MATH 195: CRYPTOGRAPHY
HOMEWORK #4

Problem 3.4'. *Let $N \geq 3$. Prove that the probability*

$$\frac{\#\{\sigma \in \operatorname{Sym} N : \exists k \in \{1, 2, \ldots, N\} : \sigma(k) = k\}}{N!}$$

is $\geq 5/8$ and is $\leq 2/3$.

Problem 2.13. *Find constants c_1 and c_2 such that the usual algorithm (shown in class) for finding the inverse of any $A \in GL(k, F)$ over any* field *F takes no more than $c_1 k^{c_2}$ arithmetic operations $(+, -, \cdot, ^{-1})$ in F; how many of these are inversions?*

Problem 3.14 (Feistel ciphers). *Let $k \geq 2$, $A = (\mathbb{Z}/2\mathbb{Z})^k$, and define the maps*

$$s, g : A \times A \to A \times A$$

$$s(x, y) = (y, x)$$

$$g(x, y) = \begin{cases} (x, y), & y \neq (0, 0, \ldots, 0); \\ (x + \underbrace{(1, 1, ..., 1)}_{k}, (0, 0, \ldots, 0)), & y = (0, 0, \ldots, 0). \end{cases}$$

Prove: s^2 and g^2 are the identity on $A \times A$, $(sg)^4 = sgsgsgsg$ moves only 3 elements of $A \times A$ (i.e. $(sg)^4((x, y)) \neq (x, y)$ for only 3 elements $(x, y) \in A \times A$), and $(sg)^{12}$ is the identity.

Date: February 19, 2002.

3.4', 2.13, 3.14.