Thought problems (22 Jan 2002)

1 An autokey cipher

Consider a cipher that works in the following way. Suppose we have an alphabet of n symbols (e.g., if we encrypt each English letter separately, we have $n = 26$, but in general n may be much larger). The secret key consists of n permutations $\pi_0, \ldots, \pi_{n-1}$, each of which is a reversible substitution on the alphabet. If the message is $m_1, \ldots, m_k$, then it will be encrypted to the ciphertext $c_1, \ldots, c_k$ given by $c_i = \pi_{c_{i-1}}(p_i)$. (We can take $c_0 = 0$.)

How secure is this? In particular, in a ciphertext-only attack, how much text would you need to break the cipher effectively, as a function of n? How much computation? How about for a known-plaintext attack?

2 Transposition ciphers (optional; for fun)

Consider a transposition cipher with n-bit blocks, whose key is chosen uniformly at random from the set of $n!$ possible permutations. In other words, our secret key is a permutation π on $\{1, 2, \ldots, n\}$, and if the n-bit message is $m_1, \ldots, m_n$, then the n-bit ciphertext will be $m_{\pi(1)}, \ldots, m_{\pi(n)}$.

How secure is this? In particular, for which of the cases below can you recover the key efficiently?

1. You are given $O(n)$ chosen plaintexts.
2. You are given $O(\lg n)$ chosen plaintexts.
3. You are given $O(1)$ chosen plaintexts.
4. You are given $O(n)$ known plaintexts.
5. You are given $O(\lg n)$ known plaintexts.