linear transformation

Any rigid transformation in space which can be represented by the successive performance of pure translations + pure rotations.

Theorem #1 - Every linear transformation can be represented by a matrix.

#2 - Every matrix represents a linear transformation -

#3 - If the determinant of a matrix is different from zero, then the transformation is non-singular and has an inverse -

The matrix of the inverse transformation is the adjoint of the original matrix with every element divided by the value of the determinant

---

Key

Represent plain text in units of fixed length as a series of vectors (vector - any ordered set of numbers of fixed length)

Key key consists of a series of substitutions which will transform the plain text into a vector

Find a non-singular matrix having as many rows & columns as the vector has elements

Each vector in turn is multiplied on the right by the matrix & the result is always a vector

Another series of substitutions is provided to change the resulting vector to cipher text. Decipherment is

accomplished in the same way
using the inverse
substitution & inverse matrix —

a change in coordinates

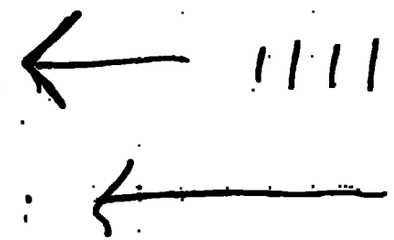
A self reciprocal matrix is its
own inverse —

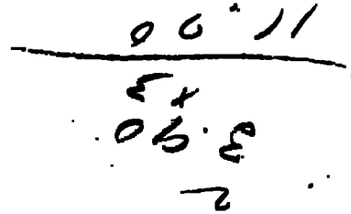
Instead of using a single matrix —
you can use a matrix polynomial

Lester H. Hill - Amer Math. Monthly
(Sept) 1929

" " " " " "
1930

Campaign (CCH-1 Talented





LINEAR TRANSFORMATION is any rigid transformation in space which can be represented by the successive performance of pure translations and pure rotations.

Thereom: # 1 - Every linear transformation can be represented by a matrix.
2 - Every matrix represents a linear transformation.
3 - If the determinant of a matrix is different from zero, the transformation is non-singular and has an inverse. The matrix of the inverse transformation is the adjoint of the original matrix with every element divided by the value of the determinant.

Cryptographical Application:

Represent plain text in units of fixed length as a series of vectors. (A vector is any ordered set of numbers of fixed length). Dailey Key consists of a series of substitutions which will transform the plain text into a vector and a non-singular matrix having as many rows and columns as the vector has elements. Each vector in turn is multiplied on the right by the matrix and the result is always a vector. Another series of substitutions is provided to change the resulting vector to cipher text. Deciphering is accomplished in the same way using the inverse substitution and inverse matrix.

Note 1. A self reciprocal matrix is its own inverse.
2. Instead of using a single matrix, a matrix polynominal can be used.

Lester H. Hill : American Mathematical Monthly for Sept.? 1929 and 1930.

Dr. H. Campaigne