Linear Algebra

MA 242 (Spring 2013)
Instructor: M. Chirilus-Bruckner

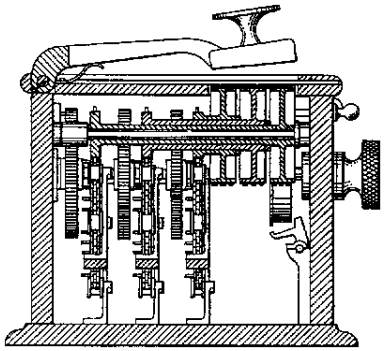
Linear Algebra in Coding Theory

– Hill Cipher –

Cryptography is the art of protecting information by transforming it into a format that is not directly readable, called cipher text. Only those who possess a secret key can decipher the message into plain text. *Coding theory* deals with the encryption process that can be viewed as a map T that maps the data vector x into the code $T(x) = y$.

The *Hill Cipher* was invented by Lester S. Hill in 1929. It is a polygraphic substitution cipher based on linear algebra. Hill used matrices and matrix multiplication to mix up the plaintext. He constructed a cipher machine for his system using a series of geared wheels and chains. However, the machine never really sold. Hill's major contribution was the use of mathematics to design and analyse cryptosystems. In general, the Hill cipher will not be used on its own, since it is not all that secure. Some modern ciphers use a matrix multiplication step to provide diffusion.

source: http://practicalcryptography.com/ciphers/hill-cipher/



A	B	C	...	_
1	2	3	...	27

$T(x) = Ax, \quad A \in \mathbb{R}^{n \times n}$