October 1, 2004

Math 65S
Cryptography and Society
Assignment 5

Due: Friday, October 8, 2004.

Journal: Write a one-page (12 pt, single-spaced) explication of the fourth chapter of Singh's book, with emphasis on the lessons to be learned from the use of Enigma.

1. Consider the 5-cycle (2 5 6 4 9), a permutation of **13**. Compute the cycle decomposition of the result of composing this permutation with itself k times, $k = 2, \ldots, 6$.

2. Let $\pi : \mathbf{13} \to \mathbf{13}$ be the permutation

$$\pi(1) = 12,\ \pi(2) = 13,\ \pi(3) = 3,\ \pi(4) = 1,\ \pi(5) = 11,$$
$$\pi(6) = 9,\ \pi(7) = 5,\ \pi(8) = 10,\ \pi(9) = 6,\ \pi(10) = 4,$$
$$\pi(11) = 7,\ \pi(12) = 8,\ \pi(13) = 2.$$

Find its decomposition into cycles. What is the least positive integer m such that $\pi^m = \epsilon$, the identity permutation, $\epsilon(k) = k$? (Here π^m means π composed with itself m times.) Now suppose given a permutation π of $\mathbf{n}$ whose cycle decomposition has cycles of length $\ell_1, \ldots, \ell_k$. Using your experience with the example in the first part of the problem, guess (with explanation!) the least integer m such that $\pi^m = \epsilon$.

3. Compute the cycle decompositions of compositions $\pi_2 \circ \pi_1$ and $\pi_1 \circ \pi_2$, where the cycle decompositions of π_1 and π_2 are

$$\pi_1 = (1\ 4)(2\ 8)(6\ 7)(3\ 5)$$

and

$$\pi_2 = (6\ 7)(3\ 4)(8\ 1)(2\ 5)$$

Do the same with

$$\pi_1 = (1\ 14)(12\ 5)(13\ 6)(7\ 9)(8\ 4)(10\ 11)(2\ 3)$$

and

$$\pi_2 = (9\ 12)(13\ 4)(5\ 6)(3\ 11)(7\ 1)(8\ 14)(2\ 10)$$

4. Show that if σ is a permutation of $\mathbf{n}$ and $\sigma^2 = \epsilon$, then the cycle decomposition of σ consists solely of transpositions. Thus, any involutory cipher on the 26 letters of the alphabet (like EM) has such a structure.

5. Show that the number of ways of wiring the reflecting drum in EM is $26!/2^{13}13!$ (*Suggestion:* Remember the reasoning used to count the number of plugboard settings.)

6. You would expect that no setting of EM would give the trivial cipher (EM(p)=p, for all plaintext letters p.) Show that the following stronger statement holds: EM(p)$\neq p$, for every p.

7. The example of the four cycles on p. 152 in Singh can't come from EM, as claimed there. Why not?

8. Suppose the two 7-cycles on p. 152 in Singh were part of the cycle decomposition coming from 1st-4th letter chains. (This could happen.) Suppose you knew that the first plain letter of some message key were D and that its corresponding cipher letter were X. If the first letter of an intercepted (encrypted) message key were N, what would the first letter of the message key have been?