a 1-time pad but are too lazy to actually generate random bits. Instead they take the digits of $1/7$ in base 10 and do the following: if a digit is even replace it with 0. If a digit is odd replace it with 1. This creates an infinite string of 0’s and 1’s.

(a) Write out the first 20 bits of the bit string they will share.
(b) Alice wants to send 1101010 to Bob. What does she send?
(c) Bob then wants to send 100001 to Alice. What does he send?
(d) Why is using this string a terrible idea?

3. (20 points) Assume that Alice and Bob are using a keyword shift cipher. Assume the keyword is *funkytown* and shift 7. Make the table to both encode and decode. (NOTE- THIS IS TWO TABLES- ONE TO ENCODE, ONE TO DECODE. ALSO NOTE- THE TABLE TO DECODE SHOULD TELL YOU HOW TO DECODE A, B, C, ETC, IN THAT ORDER, SO ITS USABLE BY ALICE AND BOB.) If Alice wants to send the message: *CS and Math are good majors*. What does she send?

4. (20 points) Alice and Bob are using the Vigenere Cipher with alphabet $\{a, b, c, \ldots, z, 0, 1, \ldots, 9\}$. The key is CS198 Alice wants to send Bob the message

*I wish I had 101 Dogs*

What does Alice send?
5. (20 points) Alice and Bob are using the Matrix Cipher. The matrix is

\[ A = \begin{pmatrix} 1 & 2 \\ 7 & 5 \end{pmatrix} \]

Alice wants to send Bob the message

\[ U \text{ are jawesome!} \]

What does Alice send?

6. (20 points) Look up on the web how to find the inverse of a 2 × 2 matrix in the normal numbers.

(a) Describe how to find the inverse of a 2×2 matrix over the rationals. Give an example.

(b) Describe what changes if it’s done mod 26. Give an example.

(c) Write informal code that will, given

\[ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \]

output the inverse matrix mod 26.