Are Matrix Codes Uncrackable Via Plaintext Only Attack?

1 Matrix Codes

I want to sent a message an encrypt it. As usual we can view a message as a sequence of numbers in the set $\{0, \ldots, 25\}$.

One way to encrypt is to take a $n \times n$ matrix M of entries from $\{0, \ldots, 25\}$ with det that is rel prime to 26 (so it has an inverse mod 26). Then encrypto the first n characters $\vec{x}$ with $M\vec{x}$, the next n chararcters $\vec{y}$ with $M\vec{y}$. etc.

A Freq analysis approach to cracking the code seems hard since, for $n = 10$, most 10-long sequences will either appear 0 or 1 time or at most 2 times.

This can be cracked by trying all roughly n^2 matrices. But can we do better?

In the real world we woudl have a prior message and how it got encrypted (or perhaps we can trick Alice and Bob into giving us that) at which point it is easy to crack with linear equations.

But can a plaintext attack work?

2 A Rigorous Formulation

We formualize the problem rigorously.

We assume Eve has the following

1. n and the alphabet size s.
2. Probabilities for all n-long sequences in English.
3. The ability to make the following query: Given i, give me the ith character of the text. We assume the text is infinite. This query takes $\log i$ to make.

Let f be the function that takes the Probs of all n-long sequences and outputs the number of different ones there are. Note that if there are many different ones then the dist is far from uniform.

Conjecture 1: There exist reasonable functions g and h such that the following holds. For all n, ϵ Eve requires $\Omega(g(\epsilon)h(f(prob))s^{n^2}))$ to find ϵn^2 entries of the matrix.

Note that our goal is not to find the matrix but to find the message. Hence here is an alternative conjecture.

Conjecture 2: There exist reasonable functions g and h the following holds. For all n, ϵ Eve requires $\Omega(g(L)h(f(prob))L(a)s^{n^2}))$ to find the first L characters in the text.

One could make other conjectures about any L chars in the text or perhaps being happy with s^n, but we stop here.