Problems from Ma 195J.18 Problem Sets 1–4

1. Supposed you are told that the plaintext `breathtaking` yields the ciphertext `RUPOTENTOIFV` where the Hill cipher is used (but the block size m is not specified). Determine the encryption matrix.
2. This problem explores the use of a one-time pad version of the Vigènere cipher.
   (a) Encrypt the plaintext `sendmoremoney` using the key $[9, 0, 1, 7, 23, 15, 21, 14, 11, 11, 2, 8, 9]$.
   (b) Using the ciphertext produced in part (a), find a key so that the ciphertext decrypts to `cashnotneeded`.
3. Write a program that can encrypt and decrypt the general shift cipher.
4. Let P be the set of real numbers, where $q \in P$ and $q \neq 1$. Define operations on P as follows:
   $$a \oplus b = ab \text{ and } a \odot b = a^{\log_q b}$$
   Prove that P is a field.
5. Find an appropriate modulus $f(x)$ such that the ring of equivalence sets $\mathbb{Z}_3[x]/f(x)$ is a field of 9 elements.
6. Find the inverse of $x^7 + x^3 + 1$ in GF(256).
7. In RSA, if the public key is $(e, n) = (17, 187)$, find the private key d.
8. Bob has a public RSA key $(e, n) = (13, 77)$. He sends Alice a message m and the digital signature of the message. The message and signature that Alice receives is $(m, s) = (3, 5)$. Should Alice accept the message as genuine or not?
9. In the ElGamal algorithm, given the prime $p = 31$:
   (a) Choose an appropriate e_1 and d, then calculate e_2.
   (b) Encrypt the message "`HELLO`" using 00 to 25 for encoding the letters of the alphabet. Use the different blocks such that $m < p$.
   (c) Decrypt the ciphertext to obtain the plaintext.
10. Consider the elliptic curve E given by the equation
    $$y^2 = x^3 + x - 1 \pmod 7$$
    (a) Determine all the eleven points on the curve.
    (b) Calculate $-(2, 3)$, $2(4, 2)$, and $(1, 1) + (3, 1)$.
11. Prove that the Kronecker product of two Hadamard matrices is a Hadamard matrix.
12. Let C be a binary code consisting of all cyclic shifts of the vectors 11010000, 11100100, 10101010, together with $\mathbf{0}$ and $\mathbf{1}$. Show that C is a $(8, 20, 3)$-code. When showing that $d(C) = 3$, the cyclic nature of the code reduces the number of evaluations of $d(x, y)$ required from $\binom{20}{2}$ to ... (how many?)
13. Given $\mathbf{u} = (u_1, u_2, \ldots, u_m)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_n)$, let $(\mathbf{u} \mid \mathbf{v})$ denote the vector $u_1 u_2 \ldots u_m v_1 v_2 \ldots v_n$ of length $m + n$. Suppose that C_1 is a binary (n, M_1, d_1)-code and that C_2 is a binary (n, M_2, d_2)-code. Form an new code C_3 consisting of all vectors of the form $(\mathbf{u} \mid \mathbf{u} + \mathbf{v})$ where $\mathbf{u} \in C_1$ and $\mathbf{v} \in C_2$. Show that C_3 is a $(2n, M_1 M_2, d)$-code, with $d = \min\{2d_1, d_2\}$.
14. Construct a standard array for the code having a generator matrix
    $$\begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Last compiled: 2017-11-01 15:57:20
Source hash: B1BA0F63DE3A3BECE27FE40C579E0A5C

(a) Decode received vectors 11111 and 01011

(b) Give examples of

   i. two errors occurring in a codeword and being corrected

   ii. two errors occurring in a codeword and not being corrected