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) Vigen`ere encryption

Closed

$$\text{Length of equivalent key=LCM}(\mathrm{l}_1,\mathrm{l}_2)$$
$$\text{KEY}_{eq} = KEY1\ KEY1 \ldots KEY1 + KEY2\ KEY2 \ldots KEY2 \ \ (mod\ 26)$$

Example: KEY1 = “BAD” KEY2=”TO”

$$\text{Length of equivalent key=LCM}(\mathrm{l}_1 = 3,\mathrm{l}_2 = 2) = 6$$
$$\text{KEY}_{eq} = BADBAD + TOTOTO \ \ (mod\ 26) = VPXTUS$$

(b) The affine cipher

Closed

$$y = a_1 x + b_1\ (mod\ 26),\ \ \gcd(a_1, 26) = 1$$
$$y = a_2 x + b_2\ (mod\ 26),\ \ \gcd(a_2, 26) = 1$$

If we plug in second equation in first one:

$$y = a_1(a_2 x + b_2\ (mod\ 26)) + b_1\ (mod\ 26)$$
$$y = (a_1 a_2)x + (a_1 b_2 + b_1)\ \ (mod\ 26)$$

Then

$$y = a_{eq} x + b_{eq}\ (mod\ 26),\ \ \gcd\left(a_{eq}, 26\right) = 1$$
$$a_{eq} = a_1 a_2$$
$$b_{eq} = a_1 b_2 + b_1$$

(c) Playfair cipher

Not closed

Playfair cipher is a permutation of pairs, but it never permutes a pair of a character to itself. However, if Playfair cipher is used twice with different keys, it is possible that a pair or a character maps to itself. Therefore, there is no equivalent Playfair cipher for this combination. Thus, it is not closed.

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

Not closed

Same as (c).

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

It is not a good thing that cipher to be closed, because deciphering of 2 times ciphered text will be easier by brute force to find an equivalent key instead of 2 separate keys.

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

(AB) (CD) (EF) (GH)

(b) g

(A D G B E H C F)

(c) fg

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

(d) gf

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

(e) f^2g

$$f^2g = \begin{pmatrix} A & B & C & D & E & F & G & H \\ D & E & F & G & H & A & B & C \end{pmatrix} = g = (A\ D\ G\ B\ E\ H\ C\ F)$$

f^2 is swapping 2 times, so it will be identical permutation.

(f) f^{-1}

$$f^{-1} = f = (A\ B)(C\ D)(E\ F)(G\ H)$$

Swapping and its reveres are the same.

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

$$f^{-1}gf = fgf = \begin{pmatrix} A & B & C & D & E & F & G & H \\ F & C & H & E & B & G & D & C \end{pmatrix} = g = (A\ F\ G\ D\ E\ B\ C\ H)$$

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

$$f = \begin{pmatrix} 1 & 2 & \dots & m-2 & m-1 & m & \dots & N \\ 2 & 3 & \dots & m-1 & 1 & m & \dots & N \end{pmatrix}$$

$$g^{-1} = \begin{pmatrix} 2 & 3 & \dots & m-1 & m & 1 & m+1 \dots N \\ 1 & 2 & \dots & m-2 & m-1 & m & m+1 \dots N \end{pmatrix}$$

$$fg^{-1} = \begin{pmatrix} 2 & 3 & \dots & m-1 & m & 1 & m+1 & \dots & N \\ 2 & 3 & \dots & m-1 & 1 & m & m+1 & \dots & N \end{pmatrix} = (1\ \ m)$$

Supplementary 560 Questions

1. Let f and g be permutations of S = {A, B, C, D, E}. We will say that $f \equiv g$ if the permutation 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) $f \equiv f$

$ff^{-1} = I$ then this permutation leaves all elements including last two. Therefore $f \equiv f$

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

$fg^{-1}.gf^{-1} = I$ so gf^{-1} is inverse of fg^{-1}. If a permutation leaves last two elements, the inverse of that will do the same. Therefore, if $f \equiv g$ then $g \equiv f$

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

If ab^{-1} leaves last two elements, and bc^{-1} leaves the last two elements, $ab^{-1}bc^{-1} = ac^{-1}$ leaves the last two elements either. Therefore, if $a \equiv b$ and $b \equiv c$ then $a \equiv c$

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 $fg = gf$.

I) $f \equiv f$

$f = f \rightarrow ff = ff \rightarrow f \equiv f$ Satisfied

II) If $f \equiv g$ then $g \equiv f$

$fg = gf \rightarrow gf = fg \rightarrow g \equiv f$ Satisfied

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

$\begin{cases} ab = ba \\ bc = cb \end{cases} \nrightarrow ac = ca$ Not satisfied

Counter example: $\begin{matrix} a = (A\ B) \\ b = (C\ D) \\ c = (B\ E) \end{matrix} \rightarrow \begin{matrix} ab = ba = (A\ B)\ (C\ D), \\ bc = cb = (C\ D)(B\ E) \end{matrix}$

But $\begin{matrix} ac = (A\ B\ E) \\ ca = (A\ E\ B) \end{matrix} \rightarrow ac \neq ca$

NOT an equivalence relation.

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

I) $f \equiv f$

$f = f^k \rightarrow f \equiv f$ Satisfied

II) If $f \equiv g$ then $g \equiv f$

$f = g^k \nrightarrow g = f^k$ NOT Satisfied

Counter example:

$g = (A\ B)(C\ D\ E),\ f = g^2 = (C\ E\ D),\ f^k = (C\ D\ E)\ or\ (C\ E\ D) or\ I \rightarrow g \neq f^k$

NOT an equivalence relation.

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

I) $f \equiv f$

$f = f \rightarrow f = IfI^{-1} \rightarrow f \equiv f$ Satisfied

II) If $f \equiv g$ then $g \equiv f$

$f = hgh^{-1} \rightarrow h^{-1}f\,h = h^{-1}hgh^{-1}h \rightarrow g = (h^{-1})f\,(h^{-1})^{-1} \rightarrow g \equiv f$ Satisfied

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

$\begin{cases} a = hbh^{-1} \\ b = kck^{-1} \end{cases} \rightarrow \begin{cases} b = h^{-1}ah \\ c = k^{-1}bk \end{cases} \rightarrow c = k^{-1}h^{-1}ahk \rightarrow c = (hk)^{-1}a(hk)$ Satisfied

An equivalence relation

3. If ≡ 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 {· · · − 675◦,−315◦, 45◦, 405◦, 765◦, 1125◦ · · · } For the equivalence relation of problem 1, describe the equivalence class of the cycle f = (A B C D E). How big is it?

Any g that fg^{-1} maps D to D and E to E is equivalence for f:

$$f = \begin{pmatrix} A & B & C & D & E \\ B & C & D & E & A \end{pmatrix}, \qquad fg^{-1} = \begin{pmatrix} \dots & D & E \\ \dots & D & E \end{pmatrix}$$

Then

$$g^{-1} = \begin{pmatrix} \dots & D & E \\ \dots & C & D \end{pmatrix}$$

And in g^{-1}all permutations for 3 first elements will be $3! = 6$

All 6 conditions of g will be equivalence for f