Eric Willard
CS 5602 Cryptography
Prelim 2 Problem 5

(a) Let D_1, D_2 be disk 1 and disk 2, respectively. Let R be the reflector.
$D_1 = D_2 = S_{26}$ Disk's 1 and 2 are the permutation group on 26 elements.
And $R < S_{26}$ where R is the set of all the derangements of S_{26} and $\forall r \in R,\ r^2 = 1$ that is all elements of R are their own inverse.

To encrpyt : $ct = d_1^{-1} * (d_2^{-1} * (r * (d_2 * (d_1 * pt))))$
To decrypt: $pt = d_1^{-1} * (d_2^{-1} * (r^{-1} * (d_2 * (d_1 * ct))))$

(b) The property reflectors need is that $\forall r \in R,\ r^2 = 1$.
To show decryption works, I will show algebraically that applying both encryption and decryption gives the plaintext back.

$pt = d_1^{-1} d_2^{-1} r^{-1} d_2 (d_1 d_1^{-1}) d_2^{-1} r d_2 d_1 pt$ by associativing we can group the middle two elements
$pt = d_1^{-1} d_2^{-1} r^{-1} (d_2 d_2^{-1}) r d_2 d_1 pt$
$pt = d_1^{-1} d_2^{-1} (r^{-1} r) d_2 d_1 pt$
$pt = d_1^{-1} (d_2^{-1} d_2) d_1 pt$
$pt = (d_1^{-1} d_1) pt$
$pt = pt$

Therefore the model proposed for mini-enigma is self-decoding with two passes. This can be generalized to an arbitrary number of rotors, let's say k.

$pt = d_1^{-1} \cdots d_k^{-1} r^{-1} d_k \cdots d_1 d_1^{-1} \cdots d_k^{-1} r d_k \cdots d_1 pt$

Following the same process it can be easily seen that it returns the plaintext.

(c) The enigma machine cannot output a character that was input into it as encrypted text because of the reflectors, since they always return something that isn't the character input. The disks can't make it to where the same character that was input is output because the disk permutations are used then inverted, so as long as the reflector property holds, mEnigma(c) != c

(d) The settings used for mini-enigma were (1, 18, 0, 3, 0)