EECE 405/560 assignment 2

1. A cipher is *closed* if encrypting twice with two separate keys is equivalent to encrypting only once with a third key. For example, performing the shift cipher twice with shifts of 3 and 2 is the same as shifting once with a shift of 5.

   Determine if the following ciphers are closed:

   (a) Vigenère encryption

   (b) The affine cipher

   (c) Playfair cipher

   (d) The Vatsyayana cipher from art 45 of the Kama Sutra

2. Is it a good thing or a bad thing for a cipher to be closed?

3. Consider the following permutations:

$$f = \begin{pmatrix} A & B & C & D & E & F & G & H \\ B & A & D & C & F & E & H & G \end{pmatrix}$$

$$g = \begin{pmatrix} A & B & C & D & E & F & G & H \\ D & E & F & G & H & A & B & C \end{pmatrix}$$

   Write the following permutations as a product of disjoint cycles:

   (a) f

   (b) g

   (c) fg

   (d) gf

   (e) f^2g

   (f) f^{-1}

   (g) $f^{-1}gf$

4. Suppose we are permuting the set $S = \{1, 2, 3, \cdots N\}$. If $1 < m \leq N$, Let $f = (1, 2, \cdots m-1)$ and $g = (1, 2, \cdots m)$. What permutation is fg^{-1}?

1. Let f and g be permutations of $S = \{A, B, C, D, E\}$. We will say that $f \equiv g$ if fg^{-1} maps D to D and E to E. That is to say, $f \equiv g$ if the permutation fg^{-1} leaves the last two elements alone.

   Prove:

   (a) $f \equiv f$

   (b) If $f \equiv g$ then $g \equiv f$

   (c) If $a \equiv b$ and $b \equiv c$ then $a \equiv c$

   A relation $\equiv$ that satisfies these three rules is called an *equivalence relation.* Examples of equivalence relations include: congruence of triangles, similarity of triangles, coterminality of angles ($370° \equiv 10°$), equivalence of two integers modulo N, equipollence of sets—sets A and B are equipollent ("equally counted") if there exists a bijection between them—equality of magnitude/length/size/area/volume/measure of any measurable things, etc. Basically any way two things can be "practically the same" without being exactly equal, is usually an equivalence relation.

2. Let f and g be permutations of $S = \{A, B, C, D, E\}$. Determine if the following are equivalence relations. If not, provide a counterexample.

   (a) $f \equiv g$ if $fg = gf$.

   (b) $f \equiv g$ if $f = g^k$ for some integer k.

   (c) $f \equiv g$ if some h exists with $f = hgh^{-1}$.

3. If $\equiv$ is an equivalence relation, and x is a thing, the *equivalence class* of x is the set of all things equivalent to x (and also to each other).

   For example, under coterminality of angles, the equivalence class of $45°$ is the set $\{\cdots - 675°, -315°, 45°, 405°, 765°, 1125° \cdots\}$

   For the equivalence relation of problem 1, describe the equivalence class of the cycle $f = (A\ B\ C\ D\ E)$. How big is it?