Mathematics 124 (Winter 2009)
Cryptanalysis of the Hill cipher

Given only the ciphertext, since frequency analysis is not really possible, a brute force attack may work. Assuming that the key matrix A is 2×2 means that the cryptanalyst needs to try out the inverse A^{-1} on the start of the ciphertext to see if sensible plaintext is produced. There are $26^4 = 456976$ possible 2×2 matrices modulo 26, but obviously not all are invertible. Therefore, assuming that a computer takes one-tenth of a second to multiply a matrix by the first few terms of the ciphertext, it would take about 12 hours to check all possibilities.

Remark. For your information only. A matrix is invertible modulo 26 if and only if it is invertible modulo 2 and it is invertible modulo 13. The Chinese Remainder Theorem can then be used to show that the number of 2×2 matrices that is invertible modulo 26 is

$$26^4(1-\tfrac{1}{2})(1-\tfrac{1}{2^2})(1-\tfrac{1}{13})(1-\tfrac{1}{13^2}) = 157248.$$

This means that, once the invertible 2×2 matrices are determined, it would take approximately 4 hours to check all possibilities.

However, if a little bit of the plaintext is known, then it is relatively straightforward to cryptanalyze.

Example. Suppose that a ciphertext begins with `WJMQ FMGG` which corresponds to `STAY HOME`. Determine the key matrix.

Solution. Since `ST` $\mapsto$ `WJ` and `AY` $\mapsto$ `MQ`, we know that

$$A\begin{bmatrix}18\\19\end{bmatrix} \equiv \begin{bmatrix}22\\9\end{bmatrix} \pmod{26} \quad \text{and} \quad A\begin{bmatrix}0\\24\end{bmatrix} \equiv \begin{bmatrix}12\\16\end{bmatrix} \pmod{26}.$$

But because of the way matrix multiplication is defined, this is equivalent to

$$A\begin{bmatrix}18 & 0\\19 & 24\end{bmatrix} \equiv \begin{bmatrix}22 & 12\\9 & 16\end{bmatrix} \pmod{26}.$$

Now, to solve for A, all we need to do is multiply both sides by

$$\begin{bmatrix}18 & 0\\19 & 24\end{bmatrix}^{-1} \pmod{26}.$$

Unfortunately, this inverse does not exist since its determinant is $432 = 16 \,\mathrm{MOD}\, 26$ which is NOT relatively prime to 26.

However, we also know that `HO` $\mapsto$ `FM` which means that

$$A\begin{bmatrix}7\\14\end{bmatrix} \equiv \begin{bmatrix}5\\13\end{bmatrix} \pmod{26}.$$

Thus, we have

$$A\begin{bmatrix}18 & 7\\19 & 14\end{bmatrix} \equiv \begin{bmatrix}22 & 5\\9 & 13\end{bmatrix} \pmod{26}.$$

Since the inverse of

$$\begin{bmatrix} 18 & 7 \\ 19 & 14 \end{bmatrix}$$

is

$$\begin{bmatrix} 20 & 3 \\ 23 & 22 \end{bmatrix} \operatorname{MOD} 26$$

we conclude that

$$A \begin{bmatrix} 18 & 7 \\ 19 & 14 \end{bmatrix} \begin{bmatrix} 20 & 3 \\ 23 & 22 \end{bmatrix} \equiv \begin{bmatrix} 22 & 5 \\ 9 & 13 \end{bmatrix} \begin{bmatrix} 20 & 3 \\ 23 & 22 \end{bmatrix} \pmod{26}$$

and so

$$A \equiv \begin{bmatrix} 9 & 20 \\ 14 & 5 \end{bmatrix} \pmod{26}.$$

Remark. There is nothing that requires the key matrix to be 2×2. For instance, a 3×3 key matrix requires that the plaintext be grouped in threes; that is,

$$X = \begin{bmatrix} x_1 & x_4 & \cdots & x_{n-2} \\ x_2 & x_5 & \cdots & x_{n-1} \\ x_3 & x_6 & \cdots & x_n \end{bmatrix}.$$

The resulting Hill alphabet has $26^3 = 17576$ letters. A 4×4 key matrix yields an alphabet of $26^4 = 456976$ letters. There are general formulas to compute inverses of matrices, and these can be implemented on a computer. It is important to note that the formula for the inverse is nice *only* for 2×2 matrices.