Computer Security Homework 2 (Due Friday 8/28/20)

1. In class, we covered a rail fence cipher with 2 rails. There can be more rails if we want. Encrypt this message CRYPTOGRAPHY with a rail fence cipher with 3 rails.

2. Use columnar transposition with the key [4, 2, 1, 3] to encrypt the message CYBERSECURITY.

3. Encrypt the message FLOODGATES using the Playfair cipher with the key STREAMCIPHER. Please follow the conventions from class (I=J, X in between repeats, Q for padding, opposite corners in the same row, move right when in same row, move down when in same column). Please show your work.

4. Encrypt the message 01101101 with a stream cipher where the keystream is 00011000.

5. Multiple choice. Choose the correct answer:
   (A) All PRNGs are insecure and should never be used in encryption.
   (B) The PRNGs built into Java and Python are not secure enough to use for encryption, but there do exist pretty secure PRNGs.

6. Multiple choice. The RC4 cipher
   (A) was widely used, but is not recommended anymore because of various weaknesses
   (B) is so insecure a five year old could break it.
   (C) is considered the strongest stream cipher currently known

7. If plaintexts P_1 and P_2 are both encrypted with a stream cipher using the same key K into ciphertexts C_1 and C_2, what will the result of $C_1 \oplus C_2$ be?

8. Suppose two messages were encrypted with the same stream cipher key. The two ciphertexts are 10001 and 01101. Suppose the plaintext corresponding to the first ciphertext is 00111. What is the other plaintext?

9. Using whatever programming language you like, compute the XOR of the following two strings of hex digits (each string is spread across two lines to fit onto the page). The answer in hex should start with `16dff`. Please submit your code for this problem along with your answers. [Hint: it's very quick in Python, using the `int` and `hex` functions along with the `^` operator. Look up the details of how `int` works.]

   ```
   6684822d38024d75b6d669cdc093faf3fad44a4770688d81047c8b365ce3d77a
   c594fb6c4435546a93046a207835336fde0be08a7b9e66d6055234801702a258

   705b76e78c28b0c4720def20156ef05916222237c66145c7980bef0a7eeafd34
   2df4d5ba4a43dd8e9b7852221d1e169ba51bc05ad68d6e65bad3cb0568a00afa
   ```

10. Included with this assignment is a file that contains two Python byte strings. These are the ciphertexts from two different plaintexts encrypted with a stream cipher using the exact same key. One of those plaintexts is 1144 characters of perfectly readable English, starting with the word 'Every'. Find that entire plaintext.