Hill Cipher: Linear transformation of digitized alphabet

- message goes in as column vectors
- A.[uncoded message] = [coded message]

$$A \begin{bmatrix} \text{col1=start of message} & \dots & \text{coln=end of message} \end{bmatrix}$$

- [uncoded message] = A^{-1}.[coded message]
- Vulnerable because of its linearity—intercept enough vector correspondances (uncoded and coded)

http://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html

A Stick Figure Guide to the Advanced Encryption Standard (AES)

Condition Number Roundoff Errors

- issue with the matrix, not with Maple
- asymptotically worst case loss of accuracy: 10^{19}: 19 digits=k, order
- use fractions when possible—if not, using r digits gets at least $r - k$ accuracy [ex: 21-19=2]
- hard to numerically distinguish between a non-invertible matrix and one with a large condition number

What is The Error ?
How did it happen ?

http://c.asstatic.com/images/1639965_634936497651212500-1.jpg