Crypto Lecture 3

§ 2.9 The Hill Cipher.

The Hill cipher uses linear algebra to encrypt messages. First, a brief refresher:

If A is a 2×2 matrix and B is a 2×2 matrix: $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$, then their product is

$$AB = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}.$$

When $\vec{v} = \begin{pmatrix} x \\ y \end{pmatrix}$ is a vector, we multiply

$$A\vec{v} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}.$$

The matrix $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity,

and if a matrix C satisfies $CA = AC = I$, then $C = A^{-1}$ is "the inverse of A". The formula is:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}, \quad ad-bc \neq 0.$$

In general, if A and B are $n\times n$ matrices,